Digital Rights Management Technologies

October, 1995

Prepared for:

Joseph S. Alen, Chairman

Committee On New Technologies

International Federation of Reproduction Rights Organizations

c/o Copyright Clearance Center

222 Rosewood Drive

Danvers, MA 01923

U.S.A.

Voice: (508) 750-8400

Fax: (508) 750-4343

E-mail: jalen@copyright.com

Web: http://www.copyright.com

Prepared by:

Dr. Robert Weber Principal Northeast Consulting Resources, Inc. One Liberty Square, 11th Floor Boston, MA 02109-4825 U.S.A. Voice: (617) 654-0621 FAX: (617) 654-0654 E-mail: weber@ncri.com Web: http://www.ncri.com

Table of Contents

---

1. INTRODUCTION

This year marks the emergence of a growing consensus that technology will provide new opportunities to proactively manage copyrights and permissions and to protect copyright for all kinds of digital content. Indicators of this growing consensus include:

* The number of companies who have said they are developing rights protection technologies or services has grown substantially;

* Large companies, such as AT&T, IBM, Novell, Xerox, and Folio (a subsidiary of Reed/Elsivier), have made major announcements or other public statements to this effect;

* The Association of American Publishers issued a report followed by a press release pledging support for development of a range of copyright management systems; and

* Copyright Clearance Center announced its intent to provide rights and permissions clearinghouse services with several partners, including InfoSafe Systems, Electronic Publishing Resources, and Folio, among others.

Rights management technologies benefit both sellers and buyers of digital content. Advanced technologies for copyright compliance, rights management, metered usage, and guaranteed payment will:

* Enable a range of new pricing methods, including usage-based transaction pricing;

* Encourage rightsholders to make available much more content in digital form, including text, film, video, and music; and

* Provide several convenient electronic payment mechanisms, including credit card, bank debit card, "stored value purses" on PCs, and for businesses, Electronic Data Interchange (EDI) billing and payment transactions.

Last year at this time, rights management technologies were the province of a few small startups, some with real products, some with great ideas in search of partners and customers. Profiles of relevant vendors are in the Appendix to this report.

Although the predominant focus of this report is the American market, we have included one Canadian effort, the IVY consortium. Another limitation is that we have excluded from this report those technology vendors whose focus is principally on software program protection. Instead, we have chosen to focus on those companies who are developing rights management technologies for a much broader range of content.

Chapter 2 briefly describes several rights management technology models now in the marketplace or that are likely to be introduced in the next 18 months. These models range from secure transport and delivery to lock/unlock technologies to secure hardware containers to cryptographic envelopes that support true superdistribution.

Now it seems likely that a few advanced technologies endorsed and deployed by major content and technology companies will succeed over the next few years. Chapter 3 addresses these emerging key issues:

* Should rightsholders prefer a multiplicity of rights management standards or just a few?

* What does it mean to manage rights proactively rather than to just protect rights?

* What services will rights and permissions clearinghouses provide and how will these new services affect rightsholders? and

* How are rights management and related technologies likely to affect digital content creation and distribution?

The last chapter (Chapter 4) addresses some of the key issues rightsholders will consider in deciding how to make use of technologies for rights management and information commerce. These include:

* Rationalizing internal policies, contracts, and systems for rights management;

* Participating in the various pilot projects that will be announced in order to experiment with different rights and pricing models; and

* Working with vendors and clearinghouses to establish major standards for content control and rights management.

The Appendix (Chapter 5) provides brief overviews of the relevant vendors and their respective technologies.

2. TECHNOLOGY MODELS

This chapter identifies models of rights protection and rights management technologies. Each model describes the technology, characterizes its advantages and limitations, and identifies the leading suppliers of the technology. Some of the technologies described here support features of two or more models even though we have characterized them as implementing a single model. And again, more detailed discussions of specific vendors can be found in the Appendix (Chapter 5) to this report.

Neither this overview of rights protection and rights management technology models nor the vendor descriptions in the Appendix are exhaustive. Some who have spoken with us prefer to remain unacknowledged in this report. And we're sure we inadvertently missed a few new companies that have not wanted to attract attention just now. Finally, there are undoubtedly large technology companies working on rights management who have not yet come forward. Notwithstanding these limitations, this chapter is likely to cover most, if not all, important models for rights protection and rights management now being discussed in the American market.

2.1 Secure Delivery

The simplest form of rights protection involves the secure delivery of content from seller to buyer over the Internet. The simplest level of protection eliminates the possibility that a third party can obtain the digital content in a usable form by monitoring the transmission of that content from seller to buyer. For example, a sophisticated student might be able to intercept Internet traffic between the bookstore and a publisher and, thereby, obtain an electronic copy of an article or book chapter that would have been sold by the bookstore. Many solutions to this kind of problem are now in the marketplace. To illustrate, we give a World Wide Web example.

A number of vendors of World Wide Web browser and server software have incorporated methods for encrypting all communications between a buyer and seller in a given "session." The encryption keys are typically changed from one session to the next. In this approach, information, such as credit card numbers, expiration dates, ordering information, and the delivery of the content itself are encrypted prior to transmission. Even if someone is monitoring the network traffic, they cannot obtain either the digital content or credit card numbers in the clear because they cannot obtain the session keys.

At present, there are two competing standards, and there is agreement among those involved to rationalize the two approaches and create a single, unified standard. The first standard is known as Secure HTTP (HTTP being the underlying standard of the World Wide Web) developed by Enterprise Integration Technologies and CommerceNet. The second standard is known as Secure Socket Layer (SSL) that was developed by Netscape, the market leader in Web browser software. Backed by several interested parties, Terisa Systems will create a single, rationalized standard.

The export version of Netscape with short encryption keys has recently been broken by three different groups. However, the American version with much longer keys remains secure from attack for some time to come. Netscape is working to correct these deficiencies.

2.2 Secure Vending Machines

A number of vendors, including AT&T, CD-MAX, InfoSafe Systems, Spyrus, Inc., and Wave Systems, make

technology that can be characterized as secure vending machines. In this model, the content is typically encrypted and stored on CD-ROM, video-on-demand server, hard disk, etc. until required. Upon completing arrangements for payment, the content is delivered to the customer. Some systems decrypt the content on the customer's PC and leave it "in the clear." Other systems provide a special application that runs on the customer's PC. This special application decrypts the content whenever the authorized customer wants to view it. If the rightsholder wishes, these systems never provide an unencrypted file for the customer's use.

These systems guarantee that the rightsholder gets paid for the first copy. They also allow for buyers to pay for content at the time of first use, rather than when the larger content database is accessed. For example, a supplier of expensive market research reports on CD-ROM would give a disk containing many reports to prospective customers. They, in turn, would typically select just one or a few items to purchase. Later, the buyer could return to the disk and buy additional reports as needed. The seller could easily distribute an updated disk monthly.

Since vending machine systems do not provide for persistent content control, the buyer can easily infringe in any number of ways once he/she has the content in the clear. In conjunction with metering and content control capabilities integrated into common applications, some of these technologies provide expanded capabilities. We return to this issue in Section 2.6.2.

Some secure vending machine technologies support not only single user models, but are consistent with subscription and site licensing pricing models as well. The key management system can shut off access when a subscription has expired. However, the technology itself does not strongly enforce site licensing or subscription models since the content is delivered in the clear and control is lost.

2.3 Hardware Containers

A team at Xerox PARC has created technologies and has applied for patents perhaps best characterized as hardware container technology. The basic idea is that by ensuring that the content is accessed only on a secure device, the system is able to ensure that only authorized users have access to the content, that rightsholders are compensated, and users cannot send unauthorized copies in the clear to others.

A secure device or "trusted system," is one that has some form of security co-processor that handles encryption/decryption and handles encryption keys in a protected, secure fashion. The trusted system is also able to detect attempts to compromise the security of the system or the protected security co-processor.

The Xerox approach represents an improvement over lock/unlock technology. The model is able to handle copies for backup purposes, loaning the content to a single person, and conveying the property to another, single person. The technology also handles a number of different pricing models.

Xerox's hardware container technology provides a complete security solution. It also affords rightsholders the opportunity to create fairly specific rights relationships with their customers. Thus, rightsholders can specify a range of rights and pricing models, and each specific model can be crafted for a particular customer, if desired.

This model has two limitations. First, the Xerox technology appears to be device and content supplier centric. This means that in order to make payments or to renew permissions or to obtain permissions one is lacking, the secure hardware device must contact the original source of the content. Many rightsholders will like this feature since it allows them to maintain direct control of their business and rights relationship with each individual customer. However, this technology does not appear to enable true superdistribution in which the one customer can convey the content and permissions to many others who, in turn, also pay the rightsholder for their use.

The second set of problems follows from the device-centric nature of the technology. Secure trusted systems are important to rightsholders. However, the Xerox technology appears to run counter to important trends in computing and communications technologies. Many capabilities that have been provided by single devices, such as mainframes

and PCs, are evolving to become services distributed in the network. Thus, search, rights management, security, billing, and payment are likely to become common services distributed in the network, rather than having devices as the important focal point. This means that the interfaces to these services reside in PCs, but the services themselves are delivered through the network.

2.4 Secure Software Containers

EPR continues to be the leader in bringing secure software container technology to market. Their complete InterTrust model includes the same hardware-based security protections found in other models, but they go beyond others in two important respects. They have developed secure software containers or envelopes that provide a substantial degree of security for any kind of digital content. Although less secure than their own or others' hardware based models, the EPR "DigiBox" container technology provides good security for all, but, perhaps, the most expensive content. The DigiBox and related system elements were designed so that it would take an effort substantially disproportionate to the value of the content to break a container. Second, the DigiBox is engineered so that even if one were able to compromise a particular container, the larger InterTrust system would not be compromised.

A second important feature of InterTrust technology is that these secure software containers can be sent from one computer to another over the network while maintaining the confidentiality and security of the digital property and rights and pricing control information. Thus, one customer can create new customers whose payments are credited to the appropriate rightsholders.

A third important feature of EPR's InterTrust is the ability for participants in the distribution chain to modify permissions and pricing information. This patented InterTrust capability is known as "chain of handling and control." Here is a simple example.

As an author, I convey an article to a publisher in a secure software container along with a set of permissions and pricing (royalty) information. To keep this example simple, I might require 50 cents each time the article is sold, prohibit exporting the article from the secure container, and authorize publishers to add to, but not negate the control information I've just created. The system has mechanisms for determining that a publisher, rather than a user, is trying to modify the control information.

Having established with InterTrust that either I'm a publisher or a particular publisher, I can now use the chain of handling and control mechanisms to increase the price to $1 each time the article is sold, with half coming back to me and half going to the author. I can, for example, also include this article in a digital anthology and impose the condition that subsequent users cannot include the article in a larger, encompassing digital work. In short, the chain of handling and control mechanisms enable secure information commerce all along the distribution chain from author to consumer. An extended example is presented in Section 3.5 of this report.

2.5 Other Models and Services

Not all relevant rights management technology and services falls into the preceding categories. Two of note are Folio's integration of rights protection and metering capabilities into their applications, and Copyright Clearance Center's announced program to provide digital rights and permissions clearinghouse services. Details of these efforts are discussed in the Appendix.

2.5.1 Application Integration

Folio Corporation has taken the clear lead in integrating metering capabilities in their line of information applications. They have announced relationships with several meter makers, including InfoSafe Systems, CD-MAX, Wave Systems, and Copyright Clearance Center for rights clearinghouse services. They are publishing a set of Application Program Interfaces (APIs) that allow meters from various vendors to exchange information with Folio

applications.

The metering system will convey to the Folio applications information regarding limitations on the kind of transactions that can be applied to a particular property. For example, the metering system could instruct the Folio application not to allow export of the content or any part of it from the secure Folio application environment. At the same time, the Folio application will report back to the metering system detailed usage information, for example, the number of times a document was opened or the number of pages printed.

The integration of metering capabilities with Folio applications is a powerful, synergistic development. From the Folio perspective, they are able to offer their significant and growing customer base fine-grained metering capabilities that do not depend on any one metering technology. From the meter maker's perspective, they are able to extend their technology model from secure vending machines to quasi-persistent content control and fine-grained transaction metering and control.

Notwithstanding the synergy between Folio and its metering partners, the chief limitation of this approach is that it solves the problem for one particular application, rather than for all applications. An important feature of Folio's infobase technology is that it does allow a user to get important content, while still in the format of a broad range of common applications, such as word processing and presentation applications. However, once incorporated in a Folio infobase, the property cannot be exported without losing the advantages of the secure Folio environment.

Many will want the advantages of content control and transaction metering across all their applications. Other technologies such as EPR's InterTrust are application independent and have multi-vendor interoperability as their chief goal . This means that a sound clip could be sent from one person to another in a secure container and be played on any computer that has InterTrust and that has any application capable of playing a file in that sound format.

2.5.2 Rights Clearinghouse Services

A rights clearinghouse is one of the interfaces between rightsholders and rights users. Two organizations have announced clearinghouse services, CCC and the Canadian IVY consortium.

2.5.2.1 Copyright Clearance Center

CCC has announced relationships with several vendors including InfoSafe Systems, Folio, and EPR, to provide or participate in providing digital rights clearinghouse services. The basic service is to provide permissions and rightsholders' prices for digital content. CCC brings the advantage of an established network of rights clearance relationships with its counterpart organizations throughout the world.

The clearinghouse also collects usage information from the meters and reports usage information to rightsholders. To protect individual privacy and company confidentiality, usage information may be aggregated before it is reported to rightsholders. An extended example is presented in Section 3.5 of this report.

2.5.2.2 IVY Consortium (Canada)

The IVY consortium is a group of Canadian companies, universities, and rights clearance organizations who are supporting a video-on-demand trial in Toronto, Ontario. They are largely concerned with clearinghouse activities rather than technology for PCs and information servers. Their vision is described in Section 5.6.2 of this report.

2.6 The Market Will Decide

Perhaps the most striking change over the last year has been increasing rightsholder interest in copyright protection and rights management technologies. At the same time, many new players have announced technologies. The following chapter addresses standards issues and some business implications of the best of breed rights protection

technologies.

3. MANAGING RIGHTS PROACTIVELY

Last year's report focused on "Metering Technologies For Digital Intellectual Property" and principally addressed copyright protection, counting, and charging for what could be counted. In the past year, the thinking of leading-edge rightsholder and technology companies has evolved to focus on proactively managing pre-approved rights and permissions.

In some segments of the copyright industries, rightsholders have wanted the ability to deny permission for uses deemed inappropriate or that may benefit one's competitor as much as oneself. While broad guidelines developed by each rightsholder often made specific decisions relatively easy, seeking and granting permissions became a labor-intensive activity in many publishing segments, most notably in book publishing. Individual permission request letters were processed one at a time. Royalties often varied depending upon use and by competitive implications, if any.

Last year at this time, rights management technologies were the province of a few small start-ups, some with real products, some with great ideas in search of partners and customers. That at least some technologies will prevail in the marketplace seems assured. Chapter 3 addresses emerging key issues, specifically, how might rightsholders:

* Think about technology standards?

* Manage rights proactively, rather than to just protect rights?

* Utilize the services of a rights and permissions clearinghouse on the net?

* Distribute content and convey rights and prices to other distribution chain participants?

3.1 Standards For Rights Management

Each of the rights management technology vendors would very much like to have their technology become a prevailing standard. Being a standard means that the technology is widely available on personal computers and is used by many large publishers and information distributors. In short, there is wide agreement on which rights management technology to use, how it will be used, and the benefits of this technology to information creators, publishers, distributors, and information consumers.

It is not necessarily the case that the best technology becomes the widely accepted standard. The triumph in the US of VHS over technologically superior Beta format for home video players is a well-known example. It's worth noting that the recent agreement by Philips, Sony, and others on a single new standard for CDs reflect increasing sophistication around standards issues. Rather than fragment the market into warring camps, they preferred a single standard. The rising tide will raise all boats.

Some companies may do well as big players in important niches. Companies like InfoSafe Systems, CD-MAX, and Spyrus may profitably exploit the CD-ROM niche. CDs are inexpensive and convenient ways to distribute and dispense a broad range of information. The coming high performance, high capacity (about 5 gigabytes) CDs that support both music, video, and other types of data will undoubtedly create expanded opportunities for those focused on physical distribution media.

However, at least in developed and many developing countries, information distribution is highly likely to be based

on personal computers and fast communications networks such as the Internet. The phenomenal growth of the World Wide Web of hyperlinked documents and services is striking. For example, more than 100 US newspapers now have a presence on the Web. Since the American home market is the fastest growing PC market segment, the Web is likely to become widely available there too, in addition to higher education, research, and business.

The Internet and Web are terrific examples of how consensus on standards enables new ways of conducting information businesses only dimly, if at all, perceived just five years ago. Although many in the information industry thought that networked information would eventually be a predominant paradigm, few observers anticipated the explosive growth of the Internet fueled in significant part by consensus on standards for network transport and basic network applications (the Internet) and on network publishing and access standards (the Web). Mosaic, the first important Web browser, was introduced in 1992. The Web and its standards (HTTP, HTML) immediately solved important problems, including making the Internet accessible to interested users who had previously been intimidated by the technical knowledge required prior to the Web.

Imagine a world in which three or four incompatible technologies compete to be the standard for networked information commerce transactions and rights management. If I am an information consumer, which standard or standards do I install on my PC? What if I purchase information from three different sources, each of which supports a different contending rights management standard? Now I have to install all three standards on my PC. But what if these three can't co-exist peacefully? What happens if incompatibilities lead to major problems so that I can't do my work? Imagine that information and entertainment consumers in the home become frustrated and give up on innovative new services that incorporate rights management technologies?

What is in the best interests of authors, publishers, and distributors of information and other digital content? We strongly believe that one major standard is much better than many competing standards each with a relatively small share of the total market. We have been told repeatedly that rightsholders want the largest possible markets for their content and to be able to reach these markets as efficiently as possible. Supporting several competing standards is inherently inefficient. And the fragmentation of large markets into smaller markets because of standards wars can't make anyone happy except those technology vendors who otherwise would not have succeeded.

3.1.1 Requirements For A Standard

The purpose of this report is not to recommend a particular technology as the standard for rights management. That would be inappropriate here. Instead, this section outlines some of the major capabilities that rightsholders should look for in rights management technologies. Also, this list is stated in such a way that more than one vendor could meet all or most of these requirements. This list can also be the basis for a more detailed and elaborated set of evaluation criteria should others wish to choose from among the several vendors.

1. Protection of multiple data types. The leading technology should be equally capable of protecting a wide range of data types, including text, image, video and video clips, and software including multimedia, for example.

2. Platform Scalability. The preferred solution can be implemented on computers and other intelligent devices large and small, from supercomputers and mainframes to handhelds and laptops, from PCs to settop boxes to game machines.

3. Volume Scalability. The system does not break as the volume of transactions goes up. Also, the technology is architected to reduce or minimize the number of administrative transactions across the network.

4. Control And Metering Of Many Operations. The technology is capable of detecting, preventing, and counting a wide range of operations, including open, print, export, copying, modifying, excerpting, and so on.

5. Support For Multiple Payment Mechanisms. Consumers of information are likely to want to pay using one or more of several methods. These include credit and charge cards (Visa, Mastercard, American Express, etc.), smart cards,

"stored value" (money stored in "purses" on the user computer or smart card), debit cards related to bank accounts, and EDI (Electronic Data Interchange) transactions for business to business purchases and payments.

6. Secure Delivery Of Content. Content in any digital form is delivered from the information distributor only to the authorized customer. Others cannot gain useful access to the content merely by copying the network transmission.

7. Secure Redistribution of Content. If one person desires to send a copy of the digital content to another, this redistribution should also be as secure as the original distribution to the initial customer. Also, the recipient should be able to pay for use and be subjected to the same restrictions as the initial customer.

8. Persistent Control of Content. There are always limitations to rights management and content control technologies. Nothing will prevent someone from scanning a printed page of a protected document (although fingerprinting or digital watermarking techniques may make it easier to trace and prosecute such infringements). Still, the best rights management technologies will be capable of protecting digital content after it is delivered to the customer and regardless of redistribution.

9. Control and Metering of Nested Objects. Many rightsholders believe it will be important to keep track of the individual objects that comprise larger ones. Multimedia products usually consist of content within content: an image and sound clip within an instructional module, for example.

10. Wide Range of Granularity of Metered Objects. Some observers have suggested that it will be desirable to meter content consisting of a few bits or a few characters. Many objects will be very large, a digitized film clip for example. Others will be very small, a sentence or two from another document. It will be important to find the right balance between practicality and rights management.

11. Rights Modification Along The Distribution Chain. The information industry consists of several different roles: author, publisher, aggregator, and repackager (and of course, customer). Technology for content control and metered usage should allow each of the different players to modify appropriately the permissions and pricing as the "chunk" of content moves from one to the next and as value is added.

12. Strong System Security. The rights management technology should be very difficult to "crack" or compromise. In addition, if it is compromised, the result of the attack should be the compromise of a particular piece of content destined for a particular customer, rather than the compromise of the rights management system as a whole.

Widely deployed technologies that enable these capabilities will provide options for new business models for authors, publishers, aggregators (like Dialog, Lexis-Nexis, AOL, Prodigy, CompuServe, etc.), and repackagers (like Individual, Hoover, Profound, etc.). Besides the enabling rights management technologies, another critical prerequisite is that rightsholders manage rights proactively.

3.2 Proactive Rights Management

Burgeoning markets for digital content of all kinds will force changes in the ways that authors, publishers, and other rightsholders deal with rights and permissions. Many publishers have still not yet rationalized their management of rights and permissions. Specifically, rightsholders should consider:

* Building internal rights management database applications

* Standard contract terms for electronic rights

* Anticipating the evolution to new, additional pricing models

* Aggressively instituting pre-approved permissions

An internal rights management database application would first contain all relevant contracts, probably as images so that signatures and last minute initialed modifications could be verified. Second, there should be appropriate data fields indicating the various terms and conditions and royalties for a broad range of permissions that could, in principle, be granted. For each content element, such as book, journal issue, article, image, sound byte, music track, or video clip, the database would contain entries in the appropriate fields. For those publishers intent on running their own permissioning operation, such a system might also contain records indicating which permissions had actually been granted and to whom. This application, in turn, might provide detailed information to the company's accounts receivable department for invoicing, receipt of payment, and crediting payments to the right accounts.

Although there have been significant improvements in the past few years, some publishers still do not know exactly what rights they have to grant, especially for backlist items. Contracts may be gathering dust in a warehouse somewhere. A more difficult problem is that the terms and conditions for similar items may vary from contract to contract. A few authors, for example, may have been able to retain certain rights or have been granted more favorable royalty terms. While publishers must continue to respond in creative ways to competitive pressures, standard terms and conditions as they apply to electronic versions makes rights management easier.

Advanced rights management technologies facilitate the creation and operation of efficient markets for information and other digital content. Already, some publishers and other rightsholders have gotten used to granting blanket or standardized permissions. For example, they set a standard fee for making photocopies or for viewing or printing electronic versions of an article regardless of who is exercising these permissions as long as royalties are paid through one of the common mechanisms. Other rightsholders are uncomfortable with such standardized permissions. They may wish to adjust pricing to specific market opportunities or competitive pressures. And, some publishers may wish to preclude competitors from making use of their content or they may wish to ensure they always know how their content is actually used.

These practices reflect standard formal business and rights practices. For example, authors and publishers, publishers and aggregators, and buyers and sellers of digital content would create formal licensing or contractual arrangements that would spell out each parties' rights and limitations plus compensation.

The best of breed rights management technologies create opportunities to move from formal to ad hoc business and rights relationships. Rather than creating broad and ongoing relationships among distribution chain participants and between them and the ultimate customer, rights management technologies allow buyers and sellers to agree on terms and conditions for that sale only.

It is possible that the terms and conditions vary among buyers, but that rightsholders need only specify their prices plus terms and conditions in advance for a particular piece of digital content. Some rights management technologies incorporate mechanisms for varying prices and permissions. Individuals would be able to prove to the rights management technology that they qualified for a particular set of prices and permissions.

For example, one set of prices and permissions may apply to large for-profit business, another set to government agencies, and yet a third set to higher education and non-profits. Once determined, any user who can show they are a member of one or another of these classes immediately knows how much they must pay to use the property and what usage rights they have been granted.

In this world, rightsholders will establish pre-approved uses and prices. Having installed the appropriate rights management and metering software on their PCs, customers will decide whether they wish to pay the price for the usage rights granted. Some pricing models secure payment at the outset, prior to use; others report transaction data and charge the buyer subsequent to use. Regardless, the business and rights relationship exists only for that copy of the property and that buyer.

Now it turns out that the best of breed rights management technologies enable buyers to become sellers, or at least to

forward copies of the property. In both circumstances the rights protection and management system protects the content. Let's assume that Alice sends Bill a market research report, music, or video clip in a cryptographic envelope that also contains pricing and rights information. Let's also assume that Bill has the appropriate envelope opening software on his PC. When Bill begins to open the envelope, the software will inform him of the price and of the relevant permissions. Or, we may assume that Bill has set some system defaults so that if the price is less than or equal to a specified amount, and if a minimal set of usage rights are conveyed, the system will allow him to open and, thereby, automatically agree to the rightsholder's prices and permissions. These scenarios assume that Bill has sufficient credit or funds stored on his PC or that the system can get his credit or charge card transaction approved.

The rightsholder may not have known immediately that the first buyer was, in fact, Alice and would not know that the second buyer was Bill until after the transaction was consummated. It is in this sense, that the business and rights relationships are ad hoc, rather than formal.

Automated rights clearinghouses play an important role in a fully deployed, best of breed rights management system. The next section examines their function.

3.3 Rights and Permissions Clearinghouse Services

As noted earlier, some rightsholders will create their own automated clearinghouses, but many are likely to leverage important economies of scale by outsourcing this function to a specialist organization. Copyright Clearance Center has announced their intention to provide automated clearinghouse services in support of several rights management technologies. This section briefly explains rights clearinghouse services and some of the issues that rightsholders should consider as rights management technologies become more widely deployed.

In support of advanced metering technologies, two kinds of clearinghouses may exist on the Internet and other large networks:

* A Financial Clearinghouse. The interface between systems for rights management and metered usage and the various financial services systems such as those for credit, debit, and stored value plus financial EDI transactions.

* A Rights and Permissions Clearinghouse (RPCH) The interface between systems for rights management and metered usage and authors, publishers and other rightsholders.

To help understand what an RPCH actually does, it is useful to distinguish between a rights template and a particular rights model. A rights template indicates what rights might be conveyed by the rightsholder; a particular rights model indicates for a particular piece of information which of the possible rights are being conveyed and which are being withheld. Every rights model incorporates a particular rights template. Example 1 presents a rights template and rights model for a particular hypothetical feature news story.

Example 1. Combined Rights Template and Rights Model For Particular Hypothetical Feature News Story

Transaction	Permission	Comments
Viewing title	Granted	
Viewing abstract	Granted	
Viewing article	Granted conditionally	after payment
Modifying abstract	Prohibited	
Modifying article	Prohibited	
Printing abstract	Granted	
Printing article	Granted conditionally	after payment
Cut and paste, excerpting	Prohibited	
Exporting from envelope	Prohibited	

A similar distinction can be made between "pricing templates" and "pricing models." A "pricing template" indicates

on which activities could, in principle, impose a charge; a "pricing model" indicates for a particular piece of information which activities have a cost of zero and which have a non-zero cost and exactly what that cost is. Example 2 presents a combined pricing and rights template and model for the same hypothetical feature news story.

Example 2. Combined Pricing and Rights Template and Model
For Particular
Hypothetical Feature News Story

Transaction	Pricing	Permission	Comments
Viewing title	$0.0	Granted	
Viewing abstract	$0.0	Granted	
Viewing article		Granted conditionally	after payment
Modifying abstract	Not applicable	Prohibited	
Modifying article	Not applicable	Prohibited	
Printing abstract	$0.0	Granted	
Printing article	$3 per page	Granted conditionally	after payment
Cut and paste, excerpting		Prohibited	
Exporting from envelope		Prohibited	

The CCC RPCH will work with rightsholders and other RROs to, first of all, define the appropriate rights and pricing templates. Also, the New Technology Committee of IFRRO has sponsored a study to gather input on pricing models. In cooperation with rightsholders, users, and other implementors and adopters of content control and usage metering technologies, master templates will be defined containing useful rights and pricing items. For each item of content or for classes of content, such as all news articles from a well-known national newspaper over 1000 word in length, the publisher would fill in the blanks and convey permission records to the CCC RPCH and to others in the distribution chain. For example, the well-known newspaper could convey the same permissions to an on-line information service and to a repackager of information.

With content control and metering technologies such as EPR's InterTrust architecture, the most complicated part of constructing an RPCH is negotiating specific roles with rightsholders and various distribution chain participants. As noted earlier, EPR's InterTrust architecture provides for a "chain of handling and control." This means that the various control records in a secure DigiBox container, including the permissions record, can be modified in specific ways as the object is conveyed down the distribution chain. Here is a hypothetical example of how content moves from creator to consumer and how each distribution chain participant might modify the control information or "control set":

Example 3: Distribution Chain Participants Modifying Control Set Information

Distribution Chain Participant	Modifications To The Control Set	Comments
Author	Author's royalties established; author imposed controls, if any	Author could self-publish on the Web, nominating CCC as his/her clearinghouse
Publisher (e.g., large newspaper)	Adds publisher's royalties to author's royalties, may impose additional constraints; author may have allowed modifications to permit the editorial staff to do it's job	The newspaper could construct it's own financial and rights clearinghouse or outsource
Distributor (e.g., large on-line service)	The on-line service takes article from newspaper, and after search and before downloading to customer adds pricing and rights info. to control set	The newspaper may have sent content to a large on-line service with fewer constraints than if they distributed the article from their own server to allow the on-line service to add

		or modify information (headlines, dates, copyright notice, on-line service branding, etc.)
Repackager (e.g., newsletter or current awareness products)	Repackager gets articles from on-line service and creates new electronic publication from several objects, and modifies pricing, rights, and other control set information. Note that royalties must be returned to the rightsholders for each of the constituent objects in addition to individual receiving its own royalties	Controls could prevent disaggregation of the digital newsletter into its constituent objects for example
Corporate info. server (Fortune 1000 company)	Objects are stored in corporate information base where people within the company can search/browse, download, etc.	Usage information could be aggregated on corporate information server
User	In conjunction with container opener and metering system, transactions are enabled, metered, and paid for	A variety of pricing models and payment methods can be enforced
Other User Outside Company	First user sends encrypted container and content to another user in another company. The metering system on that user's machine must be able to eventually reach a financial and rights clearinghouse	The object needs to phone home to establish payment and verify rights

The rights clearinghouse system will be able to receive, store, aggregate, and report usage information to rightsholders. The frequency of reporting and the level of data aggregation, by person, company, industry, etc., remains to be determined by rightsholders and CCC.

The rights and pricing templates described above are a subset of the information required by various content control and metering systems. Depending on market demand and acceptance, we expect the CCC clearinghouse to supply clearinghouse services through several different rights management technologies.

4. NEXT YEAR: WHAT MATTERS?

In the year ahead, rightsholders might want to pay attention to: (1) fixing internal policies, contracts, and systems for rights management. (2) participating in the various "betas" that will be announced in order to experiment with different rights and pricing models; and (3) working with vendors and clearinghouses to establish one (or two) major standards for content control and rights management. We address each of these in turn.

4.1 Fixing Internal Systems

Advanced technologies provide fine-grained capabilities for copyright control and rights management. The discussion in Section 3.3 of pricing and rights templates and models gives an overview of the level of detail incorporated in emerging technologies and clearinghouse services. To be an active participant, publishers and other rightsholders will have to make important changes in policies, contracts, and internal systems for rights management. It continues to be the case, we believe, that most large publishing houses have not modified their standard contracts and agreements to take into account the expanded range of pricing, rights, and permissions options that will become available over the

next few years.

4.2 Pricing Experiments

Information services based on advanced rights management technology will be "beta" tested as early as late 1995 but more likely in 1996. At least two different technology vendors will conduct betas in the first half of '96. We suggest that publishers, aggregators, repackagers participate in these projects in order to learn what will be necessary to take advantage of advanced rights management technologies, but also to try out different pricing strategies and templates. As we noted in last year's report to IFRRO, the first uses of content control and metering technologies may be to support familiar pricing strategies such as subscription pricing. In this situation, the technology allows rightsholders to impose restrictions on use: content can be printed but not modified, or can be redistributed in protected form, but not exported out of the secure environment. At the same time, the rightsholder may charge an annual or monthly subscription fee for a particular piece of content such as an article, or may license a range of articles under the single subscription fee. The rights management technology would impose usage constraints and collect the annual or monthly fees.

Some companies are betting that relatively low usage transaction fees will become widely accepted by rightsholders and customers alike. Here customers pay small fees for a variety of transactions such as viewing, printing, copying, cutting and pasting, and so on. Publishers and other rightsholders have yet to determine which operations will be enabled and which will be prohibited and which enabled operations will incur charges and how much those charges should be. This is a very complex and difficult set of issues that probably are best explored, analyzed, and decided on the basis of actual market behavior, rather than on abstract financial models with the usual range of dubious assumptions.

There is much to be learned about the practical capabilities and limitations of advanced content control and rights management technologies. Pricing experiments can be rigorously designed. More important, the results will provide valuable data and insights into market desires and market behavior that can be the basis of key pricing strategies. This early usage information is critical in that preconceived notions in other areas of how the market will react have been shown to be inaccurate. Early adoption allows an interactive process to occur, where early usage information informs pricing decisions, which will in turn affect usage, and so on.

Also, we believe that there are important "first mover" advantages. The publishers and other rightsholders that figure out transaction pricing templates and models first are likely to develop important competitive advantages over their chief rivals. The "experimenters" and "early adopters" will better understand and be able to forecast market behavior, and thus are more likely to run profitable new information businesses.

4.3 Standards Again

By the end of the century, secure digital information and entertainment commerce is likely to be worth several hundreds of billions of dollars. Essential to this vision is adoption of the same content control, rights management, and secure digital commerce standards across a variety of computing and communications "platforms." This means, for example, that the same rights management technology should be on Windows, Mac, and UNIX computers regardless of whether these are laptops, desktops, or servers, and on a variety of other information and entertainment appliances. The latter include PDAs (Personal Digital Assistants), handhelds, game machines, settop cable boxes, VCRs, and so on.

We suspect that many of the most interesting, exciting, and perhaps profitable businesses will be based on delivering content across traditional market and/or platform boundaries. For example, the ability to deliver popular music or music video clips digitally over networks while securing the royalties for use or purchase is one example. Another is the vending of music and video clips for incorporation in multimedia products so that the music and video rightsholders share in the royalty stream for using that multimedia application. It is possibly the case that the

generally. For example, the AT&T announcement mentions a broad range of information vending and electronic commerce applications, including video-on-demand, electronic publishing, electronic news and alerting services, software distribution, computer program license control, program execution metering, home shopping, remote gaming, bank-at-home service, electronic contracting, etc.

Table 5.1: IVES Supported Security Services

Security Service	Description
(SSI) Security Service Interface	Calls that access IVES services
Secure network communications protocols	Means for secure messaging across a network, including secure addressing
Security applications protocols	Application-dependent protocols, such as methods for dispensing entitlements for the service IVES is supporting
Authentication protocols	Methods for securely and reliably identifying system entities
Key management	Cryptographic key generation, distribution, and maintenance methods supporting the various security functions
Local, off-chip memory protection mechanisms	Capabilities for storing valuable information, including digital cash balances in security containers of arbitrary size, off-chip
Security kernel	Atomic security services that cannot be interrupted or interfered with
Physical layer security	Silicon-layer anti-tamper, memory protection, bus isolation, etc.

While technical details of the IVES architecture have not yet been made public, IVES appears to be a well thought out cryptographic key management system based on a secure co-processor, the RSA public key crypto system for user and device authentication and secure secret key exchange, and triple DES for content encryption/decryption.

The IVES system is based on a security co-processor manufactured for AT&T by VLSI Technology. The chips include tamper resistant memory, a 32-bit RISC processor, support for any of the standard interfaces (PCMCIA, ISA, 16550 serial, and others), a security kernel in masked ROM, a hardware randomizer, a high-speed Triple-DES processor with key cache, and a variety of non-security applications ranging from data and audio compression to communications protocols.

Devices that, in principle, can incorporate IVES chip technology range from personal computers in homes or businesses, servers, settop boxes, video game players, off-track betting machines. Once incorporated in the business or home customer device, the IVES chip supports several security services. APIs that developers can write to will be published later this year.

The IVES architecture encompasses a sophisticated lock/unlock content control system. Figure 5.1 shows a schematic view of IVES system functions. Digital content is first encrypted with a triple DES key and stored on a content server that might be another computer or static storage device such as a CD-ROM. The content and the entitlement to use that content can be stored and transmitted separately. Encrypted content can be stored anywhere on a public or private network. The content may be any digital data ranging from software to business information to video clips to feature length movies.

development of a truly burgeoning multimedia industry awaits the adoption and deployment of a standard for content control and rights management.

"Here a standard, there a standard" can't be good for most participants in the copyright industries, least of all rightsholders. Some niche technologies are likely to flourish within their specialized markets. Metering for CD-ROM delivery is a likely example. For publishers and other rightsholders who depend on large broad markets, a different standard for each large market is almost certainly not a good outcome. Rightsholders would have to customize digital products and services for each of these markets and their associated technologies, thus, adding significant expense, complexity, and user frustration and confusion.

One (or two) important winning standards sends a clear, positive message to information consumers and suppliers. Also, having fewer standards creates important economies of scale and scope to be leveraged by all.

5. APPENDIX: TECHNOLOGY REVIEW

Technologies for copyright protection and rights management have become hot topics. This Appendix reviews major technology offerings from leading vendors. As noted earlier, this review is necessarily incomplete. Some companies are still in the development phase and are not yet ready to discuss their plans in detail.

For each vendor, we present an overview of their activities regarding copyright protection and rights management technologies. The vendor profiles are organized in the same sequence as the discussion of technology models in Chapter 2. Also, this discussion presents publicly available information, for some companies there may be unannounced technologies and/or unannounced business relationships. For a few of the vendors we profiled in last year's report, the descriptions of the technology haven't changed very much. Some profiles are very short since additional details were not yet available. The length of the profile should not be taken as an indicator of either quality or significance in the marketplace.

Finally, we have intentionally omitted the several companies whose principal business is software protection, preferring instead to focus on technologies that protect a wider range of content types.

All trade and service marks mentioned in this report belong to their respective owners.

5.1 Secure Vending Machine Models

5.1.1 AT&T Secure Communications Systems

AT&T Secure Communications Systems (Dave Maher, Chief Scientist, Andover, MA, 508-691-3139) is bringing to market metering technology developed with Bell Laboratories (Mike Powers, IVES Product Manger, Bell Laboratories, Andover, MA, 508-691-3052) and VLSI Technology (Richard Takahashi, 602-752-6455). Announced publicly at the 1995 RSA Data Security Conference in January, 1995, the Information Vending Encryption System (IVES) is similar in concept to Wave Systems' WaveMeter discussed elsewhere in this appendix.

Also announced is a partnership with Cablevision to develop video-on-demand applications based on IVES technology. No Cablevision contact information was given.

The AT&T IVES announcement demonstrates significant interest in rights management and metering technologies by a large, well-known company that is also a carrier. Thus, in addition to the small, fledgling companies profiled elsewhere in this report, the AT&T entry shows that the protection of digital content, rights management, and usage metering are issues whose time has come.

IVES and advanced metering technologies from other vendors are best thought of as enablers of electronic commerce

Commercial availability is expected in late 1995 or early 1996.

Wave Systems' CEO Peter Sprague and InfoSafe Systems' CEO Thomas Lipscomb have been granted one relevant patent. The status of other Wave patents is unknown.

Wave Systems has entered into a number of alliances and created a number of new services based on WaveMeter and WaveNet:

* Folio Corporation. In March, 1995, Wave Systems announced support for Folio's Metering Applications Programming Interface. The $API provides an interface between the WaveMeter and Folio's applications.

* VLSI Technology. Wave and VLSI announced a strategic licensing agreement in March, 1995. The two firms will collaborate on the design and manufacture of Wave-enabled encryption chips for targeted markets such as electronic commerce.

* Wave Interactive Network. In August, 1995, Wave Systems announced formation of a new subsidiary company, Wave Interactive Network (WIN), that will provide pay-per-use multimedia to the consumer market.

* Network News Corporation. In August, 1995, Wave Systems announced formation of Network News Corporation to provide secure satellite delivery of news and information to the corporate desktop for sale by the story. Network News will deliver content via satellite using Hughes Network Systems' new DirecPC service, and Wave's patented metering technologies. Announced content partners include Knight Ridder/Tribune Business News, PR *Newswire*, and Businesswire.

WSC claims to have received permission from the Department of Commerce to export the WaveMeter to all non-communist countries. (This is because the user cannot control the encryption keys or the operation of the WaveMeter device; hence the WaveMeter cannot be used to encrypt data.)

5.2 Hardware Container Models

5.2.1 Xerox PARC

A team at Xerox is building rights management technology based on research at the Xerox Palo Alto Research Center. The approach lends itself to a range of implementations for different kinds of digital works, different security requirements, and different transaction costs. A key to the approach is a usage rights language, which describes rights and fees associated with particular uses of a digital work. Rights and fees are determined by authors and publishers, described in the rights language, and attached to a digital work. (Contact: Bettie Steiger, Principal, Technology and Market Development, Xerox PARC, 3333 Coyote Hill Road, Palo Alto, CA 94304, Voice: 415-812-4072; Fax: 415-812-4274; Mark Stefik, Principal Scientist, Xerox PARC, 3333 Coyote Hill Road, Palo Alto, CA 94304, Voice: 415-812-4366; Fax: 415-812-4241.)

The basic idea is that rights and fees for a digital work are written in a machine-readable language and subsequently enforced by hardware and software for using the digital work. There are distinct categories of rights for such uses as playing (or displaying), printing, copying, loaning, and transferring, as well as rights related to the making of derivative works and making and restoring backup copies. Any given right on a digital work can be governed by required digital licenses or prepaid via digital tickets. Payment for usage of a digital work is handled via secure transactions, by realtime or periodic connections with an on-line financial clearinghouse.

Different digital works have different requirements for security. At the low end are standard personal computer systems with software for handling the encryption. At the high end are trusted systems with tamper-resistant hardware. In the middle are trusted systems that have co-processors for encryption and protected storage for keys and

billing data. A digital work specifies a required level of security so that some documents could not be copied or transferred from a high security platform to a lower security one. The overall approach ensures that the content is accessed only on a secure device, that only authorized users have access to the content.

The Xerox approach represents an improvement over lock/unlock technology. The model is able to handle copies for backup purposes, loaning the content to a single person, and conveying the property to another, single person along with the permissions associated with the property. As the receiving person gains the permissions, the sending person loses them. The technology also handles a range of different pricing models, site licensing of digital works, and digital licenses in support of restricting distribution to minors according to parental and community values.

Xerox's hardware container technology provides a complete security solution. It also affords rightsholders the opportunity to create fairly specific rights relationships with their customers. Thus, rightsholders can specify a range of rights and pricing models, and a specific model can be crafted for a particular customer, if desired.

Information concerning strategic alliances is unavailable at this time.

Xerox is believed to have applied for several patents based on Stefik's research.

Information concerning the exportability of Xerox's rights management technology is unavailable at this time.

5.3 Secure Content Containers

5.3.1 Electronic Publishing Resources, Inc.

Electronic Publishing Resources, Inc. (EPR) has developed an initial implementation of a comprehensive architecture for the control of intellectual property and metered usage (Contact: Victor Shear, President, Electronic Publishing Resources, Inc., 460 Oakmead Parkway, Sunnyvale, CA, 94086, Voice: (408) 774-6100; Fax: (408) 774-6144).

EPR's InterTrust architecture is a complete solution for the control, metered usage, and guaranteed payment for all kinds of intellectual property in digital form. First product availability is expected in 1996. Among the major components of InterTrust are:

* A cryptographic envelope or secure software container known as a DigiBox

* Methods and logic for creating ad hoc rights and business relationships among distribution chain participants known as "chain of handling and control"

* Software for "middleware services" (between network transport and applications and between the PC hardware and applications) that make use of the secure container and chain of handling and control methods and logic

Together, these three components provide copyright protection, usage metering, and guaranteed payment. InterTrust can take advantage of a hardware security co-processor if present, but the integrity of the InterTrust system does not require the presence of a hardware co-processor for many application models. The software-only version of InterTrust provides effective protection for most content types. If compromised, an attack yields only the keys for a particular piece of content, and potentially the local PC, and not for the system as a whole.

InterTrust is compatible with small and large devices and can be used in conjunction with a wide range of secure electronic commerce activities.

Figure 5.7 is a schematic representation of the DigiBox cryptographic envelope. The innovation (patent pending) here is that the envelope carries not only the content, but various permissions, prices, and pointers to clearinghouses for

information use, but offers a basis for a complete solution to secure ad hoc commerce transactions in a networked environment. Unlike the other technologies mentioned in this report, EPR's system provides for the persistent, on-going control, authorization, billing, and metering of digital information without having to integrate the EPR system into each and every application being used to access the protected information.

EPR's business model is based on a tiny part of each transaction fee collected at clearinghouses plus licensing fees from computer companies and software tool and operating system companies.

EPR is negotiating agreements with major companies to provide critical parts of the distribution chain, and major announcements are expected by the end of 1995. EPR has announced a strategic alliance with Copyright Clearance Center who will provide rights and permissions clearinghouse services.

Victor Shear has four granted patents involving content control and metering technologies. Extensive other patent materials are currently pending.

EPR does not yet have an export license for InterTrust, but believes there are no significant obstacles in creating an exportable version.

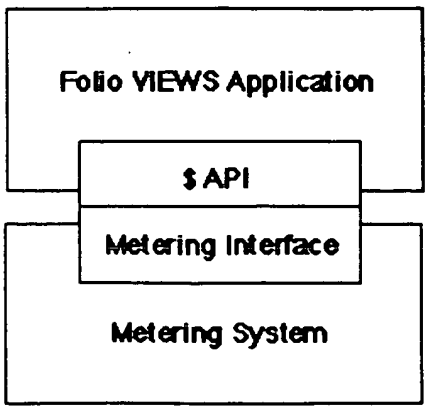
5.4 Metering Aware Applications

5.4.1 Folio Corporation

Folio Corporation, a division of Reed Elsevier plc, (Contact: Curt Allen, Executive Vice President, Folio Corporation, 5072 North Information Way (300W), Provo, UT 84604. Voice: 801-229-6700; Fax: 801-229-6785. Web home page. Folio develops and markets information base applications (infobases) worldwide. In use on more than 30 million desktops in the form of Folio VIEWSreg., on-line help for various software products and as a delivery mechanism for some 2,000 electronic titles from nearly 500 commercial publishers.

Among applications developers, Folio has taken a significant leadership position regarding the integration of metering and rights management technologies into their end user and server applications. They are adding to their applications and server software code that either tracks certain kinds of usage or that limits certain kinds of operations. An example of the former is the ability to count the number of times a document was opened, which pages were viewed on the screen, and how many pages were printed. An example of the latter is prohibiting modification of the document.

To leverage its core competency in user applications and server software, they have created a general interface, an Applications Programming Interface (API), that can be used by any maker of rights management and usage metering software. To use the API, any of Folio's metering partners would write new software that was the interface between the application and the meter.



act as a rights clearinghouse, this information is also part of the controls.

The content and the controls are put in a DigiBox software container. Some implementations will report this information to the rights clearinghouse (11).

Some publishers and authors may elect to distribute cryptographic envelopes and their contents directly to customers; others will delegate distribution. This example shows a more complex case, specifically, where there is both an aggregator (5) and a repackager or retailer (6). An aggregator, in this example, might be an organization such as Dialog or Lexis-Nexis. A repackager or retailer might be an organization such as Individual that combines articles into newsletters personalized according to the customer's current interest profile.

The chain of handling and control logic and methods permits one distribution chain participant to selectively modify the permissions and prices set previously. For example, the publisher may have established a retail price of $5.00 for an article if someone buys directly from them. The publisher may have also established a 40% discount for the aggregator. If someone buys the content from the aggregator at retail, they will pay whatever price they and the aggregator have agreed upon. This price might be $5.00, might be more, or might be less depending on the business objectives of the aggregator. In any event, InterTrust guarantees that the publisher will get their $3.00 and the aggregator will get their share as well and that the retail customer will, in fact, pay for use.

The aggregator, in turn, may modify the contents of the envelope so that the repackager pays the publisher's retail price minus 20%. The repackager might sell the article for more than publisher's retail, say retail plus 20%, or $6.00 since they have added the value of finding and repackaging the article according to the interests of their customer. All of the complexity of the real information creation and distribution industry can be implemented in a fully deployed InterTrust system.

Regardless of the actual distribution chain, the secure DigiBox container arrives at the customer's computer. In some cases, the credit and billing information may be established with the retailer prior to receiving the object. In other cases, the credit and billing information will be established when the object (envelope) is first opened. User authorization (7) and a number of the reporting steps can happen via the Internet.

The EPR InterTrust system keeps track of use (8) and periodically (the time intervals are set by the rightsholder, aggregator, and/or retailer), the metering system reports to a financial clearinghouse (10). The financial clearinghouse may be an organization established especially for this purpose or a financial institution, such as a bank or credit card company. In some instances, clearinghouse functions might be performed by others in the distribution chain, such as publishers, wholesalers or retailers. It is likely that eventually several financial clearinghouses will exist. The rights management system will contact the clearinghouse via networks or modems. In turn, the financial clearinghouse will report billing or credit card information to banks and credit card companies as appropriate.

A fully implemented InterTrust system is capable of capturing, storing, and reporting extremely detailed usage information including supporting simple to sophisticated advertising schemas. This detailed use information can be reported to the financial clearinghouse or aggregated by the metering technology on the user's computer. In instances where the full, detailed information is conveyed to a financial clearinghouse, it is anticipated that the financial clearinghouse will, in turn, report the detailed usage information to a rights clearinghouse, such as Copyright Clearance Center (11). In turn, the rights clearinghouse could aggregate the detailed usage information and report aggregate statistics to authors, publishers, and other rightsholders (1).

The banks and credit card companies will periodically convey the royalties to the appropriate rightsholders based on the information conveyed to them from the rights management system and as associated with the cryptographic envelope content.

Of the technologies investigated for this report, EPR's metering and rights architecture and system appears to be the most comprehensive and robust. It provides a general technology, not only for the control, metering, and billing of

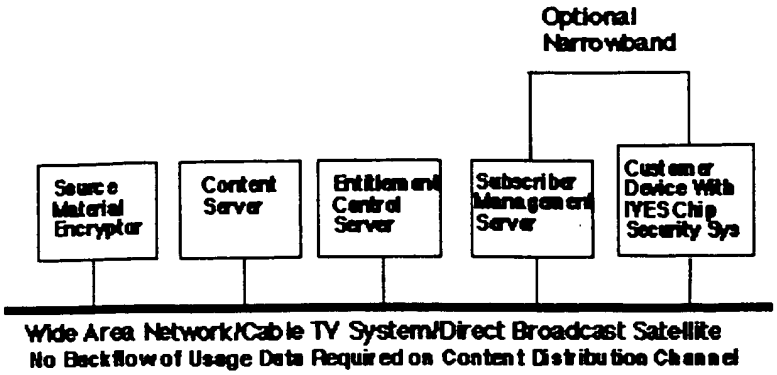


Figure 5.1. Schematic Representation of General IVES Architecture

The decryption key is stored on an "entitlement" control server. Entitlements are marketed on the network. When a customer purchases an entitlement for a specific piece of content, the entitlement is addressed to a specific device or set of devices designated by the customer.

The architecture also envisions a subscriber management server and applications that can respond to requests to purchase entitlements and see that the appropriate entitlements are distributed to the correct customer device or devices. The administrative system also handles billing and financial transactions.

Having purchased an entitlement for a particular piece of digital content, the user's system decrypts the content with the keys associated with the entitlement. As in other lock/unlock systems, once the content is paid for, no further protection is provided by the system. It appears, for example, that the user could record a video program for subsequent playback or redistribute the unencrypted content over networks or other media.

Supported payment systems include count-down and count-up credit. In the former, the user pre-pays some amount into an account. The system debits the account as usage occurs. In the latter, credit is authorized up to a specified amount and usage charges accumulated until that amount is reached. In either case, when the account is exhausted or the credit limit reached, no further entitlements will be dispensed. Credit information can be stored either on the customer device or on a server or both.

No further information is available at this time regarding AT&T's patent position, business model, exportability, or position on customer privacy issues.

5.1.2 CD-MAX, Inc.

CD-MAX, Inc. is a wholly owned subsidiary of InfoServe, Inc. with principal offices in New Jersey (219 South Street, Suite 203, Murray Hill, NJ 07974-2100, voice: (908) 771-0022, fax: (908) 771-0444, contact: David B. Boelio, Executive Vice President, Marketing, (908) 464-1878). Their chief business activities are copyright protection and usage billing services to information providers based on patented technology.

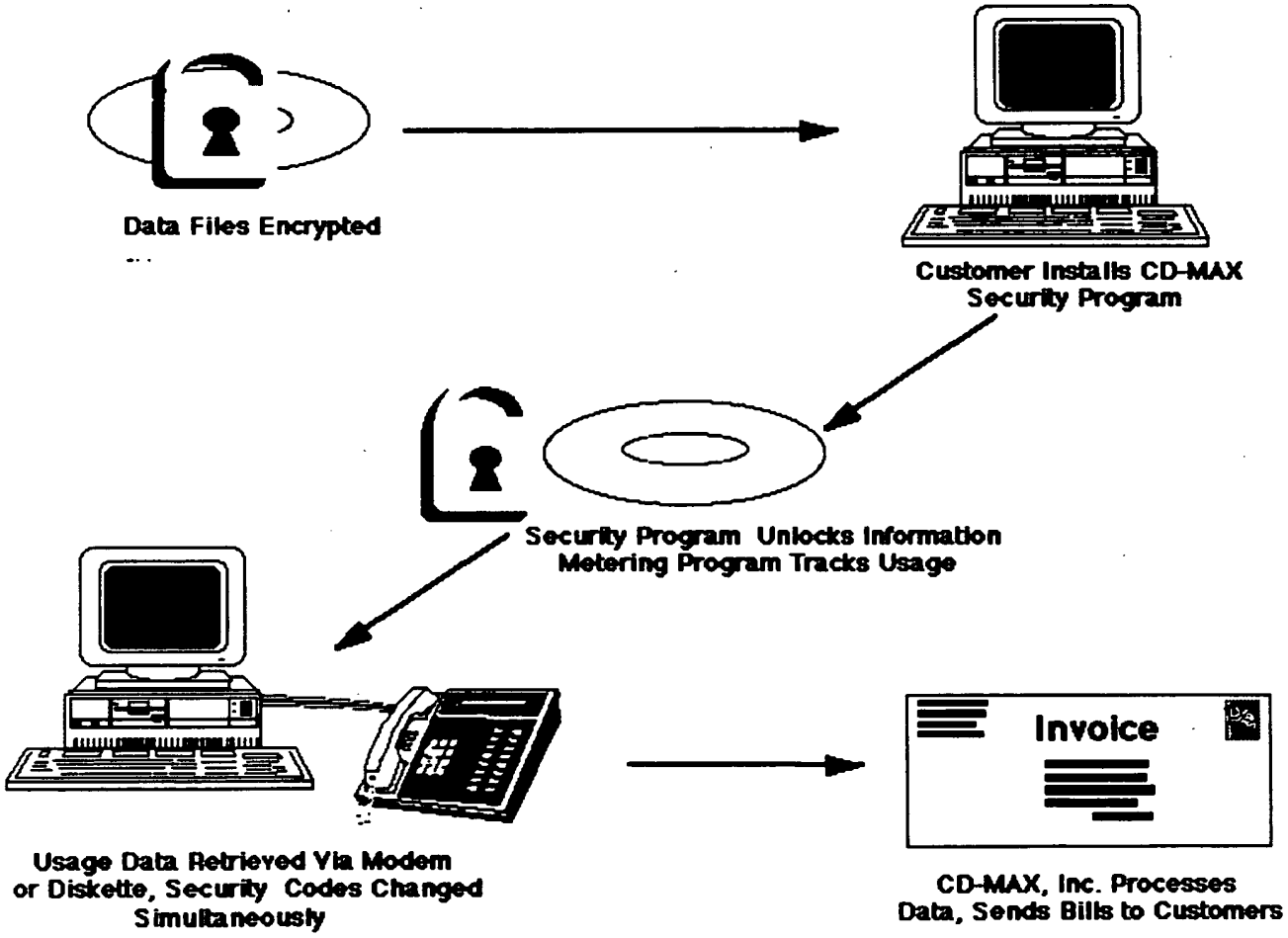
CD-MAX's approach to controlling content and metering begins with encrypting the content during development of the information base and before the CD-ROM is manufactured. CD-MAX provides a security program that is installed on the customer's PC. This security program transparently decrypts the information on the CD-ROM as it is accessed by the customer. DOS and Windows versions of the system have been delivered to client publishers. MAC and UNIX versions will be developed in response to demand.

Selected files on the CD-ROM is marked with a security code and the contents is encrypted with a proprietary encryption algorithm. This encryption method was designed especially for the PC environment. CD-MAX claims that the computing overhead for decryption is minimal and is not apparent to the user.

CD-MAX supplies the program that does the encryption of the content to publishers. Each program requires some modification depending on the search and retrieval software used by the publisher, so that, in effect, each program is unique.

Once processed by CD-MAX's encryption program, the files on the CD-ROM cannot be accessed except by the CD-MAX security application program running on the user's PC either from a diskette that accompanies the CD or from the CD itself. The CD-MAX security program is installed on the user's PC. A protected file is created at installation time on the user's hard disk that contains, among other things, security keys and usage information. This security system is dynamic in that it is designed to accept new keys periodically, and to prevent use when existing keys have expired. The keys are updated from diskette or by modem with a call to CD-MAX.

Publishers can choose from among a number of charging options. The particular actions that can be metered and billed include browsing, viewing, printing, and downloading. Publishers can choose a number of payment schemes, including customer prepayment or unrestricted use up to a specified credit limit. CD-MAX, Inc. processes usage data and payments for publishers.



Used with permission of CD-MAX, Inc.

Figure 5.2. CD-MAX Process Flow

A market research function is also offered as part of the usage reports CD-MAX makes to publishers as part of its billing services.

In February, 1995, the Bureau of Export Administration of the U.S. Department of Commerce granted CD-MAX an unrestricted export license for its copyright protection and usage billing services. This license allows their technology to be freely exported and deployed everywhere, except Cuba, Cambodia, Libya, North Korea, or Viet Nam.

According to CD-MAX, their security, metering, and billing solutions are media-independent and multi-platform in their design. While CD-ROM and local area networks have been their first priority, they intend to demonstrate in the near future CD-MAX's ability to operate effectively in wide area networks, including the Internet.

CD-MAX, Inc. claims protection, in part, from at least four patents granted and applied for by Dr. John David Wiedemer, a founder of the company.

CD-MAX's business model is based on performing clearinghouse functions for billing and taking a small fee for handling each billing transaction. Details of pricing and other financial information were not available.

Since last year, CD-MAX has entered into a number of strategic alliances:

* Folio. In March, 1995, CD-MAX announced that it has been designated a Technology Partner by Folio Corporation. The relationship plans to incorporate CD-MAX technology with Folio Metering Application Programming Interface and Folio VIEWSreg. software.

* Mitchell International. In June, 1995, CD-MAX announced that Mitchell International will include CD-MAX's copyright and billing technology in Mitchell's new version of Mitchell On-Demand(TM) Repair Information System product line. 10,000 service stations and dealerships presently use this product line. The new version of Metered On-Demand was released in August, 1995.

* Disclosure. In August, 1995, CD-MAX and Disclosure, Inc. announced an alliance to produce a metered product entitled, "Metered New Issues Database." The product is expected to be released in September, 1995. Disclosure has plans to use CD-MAX's technology to offer new customers a free trial of the database while also using CD-MAX's technology to register, track information usage and bill customers. Reporting is planned to be completed via modem or mailing in a disk.

Regarding user privacy issues, CD-MAX endorses the Information Industry Association's "Fair Information Practices Guidelines" and has implemented procedures and policies to ensure security and privacy. The exact nature of these procedures and policies has remained confidential.

5.1.3 Infosafe Systems, Inc.

Infosafe Systems, Inc. offers a hardware-based system for protecting and metering information (Contact: Thomas H. Lipscomb, President, Infosafe Systems, Inc., 342 Madison Avenue, Suite 622, New York, NY 10173, Voice: 212-867-7200; Fax: 212-867-7227. Web home page.

Their technology is proprietary and employs both hardware and software. An external "box," the Infosafe-Mark III, is connected via an SCSI interface (Small Computer System Interface) to either an individual's computer, or to a server machine capable of supporting several users. Presently supported are Macintosh and Intel Architecture computers (DOS, Windows). Infosafe provides software to run on the subscriber's computer; no modifications are required to the operating system that runs the subscriber's computer.

Prior to delivery to the customer, the publisher/rightsholder identifies appropriate chunks of information such as articles, paragraphs, images, and the like that would constitute a basic "packet" of information that could be priced and charged for separately. Typically, the publisher also creates a separate abstract and/or index for each packet. As part of the production process, each packet is assigned a separate encryption key, encrypted, and put on the CD-ROM or other delivery media together with the un-encrypted and hence, searchable, abstracts and indices. Packets may be of any size, including a single graph, photograph, article, paragraph, typeface, word, statistic, or data-point.

In a typical application, the user browses the abstracts or search results at no charge and is informed of the costs

associated with purchasing the decrypted information packets. Once purchased, the information packets are decrypted and released to the user under the terms of the appropriate information provider's license agreement.

The Mark III is also equipped with a modem and a phone line that can be conveniently shared with other devices, including fax and voice calls. The modem is used by the Infosafe system to communicate with Infosafe or with an information provider's service bureau. Credit authorizations and decryption keys are sent to the Infosafe system; usage information is sent back to the publisher and/or to Infosafe, Inc. The Infosafe Mark III comes with an installed credit card reader to allow billing to credit cards instead of pre-establishing credit with the publisher and/or Infosafe.

The Infosafe system supports a wide range of charging algorithms, ranging from monthly or annual subscriptions with unlimited use, to "pay-per-view" for the smallest packet of information.

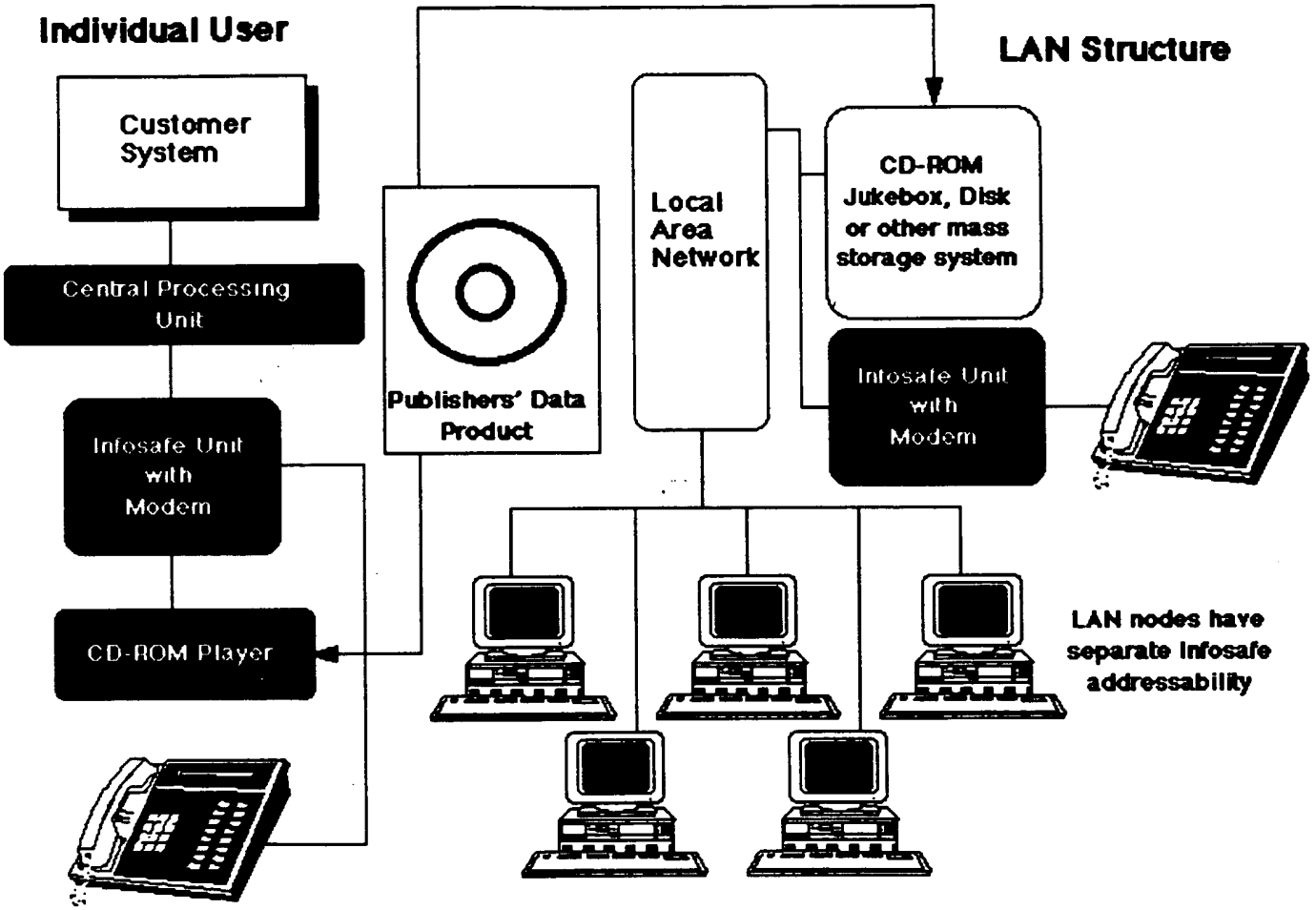


Figure 5.3 Typical Infosafe System Individual and Client/Server Configuration

The Infosafe system generally employs the widely used Digital Encryption Standard (DES) and also supports other encryption techniques, as applicable to the needs of a given customer, such as RSA public key encryption. Proprietary encryption key management techniques, plus the assignment of a different key to each packet, ensure that in the highly unlikely event of an encryption key being compromised, the loss would be a single packet, rather than an entire information base. Also, each Infosafe device communicates via the modem to Infosafe Systems, Inc.'s "back office" to validate the on-going integrity of the subscriber's hardware device.

The "back office" operation consists of four major functions: (1) encryption key management and hardware services, which involve setup and support on the Infosafe system, and on-going encryption key oversight and management services; (2) subscriber support services, which involve handling or distributing customer service inquiries and user support inquiries regarding the Infosafe system or the publishers' data; (3) billing and credit services, which involve

monitoring subscriber usage information, conveying electronic information regarding credit balances and requests between the subscriber and publisher, and coordinating management of publisher mailings and processing of bills; and (4) market support services, which involve frequent communications between Infosafe Systems, Inc. and the publisher to assist the publisher in realizing the maximum return on their investment in the Infosafe system. Based on information returned from the metering device, publishers can analyze usage information to yield marketing information showing patterns of use. This allows rightsholders to re-configure or update products or change prices, either universally or at specific locations, using the memory storage available in each Mark III.

While Infosafe can perform clearinghouse operations, the Mark III is compatible with each publisher or their delegated agent performing clearinghouse functions. Infosafe's business model appears to be based on receiving a portion of the publisher's revenue stream from the protected data.

Additionally, Infosafe works with its clients to design, configure, and sell digital streams of information delivered through the Mark III. It charges a fee for initial configuration and software design and takes a portion of the publisher's revenue from the data it protects and delivers through the system. The size of the initial fee varies and depends, in part, on the extent of revenue sharing going forward. No detailed pricing information was made available by Infosafe.

One patent has been granted to Robert Nagel (InfoSafe Chief Scientist) and Thomas Lipscomb (CEO). At least one other is pending. In addition, Lipscomb and Peter Sprague (Wave Systems' CEO) have been granted a relevant patent.

In the past year, InfoSafe has entered into a number of strategic alliances and made one acquisition:

* Folio. In March, 1995, Folio Corporation, a division of Reed-Elsevier, announced Infosafe as a key supplier for its new Folio Metering API (application programming interface). Folio Corporation is a leading provider of infobase software with products installed on an estimated 30 million desktops in the form of Folio VIEWSreg., on-line help for various software products, and as the delivery mechanism for some 2,000 electronic titles from nearly 500 commercial publishers.

* Design Palette(TM). InfoSafe has branched out from being a supplier of copyright protection systems to a provider of content. In April, 1995, Infosafe Systems, Inc. announced that it purchased Design Palette from one of its largest customers, International Typeface Corporation (ITC). The vendor relationship between Infosafe and ITC will continue. ITC will remain responsible for managing 25 vendors' content for a 40 plus CD-ROM library. Vendors include PhotoDics, AGFA, Adobe and Letraset.

* Copyright Clearance Center. In August, 1995, InfoSafe Systems and Copyright Clearance Center announced they will work together to develop fully secure, auditable and interactive digital clearance for copyrighted materials.

InfoSafe has applied for, but not yet been granted, an export license by the Department of Commerce for the Mark III.

5.1.4 Spyrus, Inc.

Spyrus, Inc. is a small designer and implementor of strong security systems based on cryptography that is well-respected in the cryptography and security communities. (Contact: Sue Pontius, CEO, Spyrus, Inc., 2841 Junction Ave., Suite 110, San Jose, CA 95134, Voice: 408-432-8180; Fax: 408-432-8415). For example, they are among the leaders in security tokens on PCMCIA cards that authenticate individuals to various security systems.

Spryus has brought to market a third party software developer's kit (SDK) for content protection and usage metering. The SDK implements strong cryptographic methods for secure communications between publishers and users and between users and data bases principally on CD-ROM.

Spyrus does not itself develop the complete metering application, but instead relies on third party partners.

Spyrus has applied for one or more patents in this area.

No public information is available regarding current licensees of their SDK.

No public information is available regarding licensing fees for their SDK.

No information is available regarding exportability of their SDK and resulting applications.

5.1.5 Wave Systems Corporation

Wave Systems Corporation (WSC) (Peter Sprague, CEO, Corporate Headquarters: 540 Madison Ave. New York, NY 10022 Phone: (212) 755-3282, Fax: (212) 755-3436. Web home page: http://emporium.turnpike.net/W/wave/wavhome.htm) plans both CD-ROM and networked versions of the encryption-based metering technologies. Wave Systems completed a successful public stock offering in September, 1994.

The Wave System has five basic components: (1) the WaveMeter, a device for control and metering, (2) data preparation, (3) information delivery, (4) search and retrieval applications, and (5) WaveNet, the "back office" system. Figure 5.4 shows a typical application in which the WaveMeter is attached to a computer that acts as an information server for several other nearby computers connected through a network. Each of the major components is discussed below.

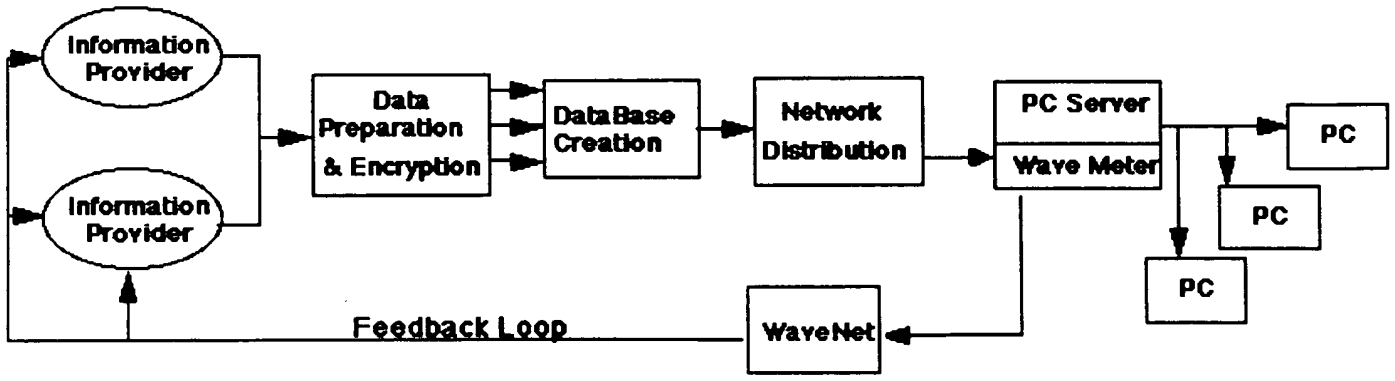


Figure 5.4 Typical WaveMeter Application

The WaveMeter is a microprocessor-based device that decrypts information and tracks usage information. It is attached to a computer or computer network. Figure 5.5 shows schematically the functions it performs, including key management, decryption, credit/debit accounting, storing pricing and tax data, and maintaining the usage log. To initialize the WaveMeter, the user starts by electronically dialing into WaveNet, a WSC operated system, using a modem and telephone lines. Once connected, the customer uses a credit card to establish a credit balance, which is automatically loaded into his/her WaveMeter. Organizations are expected to establish credit balances directly with WaveNet, rather than through credit cards. Having established credit, the customer automatically receives keys for databases s/he may wish to purchase. After initializing the WaveMeter, the user can browse through and purchase information using the appropriate search and retrieval applications. For each information packet selected, a purchase price is displayed. To make a purchase, the user fills in information on the screen, including cost accounting information. The information is then decrypted by the WaveMeter and handed off to the search and retrieval application for presentation or printing. As decryption occurs, the usage information is stored within the WaveMeter.

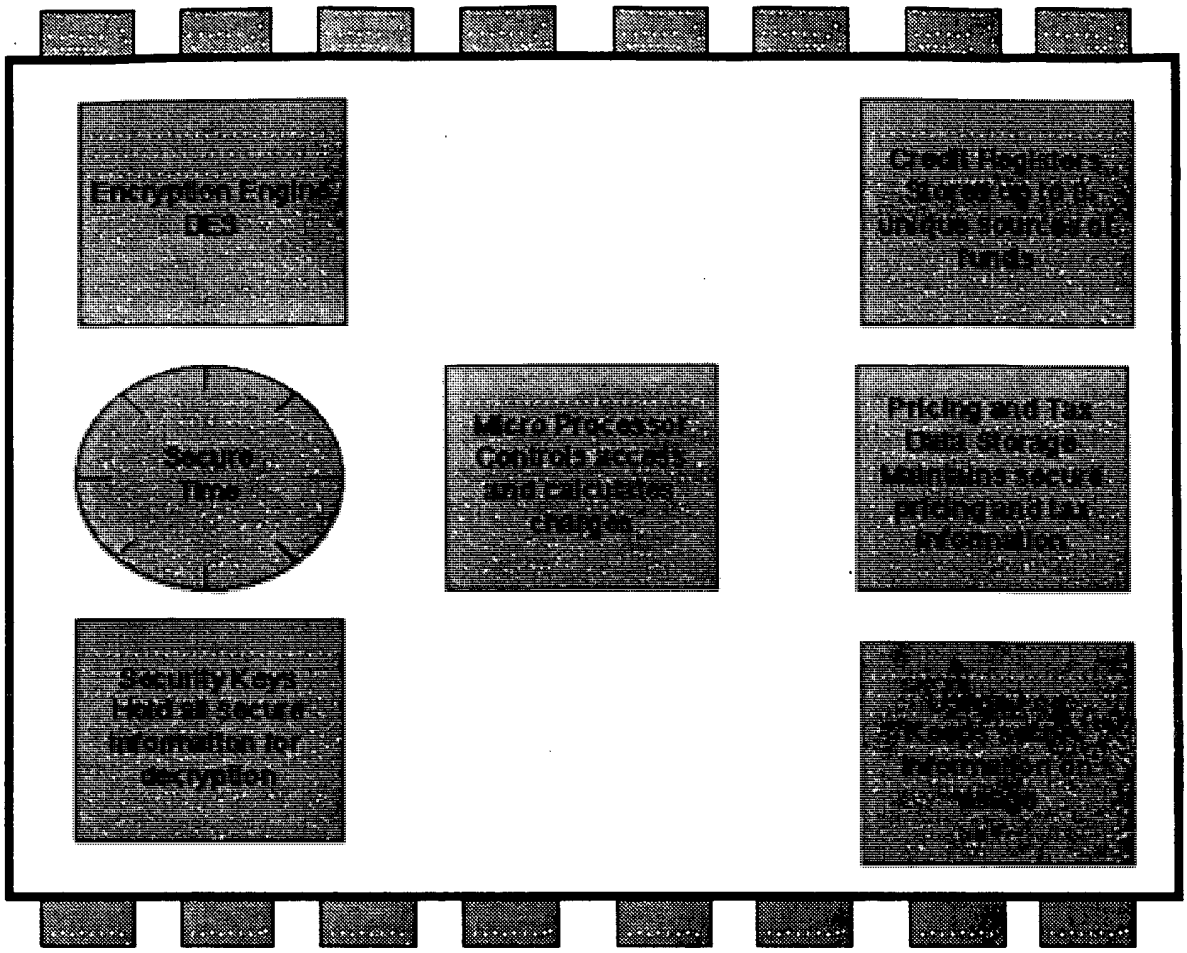


Figure 5.5 WaveMeter Functional Schematic

Data Preparation. In preparing the information to be protected by the Wave System, the publisher performs four basic tasks. First, the publisher defines logical groupings of information that can be purchased as a single item. This might be an article, a page, an entire volume or database, and so on. Next, the publisher sets the pricing for each logical unit of information, such as an article and what is called the "pricing factor," for each database. The "pricing factor" is a multiplier to be applied against the prices set for each unit in the database. Pricing factors can be changed over time by the publisher. WSC provides a publisher interface to WaveNet for this purpose. The third data preparation step is to define abstracts and keywords. Wave System stores information in packets that have an encrypted part and a "clear" area in which publishers typically put abstracts and keywords that can be searched easily. The fourth and final step consists of encrypting the information to be protected. The encryption is fully automated and represents no burden to the publisher. Wave uses the Data Encryption Standard (DES).

Information Delivery. Once encrypted, the information can be delivered to customer locations by a variety of means. Early implementations of Wave System will be CD-ROM based. Later versions are expected to use Wide Area Networks, such as the Internet, satellite, or sideband FM radio broadcasting (combining text information with FM radio broadcasts that don't interfere with the primary content of the broadcast).

Search and Retrieval Applications. WSC does not provide its own search and retrieval or other end-user applications. Instead, WSC provides what are known as Application Programming Interfaces (APIs) that define how software developers can incorporate WaveMeter functions in their applications.

WaveNet is comprised of all the "back office" data communications and information processing systems. The way to think about WaveNet is as a transaction processing system for electronic commerce. Each transaction is initiated by the user through the WaveMeter over dial-up lines to WaveNet. Each call results in one of four types of transactions:

(1) registration of a new WaveMeter; (2) establishing and downloading credit; (3) downloading decryption keys for selected databases, and (4) uploading usage transaction information (See Figure 3.6.). WaveNet also performs encryption and clearinghouse functions for publishers over electronic connections (modems and telephone lines). The Information Management Processing Center (IMPC) component of WaveNet provides the management, control, and distribution of all encryption and decryption keys. This includes distributing encryption keys to publishers for each information packet, and managing the delivery of decryption to WaveMeters. Also, through the IMPC, publishers can establish prices on new databases, change prices on previously released databases, and change the types of transactions permitted for released databases. The IMPC also performs billing in those cases where WSC extends credit to individuals or to corporations. The IMPC also delivers usage reports to publishers and remits royalty payments regardless of whether payment was made through credit cards or through WSC.

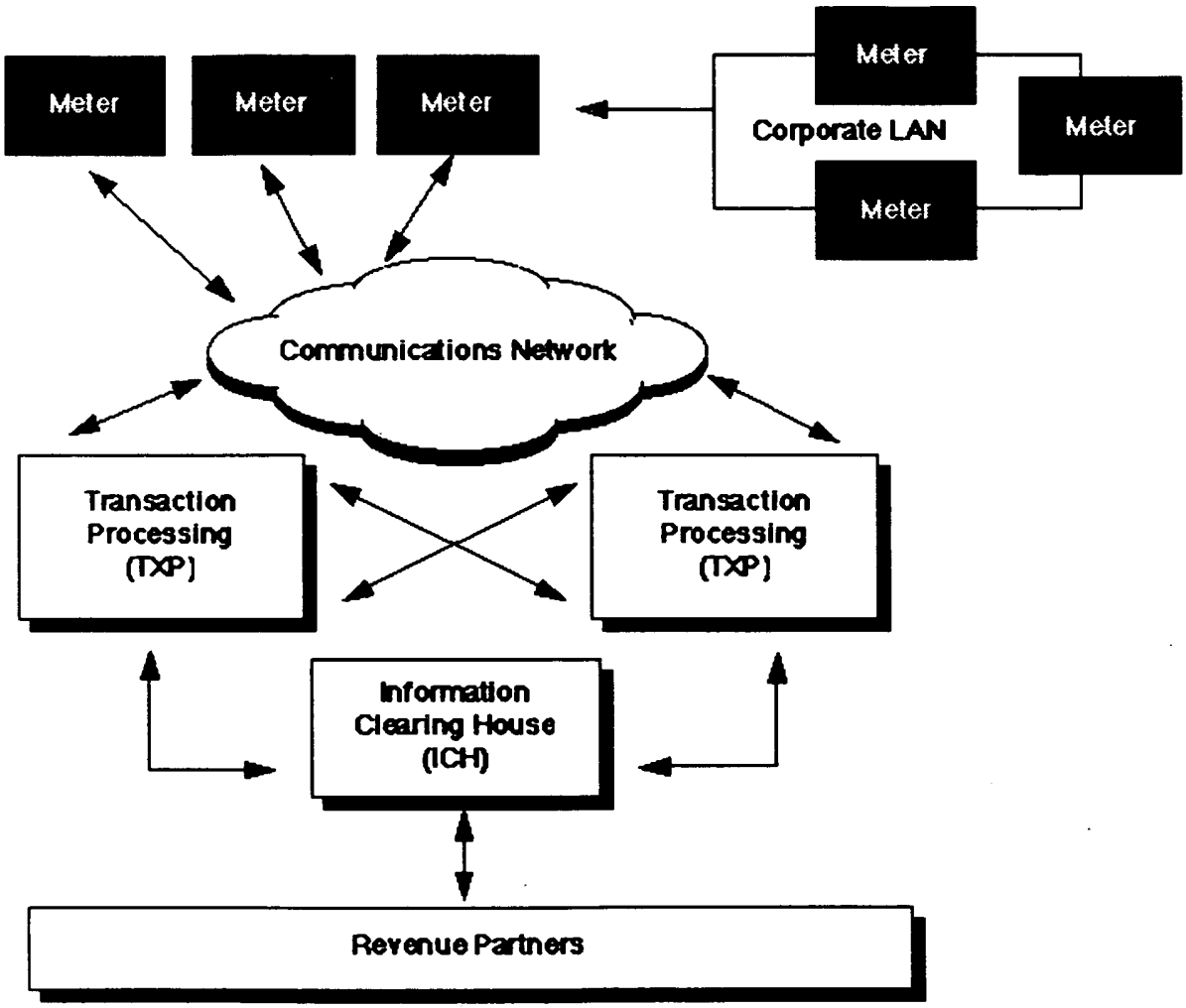


Figure 5.6 WaveNet Schematic

In its present implementation, once the user has paid for and received the decrypted information, the system provides no persistent, on-going control and usage metering capability of the digital information unless the Wave system is integrated with the application being used to access and process the purchased information.

The WSC business model is based on providing a set of standards for the WaveMeter and for the software that interacts with it. As noted, they also perform clearinghouse functions and retain a part of the royalty stream. No information was provided regarding the percentage retained by WSC.

Prices for the WaveMeter will vary according to how it is implemented. When built into a computer, the additional cost might be in the neighborhood of $15. A networking card version is expected to cost about $150. An external box with a SCSI interface is expected to cost about $180. Early release of the product began in the summer of 1995.

payment, usage reporting, and new or additional permissions.

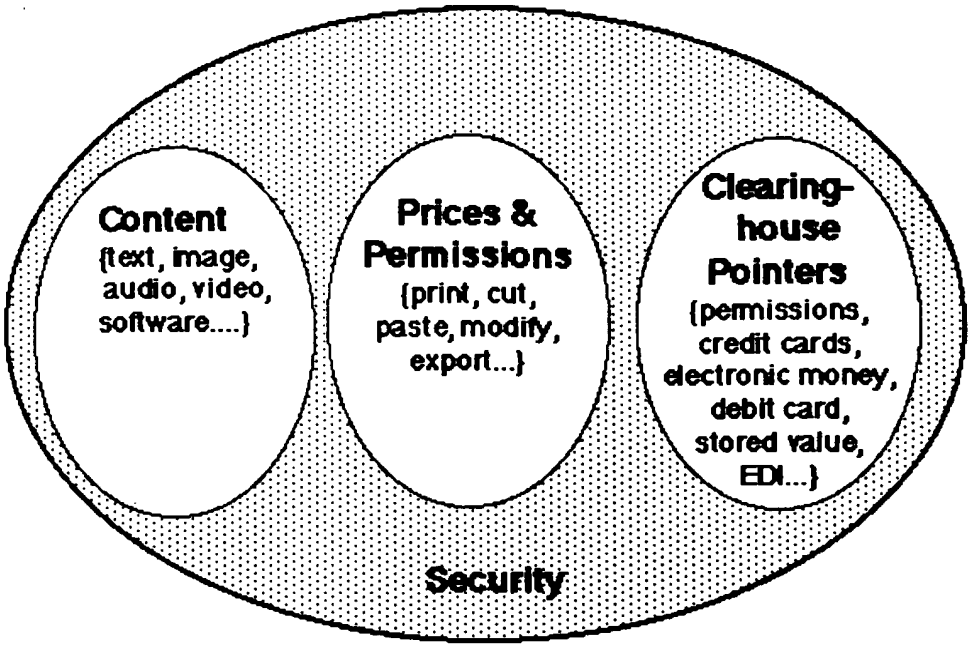


Figure 5.7. EPR DigiBox Container Schematic

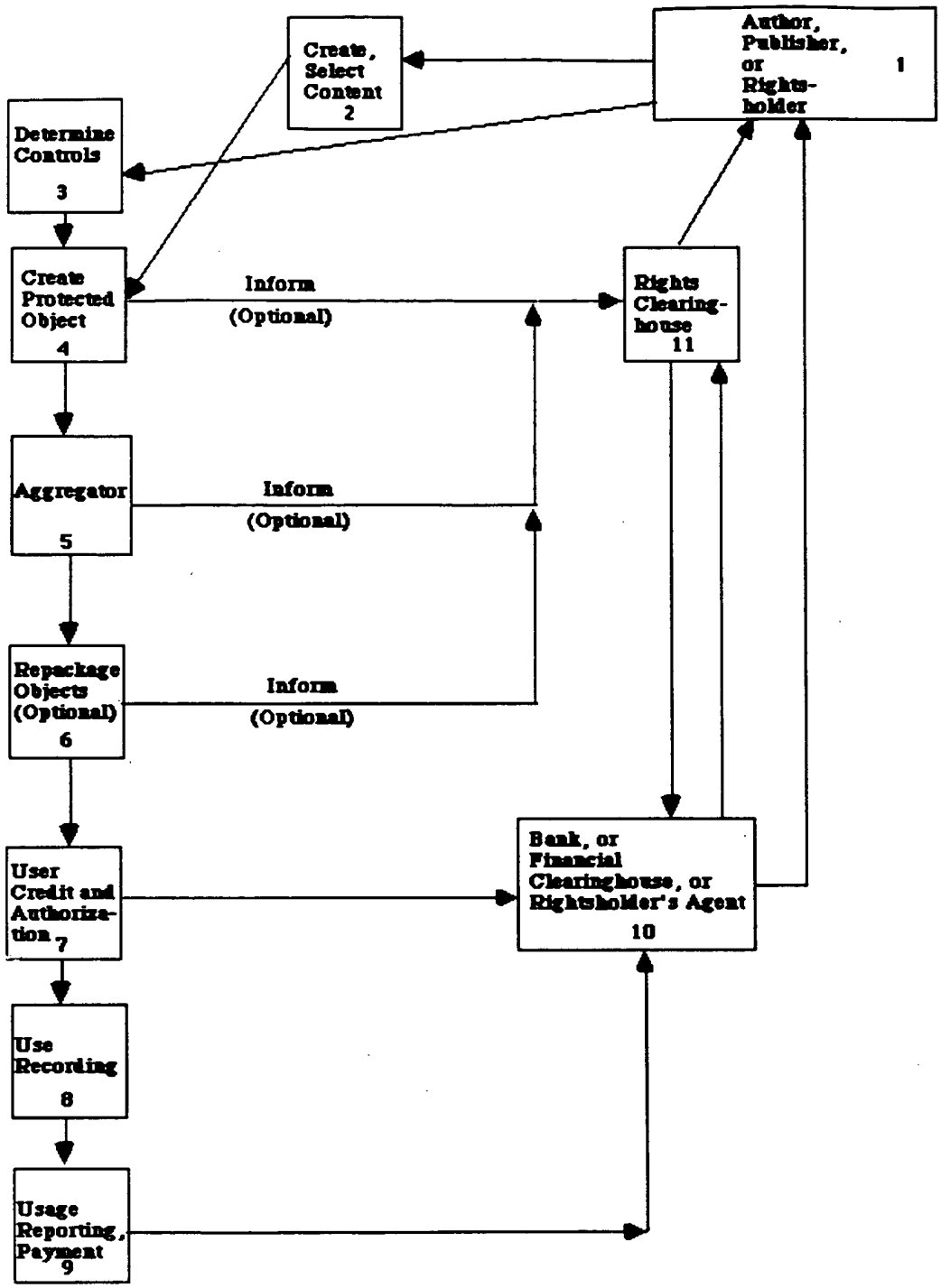


Figure 5.8. EPR System Elements and Process Flow Example

In the description that follows, the numbers refer to the numbered boxes in Figure 5.8. An author, publisher, or other rightsholder (1) selects content to be protected by InterTrust (2) and a set of permissions, prices, and other control information (3) that apply to the content. Imagine, for the sake of this illustration, that the content is an article from a newspaper or science journal.

Authorized uses might include any or all of those listed in Chapter One, such as printing, excerpting, or transmitting. The prices for each authorized use are also established, for example, $X per printed page or per 2,500 characters printed (since ASCII text, for example, might not have page break information). The control information also contains pointers to certain operators of clearinghouse functions. If the rightsholder has established accounts at a particular bank or has nominated a financial clearinghouse or an organization such as Copyright Clearance Center to

Figure 5.9. Schematic View of Folio $ API

Figure 5.9 presents a schematic representation of the $ API. Each of Folio's partners will create their own metering interface that will exchange rights management and usage information to the application by communicating with the $ API.

Thus far, Folio has announced strategic alliances with CD-MAX, Inc., InfoSafe Systems, and Wave Systems. Another alliance with Copyright Clearance Center for clearinghouse services has also been announced. Additional announcements are expected in late 1995 and early 1996.

No public information is available on Folio patents in this area.

Since encryption/decryption is likely to be performed by the metering systems, rather than by the Folio applications, there does not appear to be limitations on exportability of the Folio software.

5.5 Rights Clearinghouses

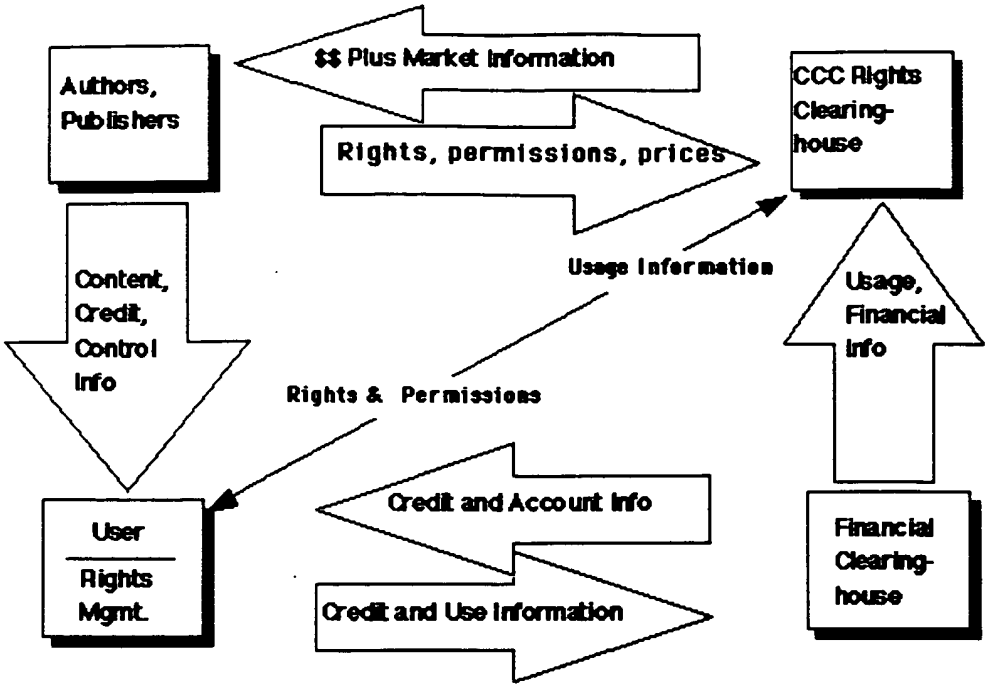
This section reports one American and one Canadian effort to create on-line rights clearinghouses.

In conjunction with the deployment of rights management technologies, some meter makers and some rightsholders may elect to operate their own on-line clearinghouses. In addition, there is likely to be one or more on-line clearinghouses that are not operated directly by meter makers or by any one publisher or other rightsholder organization. As noted in Chapter 3 of this report, Copyright Clearance Center will operate a vendor and publisher neutral clearinghouse.

In addition, a consortium of Canadian rights, technology, and academic organizations have put together the IVY Consortium to develop rights clearinghouse technologies.

5.5.1 Copyright Clearance Center

In support of several announced partnerships, Copyright Clearance Center (CCC) will provide rights and permissions clearinghouse services. (Contact: Kelly Frey, Director, New Business Development, Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, Voice: 508-750-8400; Fax: 508-750-4343; E-mail: kellyfrey@copyright.com; Web Home Page. CCC's base business has been in the permissions and usage royalties for photocopying. They license on behalf of over 9,200 publishers who, in turn, represent hundreds of thousands of authors. For the past several years, CCC has instituted several new programs focused on permissions for digital content in the business and higher education markets. This brief section augments the discussion of rights and permissions clearinghouses in Chapter 3 of this report.



5.10. Clearinghouses In A Metering Environment

Figure 5.10 shows how information and money flows among rightsholders, users, and financial and rights clearinghouses.

CCC has no patents in the area of rights management. They intend to license the appropriate technologies from other companies, if necessary.

CCC has announced strategic alliances with three companies that have agreed to work together. These are Folio and InfoSafe Systems.

CCC has also announced a separate strategic alliance with EPR. Other announcements are expected over the next year.

CCC has announced its intentions to provide digital rights clearinghouse services on the global Internet, working with its network of RRO relationships. In doing so, it will be constrained by the export restrictions, if any, on its several technology partners.

5.5.2 The IVY Group

IVY is a comprehensive intellectual property management system for digital content. It includes components for rightsholders, producers and end users. Owners have a simple method of enrolling their works individually or in bulk (for large catalogues). Producers are offered a catalog of content from which they can select unimedia or multimedia works for inclusion as components in a CD-ROM, for example, or in content made available on digital networks. IVY tracks usage and reconciles it with distribution agreements to generate authorizations, authentications, and billing components. IVY accommodates all known and proposed billing schemes. It uses state-of-the-art protection schemes including encryption, fingerprinting, tagging and copy prohibition. The IVY League is a group of Canadian stakeholders who are endorsing and using the IVY system for both Internet and broadband network delivery on a trial basis, and for clearing rights to CD-based products. IVY Leaguers include SOCAN (performing rights), CANCOPY (literary rights), CMRRA (music reproduction rights), ACTRA (actors & performers), CBC (national broadcasters), CRIA (Canadian Record Industry Association), AYLA (audio visual rights). IVY is being deployed in 1995 on Intercom Ontario, a $100 million network connecting residential housing, schools and governments in Ontario, Canada. Major Intercom partners include Bell Canada, IBM, and Apple along with more than seventy other

companies, schools and governments.

IVY was developed at York University, Toronto by CulTech Research Centre who partnered with Disus and SOCAN to bring IVY to commercial reality. Disus is a well known telecommunications software firm and SOCAN is Canada's largest copyright collective with more than $70 million annual income from music performances. Contact: Paul Hoffert, Executive Director, 4700 Keele Street, North York, Ontario, Canada M3J 1P3, Voice: 416-736-5405, Fax: 416-736-5404, Web Home Page; contact: Tom Jurenka, Director, Empirics/Disus, 47 Colborne Ave, Suite 303, Toronto, Ontario, Canada M5E 1P8; Voice: 416-417-7035, Fax: 416-461-8439.

According to Paul Hoffert, Director of CulTech, IVY is an intellectual property management and accounting system that incorporates:

* Intellectual property accounting software

* Trusted rights administration

* Accommodations for financial clearinghouses

* Interactive network and CD-ROM delivery

A simplified diagram of IVY's structure of rights administration is shown in Figure 5.11. There is both a financial clearinghouse to handle billing and payment and a separate agency - The IVY League - for rights clearings.

The owner licenses limited exploitation rights to a producer who licenses distributors, who in turn, license retailers who sell to users. The structure may be collapsed so that an owner may be a producer, distributor, and retailer or any other permutation of functions among the food chain categories. Owners and producers must enroll a work with the rights administration agency so that it may grant a license to the user.

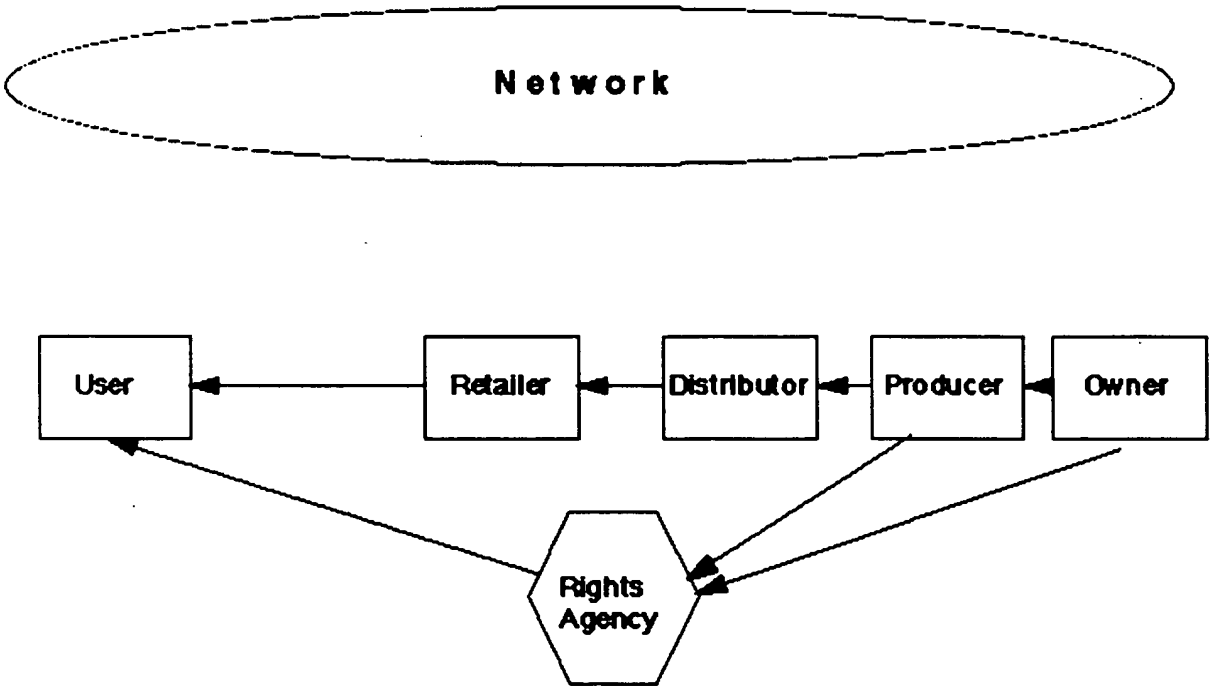


Figure 5.11. Typical Flow of Rights

At the same time, various distribution chain participants need to be authenticated: how do we know that the person claiming to be user "Laura-who-lives-on Maple-Street" is really the person she says she is. The authentication and security methods being implemented in IVY similar to the Kerberos system for security and authentication developed

at MIT's Project Athena. A second security function is authorization. Once having ensured the identity of the user, the IVY system authorizes their use and/or purchase of specific properties.

Figure 5.12 shows an example of how authorization might flow in a video-on-demand environment. Here the network authorizes the connection of servers to it and the servers in turn, rent media space to authorized retailers who upload their content to the servers. The financial clearinghouse authorizes both users (credit or debit accounts) and retailers (merchant ID number). In addition, the rights agency must authorize both the retailer and the user by sending appropriate decryption keys for the content.

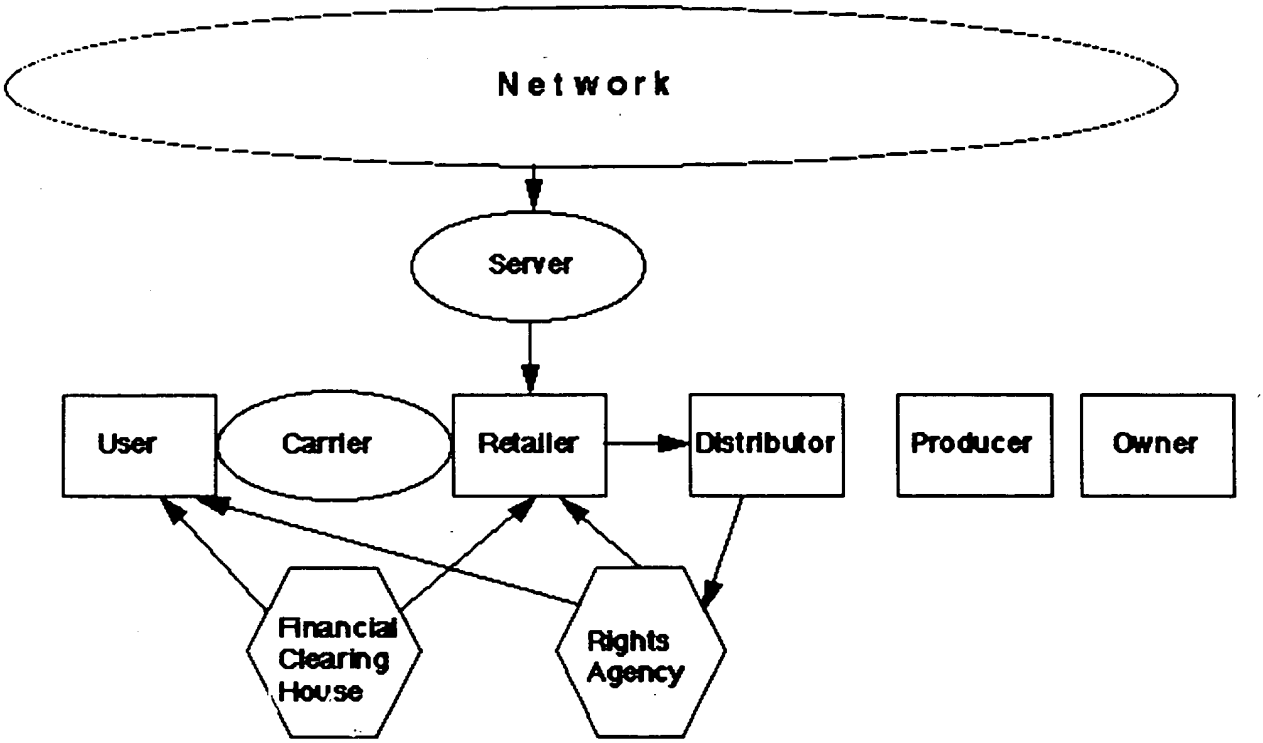


Figure 5.12. IVY Authorization Flow

Payment, of course, is a vital part of the IVY vision (Figure 5.13). Payment flows from the user to the financial clearinghouse and from there to the retailer. The analogy is to a physical mall (server) renting space to a merchant (retailer) who receives a merchant ID (authorization number). In a parallel structure, the rights agency collects payment from distributors and pays owners and producers.

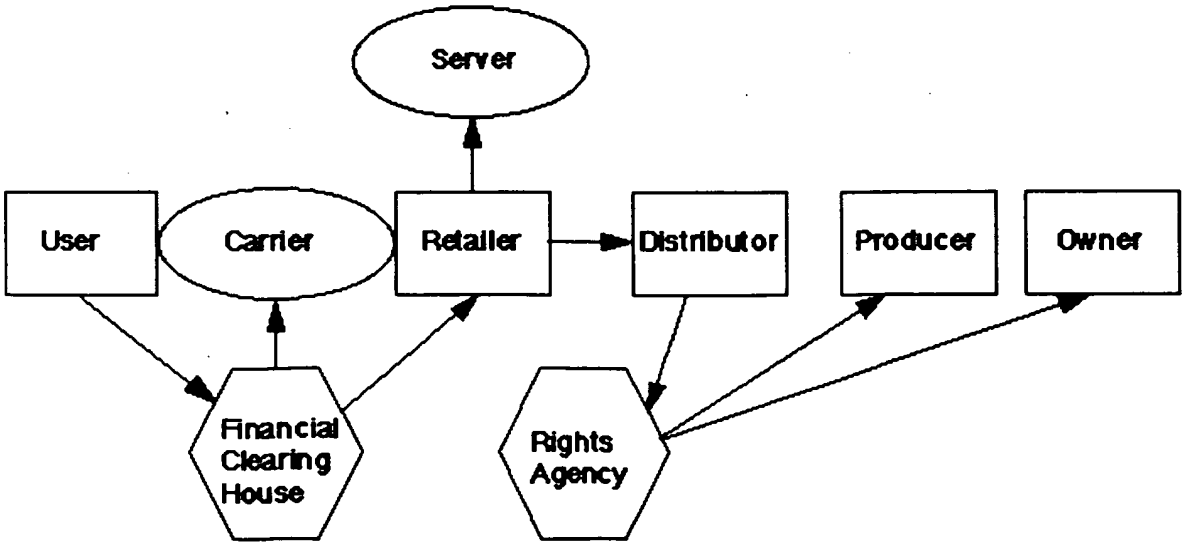


Figure 5.13. The IVY Vision

The IVY effort is backed by several major technologies, telecommunications, and content companies. Although their initial focus is video-on-demand and other multimedia over broadband applications, the rights management issues IVY addresses are generic. Thus, their rights clearinghouse may service content distribution business other than video-on-demand.

The IVY group is less interested in developing new technologies than applying existing technologies to rights and financial clearinghouse activities.

IVY will likely be the first IP management system to go into regular operation with backing from a broad range of content collectives, network operators and users. No public information is yet available on the business models for their financial and rights clearinghouses.

THIS PAGE BLANK (USPTO)

PCMCIA Redefines Mobile Computing

Finally, your notebook PC has expansion slots—and a full complement of high-performance peripherals.

BY EARLE J. ROBINSON

Although its name doesn't exactly roll off the tongue, PCMCIA is changing mobile computing more dramatically than any technology today. And after years of unfulfilled expectations, we finally have the products to prove it.

Developed in 1989 by the Personal Computer Memory Card International Association, a consortium of more than 300 manufacturers that includes Apple, IBM, and Toshiba, PCMCIA is a completely open, nonproprietary bus standard that does for notebooks, subnotebooks, and palmtops what the ISA bus did for desktop PCs. The compatibility PCMCIA promises—though hardly perfect yet—will allow you to plug any manufacturer's PCMCIA peripheral into your notebook.

We've all seen credit-card-size PCMCIA peripherals (about 2.1 by 3.4 inches), most typically as memory cards or modems. But the full I/O capability supported by the standard also allows mechanical devices such as tiny IDE hard drives to use the slots. PCMCIA LAN cards are already making inroads into traditional notebook docking stations. A host of peripherals, including sound cards, SCSI and CD-ROM controllers, and tape backup drives, looms on the horizon. Wireless modems are already here, and wireless LAN connectors are slowly emerging as well.

Unfortunately, you can expect to pay a hefty premium for these devices: roughly double that of their full-size ISA counterparts. The prices won't remain high, however. As more peripherals begin to reach the market, resulting competition will pull prices earthward. By 1995, for example, modem prices will be within $50 of what you'd pay for an ISA-bus peripheral, according to AP Research.

To find out how compatible, powerful, and easy to use current PCMCIA peripherals really are, we looked at representative PCMCIA products in each of three categories—modems, LAN adapters, and hard drives—and tested them on a Dell 320SLi, an NCR 3170, and a Toshiba T4500. And to give you an idea of the scope of available PCMCIA peripherals, we compiled resource directories listing specs and prices on PCMCIA modems, LAN cards, and hard drives that you can buy today.

Yes, the standard does have some rough edges—there's a haze of types and version numbers—and, yes, universal compatibility remains a goal, not a reality. Still, if you're in the market for a notebook today, you'd be foolish to consider anything without at least one Type II PCMCIA slot, preferably two. When compatibility issues get ironed out and prices start to fall, you'll be

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1016, p. 1037

The PCMCIA Payoff

- Universal notebook upgrade
- Easy installation and configuration
- High prices will drop with competition
- Will soon be interchangeable with desktop slots

BEST AVAILABLE COPY

able to choose from among a flood of high-performance, plug-and-play peripherals that could be interchangeable with a PCMCIA-slot-equipped desktop PC. Look for our full review of PCMCIA-equipped notebooks and peripherals in an upcoming issue.

PLUG AND PLAY? The key to PCMCIA's success is its auto-configurability. Instead of fiddling with DIP switches and configuration programs, you merely pop a peripheral into a slot. The host system automatically recognizes it, which it confirms with a single beep. At least that's what the specification is designed to do. The cards we tested required some installation and running of software. These problems, combined with the confusing array of substandards within PCMCIA, explain why the standard has been slow to win widespread acceptance.

FOUR FLAVORS There are three, soon to be four, types of PCMCIA slots, each identified by the thickness of the card that fits in it. Type I slots, which are 3.3 millimeters thick, accommodate memory cards only. Type II slots, which are backward compatible, hold cards that are 5mm thick (but otherwise maintain the same form factor as Type I cards) and support full I/O capabilities. Older cards can be used in slots that are thicker, because the guides that seat the cards remain the same thickness. Only the center portion of the slot is higher.

Last autumn, Type III slots emerged. Measuring a full 10.5mm thick, they're designed primarily for removable hard drives. Type III is also backward compatible. Type IV slots, which will debut in notebook computers by year end, will accept even thicker hard drives, though the exact size hasn't yet been settled.

Most notebooks—even those now coming to market, such as the IBM ThinkPad 720C—offer only Type II PCMCIA slots. If you plan to install a PCMCIA hard drive in your notebook, your purchase may have to wait until more Type III slots are available. Several manufacturers, including IBM and Hewlett-Packard, also plan to provide PCMCIA slots in desktop computers, a development that will make peripherals interchangeable between portable and deskbound machines.

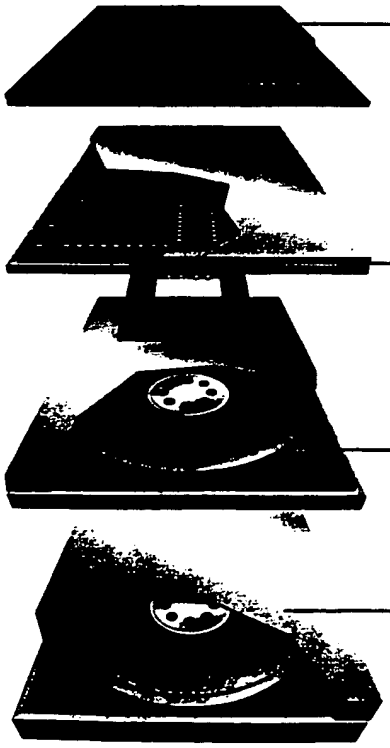
There are also two versions of the standard itself. Release 1.0, published in 1991, was for memory storage devices, such as those found on the Poqet PC and Hewlett-Packard's HP 95LX. With Release 2.0, announced in 1992, PCMCIA slots got full I/O capability, which enabled them to accept modems, fax modems, and LAN adapters. Release 2.0 also permits the cards to derive power directly from the socket and provides for an execute-in-place (XIP) layer, which permits the system to execute a file directly from the card instead of loading it into RAM first.

Meanwhile, Intel has added an extension to the PCMCIA specification, Exchangeable Card Architecture (ExCA), to ensure that PCMCIA cards are interchangeable on systems using Intel CPUs. As more card makers work with system manufacturers, incompatibilities will be ironed out. Systems that have already earned reputations for compatibility with a wide range of PCMCIA cards include the Dell 320SLi, the NCR 3170, and the Toshiba T4500. Unfortunately, we were often forced to reboot after swapping cards in order for our system to recognize the new card.

SIZING UP A PCMCIA SLOT

As PCMCIA has developed, so have the types of slots.

PCMCIA cards take up less than 2 cubic inches of notebook chassis space. The three, soon to be four, types of cards essentially describe the card's thickness. All types are backward compatible.



Type I cards, measuring 3.3mm in thickness, are used as RAM, flash memory, EEPROM, and one-time programmable memory primarily in personal digital assistants and hand-held devices.

Type II cards are 5mm high and are fully I/O capable. You can use them for modems and LAN adapters as well as for memory.

Type III cards are 10.5mm thick (almost one-half inch) and typically house miniature removable hard drives.

Type IV, not yet ratified by the PCMCIA consortium, will be 18mm high and will be used for large-capacity hard drives.

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1039

RESOURCE DIRECTORY: MODEMS

Fax support and 14,400-bps data speed in credit-card-size modems.

StarCard 1442fx Data/Fax
AMT
(714) 375-0306
Speed: 14,400 bps (data and fax)
Protocols: V.32bis, V.42bis, MNP 5
Format: Type II
Price: unavailable

StarCard 2400fx Data/Fax
AMT
(714) 375-0306
Speed: 2,400/9,600 bps (fax)
Protocols: V.22bis
Format: Type II
Price: $269

StarCard 2442fx Data/Fax
AMT
(714) 375-0306
Speed: 2,400/9,600 bps (fax)
Protocols: v.42bis, MNP 5
Format: Type II
Price: $299

StarCard 2442vx Data/Fax
AMT
(714) 375-0306
Speed: 2,400/9,600 bps (fax)
Protocols: V.22bis, V.42bis, MNP 5
Format: Type II
Price: unavailable

Angia PCMCIA
Angia Communications
(800) 877-9159, (801) 371-0488
Speed: 14,400 bps (data and fax)
Protocols: V.32bis, V.42, V.42bis, MNP 5
Format: Type II
Price: $899

KeepInTouch Card
AT&T Paradyne
(800) 482-3333, (813) 530-2000
Speed: 14.400 bps (data and fax)
Protocols: V.32, V.32bis, V.42, V.42bis, MNP 5
Format: Type II
Price: $599

CC9624FM
Centennial
(800) 535-3668, (508) 670-0646
Speed: 9,600 bps (data and fax)
Protocols: V.42, V.42bis, MNP 5
Format: Type II
Price: $300

FaxXpress 942
Complus
(510) 623-1000
Speed: 2,400/9,600, 4800 bps (fax)
Protocols: V.42bis, ExCA
Format: Type II
Price: $269

FaxXpress 1414
Complus (TDK OEM)
(510) 623-1000
Speed: 14,400 bps (data and fax)
Protocols: V.32bis, V.42bis, MNP 5
Format: Type II
Price: $499

PCMCIA—Model 2496
CP Plus (Computer Products Plus)
(800) 274-4277, (714) 847-1799
Speed: 2,400/9,600 bps (fax)
Protocols: V.42, V.42bis, MNP 5
Format: Type II
Price: $399

Business Card 2496c
Data Race
(800) 749-7223, (210) 558-1900
Speed: 2,400/9,600 bps (fax)
Protocols: V.42 bis, V.42, MNP 5, ExCA
Format: Type II
Price: $349

RediCARD v.32bis Fax Modem
Data Race
(800) 999-7223, (210) 558-1900
Speed: 14,400 bps
Protocols: V.32bis
Format: Type II
Price: $595

Credit Card 2496CFM
DataTrek
(219) 522-8000
Speed: 2,400/9,600 bps (fax)
Protocols: V.42, V.42bis, MNP 5
Format: Type II
Price: $395

C1414AX
E-Tech Research
(800) 328-5538, (408) 730-1388
Speed: 14,400 bps (data and fax)
Protocols: V.32, V.32bis, V.42bis, MNP 5
Format: Type II
Price: $499

C1414MX
E-Tech Research
(800) 328-5538, (408) 730-1388
Speed: 14,400 bps (data and fax)
Protocols: V.32, V.32bis, V.42bis, MNP 5
Format: Type II
Price: $449

C9624MX
E-Tech Research
(800) 328-5538, (408) 730-388
Speed: 2,400/9,600 bps (fax)
Protocols: V.42, V.42bis, MNP 5
Format: Type II
Price: $349

C9624RX
E-Tech Research
(800) 328-5538, (408) 730-1388
Speed: 2,400/9,600, 4,800 bps (fax)
Protocols: V.22bis
Format: Type II
Price: $299

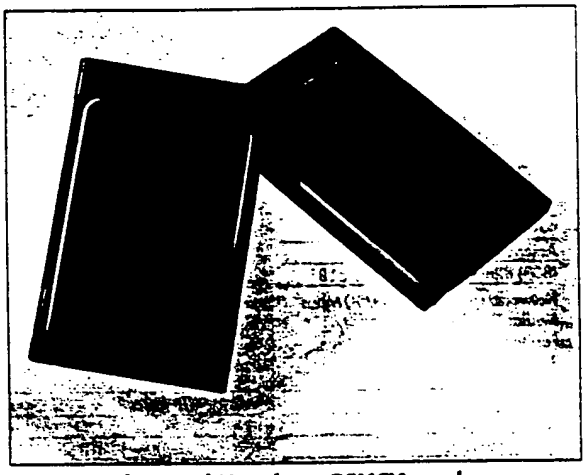
Fury Card 14.4
Dr. Neuhaus Mikroelectronik (MicroGraf)
(714) 557-8305
Speed: 14,400 bps (data and fax)
Protocols: V.32, V.32bis, V.42, V.42bis, MNP2-5
Format: Type II
Price: $489

Fury Card 2400
Dr. Neuhaus Mikroelectronik (MicroGraf)
(714) 557-8305
Speed: 2,400 bps (data and fax)
Protocols: V.42, V.42bis, MNP 5
Format: Type II
Price: $349

ThinFax 9624 Modem
EXP Computer
(516) 496-37503
Speed: 2,400/9,600 bps (fax)
Protocols: V.42, V.42bis, MNP 5
Format: Type I
Price: $369

Fax/Modem 332496
MagicRAM
(213) 413-9999
Speed: 2,400/9,600, 4,800 bps (fax)
Protocols: V.42, V.42bis, MNP 5
Format: Type II
Price: $395

PCMCIA Data/Fax 1144
Megahertz
(800) 527-8677, (801) 272-6000
Speed: 14,400 bps (data and fax)
Protocols: V.32, V.32bis, V.42, V.42bis, MNP 5
Format: Type II
Price: $599



AT&T Paradyne and Megahertz PCMCIA modems

FM144/144V (P)
GVC Technologies
(800) 289-4821, (201) 579-3630
Speed: 14,400 bps (data and fax)
Protocols: V.32, V.32 bis, V.42, V.42 bis, MNP 5
Format: Type II
Price: $499

FM9648/24 (P)
GVC Technologies
(800) 289-4821, (201) 579-3630
Speed: 2,400/9,600, 4,800 bps (fax)
Protocols: V.42, V.42bis, MNP 5
Format: Type II
Price: $269

Optima 24 Plus Fax96
Hayes Microcomputer
(404) 441-1617
Speed: 2,400/9,600 bps (fax)
Protocols: V.42, V.42bis, MNP 5
Format: Type II
Price: $399

SatisFaxtion MobileCard 96/24
Intel
(800) 628-8686
Speed: 2,400/9,600 bps (fax)
Protocols: V.22bis, V.42bis, MNP 5
Format: Type II
Price: $360

PCMCIA Data/Fax 2400/9600
Megahertz
(800) 527-8677, (801) 272-6000
Speed: 2,400/9,600 (fax)
Protocols: V.42, V.42bis, MNP 5
Format: Type II
Price: $379

PalmModem
New Media Corp.
(800) 227-3748, (714) 453-0100
Speed: 2,400/4,800 bps (fax)
Protocols V.22bis
Format: Type I
Price: $259

Info Blitz
New Media Corp.
(800) 227-3748, (714) 453-0100
Speed: 9,600/9,600 bps (fax)
Protocols: V.42, V.42bis, MNP 5, 10
Format: Type I
Price: $299

Impala 24/96 PCMCIA
Omron Office Automation Products
(800) 362-4411, (408) 727-1444
Speed: 2,400/9,600 bps (fax)
Protocols: V.42, MNP 5
Format: Type II
Price: $399

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1040

HOW PCMCIA WORKS The PCMCIA specification uses a 68-pin connector, with power and ground pins that are longer and therefore accessed first. The basic software interface, called Socket Services, uses a set of function calls that work at the same level as the system's CMOS. This gives hardware-independent access, as if the interface were the BIOS of the computer. Though the specification for Socket Services was defined to be part of the computer's BIOS, many system manufacturers implement it as a device driver. Manufacturers who take this shortcut risk making their machines incompatible with many PCMCIA cards.

The programming interface for PCMCIA, called Card Services, provides the calls to link Socket Services to the operating system and applications. Card Services can be implemented either in the operating system, as IBM did for its version of DOS 6.0, or as a driver. Each card must identify itself to the host system, providing it with relevant information about how the card functions.

A PAIR OF MODEMS By far, modems make up the widest selection of PCMCIA peripherals today. We examined two: the AT&T Paradyne KeepInTouch Card ($599) and the Megahertz PCMCIA 2.0 Data/Fax Modem with XJack ($379). Both modems provide 14,400-bps fax and data transmission speeds.

With the AT&T modem, we were able to get throughputs of 3,400 to 3,500 characters per second with plain text files in notebooks that support high port speed. This compares favorably with the high speeds you'll get from standalone or card-mounted modems on desktop systems. Much of the AT&T's outstanding performance was due to the modem's built-in 16550 UART chip. Add to this its cellular capability, and you get an exemplary PCMCIA peripheral.

RESOURCE DIRECTORY: LAN ADAPTERS

Forget notebook docking stations—tie in easily with a PCMCIA LAN card.

AMI LAN PCMCIA
American Megatrends
(800) 828-9264, (404) 263-8181
Network/speed: Ethernet/10 Mbps
Media: Thin Coax, UTP
Format: Type II
Price: $235

StarLAN Ethernet LAN Card
AMT Industries
(714) 375-0306
Network/speed: Ethernet/10 Mbps
Media: UTP Int'l
Format: Type II
Price: unavailable

ENET-MCIA TP
Compex
(714) 630-7302
Network/speed: Ethernet/10 Mbps
Media: Thin Coax, UTP
Format: Type II
Price: $319

PCMCIA Adapter DE-650C
D-Link Systems
(800) 326-1688, (714) 455-1688
Network/speed: Ethernet/10 Mbps
Media: Thin Coax
Format: Type II
Price: $375

PCMCIA Adapter DE-650T
D-Link Systems
(800) 326-1688, (714) 455-1688
Network/speed: Ethernet/10 Mbps
Media: UTP
Format: Type II
Price: $375

Ethernet NetCard
DataTrek
(219) 522-8000
Network/speed: Ethernet/10 Mbps
Media: 10Base2
Format: Type II
Price: $345

G/LapCard Adapter
Gateway Communications
(800) 367-6555, (714) 553-1555
Network/speed: Ethernet/276 Kbps
Media: 10Base T, UTP
Format: Type I
Price: $445

Token-Ring 16/4 Credit Card
IBM
(800) 426-3333, (914) 765-1900
Network/speed: Token Ring/16 Mbps
Media: UTP, STP/4
Format: Type II
Price: $595

Ethernet Credit Card Adapter
IBM
(800) 426-3333, (914) 765-1900
Network/speed: Ethernet/10 Mbps
Media: Thin Coax, UTP
Format: Type II
Price: $280

Ethernet Adapter
MagicRAM
(213) 413-9999
Network/speed: Ethernet/ n/a
Media: UTP, Thin Coax
Format: Type II
Price: UTP, $349; Thin Coax, $369

Token-Ring Adapter
MagicRAM
(213) 413-9999
Network/speed: Token-Ring/4, 16 Mbps
Media: UTP, Thin Coax
Format: Type II
Price: $775

10BaseT Ethernet LAN Card
New Media Corp.
(800) 227-3748, (714) 453-0100
Network/speed: Ethernet/600 Kbps
Media: UTP
Format: Type I
Price: $249

10Base2 Ethernet LAN Card
New Media Corp.
(800) 227-3748, (714) 453-0100
Network/speed: Ethernet/600 Kbps
Media: Thin Coax
Format: Type II
Price: $329

Socket Communications LAN card.

RangeLAN/PCMCIA
Proxim
(800) 229-1630, (415) 960-1630
Network/speed: Ethernet/242 Kbps
Media: Wireless radio
Format: Type II
Price: $595

Socket EA+
Socket Communications
(800) 552-3300, (510) 670-0300
Network/speed: Ethernet/10 Mbps
Media: Thin Coax, UTP, STP
Format: Type II
Price: $420

Socket EA
Socket Communications
(800) 552-3300, (510) 670-0300
Network/speed: Ethernet/10 Mbps
Media: UTP, STP
Format: Type II
Price: $399

TC-Card Token-Ring Adapter
Thomas-Conrad Corp.
(800) 332-8683, (512) 836-1935
Network/speed: Token Ring/4, 16 Mbps
Media: STP
Format: Type II
Price: $779

10BaseT TC-Card Ethernet
Thomas-Conrad Corp.
(800) 332-8683, (512) 836-1935
Network/speed: Ethernet/10 Mbps
Media: UTP
Format: Type II
Price: $359

10Base2 TC-Card Ethernet
Thomas-Conrad Corp.
(800) 332-8683, (512) 836-1935
Network/speed: Ethernet/10 Mbps
Media: Thin Coax
Format: Type II
Price: $375

CreditCard Ethernet CE-10B2
Xircom
(800) 438-4526, (818) 438-4526
Network/speed: Ethernet/10 Mbps
Media: Thin Coax
Format: Type I
Price: $349

CreditCard Ethernet CE-10BC
Xircom
(800) 438-4526, (818) 438-4526
Network/speed: Ethernet/10 Mbps
Media: UTP, Thin Coax
Format: Type I
Price: $399

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1041

RESOURCE DIRECTORY: HARD DRIVES

Minimarvels include mechanical hard drives as small as 3¼ by 2 inches.

Model Au63-P
Aura Associates
(408) 252-2872
Capacity: 63MB
Access times: 17ms
Format: Type III
Price: $399

Model Au126-P
Aura Associates
(408) 252-2872
Capacity: 126MB
Access times: 17ms
Format: Type III
Price: $499

Derringer CP-1044
Conner Peripherals
(800) 426-6637, (408) 456-4500
Capacity: 42MB
Access times: 19ms
Format: Type III
Price: $350

PocketFile 42
Integral Peripherals
(303) 449-8009
Capacity: 42MB
Access times: 18ms
Format: Type III
Price: $495

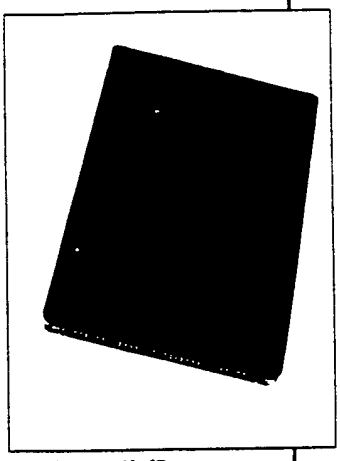
PocketFile 85
Integral Peripherals
(303) 449-8009
Capacity: 85MB
Access times: 18ms
Format: Type IV
Price: $695

MXL-105-III
Maxtor
(800) 462-9867, (408) 432-1700
Capacity: 105MB
Access times: 18ms
Format: Type III
Price: $499

MiniPort 42P
MiniStor Peripherals
(408) 943-0165
Capacity: 42MB
Access times: 16ms
Format: Type III
Price: $449

MiniPort 64P
MiniStor Peripherals
(408) 943-0165
Capacity: 64MB
Access times: 16ms
Format: Type IV
Price: $489

Caviar UltraLite CU140
Western Digital
(800) 832-4778, (714) 932-4900
Capacity: 42MB
Access times: 19ms
Format: Type III
Price: $299



MiniStor MiniPort

The Megahertz modem was unable to handle port speeds higher than 19,200 bps in any of the three notebooks in which we tested it. This may be because of problems in the Socket Services or Card Services drivers rather than in the modem itself, though the lack of the 16550 UART (and the larger buffers provided by it) may also have slowed it down.

When we transferred files archived with PKzip, we were able to get throughput of 19,200 bps on both the Megahertz and the AT&T modems. This translates to 1,600 to 1,650 cps for such files, which is similar to conventional external modem rates.

Though the Megahertz lacks built-in support for high-speed compressed transfers, it gets high marks for ergonomics. It includes a device called XJack, which is an RJ-11 connector that pops up out of the modem itself. This eliminates the need for external adapters—which on many PCMCIA modems are bulkier than the modem itself. When you're ready to disconnect, push the jack down; it locks into place like the button on a ballpoint pen.

NETWORKS AND STORAGE Notebook PCs present unique networking and storage challenges, precisely because they lack slots. In most cases, upgrading a notebook's hard drive is either impossible or prohibitively expensive. Likewise, communicating with a network via a parallel port connection is an unacceptably slow alternative. Enter PCMCIA, which allows an adapter to work at full bus speeds. We looked at the Socket EA Ethernet LAN card from Socket Communications. It combined an RJ-45 connector and a coaxial connection on a module that was somewhat larger than the card itself.

Performance was superb. In ZD Labs' NetBench test, the card's throughput was nearly three times as fast as Xircom's parallel-port Ethernet adapter. The Socket EA makes clear that the main competition for PCMCIA LAN adapters will be desktop docking stations that use traditional, full-size LAN cards.

The Socket EA connects to 10Base-T; the EA Plus can also attach to 10Base-2 Ethernet. Both products include 64K of multipacket buffer SRAM, their own PCMCIA bus logic, and configuration and diagnostic software. As LAN solutions go, they clearly point to the future.

Miniature PCMCIA hard drives are beginning to appear as well. We evaluated the MiniPort 64P from MiniStor Peripherals. This drive, self-contained on its card and without any extra modules, was somewhat slower than a non-PCMCIA hard disk in our tests. For many users, the performance penalty matters little compared to the auxiliary storage the drive offers—and the fact that it's removable.

IBM, Maxtor, and Conner have announced plans to build 1.8-inch PCMCIA hard drives that will appear in permanent mounts in subnotebooks as well. Though 40MB, 60MB, and 80MB drives should hit the streets in the near future, the greatest interest lies with 105MB drives, given the increasing demand for storage space.

For all its future potential, however, PCMCIA products are available today—despite their compatibility glitches and lofty prices. In an upcoming issue, we'll fully test PCMCIA-equipped notebooks and peripherals. If you're buying a notebook now, you'd be foolish to consider anything without PCMCIA slots. ◩

Earle J. Robinson is a Paris-based computer consultant.

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1042

24

67

Authentication and Delegation with Smart-cards

M. Abadi, M. Burrows, C. Kaufman, B. Lampson

October 22, 1990, Revised July 30, 1992

Petitioner Apple Inc. - Exhibit 1012, p. 1043

Systems Research Center

DEC's business and technology objectives require a strong research program. The Systems Research Center (SRC) and three other research laboratories are committed to filling that need.

SRC began recruiting its first research scientists in 1984—their charter, to advance the state of knowledge in all aspects of computer systems research. Our current work includes exploring high-performance personal computing, distributed computing, programming environments, system modelling techniques, specification technology, and tightly-coupled multiprocessors.

Our approach to both hardware and software research is to create and use real systems so that we can investigate their properties fully. Complex systems cannot be evaluated solely in the abstract. Based on this belief, our strategy is to demonstrate the technical and practical feasibility of our ideas by building prototypes and using them as daily tools. The experience we gain is useful in the short term in enabling us to refine our designs, and invaluable in the long term in helping us to advance the state of knowledge about those systems. Most of the major advances in information systems have come through this strategy, including time-sharing, the ArpaNet, and distributed personal computing.

SRC also performs work of a more mathematical flavor which complements our systems research. Some of this work is in established fields of theoretical computer science, such as the analysis of algorithms, computational geometry, and logics of programming. The rest of this work explores new ground motivated by problems that arise in our systems research.

DEC has a strong commitment to communicating the results and experience gained through pursuing these activities. The Company values the improved understanding that comes with exposing and testing our ideas within the research community. SRC will therefore report results in conferences, in professional journals, and in our research report series. We will seek users for our prototype systems among those with whom we have common research interests, and we will encourage collaboration with university researchers.

Robert W. Taylor, Director

Petitioner Apple Inc. - Exhibit 1012, p. 1044

Authentication and Delegation with Smart-cards

M. Abadi, M. Burrows, C. Kaufman, B. Lampson

October 22, 1990, Revised July 30, 1992

Petitioner Apple Inc. - Exhibit 1012, p. 1045

C. Kaufman works at Telecommunications and Networks, Digital Equipment Corporation, 550 King Street, Littleton, MA 01460.

©Digital Equipment Corporation 1990

This work may not be copied or reproduced in whole or in part for any commercial purpose. Permission to copy in whole or in part without payment of fee is granted for nonprofit educational and research purposes provided that all such whole or partial copies include the following: a notice that such copying is by permission of the Systems Research Center of Digital Equipment Corporation in Palo Alto, California; an acknowledgment of the authors and individual contributors to the work; and all applicable portions of the copyright notice. Copying, reproducing, or republishing for any other purpose shall require a license with payment of fee to the Systems Research Center. All rights reserved.

Petitioner Apple Inc. - Exhibit 1012, p. 1046

Authors' Abstract

The authentication of users in distributed systems poses special problems because users lack the ability to encrypt and decrypt. The same problems arise when users wish to delegate some of their authority to nodes, after mutual authentication.

In most systems today, the user is forced to trust the node he wants to use. In a more satisfactory design, the user carries a smart-card with sufficient computing power to assist him; the card provides encryption and decryption capabilities for authentication and delegation.

Authentication is relatively straightforward with a sufficiently powerful smart-card. However, for practical reasons, protocols that place few demands on smart-cards should be considered. These protocols are subtle, as they rely on fairly complex trust relations between the principals in the system (users, hosts, services). In this paper, we discuss a range of public-key smart-card protocols, and analyze their assumptions and the guarantees they offer.

Petitioner Apple Inc. - Exhibit 1012, p. 1047

Contents

1 Introduction 1

2 Notation 3

3 A protocol for ideal smart-cards 4
- 3.1 Discussion 5
- 3.2 Notation and assumptions 7
- 3.3 The protocol analyzed 10

4 A more realistic smart-card protocol 12
- 4.1 Concessions in smart-card design 13
- 4.2 Notation and assumptions 14
- 4.3 The protocol analyzed 15

5 A protocol with trusted agents 17
- 5.1 Trusted agents 17
- 5.2 Notation and assumptions 18
- 5.3 The protocol analyzed 19

6 Conclusions 20

Appendix 20

Acknowledgements 23

References 24

Petitioner Apple Inc. - Exhibit 1012, p. 1048

1 Introduction

In a secure distributed environment, there is a need for users to prove their identities to nodes, from mainframes to automatic teller machines. There is also a need, though less recognized, for nodes to prove their identities to users, as each user may trust different nodes to different extents. Furthermore, users must be able to delegate some of their authority to the nodes that they trust.

Authentication protocols serve for these purposes, typically relying on secrets and encryption (e.g., [2, 10, 11]). The authentication of users poses special problems, because users lack the ability to encrypt and decrypt.

In the simplest approach to user authentication, the user owns a secret (his password) that he gives to a node that he wishes to use. It is likely that the password will be short and memorable, or that the user will need to write it down. In either case, it may be easy for an attacker to discover the user's password and hence obtain all his rights.

This weakness can be eliminated by introducing a simple card with a small amount of read-only memory. Each user carries a card, and each card contains a different secret, which the node verifies before granting access to the user. The secret can be quite long, and hence hard to guess, but theft of the card is a significant danger.

A further improvement consists in introducing a Personal Identification Number (PIN), which the user types when he presents his card. Thus, theft of the card alone no longer suffices for a security breach. This scheme is essentially that used by most Automated Teller Machines (ATMs).

All of these approaches suffer from a serious flaw: the node must be completely trusted, as it obtains all of the user's secrets. It is impossible for a user to delegate only part of his authority, or to delegate his authority for only a limited time. Moreover, a malicious node could remember the user's secrets for future mischief. This threat seems important—consider, for example, the users of public terminals in hotels.

A smart-card with sufficient computing power solves these problems. The smart-card we envision has its own keyboard, display, clock, logic for performing public-key encryption [5, 12], and can be electrically coupled to the node.

Authentication would be relatively straightforward with this powerful smart-card. The smart-card might operate only when fed a PIN, so an attacker would need to steal the smart-card and to discover the user's PIN in order to impersonate the user. The keyboard and display allow the user to

Petitioner Apple Inc. - Exhibit 1012, p. 1049

communicate directly with the smart-card, so that the node never sees the password. Since the smart-card performs public-key encryption, no secrets ever need be revealed to the node.

After authentication, the smart-card can sign timestamped certificates to delegate part of the user's authority for a limited time. For example, the smart-card could issue a certificate that allows the node to manipulate the user's remote files for the next hour. The timestamp provides protection against replay attacks, and careful use of lifetimes can prevent mischief by the node at a later time.

Unfortunately, no one is currently selling a smart-card of the type we have described, though one may be available at some time in the future. More realistic protocols that place weaker demands on smart-cards should therefore be considered. Various compatible solutions can be implemented with reduced degrees of security and user convenience. The protocols are subtler, as they rely on more complex trust relations between the principals (users, hosts, services) in the system.

Consider, for example, a smart-card with no clock. Such a smart-card is attractive because it avoids the need for a battery. Unfortunately, the smart-card can no longer generate timestamps for its certificates, and it cannot check that other certificates have not expired. A variety of replay attacks becomes possible, unless the card can obtain the time somehow. To counter replay attacks effectively, the card may obtain the time from a network time service, which must then be secure and trusted.

In this paper, we describe a range of public-key smart-card authentication protocols, with different compromises between cost and security. The protocols were developed in the context of the Digital Distributed System Security Architecture [6]. Most previous work focuses on user authentication using shared-key cryptography, with little discussion of delegation (see, for example, [3]). We believe that public-key cryptography is more suitable than shared-key cryptography for authentication and delegation, and that it is not prohibitively expensive when used wisely. The protocols considered can be based on RSA encryption [12], but other algorithms (e.g., [7]) could also be used.

We analyze the protocols with a logic of authentication. This is essentially the logic of Burrows, Abadi, and Needham [1], with a simple extension to handle secure and timely channels. It should be noted that our logical account is not the only one possible. However, the formalism enables us to describe the assumptions and the guarantees of each protocol, clarifying the trust relations between principals. Moreover, a logical account helps in

Petitioner Apple Inc. - Exhibit 1012, p. 1050

avoiding certain security flaws commonly present in authentication protocols [1].

In the next section, we summarize the notation of the logic; the logic is discussed further in an Appendix. In later sections, we describe smart-card authentication protocols, starting with those that require the more ambitious smart-card designs and the weaker trust relations. We analyze three cases in some detail; the reader can interpolate between these. The informal descriptions (without the logic) are self-contained, and the formal passages may be skipped in a first reading.

2 Notation

In the analysis of smart-card protocols, we apply a logic for describing the beliefs of the principals in the course of authentication. Several sorts of objects appear in the logic: principals, encryption keys, formulas, and communication links. (The original logic does not discuss links.) In what follows, the symbols P, Q, and R range over principals; X and Y range over formulas; K ranges over encryption keys; L ranges over communication links. The constructs that we use are listed below.

P **believes** X

P **controls** X: P has *jurisdiction* over X. The principal P is an authority on X and should be trusted on this matter. For example, a certification authority may be trusted to provide the public keys of principals.

P **said** X: P *once said* X. The principal P sent a message including X, either long ago or during the current run of the protocol. In any case, P believed X when he sent the message.

P **said**$_L$ X: P *once said* X on the communication link L.

P **sees** X: P *sees* X. A message containing X has been sent to P, who can read and repeat X (possibly after doing some decryption).

P **sees**$_L$ X: P *sees* X on the communication link L.

fresh(X): X is *fresh*, that is, X has not been sent in a message at any time before the current run of the protocol. This usually holds for timestamps and for *nonces*—expressions invented for the purpose of being fresh.

Petitioner Apple Inc. - Exhibit 1012, p. 1051

timely(L): The link L is a *timely channel*: all messages on link L are known to have been sent recently.

$\overset{K}{\rightarrowtail} P$: P has K as a *public key*. The matching *secret key* (the inverse of K, denoted K^{-1}) will never be discovered by any principal except P, or a principal trusted by P.

$\overset{L}{\prec} P$: The link L is a *secure channel* from P: all messages on link L are known to have been sent by P, or a principal trusted by P.

$P \overset{X}{=\!=} Q$: X is a *secret* that will never be known to anyone but P and Q, and possibly to principals trusted by them. Only P and Q may use X to prove their identities to one another. An example of a shared secret is a password or a PIN.

$\{X\}_K$: This represents the formula X encrypted under the key K.

$\langle X \rangle_Y$: This represents X combined with the formula Y; it is intended that Y be a secret, and that its presence prove the identity of whoever utters $\langle X \rangle_Y$. In implementations, X may simply be concatenated with Y; our notation highlights that Y plays a special rôle, as proof of origin for X.

3 A protocol for ideal smart-cards

We start with a description of how user authentication would work given the ultimate smart-card, with its own keyboard, display, clock, and logic for performing public-key encryption. Other schemes are best thought of in terms of their differences from this scheme.

We assume that a distributed name service is available. The name service contains *certificates* with information about which nodes each user should trust and which public keys belong to which agents. A certificate is a statement that has been signed by a principal. Often, certificates are signed by a widely trusted service, known as a *certification authority*. A certificate typically includes a timestamp, with its time of issue, and sometimes an explicit lifetime, which limits its validity. The certification authority need not be on-line; the name service need not be trusted.

We also assume that principals know the time accurately enough to check the validity of certificates and to detect the replay of timestamped messages. A trusted time service is one way of achieving this.

Petitioner Apple Inc. - Exhibit 1012, p. 1052

We first describe the protocol informally, and then more formally.

3.1 Discussion

For the sake of concreteness, let us imagine that a user wants to prove his identity to a workstation. Moreover, the user wishes to allow the workstation to access files on his behalf.

1. The user sits down at the workstation and presents his smart-card. The smart-card is willing to give certain information, including the name of the user, to anyone.

2. The workstation now authenticates itself to the smart-card. Given the name of the user, the workstation can retrieve all the certificates the smart-card needs to determine that it is allowed to delegate authority to the workstation; it forwards these to the smart-card. The workstation also generates a new public key and a matching secret key; we refer to these keys as *delegation keys*. It sends the public key and a timestamp to the smart-card, signed with its own secret key.

3. The smart-card examines the information presented by the workstation, verifying the signatures and lifetimes on all of the certificates. At this point, the smart-card knows the public key of the workstation and that the workstation can be trusted to act on behalf of the user. The smart-card shows that it is satisfied on its display and requests the user's PIN. In addition, it might give the identity of the workstation, or at least an indication, such as a group nickname. It might also provide some means to identify the workstation's display, such as a name or location.

4. Now the user has some evidence of the workstation's identity. The user responds by entering a PIN into the keyboard of the smart-card, thus authorizing the use of this workstation.

5. The entry of the correct PIN indicates that the genuine user is present, rather than some smart-card thief. Hence, the card constructs and signs a *delegation certificate*. This delegation certificate authorizes anyone who can demonstrate knowledge of the secret delegation key to act on behalf of the user for a limited period of time. It sends that certificate to the workstation.

Petitioner Apple Inc. - Exhibit 1012, p. 1053

6. The workstation verifies that the delegation certificate is signed with the card's secret key and contains the public delegation key. At this point, the workstation has authenticated the user, in the sense that it knows that whoever is at the keyboard has a particular public key. The workstation has enough information to consult an access control list and to determine whether it should provide its services to this user. Moreover, the delegation certificate enables the workstation to convince another node, such as a file server, that the workstation acts on behalf of the user.

This completes the authentication process. The workstation now knows the user's identity. It can prove that it acts on the user's behalf by presenting the delegation certificate and proving that it knows the secret delegation key. The user also knows something about the workstation—perhaps its name, but at least that the workstation can be trusted, according to the certification authority.

For authentication, it does not suffice for the user and the workstation to know each other's names. They must also know that they are communicating via a particular keyboard and a particular display, and for example that no malicious principal is interposed between the user and the workstation. An implementation of this protocol should provide this guarantee.

An important variation on this scheme has to do with rôles. A user may need and want different privileges when he acts as member of a research group and as manager, for example. A user may also want different privileges depending on his trust of the systems that act on his behalf. Software and hardware trusted in one rôle should be prevented from gaining privileges reserved for another rôle. One way of providing this capability is to issue multiple smart-cards to the user, one for each rôle. A more satisfactory solution is to have a single smart-card support multiple rôles. By typing at the card's keyboard, the user could select a rôle, to be mentioned in the delegation certificate. In addition, the smart-card could restrict the rôles available, to save the user from misplaced trust in unsafe environments.

For the purposes of a logical analysis, it would be adequate to conceive of the user in each of his rôles as a different user. For simplicity, we do not discuss rôles further in this paper.

3.2 Notation and assumptions

The notation used in the remainder of this section is as follows:

Petitioner Apple Inc. - Exhibit 1012, p. 1054

- S is the certification authority, W the workstation, C the smart-card, U the user, and F a file server (or any other node) that the workstation contacts on behalf of the user;
- K_s, K_w, and K_c are the public keys of S, W, and C, respectively;
- K_d is the public delegation key, generated by W;
- PIN is U's personal identification number;
- T_w, T_c, T_s, T_s', and T_s'' are timestamps;
- I_c is the smart-card's keyboard (input to the card);
- O_c is the smart-card's display (output from the card);
- I_w is the workstation's keyboard (input to the workstation); and
- O_w is the workstation's display (output from the workstation).

The name C is useful only in connecting U with K_c, and need not be present in an implementation. Similarly, the names for I_w and O_w will quite likely be related to one another, and to W. For example, if I_w and O_w are referred to by location, then the names could be identical.

In order to analyze the protocol with the logic, we have to state its assumptions and describe it more formally. We leave the description of the protocol to the next subsection, and now proceed to discuss its assumptions. The assumptions naturally fall into several classes:

Assumptions about timestamps: the smart-card, the workstation, and the file server believe that certain timestamps were generated recently:

1. C **believes fresh**(T_s), C **believes fresh**(T_s'), C **believes fresh**(T_w);
2. W **believes fresh**(T_c), W **believes fresh**(T_s'');
3. F **believes fresh**(T_c), F **believes fresh**(T_s'').

Assumptions about keys and secrets:

1. S **believes** $\overset{K_c}{\mapsto} C$, S **believes** $\overset{K_w}{\mapsto} W$: the certification authority believes the smart-card's public key is K_c, and the workstation's public key is K_w;

Petitioner Apple Inc. - Exhibit 1012, p. 1055

2. C **believes** $\overset{K_s}{\mapsto} S$: the smart-card believes the certification authority's public key is K_s;

3. C **believes** $C \overset{PIN}{=} U$: the smart-card believes that PIN is a secret shared with the user;

4. W **believes** $\overset{K_s}{\mapsto} S$: the workstation believes the certification authority's public key is K_s;

5. W **believes** $\overset{K_d}{\mapsto} U$: the workstation believes that K_d is a good key for U (probably because W has constructed the key);

6. F **believes** $\overset{K_s}{\mapsto} S$: the file server believes the certification authority's public key is K_s.

Assumptions about channels:

1. W **believes** $\overset{O_w}{\prec} W$: the workstation believes that the display is a secure channel from it;

2. U **believes** $\overset{O_c}{\prec} C$, U **believes timely**(O_c): the user believes that the smart-card's display is a secure and timely channel from the smart-card;

3. U **believes** $\overset{I_w}{\prec} U$: the user believes that the workstation's keyboard is a secure channel from him;

4. C **believes timely**(I_c): the smart-card believes that its keypad is a timely channel.

Assumptions about trust:

1. U **believes** $\forall K.(W$ **controls** $\overset{K}{\mapsto} U)$: the user believes that the workstation can choose an appropriate public key; intuitively, the user is willing to delegate to this workstation;

2. S **believes** U **controls** $\forall K.(W$ **controls** $\overset{K}{\mapsto} U)$: the certification authority trusts the user to decide whether to trust this workstation in the choice of a key; intuitively, W is believed to be a safe workstation for the user to delegate to;

Petitioner Apple Inc. - Exhibit 1012, p. 1056

3. S **believes** $\forall X.(C$ **controls** U **believes** $X)$: the certification authority trusts the smart-card to relay the user's beliefs;

4. S **believes** $\forall K.(C$ **controls** $\overset{K}{\mapsto} U)$: the certification authority trusts the smart-card to set a key for the user;

5. U **believes** W **controls** $\overset{O_w}{\prec} W$: the user trusts the workstation when it says that the display O_w is a channel from it;

6. U **believes** $\forall W.(C$ **controls** W **believes** $\overset{O_w}{\prec} W)$: the user trusts his card to pass on beliefs of the workstation;

7. W **believes** U **controls** $\overset{I_w}{\prec} U$: the workstation trusts the user when he claims to be at the keyboard.

In addition, there are a few assumptions about trust in the server; for the sake of brevity, we assume that every principal trusts the server completely.

Some of the assumptions are rather strong, and could be weakened. In particular, the assumption

$$W \textbf{ believes } U \textbf{ controls } \overset{I_w}{\prec} U$$

is a simplification of the more accurate "the workstation trusts whoever claims to be at its keyboard to identify himself properly *through the smart-card*." Our simple logic is unable to express this satisfactorily in a single formula.

3.3 The protocol analyzed

Now we discuss the protocol in detail, and show that it establishes channels (the keyboard and the display) between the user and the workstation, and that it provides a delegation key that the workstation can use on behalf of the user in dealing with other nodes:

$$U \textbf{ believes } \overset{O_w}{\prec} W, \qquad W \textbf{ believes } \overset{I_w}{\prec} U, \qquad F \textbf{ believes } \overset{K_d}{\mapsto} U$$

Step by step, we can follow the evolution of the beliefs of the participants, from the initial assumptions to these conclusions. We summarize the major deductions, and at the same time we explain the messages in the protocol.

Petitioner Apple Inc. - Exhibit 1012, p. 1057

The reasoning deals with an idealized version of the protocol, in which messages are replaced by formulas of the logic. These formulas should be believed by the principals that send them. An implementation of the protocol need not transmit these formulas literally; any unambiguous bit representation will do, and one is typically obvious from the context.

The transmission of certificates is represented explicitly. We do not show the exact routes these follow, however, as the routes do not affect the properties of the protocol—they are merely an implementation choice. In practice, one would expect certificates to be cached, so that they do not need to be transmitted or checked repeatedly.

1. $W \rightarrow C$: $\{\overset{K_d}{\mapsto} U,\ \overset{O_w}{\prec} W, T_w\}_{K_w^{-1}}$
   The workstation asserts that it has a public key K_d for the user and that the display O_w is a secure channel from W.

2. $S \rightarrow C$: $\{\overset{K_w}{\mapsto} W, T_s\}_{K_s^{-1}}$,
   $\{U$ **controls** $\forall K.(W$ **controls** $\overset{K}{\mapsto} U), T_s'\}_{K_s^{-1}}$
   The certification authority provides the public key of the workstation to the smart-card. At this point, the smart-card can decrypt and attribute the previous message, as well as check the freshness of the timestamp T_w. The certification authority also states that the user can let this workstation choose a delegation key. The smart-card trusts the certification authority; in the logic, we obtain:

   $$C \textbf{ believes } \overset{K_w}{\mapsto} W, \quad C \textbf{ believes } U \textbf{ controls } \forall K.(W \textbf{ controls } \overset{K}{\mapsto} U)$$

   and then also

   $$C \textbf{ believes } W \textbf{ believes } \overset{O_w}{\prec} W$$

3. $C \rightarrow U$: W **believes** $\overset{O_w}{\prec} W$ *on* O_c
   On its display, the card provides the name of the workstation to the user; the card also gives enough information for the user to check whether the display in front of him is W's. More precisely, the smart-card states that W believes that O_w is its display (formally, that O_w is a secure channel from W). Since the user trusts the smart-card on this matter and it knows that the smart-card's display is both secure and timely, it believes the card's assertion. We can now derive:

   $$U \textbf{ believes } \overset{O_w}{\prec} W$$

Petitioner Apple Inc. - Exhibit 1012, p. 1058

because the user trusts W on $\overset{O_w}{\preceq} W$. Thus, the workstation has authenticated itself to the user.

4. $U - C$: $\langle \forall K.(W \textbf{ controls } \overset{K}{\mapsto} U),\ \overset{I_w}{\preceq} U \rangle_{PIN}$ *on* I_c
   If the user wishes to proceed, he enters his PIN on the card's keypad. Thus, the user indicates that he trusts the workstation to choose a key and that he is at the keyboard I_w. He uses his personal identification number to convince the smart-card of his identity. We can prove:

   $$C \textbf{ believes } \forall K.(W \textbf{ controls } \overset{K}{\mapsto} U),\quad C \textbf{ believes } U \textbf{ believes } \overset{I_w}{\preceq} U$$

   Using S's certificates and W's claims, we can also obtain:

   $$C \textbf{ believes } \overset{K_d}{\mapsto} U$$

5. $C - W$: $\{U \textbf{ believes } \overset{I_w}{\preceq} U, T_c\}_{K_c^{-1}}$
   The smart-card communicates to the workstation that the user believes he is at the keyboard. In an implementation where U and I_w are clear from context, it suffices for C to send a signed message to W, such as the delegation certificate below.

6. $S - W$: $\{\overset{K_c}{\mapsto} C, \forall X.(C \textbf{ controls } U \textbf{ believes } X), T_s''\}_{K_s^{-1}}$
   The certification authority gives the smart-card's public key to the workstation, and connects this key to U. At this point, the workstation can decrypt the previous message and check its timestamp. With a few applications of the logical postulates, we prove:

   $$W \textbf{ believes } \overset{I_w}{\preceq} U$$

   This statement means that the workstation believes that the user is at its keyboard, and hence that the user has authenticated himself to the workstation.

7. $C - F$: $\{\overset{K_d}{\mapsto} U, T_c\}_{K_c^{-1}}$
   The smart-card certifies that K_d is a delegation key for the user.

8. $S - F$: $\{\overset{K_c}{\mapsto} C, \forall K.(C \textbf{ controls } \overset{K}{\mapsto} U), T_s''\}_{K_s^{-1}}$
   The certification authority gives the smart-card's key to the file server. At this point, the file server can decrypt the certificate from the smart-card and check the timestamp in it. Furthermore, the certification

Petitioner Apple Inc. - Exhibit 1012, p. 1059

authority asserts that the card can set a key for the user, and the file server trusts the certification authority in this matter as well. Hence, we obtain:

$$F \textbf{ believes } \overset{K_d}{\mapsto} U$$

Informally, the file server has accepted the delegation key generated by the workstation, and thus the workstation can act on the user's behalf.

After this message sequence, the file server F has not heard about W. All the responsibility for checking the suitability of W rests on the user and the smart-card. This is not entirely unreasonable, as we are assuming a powerful smart-card. In the next section, we describe protocols where F participates in this checking.

4 A more realistic smart-card protocol

The smart-card design required for the protocol of the previous section is rather ambitious with today's technology. In this section, we consider a protocol that requires much less from the smart-card. Another one appears in the next section.

4.1 Concessions in smart-card design

The first feature to eliminate is the clock on the card. Having a clock on the card is particularly difficult because it requires a battery. The clock could be eliminated by having the user enter the time; it is equivalent, but much more practical, to have the workstation supply the time to the card and the user verify it on the display. This solution is not as convenient or as secure (the user will probably not check very carefully), but it works. There are two threats if the smart-card has an incorrect notion of time. First, the card could be tricked into signing a delegation certificate for some time far in the future and the workstation could then impersonate the user without the smart-card being physically present. Second, a workstation whose certificate has expired at some time in the past could convince the smart-card the certificate is still valid.

Another feature we could eliminate is the keyboard on the card. It may be quite difficult to make a small, mechanically strong keyboard that can be reached even when the card has been connected to a reader. The user could instead enter his PIN on the workstation's keyboard, which could forward

Petitioner Apple Inc. - Exhibit 1012, p. 1060

the PIN in a message to the card. The danger here, though not a particularly worrisome one, is that a misbehaving workstation could capture the PIN. The workstation could give the PIN to someone who subsequently steals the card, or the workstation could use the PIN more than once on a single insertion of the card to obtain the delegation of more rôles than the user intended. These threats can be avoided entirely by having the card display a nonce secret and having the user "modify" it into the PIN with a series of '+' and 'nextdigit' operations sent via the workstation keyboard. We can view this nonce secret as an encryption key (or a one-time pad) that the card supplies to the user to establish a secure channel that the workstation cannot read or write. In this way, PIN entry goes through the keyboard but is not subject to replay.

A similar concession is to remove the display from the card, instead of the keyboard. In this case, it is straightforward for the user to enter the PIN, but it is much harder for the smart-card to identify the workstation to the user. A single LED is a partial substitute for a display.

A final compromise consists in limiting the smart-card's ability to encrypt and decrypt. We consider the extreme case where the smart-card signs one message but is not able to decrypt. In this case, it is desirable to provide a secure channel from the workstation (such as a secure card reader).

In the remainder of this section, we study a protocol where the smart-card has a display, but has neither a clock nor a keyboard, and has reduced encryption capabilities. (We leave to the reader the derivation and analysis of variants.)

These concessions in smart-card design may leave the user at the mercy of the workstation. It is therefore desirable to transfer some trust from the workstation to other principals in the distributed environment.

The simplest choice is to give a more prominent rôle to the principals that check delegation certificates, such as the file server F. Thus, F takes into account W's identity before accepting a delegation key for U. Moreover, F may grant some requests from W on behalf of U, and not others (as in the general approach to delegation of [8]). The user obtains no real guarantee of the identity of the workstation, since the card cannot decrypt. However, the user can be sure that his authority is not delegated inappropriately, because of the check performed by F. This is the approach we adopt in the following protocol.

In the next section, we discuss a more elaborate design, where dedicated *trusted agents* assist the smart-card in the process of delegation.

Petitioner Apple Inc. - Exhibit 1012, p. 1061

4.2 Notation and assumptions

Some additional notation is needed:

- K_{cu} is a short secret nonce generated by the card, to protect the entry of the user's PIN—as the notation suggests, we view the secret as an encryption key for the PIN;
- L_r is the smart-card reader; and
- $\{T_b\}_{K_b^{-1}}$ is a timestamp signed by B, a trusted time service; B is trusted never to sign a timestamp for a time in the future; W obtains the certified timestamp by whatever means, and may check T_b.

The following are the main novelties in the initial assumptions; we omit a full list. In these, it is convenient to use the name W' for the workstation that controls the channel L_r (with any luck, of course, W' is the intended W). We need this notation because the user must reason about the workstation behind L_r before believing it is W.

1. C **believes** $\overset{L_r}{\prec} W'$, C **believes timely**(L_r): the smart-card believes that the smart-card reader provides a timely, secure channel to the workstation W';
2. C **believes** $C \overset{K_{cu}}{\rightleftharpoons} U$, C **believes fresh**$(C \overset{K_{cu}}{\rightleftharpoons} U)$: the smart-card has a secret, to be used to hide the PIN from the workstation; this secret is a nonce, and hence its mention in a message proves the freshness of this message.
3. U **believes** W' **controls** $\overset{O_w}{\prec} W$: the user trusts the workstation behind the smart-card reader to give its name correctly, asserting that the display is a secure channel from W—the user may reject outrageous names, though: this assumption is strong, since the user gets no real guarantee of the workstation's identity;
4. F **believes fresh**$(\{T_b\}_{K_b^{-1}})$: the file server believes in the timeliness of the certified timestamp; B's signature convinces F of the validity of T_b, even though C does not have a clock, because B is trusted not to sign future timestamps.

Petitioner Apple Inc. - Exhibit 1012, p. 1062

4.3 The protocol analyzed

The protocol presented here achieves the same properties as the one for ultimate smart-cards, namely,

$$U \textbf{ believes } \overset{O_w}{\prec} W, \qquad W \textbf{ believes } \overset{I_w}{\prec} U, \qquad F \textbf{ believes } \overset{K_d}{\leftharpoondown} U$$

This amounts to mutual authentication and delegation. However, stronger assumptions are required here, particularly for the first conclusion.

The messages and the deductions can be explained thus:

1. $W - C$: $\overset{O_w}{\prec} W \quad on\ L_r$
   The workstation names itself and its display.

2. $C - U$: W' **believes** $\overset{O_w}{\prec} W, C \overset{K_{cu}}{\leftharpoondown} U \quad on\ O_c$
   The card passes the workstation's message on to the user. It also provides a one-time pad K_{cu}. Notice that the user has no assurance that the named workstation is actually the workstation in front of him. However, he can be sure that he is delegating authority only to the machine named. The user simply trusts the workstation to give its name correctly. Thus, we have:

   $$U \textbf{ believes } \overset{O_w}{\prec} W$$

3. $U \rightarrow C$: $\{\overset{I_w}{\prec} U, \forall K.(W \textbf{ controls } \overset{K}{\leftharpoondown} U), C \overset{K_{cu}}{\leftharpoondown} U\}_{K_{cu}}$
   The user enters his PIN. The PIN is not entered directly; instead, the user types a sequence of keys which modify the displayed value K_{cu} until the PIN is displayed. Thus, the user asserts that he is at the keyboard, and gives jurisdiction to the workstation over the choice of a key. The key K_{cu} appears inside the message as proof of timeliness. (In an implementation, the use of K_{cu} as a one-time pad suffices as proof of timeliness.)

4. $C \rightarrow W$: $\{U \textbf{ believes } \overset{I_w}{\prec} U, \{T_b\}_{K_b^{-1}}\}_{K_c^{-1}}$
   As in the previous protocol, the smart-card communicates to the workstation that the user believes he is at the keyboard. The certified timestamp, which may have been obtained via W, is included as proof of timeliness.

Petitioner Apple Inc. - Exhibit 1012, p. 1063

5. $S - W$: $\{\overset{K_c}{\mapsto} C, \forall X.(C \textbf{ controls } U \textbf{ believes } X), T_s''\}_{K_s^{-1}}$
   The certification authority provides the smart-card's public key to the workstation and certifies that the smart-card is allowed to transmit the user's beliefs. At this point the workstation can interpret the previous message. As in the previous protocol, the user has authenticated to the workstation:
   $$W \textbf{ believes } \overset{I_w}{\prec} U$$

6. $C - F$: $\{U \textbf{ believes } W \textbf{ controls } \overset{K_d}{\mapsto} U, \{T_b\}_{K_b^{-1}}\}_{K_c^{-1}}$
   In this delegation certificate, the smart-card asserts that the user has delegated to the workstation: it says that the user believes that the workstation has jurisdiction over setting K_d as his delegation key. The certificate includes $\{T_b\}_{K_b^{-1}}$ as proof of timeliness.

7. $W - F$: $\{\overset{K_d}{\mapsto} U, \{T_b\}_{K_b^{-1}}\}_{K_w^{-1}}$
   The workstation asserts that K_d is a delegation key for U.

8. $S - F$: $\{\overset{K_w}{\mapsto} W, T_s\}_{K_s^{-1}}$,
   $\{\forall K.(U \textbf{ controls } W \textbf{ controls } \overset{K}{\mapsto} U), T_s'\}_{K_s^{-1}}$,
   $\{\overset{K_c}{\mapsto} C, \forall X.(C \textbf{ controls } U \textbf{ believes } X), T_s''\}_{K_s^{-1}}$
   The certification authority provides the public keys of the smart-card and the workstation. It certifies that the user can delegate to this workstation, and that the smart-card is allowed to transmit the user's beliefs. Using the previous messages, we obtain the desired delegation result:
   $$F \textbf{ believes } \overset{K_d}{\mapsto} U$$

It is not strictly necessary to include the key K_d in the delegation certificate, as we have. However, the mention of the key makes it simple for the workstation to renounce delegated powers when they are no longer needed, by forgetting the matching secret key K_d^{-1}. Thus, the user is protected against future compromise of the workstation, even if the delegation certificate has a long lifetime.

As usual, the number of messages can be reduced by caching commonly used certificates. Furthermore, the smart-card need perform only one signing operation, and this can be done while the user enters his PIN. Hence the card need not be particularly fast. The total complexity of the protocol has increased slightly, but the demands on the smart-card have decreased. This protocol, or similar ones, may well be practical.

Petitioner Apple Inc. - Exhibit 1012, p. 1064

5 A protocol with trusted agents

An alternative approach to reducing the demands on the smart-card is based on the use of trusted agents. We discuss this solution here.

5.1 Trusted agents

An on-line trusted agent can relieve the smart-card from the elaborate rituals of generating timestamps and verifying certificates. As this trusted agent can check that W is a suitable workstation for U, this burden is removed from principals such as F. Moreover, a trusted agent simplifies the process of revocation for a compromised workstation—a trusted agent may be a convenient place for a workstation black list. The workstation and the trusted agents can check on one another.

As we envision them, these trusted agents are dedicated, physically protected machines. There would be a large number of trusted agents widely dispersed. Each trusted agent assists a community of users under a single domain or management. Any such arrangement reduces availability (when all replicas are down or inaccessible, the user cannot work) and lessens security (the agents are an attractive target).

If the smart-card can execute only the DES algorithm [4], then the trusted agent will get access to the user's private key during the login process. It can still be arranged that compromise of a trusted agent will not permit the impersonation of all users who trust it—only of those who use it while it is compromised.

If the smart-card can perform the RSA signing operation, a protocol can be obtained whereby the trusted agent cannot impersonate the user. The compromise of a trusted agent does not destroy security per se. In the solution explored in the rest of this section, the smart-card will sign anything the workstation gives it, but no one will believe anything signed by the smart-card without a certificate from a suitable trusted agent. As in the previous protocol, the user obtains no real guarantee of the identity of the workstation, since the card cannot decrypt. However, the user can be sure that his authority is not delegated inappropriately, because of the check performed by the trusted agent.

5.2 Notation and assumptions

Let A be a trusted agent, K_a his public key, and T_a a timestamp he generates.

Petitioner Apple Inc. - Exhibit 1012, p. 1065

The most important new assumptions are:

1. S **believes** $\forall K \forall W.(A$ **controls** W **believes** $\overset{K}{\mapsto} U)$.
   S **believes** $\forall K \forall W.(A$ **controls** U **controls** W **controls** $\overset{K}{\mapsto} U)$: the certification authority believes that the user is in the domain of the trusted agent A; the formulas represent consequences of this belief.

2. A **believes** $\forall K.(U$ **controls** W **controls** $\overset{K}{\mapsto} U)$: the trusted agent A believes that U can delegate to W.

We treat A as different from B, the trusted time provider, although A and B could obviously be implemented by a single node.

5.3 The protocol analyzed

Many of the messages are identical to those of the previous protocol. We discuss only the changes.

1. $W \rightarrow A$: $\{\overset{K_d}{\mapsto} U, T_w\}_{K_w^{-1}}$
   The workstation asserts that K_d is a delegation key for U.

2. $S \rightarrow A$: $\{\overset{K_w}{\mapsto} W, T_s\}_{K_s^{-1}}$
   The trusted agent consults a certificate that contains W's key.

3. $W \rightarrow C$: $\overset{O_w}{\prec} W$ *on* L_r

4. $C \rightarrow U$: W' **believes** $\overset{O_w}{\prec} W, C \overset{K_{cu}}{\mapsto} U$ *on* O_c

5. $U \rightarrow C$: $\{\overset{I_w}{\prec} U, \forall K.(W$ **controls** $\overset{K}{\mapsto} U), C \overset{K_{cu}}{\mapsto} U\}_{K_{cu}}$

6. $C \rightarrow W$: $\{U$ **believes** $\overset{I_w}{\prec} U, \{T_b\}_{K_b^{-1}}\}_{K_c^{-1}}$

7. $A \rightarrow F$: $\{W$ **believes** $\overset{K_d}{\mapsto} U, U$ **controls** W **controls** $\overset{K_d}{\mapsto} U, T_a\}_{K_a^{-1}}$
   The trusted agent checks that the workstation is a reasonable machine for the user to trust. It signs a certificate to that effect, including the delegation key for the subsequent session. The trusted agent states that W has chosen K_d, and that U can let W use K_d as a delegation key.

Petitioner Apple Inc. - Exhibit 1012, p. 1066

8. $C \rightarrow F$: $\{U$ **believes** W **controls** $\stackrel{K_d}{\mapsto} U, \{T_b\}_{K_b^{-1}}\}_{K_c^{-1}}$
   The file server checks that values of U and W match those in the previous message. This check ensures that both the user and the trusted agent refer to the same workstation.

9. $S \rightarrow F$: $\{\stackrel{K_a}{\mapsto} A, T_s'\}_{K_s^{-1}}$
   $\{\forall K \forall W.(A$ **controls** W **believes** $\stackrel{K}{\mapsto} U)$,
   $\forall K \forall W.(A$ **controls** U **controls** W **controls** $\stackrel{K}{\mapsto} U), T_s''\}_{K_s^{-1}}$
   $\{\stackrel{K_c}{\mapsto} C, \forall X.(C$ **controls** U **believes** $X), T_s'''\}_{K_s^{-1}}$
   The file server obtains certificates for A and C.

The result is the usual one: mutual authentication and delegation.

6 Conclusions

Authentication protocols that use smart-cards are a significant improvement over those that use simple passwords. We have described a few smart-card protocols and the guarantees they offer. We feel that the use of a formalism has helped us elucidate and compare some of the subtle trust relations that underly these protocols.

A trade-off is inevitable, between the trust that the user needs to place in the environment, and the power, cost, and size of his smart-card. Each of the protocols—and there are others—has its own problems and addresses specific threats, with specific technological requirements.

Appendix: The logic

In the analysis of smart-card protocols, we apply a logic of authentication. The notation is as given in Section 2; here we give a few of the main rules of inference and briefly explain how to use them. The logic is presented in [1]; a Kripke semantics is currently being developed by M. Tuttle and M. Abadi.

Rules of inference

We manipulate formulas of the logic with rules of inference, such as the following.

Petitioner Apple Inc. - Exhibit 1012, p. 1067

- The jurisdiction rule reflects that if P believes that Q is an authority on X then P trusts Q on the truth of X:

$$\frac{P \textbf{ believes } Q \textbf{ controls } X, \quad P \textbf{ believes } Q \textbf{ believes } X}{P \textbf{ believes } X}$$

- The public-key message-meaning rule concerns the interpretation of encrypted messages:

$$\frac{P \textbf{ believes } \overset{K}{\mapsto} Q, \quad P \textbf{ sees } \{X\}_{K^{-1}}}{P \textbf{ believes } Q \textbf{ said } X}$$

That is, if P believes that the key K is Q's public key and P sees X encrypted under K's inverse, then P believes that Q once said X.

- A similar message-meaning rule applies to links:

$$\frac{P \textbf{ believes } \overset{L}{\prec} Q, \quad P \textbf{ sees}_L X}{P \textbf{ believes } Q \textbf{ said}_L X}$$

- A nonce-verification rule expresses the check that a part of a message is recent, and hence that the sender still believes in the message:

$$\frac{P \textbf{ believes fresh}(X), \quad P \textbf{ believes } Q \textbf{ said } X}{P \textbf{ believes } Q \textbf{ believes } X}$$

That is, if P believes that X could have been uttered only recently and that Q once said X, then P believes that Q has said X recently, and hence that Q believes X. A variant of this rule is sometimes useful:

$$\frac{P \textbf{ believes fresh}(Y), \quad P \textbf{ believes } Q \textbf{ said } (X, Y)}{P \textbf{ believes } Q \textbf{ believes } X}$$

For the sake of simplicity, we use this rule only when X is cleartext, that is, it has no subformulas of the form $\{Y\}_K$. A similar remark applies to all other rules that introduce the **believes** operator.

- Another way to guarantee timeliness is by using timely communication links:

$$\frac{P \textbf{ believes timely}(L), \quad P \textbf{ believes } Q \textbf{ said}_L X}{P \textbf{ believes } Q \textbf{ believes } X}$$

Petitioner Apple Inc. - Exhibit 1012, p. 1068

On quantifiers in delegations

Delegation statements usually mention one or more variables. For example, the user U may let the workstation W generate an arbitrary delegation key. We can express this as

$$U \textbf{ believes } W \textbf{ controls } \stackrel{K}{\rightharpoonup} U$$

Here the key K is universally quantified, and we can make explicit this quantification by writing

$$U \textbf{ believes } \forall K.(W \textbf{ controls } \stackrel{K}{\rightharpoonup} U)$$

For complex delegation statements, it is generally necessary to write quantifiers explicitly in order to avoid ambiguities. In some previous works on the logic, this need was not recognized, as in fact it did not arise. (There were no nested jurisdiction statements.) This need does arise in the proofs above.

Our formal manipulation of quantifiers is quite straightforward. All we use is the ability to instantiate variables in jurisdiction statements, as reflected by the rule

$$\frac{P \textbf{ believes } \forall V_1 \ldots V_n.(Q \textbf{ controls } X)}{P \textbf{ believes } Q' \textbf{ controls } X'}$$

where Q' **controls** X' is the result of simultaneously instantiating all of the variables $V_1, \ldots, V_n$ in Q **controls** X.

Protocol analysis

Authentication protocols are typically described by listing their messages in the form

$$P \rightarrow Q : \mathit{message}$$

This denotes that P sends the message to Q. Occasionally, it is stated that the message follows a particular route, such as a secure channel.

The message is presented in an informal notation designed to suggest the bit-string that a particular concrete implementation would use. In the interest of formal analysis, we rewrite each message as a logical formula. For instance, the protocol step

$$A \rightarrow F : K_a \textit{ on link } L_1$$

Petitioner Apple Inc. - Exhibit 1012, p. 1069

may tell F, who knows that L_1 is a secure channel from A, that K_a is A's public key. This step should then be idealized as

$$A \rightarrow F : \stackrel{K_a}{\mapsto} A \quad on\ L_1$$

We annotate idealized protocols with logical formulas, much as in a proof in Hoare logic ([H]). We write formulas before the first message and after each message. The main rules for deriving legal annotations are:

- if X holds before the message $P \rightarrow Q : Y$ then both X and Q **sees** Y hold afterwards;
- if X holds before the message $P \rightarrow Q : Y \quad on\ L$ then both X and Q $\mathbf{sees}_L$ Y hold afterwards;
- if Y can be derived from X by the logical postulates then Y holds whenever X holds.

An annotation of a protocol is like a sequence of comments about the beliefs of principals and what they see in the course of authentication, from initial assumptions to conclusions.

Acknowledgements

Jim Saxe invented the method for entering a PIN by modifying a nonce with a series of '+' and 'nextdigit' operations. Dorothy Denning and Roger Needham read drafts of this paper. Cynthia Hibbard provided comments on the presentation.

Petitioner Apple Inc. - Exhibit 1012, p. 1070

References

[1] M. Burrows, M. Abadi, and R.M. Needham. A Logic of Authentication. *Proceedings of the Royal Society of London A* Vol. 426, 1989, pp. 233–271. A preliminary version appeared as Digital Equipment Corporation Systems Research Center report No. 39, February 1989.

[2] CCITT. CCITT Blue Book, Recommendation X.509 and ISO 9594-8: The Directory-Authentication Framework. Geneva, March 1988.

[3] D. Chaum and I. Schaumüller-Bichl, editors. Smart Card 2000: The Future of IC Cards. Proceedings of the IFIP WG 11.6 International Conference on Smart Card 2000: The Future of IC Cards, Laxenburg, Austria, October, 1987. North-Holland, Amsterdam, 1989.

[4] National Bureau of Standards. Data Encryption Standard. Fed. Inform. Processing Standards Pub. 46. Washington DC, January 1977.

[5] W. Diffie and M. Hellman. New Directions in Cryptography. *IEEE Transactions on Information Theory* IT-22, No. 6, November, 1976, pp. 644–654.

[6] M. Gasser, A. Goldstein, C. Kaufman, B. Lampson. The Digital Distributed System Security Architecture. Proceedings of the 1989 National Computer Security Conference, Baltimore, 1989, pp. 305-319.

[7] U. Feige, A. Fiat, A. Shamir. Zero Knowledge Proofs of Identity. Proceedings of the Nineteenth Annual ACM Symposium on Theory of Computing, New York, 1987, pp. 210–217.

[8] M. Gasser, E. McDermott. An Architecture for Practical Delegation in a Distributed System. Proceedings of the 1990 IEEE Symposium on Security and Privacy, Oakland, 1990, pp. 20–30.

[9] C.A.R. Hoare. An Axiomatic Basis for Computer Programming, *CACM* Vol. 12, No. 10, October 1969, pp. 576–580.

[10] S.P. Miller, C. Neuman, J.I. Schiller, and J.H. Saltzer. Kerberos Authentication and Authorization System. *Project Athena Technical Plan* Section E.2.1, MIT, July 1987.

Petitioner Apple Inc. - Exhibit 1012, p. 1071

[11] R.M. Needham and M.D. Schroeder. Using Encryption for Authentication in Large Networks of Computers. *CACM* Vol. 21, No. 12, December 1978, pp. 993–999.

[12] R.L. Rivest, A. Shamir, and L. Adleman. A Method for Obtaining Digital Signatures and Public-key Cryptosystems, *Communications of the ACM* Vol. 21, No. 2, February 1978, pp. 120-126.

Petitioner Apple Inc. - Exhibit 1012, p. 1072

#25

Most fascinating, however, are her accounts of the value of the most transitory information on the network. In traditional publishing, there is a hierarchy of permanence for works published in a hierarchy of materials: hardbound books, paperback books, magazines, newspapers, and fliers. The more durable the package, presumably, the longer-lived the information. On the Net, however, when the value of information is very time-sensitive the risks to the digital publisher of having information pirated and resold are minimized. In the extreme case, the information might be a packaged, real-time experience, either in personal consulting or in social group participation.

One of Fillmore's compelling conjectures is that readers might not "pay $5 for an on-line "contained" or finite, static, linear text of James Michener's Chesspeake, but might be willing to pay even more to "follow the electronically generated thought path resulting from a course taught by the author himself about factual fiction, a course where one could navigate the links students make in their critical thinking about the novel, navigate and link to related documents, graphics, videos, sounds, experiences, and the author himself—all in real time."

The transition leaps across our classifying metaphors. What amounts to an on-line writer's workshop goes beyond the digital library metaphor, through the electronic marketplace and into the digital worlds metaphor we discuss in the last section of this book. The changes at hand challenge us to understand the possibilities. Fillmore, the hunter-trickster, hunts cleverly for business possibilities, using multiple metaphors to make sense of the search.

Given Fillmore's conundrums about fees, it is ironic that net mavens can find the full text of her speech on the Internet (for free) at

http://cism.bus.utexas.edu/ravi/laura_talk.ht

The Online BookStore can be found at

http://marketplace.com/obs/obshome.html

Letting Loose the Light: Igniting Commerce in Electronic Publication

Mark Stefik

Connections

In "The Digital Library Project: The World of Knowbots" in Part 1, Robert Kahn and Vinton Cerf ask, "If a thousand books are combined on a single CD-ROM and the acquirer of the CD-ROM only intends to read one of them, what sort of royalty arrangement is appropriate to compensate the copyright owners? How would compensation be extended for cases in which electronic copies are provided to users?" Their questions show how, in 1988, issues about copyright protection and payment for using information arose in the context of early CD-ROM distribution.

By 1994 copyright issues not only had not been settled, they were coming to a boil. Laura Fillmore's effort to build a successful publishing business on the Internet reveals the limitations of what was practical in May of 1994. Although digital works were being sold on the Internet, provisions for commerce were primitive. Furthermore, the ease of copying digital works had led many people to believe that digital information should be free. Fast access to the network had made trading programs or other data as easy as mixing songs on audio tape. In short, it had become much simpler for network users to infringe copyright than to uphold it.

This is the context for the oft-quoted statement by John Perry Barlow of the Electronic Freedom Foundation, "Copyright is dead." Advocates of free information argue that because you don't lose the original when you make a copy of a digital work, there should be no charge for copying information. The conventional wisdom among publishers in late-1994, when this article was written, was that digital containers for software

Petitioner Apple Inc. - Exhibit 1012, p. 1073

MSI028769

were inherently leaky vessels and that no viable solution would ever be found. The article suggests, however, a way to sustain commerce for those who want to sell information on the network.

Throughout the time I've been groping around cyberspace, an immense, unsolved conundrum has remained at the root of nearly every legal, ethical, governmental, and social vexation to be found in the Virtual World. I refer to the problem of digitized property. The enigma is this: If our property can be infinitely reproduced and instantaneously distributed all over the planet without cost, without our knowledge, without its even leaving our possession, how can we protect it? How are we going to get paid for the work we do with our minds? And, if we can't get paid, what will assure the continued creation and distribution of such work?

John Perry Barlow, "The Economy of Ideas"

No problemo.

T-101 (Arnold Schwarzenegger) in *Terminator 2*

It all depends on whether you really understand the idea of trusted systems. If you don't understand them, then this whole approach to commerce and digital publishing is utterly unthinkable. If you do understand them, then it all follows easily.

Ralph Merkle

Across many cultures, knowledge and inner knowing are described as light. *Letting loose the light* refers to spreading knowledge in the world, typically in written form. Consistent with this metaphor, the period in the eighteenth century characterized by a burst of writings in philosophy and science is called the *Enlightenment*. In the present century the metaphor of knowledge as light is both poetic and physically realized. Books, pictures, movies, musical performances, and other works can be conveniently represented digitally. With fiber optics, digital works are actually transmitted by the shining and pulsing of light.

The digital representation of works and their nearly instantaneous transmission has profound consequences for commercial publishing. Three of the fundamental economic factors affecting the publishing industry—printing costs, inventory costs, and transportation costs—can be drastically reduced. Digital works can be copied at minuscule costs, stored in almost no space, and transported instantly anywhere in the world.

This portability opens up visions of a greater information age. For libraries, universal access to the world's written knowledge is a centuries-old vision. Today many libraries have electronic catalogs accessible to anyone with a computer. Articles can be delivered to anyone with a fax machine. In the technophile's idealized vision, books and magazines need never be printed on paper at all; any digital work could be made available to anyone, anytime, anywhere in the world.

However, the dream of universal digital access to high-quality works dangles just beyond reach. Such works are not usually available, because of publishers' concerns that uncompensated copying will infringe and erode their ability to make a living. History suggests that this problem will not go away. Publishing thrives only when it is profitable, and profitability depends on limiting uncompensated copying.

The conventional wisdom—based on the way computers are used for word processing, electronic mail, and computer networking—is that copying digital works is easy and, therefore, inevitable. There appears to be a clear, inherent conflict between representing works digitally and honoring the commercial and intellectual property interests of creators and publishers. Fortunately, computers need not be blind instruments of copyright infringement. Properly designed digital systems can be more powerful and flexible instruments of trade in publications than any other medium. The seeming conflict between digital publishing and commerce is merely a consequence of the way computer systems have been designed to date.

The technological means for commerce in digital works are now at hand. New and unconventional when compared with today's uses of computers, these means will enable us to buy, sell, and lend digital works much as we now buy, sell, and lend printed books and other publications. They will change the way digital works are purchased and delivered and will give consumers access to all sorts of works at any time of the day—though not necessarily for free. Consumers will be able to sample works, borrow them, rent them for nominal fees, and make copies for friends. Creative people will be able to circulate their works to networks of friends while earning a reliable living from people who make copies of them. This technological system will affect everything from digital books to digital television, from digital music to digital video

Petitioner Apple Inc. - Exhibit 1012, p. 1074

MSI028770

games. It will radically change our concepts of digital libraries, digital bookstores, digital music stores, digital newspapers, and digital television stations. Moreover, any competent technological company will be able to implement the required systems.

Here is a road map to this new land. First, we discuss the history of copyright law and the reasons for the widespread, but incorrect, belief that works represented digitally will be copied without permission. We then describe the technological innovations that can enable and support commerce in digital publishing. Finally, we introduce the institutional and business challenges that lie ahead. What we require to overcome them is the wit, will, and means to create institutions that provide the necessary security, convenience, vision, and longevity.

The Origin and Rationale of Copyright

It is harder to be honest than to cheat when copying digital works on general-purpose computers. The license printed on the package of most purchased computer software authorizes a buyer to load the software into one computer and use it there. Getting another legal copy for a friend involves driving to the computer store and buying it. It is much easier, faster, and cheaper to simply load the same software into another computer. Such copying is so private and easy to do that most people do it without thinking, and without guilt.

Unauthorized copying on computers is not, of course, limited to purchased software. With a few keystrokes, it is often possible to copy a paragraph, an article, a book, or a life's work without compensating its creators or publishers. Nor are unauthorized copying and use new phenomena. Anyone who ignores the FBI warning message on video tapes to make copies for friends infringes a copyright, as do people who copy compact discs onto cassettes. As a practical matter, it has not been feasible to enforce the copyright law in these cases. There are simply too many people with recording devices to make rigorous enforcement practical or cost-effective.

It is widely believed that there is no viable technical solution to this problem for digital information. John Perry Barlow, a prominent spokesperson in the computer industry, says that the idea of patents and copyrights needs to be rethought in the digital age. Information, he argues, cannot be contained or owned. It wants to be free. Cyberspace is the new frontier, and its leaders and pioneers are today's radical thinkers about freedom of information. Barlow suggests, in fact, that we abandon all notions of intellectual property and market regulation. This solution was tried at least once, and it didn't work. Apparently, for high-quality works to spread in the world people need to be able to make a living from creating and distributing them.

Barlow's arguments are reminiscent of the intense debates about intellectual property that took place in France during the French Revolution. Like Barlow, revolutionaries argued that ideas cannot be owned and should not be regulated. During the revolution, many writers and underground publishers emerged as civic heroes of public enlightenment by arguing against tyranny and for freedom of the press. The revolution of the mind, they said, required the dismantling of the laws and institutions governing authorship, printing, publishing, and bookselling. Absolutely free communication was one of the most precious rights of man. All citizens should be able to speak, to write, and crucially, to print freely. According to this philosophical ideal, people had a will to know and should be allowed to read and learn from anything they liked. The wide availability of books and the right to publish were seen as keys to this spread of knowledge.

In 1789, the revolutionary government wholly deregulated the press, believing that the works of the great writers of the Enlightenment would thus be made universally and cheaply available. The writers and publishers certainly never expected what actually happened. Instead of works of enlightenment, the presses turned out mostly seditious pamphlets and pornography. Printers also competed with each other to bring out cheap editions of books others had spent money developing. So little money could be made producing the good books that quality declined; most editions were abridged and contained many errors. Publisher after publisher went into bankruptcy and then out of business. The disastrous nature of an unregulated press, largely unanticipated in the heat of the revolution, became blatantly obvious as the publishing industry fell into shambles. The same leaders who had clamored for the freeing of the presses came belatedly to understand the folly of their action. In the

Petitioner Apple Inc. - Exhibit 1012, p. 1075

MSI028771

chaos of the unregulated press, some prominent and popular writers even stopped publishing; because they could not control the printing of their works, they could not make a living by writing.

In 1793 legislation to restore order to publishing was passed. It recognized the rights of authors and grounded the publishing industry in the principles of the marketplace, establishing the author as creator, the book as property, and the reader as an elective consumer. This law reflected a fundamental shift in the Enlightenment perspective, which now saw that the widespread creation and publication of creative works was better served when the authors could own the products of their minds. This history of the treatment of intellectual property in France is discussed by Carla Hesse in her book *Publishing and Cultural Politics in Revolutionary Paris, 1789–1810.*

Today, most people see the infringement of copyright on digital systems as unavoidable. In the remainder of this section, we describe the assumptions about computer design behind this belief and argue that we need to go beyond conventional ways of thinking to solve the problem.

Three main factors currently inhibit the development of digital publishing: (1) the absence of high-contrast, low-power, cheap flat-panel displays; (2) lack of an inexpensive and reliable way of handling money digitally; and (3) the need for a widely accepted means of accounting for the use and copying of digital works. Improvements in technology will almost certainly solve the display problem in the next five to ten years. Most people see such displays as crucial to making electronic books and newspapers portable. They matter less, however, in applications for which desktop displays are satisfactory or where displays are not necessary—such as in transmitting musical works. The second factor—methods of handling money digitally, in the form of checks, credit cards, or anonymous cash—has recently become the subject of much field experimentation. Our focus is on the third problem, techniques for commerce in what we call *digital property* rights or *usage rights*, a generalization of the idea of copyright that delineates several kinds of rights besides copying.

Some publishers see illicit copying as too big a business risk and do not publish in digital form at all. Digital newspapers often leave out important and high-value content such as the pictures or graphics, and consumers of these lower-quality papers are unwilling to pay much for them. The perception of low quality leads to a chicken-and-egg problem in which the publishers make little money and consumers have few choices. Ironically, publishers of works that need periodic upgrading, such as computer software, have found that some leakage increases their customer base, even though it is often reported that there are more unauthorized copies of a program in use than authorized ones. Software publishers have decided that the revenue losses of illegal copying are affordable, although they lead to unfair billing. Software publishers charge all users the same price, regardless of the use to which they put the program, arguably overbilling people who use the work infrequently.

As computers and computer networks have proliferated, the need for a better approach to protecting digital works has become more widely appreciated. Moreover, as new kinds of works—such as music, video, and multimedia works that mix these forms—are now available digitally, people from different industries are searching for solutions. Given this wide acknowledgment of the need, why have solutions seemed so elusive? Apparently, we are stuck in a rut, assuming that things must be done the way they have always been done with electronic mail, word processing, and other current applications.

Conventionally, we use general-purpose computers with general-purpose operating systems and general-purpose programs. The computer industry, grounded on the premise that computers can do anything that can be programmed in software, produces a wide range of programs—word processors, spreadsheets, databases, calendars, graphics programs, and computer games. Manufacturers accept no liability when someone uses a computer to copy a copyrighted file. After all, one company builds the computer, another writes the software that does the copying, and both hardware and software are intended for general purposes—that is, any purpose the user wants to put them to. The manufacturer wants no responsibility for someone who uses the computer in a way that just happens to infringe a copyright, nor does the software publisher. The perpetrator is the consumer, who finds it easier to make an unauthorized copy than to be strictly honest.

Petitioner Apple Inc. - Exhibit 1012, p. 1076
MSI028772

Stuck within this framework the community of computer users protests against any attempt to regulate the copying of digital property. If we continue to accept this framework, with all of its assumptions, no party will be motivated or empowered to break the cycle and no effective way to protect digital property will be developed. At present, without enforceable property rights, the writers of words, interactive games, and songs often are not compensated for their work. And without their works the world is a darker, poorer place. Honoring their creative work in the digital systems of tomorrow requires us to challenge the design assumptions of the systems we use today.

A New Design for Digital Publishing

The technical core of the approach we propose is based on two ideas: (1) that digital works can be bought and sold among trusted systems, and (2) that works have attached usage rights that specify what can be done with them and what it costs to exercise those rights.

Trusted Systems

The term *trusted system* refers to computers that can be relied on to do certain things. For example, suppose that a creator or publisher forbids all copying of a particular digital work. A trusted system in this context would reliably and infallibly carry out that stipulation; no amount of shouting or coaxing would coerce it to copy the work. The trusted system might be very polite, but ultimately it would always refuse to make an unauthorized copy. Similarly, suppose that a trusted system *could* copy a work but only if it reliably records a *set fee* to be paid when it has done so. A trusted system would always record the fee whenever the work was copied. If the copying process is interrupted part way through, the trusted system would follow a standard policy; for example, it might delete the partial copy, record no fee, and note that a copying attempt was begun but not completed. Again, no amount of coaxing would change its behavior. It could always be counted on to follow the rules of the trust.

A common but false analogy claiming to show why digital works cannot be protected in computers is that of genies and bottles. In this analogy, a valued digital work corresponds to a genie and the bottle is a place to store it. When a digital work is sent to a computer, for example, it may be sent in coded form, so that even if the transmission is intercepted it is useless to a wiretapper. Once people have a legal copy of a digital work, however, they can make more copies of it. Since they have a key, they can just decode the work and make copies of it. Alternatively, they can copy the coded version and give away copies of the key. Once the content genie is out of the bottle, according to this scenario, you can't put it back in and unauthorized digital copies are sure to circulate. This is the problem trusted systems can fix.

Trusted systems speak a communications protocol with other trusted systems and will not transmit information to any system not recognized as another trusted system. This strategy ensures that copies of digital works are either inside trusted systems or they are encrypted. When they are inside trusted systems, usage is controlled. When they are outside trusted systems, usage is practically impossible without breaking the code. The important issue, however, is not just protection and containment. The greater good is not served by simply limiting the flow of information. It is served by supporting and encouraging a lively trade in information. *Rather than just confining genies to specific bottles, we want to encourage them to travel between bottles under rules of commerce.*

A very concrete question about such a system is "Why couldn't I just copy a file onto a diskette and give that away?" Unless there is permission to do so, a trusted system would never copy a work to a diskette or anywhere else. Even if permission to copy a work is given, a trusted system would not make a copy on a diskette, because a diskette is not a trusted system. Nor are magnetic tapes, compact discs, or, even, the disk drives of trusted systems. Trusted systems contain computers, have internal protected storage, and communicate by protocol. From a user's point of view, the trusted system is the storage device. Trusted systems only make copies of a digital work on themselves or on other trusted systems. Putting an unencrypted copy on a diskette is letting the genie out of the bottle onto an unprotected medium that can be accessed by a general-purpose computer that does not honor usage rights.

Petitioner Apple Inc. - Exhibit 1012, p. 1077

MSI028773

There is an important issue about the perception of trusted systems. One way of looking at them is to say that trusted systems presume that the consumer is dishonest. This perception is unfortunate, and perhaps incorrect, but nonetheless real. Unless trusted systems offer consumers real advantages they will probably view them as nuisances that complicate our lives. A more favorable way to look at trusted systems is to compare them to vending machines. They make it possible to order digital works any time of the day and get immediate delivery. Faster than a telephone-order pizza, a digital work can be delivered immediately over the same telephone line it was ordered over.

In summary, the first key to commerce in digital works is to use trusted systems. We have spoken of these systems as computers, but they are not limited to devices like personal computers and need not seem like computers at all. They could be personal entertainment devices for playing music, video game devices, laptop reading devices, personal computers, devices for playing digital movies at home, credit-card-sized devices that fit in your pocket, or whatever. In the following discussion we refer to these trusted systems as *repositories*, an architectural plan that can have different embodiments. Repositories communicate digitally with other repositories and not with anything else. In contrast to such current passive media as compact discs, repositories have no externally defined limits on storage capacity; so successive generations of repositories could increase in capacity while remaining completely compatible with earlier systems. Digital works would be communicated between repositories using secure coded protocols. Repositories would read the rules that apply to a given digital work and follow them. This brings us to the next issue: How do repositories know what the rules are?

Attached Usage Rights

We start with an analogy. When we go to a store to buy a shirt, there are various tags attached to it. One kind of tag is a price tag. If we want to buy the shirt, we must pay the amount on the tag. Another tag gives cleaning instructions: for example, wash by hand in cold water or dry clean only. Still another tag might say something about the style of the shirt or the history of the shirt company.

This is roughly the idea of *usage rights* on digital works. Digital works would come with tags on them. The tags—put there by the creators, publishers, and distributors—would describe the usage rights for the digital work: what can be done with it and what it costs.

There are some important differences from the shirt's tags. The first is that the tags are digital and intended to be read and used by the repository itself, although consumers can also read the tags through the repository's user interface. They are written in a machine-readable language and give the repository the rules for using the work; they are an electronic contract enforced by the repository. Another difference is that the tags are not removable. Finally, there can be tags attached to different parts of a work. For a shirt, it is as if there were tags on the pockets, tags on the buttons, tags on the collar, tags on the sleeves, and so on. Each tag would grant rights to that part, and different rights could pertain to different parts of a work. For example, a digital newspaper might have certain rights on local stories, others on photographs or wireline stories or advertisements, and so on.

Suppose that the digital work is a piece of music. A statement describing a right might say the following:

> This digital work can be played on a player of type Musica-13B. This right is valid from February 14, 1995 to February 14, 1996. The repository must have a security level of three. No other authorizations are needed. The fee for exercising this right is one cent per minute with a minimum of five cents in the first hour. Usage fees are paid to account 1997-200-567131.

Of course, such an internal statement would not be in English, although it should be in a well-defined computer language. Here is an example of a machine-readable statement in a usage rights language:

Right Code:	Play Player: Musica-13B
Copy Count:	1
Time-Spec:	From 95/02/14 Until: 96/02/14
Access-Spec:	Security-Level: 3
Fee-Spec:	Fee: Metered $0.01 per 0:1:0 Min: $0.05 per 0/1/0
Account:	1997-200-567131

Petitioner Apple Inc. - Exhibit 1012, p. 1078
MSI028774

Computer languages are more precise than natural languages and have formal grammars and semantics that define how to interpret each phrase in the language. Computer languages are not at all poetic, but they are much less ambiguous, if less expressive than natural languages. Because the sentences of a digital property language are parts of potential contracts between the creators of digital works and consumers, clarity and simplicity are exactly what we want. Interpreting a usage rights language is quite simple. In level of difficulty, it is more like reading bar codes from packages at the supermarket checkout than it is like reading and understanding an English sentence in a story.

A digital property language needs to define several different kinds of rights, mainly those concerned with how the work can be transported, how it can be rendered, and whether it can be used in derivative works. Other, special rights relate to making and restoring backup copies to protect against hardware failure. The easiest way to understand usage rights is to consider some examples.

Transferring Digital Works When we copy files for friends on a general-purpose computer, we increase the number of copies of a digital work, fail to compensate the work's creator, and infringe the copyright. A repository, in contrast, never infringes copyright.

Our first scenario illustrates how copy and transfer rights would work in a repository system. Suppose that Morgan buys a copy of a digital book, perhaps at the book kiosk at the supermarket. To do so, he exercises a right to copy the book and pays a fee; copying the book records a transaction between the seller's repository and (say) a card-sized repository that Morgan carries with him. Alternatively, he could buy a copy of the digital book from home by telephone. In either case, the digital book is delivered electronically by a communications protocol between the vendor's repository and Morgan's repository. At the end of the transaction, Morgan has spent some money, has a copy of the digital book in his repository, and can now read it on a reader. The book arrives with all its usage rights intact.

Now suppose that, when Morgan finishes reading the book, his friend Andy asks to borrow it. They plug their repositories together, and Morgan exercises a *transfer right* to move the digital book to Andy's repository. With paper books, once we have bought a book we can give it away or dispose of it in any way we please, and the same right could apply to Morgan's digital book. At the end of the transfer transaction, the digital book resides on Andy's repository and not on Morgan's, and no money has been exchanged. Andy can now read the book, but Morgan cannot. The crucial point is that the transfer transaction preserves the number of copies of the digital book.

We now consider a scenario involving a loan right. Again Morgan has a digital book that his friend Ryan wants to borrow for a week. They plug their repositories together and Morgan exercises a *loan right*. Again, while the digital book is loaned out, Morgan cannot use it. Suppose, however, that Ryan goes off on vacation and, while he is playing volleyball on a beach thousands of miles away, the week's loan period runs out. He has completely forgotten the book. Because both repositories have clocks in them, Ryan's repository deactivates its copy when the week is up. Meanwhile, Morgan's repository also notices that the loan time is up and marks its temporarily deactivated copy as usable again. Without any action by either person, or even any communication between their repositories, the digital book has been returned automatically. If Ryan still wants to access it later, he could pay a nominal fee to rent the work or to make his own copy. The point of both scenarios is that the repositories follow rules, which in this case mimic and improve on the rules of loaning for paper books. The ability to return loaned materials automatically would probably be widely used in digital libraries.

Rendering Digital Works To read a digital book you have to be able to see it; to listen to digital music you have to be able to hear it; to enjoy a digital video game, you have to be able to see and hear it. We use the term *render* to mean the processing of a digital work so that it can be experienced. Like copying, transferring, and loaning, rendering is controlled by usage rights.

We distinguish two forms of rendering: playing and printing. When we play a digital work we send it to another person through some kind of transducer so that he or she can experience it. The term play, usually employed in phrases like *playing music* or *playing a movie*, is also used to

Petitioner Apple Inc. - Exhibit 1012, p. 1079
MSI028775

denote displaying part of a book, running a computer program, or running an interactive video game. The term *print* in the digital context means to make a copy of the work on media outside usage rights control, either on paper or by writing a file to an external storage device.

The concept of usage rights allows great flexibility in marketing digital works. Today, when you buy a compact disc at the music store, you pay for the copy and play it for free. The same is true for a book. You buy the book and read it as often as you want; generally, you aren't supposed to make copies of it, but you can give it away. By contrast, keeping digital works in repositories would provide more flexibility.

Suppose for example that Andrea's mother is at the music store but does not know exactly what music her teenage daughter wants to buy. She transfers a selection of music to her own repository, choosing collections by half a dozen bands that she knows Andrea likes. At this point she does not need to pay anything for the right to make the copies. When she gets home, she transfers the music to Andrea's repository for her to checks out at her leisure. Like all repositories, Andrea's home repository has a built-in credit server that transfers funds electronically. She can listen to short demonstration samples for free or listen to pieces she selects for twenty-five cents an hour; or she can pay for five years of unlimited playing for $10. Thus, Andrea exercises a pay-for-play right rather than a pay-for-copying right. If pay for play has an infinite term, there are no fees for playing the music as often as she likes. The terms and alternatives for usage rights and usage fees would be set by the music's creators and distributors. What Andrea gains by this arrangement is flexibility and the convenience of trying out different digital works. She might even be able to use technology similar to a cellular telephone to order music and download it from the music store to her car repository.

For books, however, the idea of pay for play may not seem very useful if the typical book we have in mind is the paperback novel. As it is already cheap, it does not seem worthwhile to charge for the time needed to read it. Besides, why should slow readers pay more than fast readers? On the other hand, consider large, expensive reference works like encyclopedias. People do not casually pay out hundreds of dollars for these works; nor do they usually read them from beginning to end. Paying a small fee for each hour of actual use may make it feasible to bring high quality digital encyclopedias into many households that could not otherwise afford them. As in the music example, purchasers could decide whether to pay by the hour or for large or infinite blocks of usage time.

As yet another example, consider the digital newspaper, which could, in principle, be delivered in several ways: bought at the corner newsstand, downloaded over the telephone, or broadcast by a digital radio station. It could be available though pay-for-play usage rights or by monthly subscription. Suppose, however, that a particular newspaper is reluctant to allow its customers to make paper copies of the newspaper, even for a fee, for fear that some enterprising person will print up enough copies for the entire neighborhood and cut into circulation. To prevent this occurrence, usage rights could be designated so that people trying to print the newspaper would discover they have no printing rights.

Suppose, again, that a month later customers find that they can print the newspaper's old news without hindrance but not its new stories. In that case, the usage right for printing would be dated to prohibit printing until a month had passed since publication, perhaps because the publisher figures that printouts of old news are more like advertisements for the newspaper than threats to circulation. Variations in what the publishers might allow or encourage are virtually endless. The rights granted on stories or photos or whatever could even become a basis for competition among digital newspaper publishers.

Making Derivative Works Distributors add value to products by advertising and selecting works and presenting them to consumers, making a living by performing these functions and requiring compensation for them. Today bookstores and music stores operate on a per-copy basis, charging for "hard copies" of books or compact discs. If pay for play became popular for digital works, how would distributors make money? What is needed, of course, is a mechanism for paying distributors when a consumer chooses to pay for play. This mechanism, called a *shell*, would enable distributors to modify rights and add new usage fees.

We can understand shells as analogous to gift boxes of different sizes. A common and amusing trick is to put a present in a small box, wrap it, and put that box in a bigger box, wrapping that box and putting it in a

Petitioner Apple Inc. - Exhibit 1012, p. 1080
MSI028776

bigger box, and so on, perhaps attaching a gift card to each package. In digital work, the boxes would correspond to digital containers (shells) and the gift tags would correspond to attached usage rights. Putting a digital work into an empty shell, or into a shell containing another digital work, is called *embedding*, and it is controlled by an *embed usage right*.

Consider the following case. Nick has written a novel and offers it in digital form. He determines what he wants to charge per copy and attaches usage rights to it, specifying the fee to be paid into his account every time a copy is made. His publisher agrees to publish the book and puts another shell around it directing that when the work is copied, an additional fee is to be paid to the publisher. The publisher may help the author improve the book in various ways and spend money advertising it. Finally, a bookstore puts an additional shell around the publisher's shell, directing that when the kiosk makes a copy of the book, a fee should be paid to the bookstore. Thus when a customer buys a copy of the work, he or she pays, automatically, a fee to the bookstore, to the publisher, and to Nick. This works because the accounting system follows the instructions embedded in every shell of the copied work.

Or consider Paige, a college professor at a business school that bases courses on case studies collected into a reader. Paige chooses the cases of interest for her course as digital works with attached rights. If an interesting case has an extraction right, she can remove a copy of it from its digital source; if it has qualified editing rights, she can make certain kinds of changes to it; if it has embed rights, Paige can add it to her own collection. At each stage, the continuing rights to the work are controlled by its creator's specifications. Paige can put all the works she has collected into a shell and add her own usage right specifications to the shell. When a student buys a copy of her course reader, fees are paid to the creators of each case study and to Paige herself.

It is interesting to compare this process of controlled reuse to the existing practice in which one author requests reprint permission for an article by another author. The process of granting and obtaining permissions is tedious and time consuming and is often assigned to editorial assistants by publishers who do not expect to earn much from reprint requests. This approach assumes that they are willing to agree to the most usual rights, fees, and conditions for reprinting a work. By lowering the perceived hassle and cost of reuse, usage rights may trigger a substantial increase in the commercial reuse of works.

Consumer-based Distribution One of the most radical possibilities for distributing digital works is *consumer-based distribution*, sometimes called super distribution. With ordinary media, consumer copying and sale of works is considered a problem, because creators and publishers receive no compensation for such copying. In contrast, consider what would happen in our earlier scenario if Morgan, instead of giving or lending his digital book, makes a copy of it for his friend Andy. The repositories would record the transaction and bill Morgan or Andy for the new copy. Depending on how the shells have been set up, fees would be collected for the store where Morgan originally bought the work, for the distributor, for the publisher, and for the creator, even though none of them are present at the transaction. Every consumer would become a potential salesperson, a word-of-mouth sales channel.

This possible future is in radical contrast to the problem foreseen by Barlow in the quotation at the beginning of this piece. Digital property can be anywhere on the planet without the knowledge of its creators and still make money for them whenever it is used or copied by a repository.

Licenses and Tickets In a trusted system, licenses and tickets would be special kinds of digital works that play direct roles in commerce. *Licenses* would be digital certificates that enable someone to exercise certain usage rights. Think of them as similar to driver's licenses or identification cards that authorize someone to drive a car or enter a restricted area. A digital license would let someone exercise certain rights, such as copying or printing a particular work. When a consumer asks to use a licensed work, an authorization server or "digital authority"—a program on a repository—would check his or her digital license. *Digital tickets*, a kind of coupon offered by publishers for prepaid uses or discounts, would enable a possessor to exercise a right exactly once. Think of digital tickets as comparable to movie or train tickets; once you have entered the theater or boarded the train, the ticket is punched and cannot be used again. A digital ticket is punched by a digital ticket agent that is a program on a repository.

Petitioner Apple Inc. - Exhibit 1012, p. 1081

MSI028777

When an author creates a work and specifies its usage rights, he or she can require buyers to have particular licenses or tickets to exercise certain rights. These digital licenses and tickets would be essentially impossible to forge; would let consumers exercise usage rights in living rooms, school dormitories, or anywhere else; and would assure authors that fees will be collected and that the tickets and licenses specified will be required.

Different areas of publishing have different crucial problems for which digital licenses and digital tickets could offer solutions. In some industries, there is an advantage in ensuring that only authorized distributors can sell digital works. The author of a computer game, for example, may want his or her game sold only through distributors licensed to advertise, promote, and demonstrate it. If a dealer without that license tries to copy and sell the game, the repository would refuse the transaction. By determining who gets distributor's licenses and arranging that licenses cannot be transferred between repositories without authorization, the author could maintain control over distribution. Such digital licenses could also restrict distribution rights to a certain time period.

In the music and video industries, companies try to limit the playing of their recordings to home use. While current technology provides no effective way to enforce this provision, trusted entertainment systems using licenses could distinguish between equipment for home use and equipment for theater or broadcast use. Equipment for playing digital recordings would come with different licenses and fee schedules for home and public use. Alternatively, radio transmitters and receivers might all be linked to repositories; a station might broadcast a work but require each listener to pay a nominal fee for receiving it. Trusted systems could provide a basis for many different kinds of relationships between creators, broadcasters, and the public than are feasible today.

In the book publishing industry, it is common to offer big discounts on books that remain unsold after a certain period of time. Imagine a usage right that allows a copy of a digital book to be made for nothing in exchange for a certain ticket. Later, a book club might offer these tickets for sale and let a holder get any three digital books in exchange for three tickets. The price of a digital book could thus be determined later by the price of the ticket, which could vary according to demand.

In the computer software industry, it is common to release new versions of software to fix bugs in earlier versions and to offer the upgraded software for free or for low prices to purchasers of the original version. The problem lies in making sure that the upgraded versions are not given to people who did not purchase the original software. Digital tickets would offer a solution by allowing vendors to bundle upgrade tickets with the original works. Consumers could use any copy of the upgrade versions of the software to make their own new copy by simply using their tickets; this approach lets consumers upgrade their software without going back to the dealer. Because digital tickets get punched when they are used, the approach would allow exactly one upgrade per original version.

Because metered and per-copy fee arrangements can make usage budgets unpredictable for organizations, they may prefer *site licenses*. Such licenses would grant members of an organization the right to use a digital work subject to restrictions. For example, a site license would generally preclude making copies for use by people not in the organization; or it might distinguish between different kinds of uses in different departments. It might also limit the number of people who can use a work at the same time, perhaps leaving its administration to someone in the organization. The supplier of the digital work would specify in the usage rights that the organization's site license be recorded on a repository before the work could be used. If different departments require different regulated uses, then each department would have its own specialized license. To monitor such global constraints as the number of copies of a work simultaneously in use, a digital license could instruct the repository's authorization server to communicate periodically with a site authorization server that registers and counts users.

Licenses and tickets could be established for diverse categories and purposes, including social purposes. For example, a charity or governmental organization could issue certificates to low-income people or inner-city youth. Socially conscious publishers could then offer discounts or limited free use of certain digital works to people holding such certificates. From a profit perspective, they may assume that offering the certificates will increase the potential base of customers by contributing to public literacy and that, in any case, these consumers would not buy the

Petitioner Apple Inc. - Exhibit 1012, p. 1082
MSI028778

work. The same digital-license mechanism could provide special rights to certified librarians, researchers, and teachers; and certificates could be dispensed at libraries to allow readers to browse works for limited periods.

One area that has been much discussed recently is control of access to works on computer networks. In the present free-wheeling environment of computer networks, interested people can set up discussion groups on explicit and adults-only topics. The same computer network that offers on-line museums and information sources for kids may also offer on-line pornography. Controlling access to such materials requires an approach that balances social interests in free speech and commerce with community interests and responsibilities regarding adult materials.

In public settings off the network, the issue of adult material usually arises in reference to magazines and videos. It is common practice for dealers to display adult magazines so that passersby need not see suggestive covers. Video distributors generally follow the movie rating system: G for general audience, PG for parental guidance advised, R for restricted, and X for adult movies. Both these approaches have analogs to digital licenses. Thus, works can come with ratings established by appropriate institutions or community organizations. For example, a G-rated movie would require no license, whereas viewing a digital movie rated PG-13 would need either an identity certificate specifying that the consumer is over 13 or a permission ticket issued by his or her parent.

The foregoing examples show how central digital tickets and licenses are to the usage rights approach and how one overall infrastructure could serve a wide range of social and commercial purposes.

Foundations of Trust in Repositories

Next we explore the question, what is it that we want to trust about repositories and what is the basis *for* such trust? In general, a trusted system is one that can be relied upon to take responsibility for a given operation or set of operations. In the case of digital works on repositories, the requirement for trust is that the repositories follow—at all times and in every instance—the rules about how digital works are used. They must be accountable for all uses of the works and for the fees charged for those uses. Responsibility is, fundamentally, an issue of *integrity*. For

repositories that integrity has three parts: *physical integrity* refers to the soundness of the physical device itself; *communications integrity* means roughly that repositories cannot be easily fooled by telling them lies; and *behavioral integrity* means that repositories will exercise their functions exactly as they are supposed to, 100 percent of the time.

Physical integrity applies both to the repositories and to the digital works they protect. One threat to a repository is that someone will pry open the case and gain access to what is stored inside. In a trusted system different repositories could have different levels of security. A repository that can be compromised with a power drill and a screwdriver would have a low security level. A somewhat higher level of physical security would be a system with sensors that enable it to detect a threat and erase certain key data. A still higher level of security, suitable perhaps for a real life James Bond, might be a system that self-destructs when it detects that it is under threat, perhaps setting off alarms and telephoning for help.

Even at its lowest level, security for a repository would be much higher than the security for such passive media as videotapes, compact discs, or computer diskettes. These media record their information out in the open where it can be accessed by any general-purpose reading device; they cannot detect intrusion or take any kind of protective or evasive action. Repositories, on the other hand, would never present data to any device that fails to establish itself as a bona fide, qualified repository.

The second kind of system integrity, communications integrity, would ensure that repositories could not be easily fooled by being connected to illegitimate computer systems masquerading as legitimate repositories. When repositories connect with each other, they would go through a registration process identifying themselves to each other and establishing their bona fides. Imagine, for example, two secret agents unknown to each other who meet by arrangement. What's the secret word? How do I know you are who you say you are? Are we sure that nobody else is listening? These are the kinds of concerns two repositories would have when they are connected. They would put each other through a series of tests intended to weed out impostors and protect the works with which they are trusted. Only when registration succeeds would they establish a trusted session.

A few words about how this works are in order. At the heart of the registration process is a security concept called *public key encryption*, a

Petitioner Apple Inc. - Exhibit 1012, p. 1083

MSI028779

well-known and much-studied system for secure and secret communication. In this approach, each repository is given a private key or code, which it keeps secret, and a public key. In a trusted system, these keys would be given to a repository when it is manufactured and would be certified by a master repository known to be highly secure. (One of the principal requirements for the system architecture—discussed in the last section of this paper—is an institution that can control and safeguard the master repositories.) Communications integrity is ensured because all communications among repositories are in codes that are extremely difficult to break. In addition, provisions to detect attempts to tamper with communication and to isolate repositories identified as compromised can be built into the protocols.

Finally, we come to behavioral integrity. Even if the repositories have not been physically compromised and can prove their identities to each other, how do we know they will work properly? In the secret agent analogy, how do we know that the other agent hasn't been compromised or turned? Because the behavior of computers is determined by their programming, the programs used in repositories must be thoroughly tested and certified, which is a lot of work. What makes the certification task easier for repositories than for computers in general is that repositories would have limited functions. They would need to carry out a limited number of very specific operations relating to usage rights, protocol handling, and accounting. Furthermore, there would be procedures that guarantee that all installed software is invulnable to tampering or modification. Finally, even if a repository were compromised, it would need to identify itself for any transaction with a certificate from a master repository; other repositories, given the identity of the compromised repository, would refuse to carry out further transactions.

In summary, the physical integrity, communications integrity, and behavioral integrity of a repository are the foundations of a trusted system. A repository is designed with the ability to detect tampering and communications errors and to ensure certified behavior. These characteristics could be achieved by computers. Until now, however, the value of these attributes has not been appreciated, so that elements of the technology are not widely available and computers are designed without these goals in mind.

The Accountant Inside When someone makes a copy of a digital book and the repositories record the charges, what's to say that the author or publisher will ever get paid? Suppose, for example, that the repository is a credit-card-sized device. Why not just throw it away when a large enough bill accumulates on it? Also, if repositories contain the equivalent of money, what will prevent theft of that money?

There are many ways to approach these questions. During 1994 several groups conducted field trials of the national computer networks that operate digital checking accounts, cash, and network credit cards. These trials provide a base of experience relevant to usage rights.

Repositories would have a substantial advantage over such systems because they would record a transaction without requiring an immediate telephone or computer-network connection to a financial clearinghouse. This is especially relevant for billing tiny amounts, microtransactions, for which the cost of a telephone call would dwarf the amount of the payment. Monthly connections to a clearinghouse would be more convenient. A repository could be connected to a clearinghouse in any of several ways: by plugging it into a bank teller machine or a special telephone or connecting it to a computer network through a personal computer. In such an operation, the repository would open a channel to a clearinghouse with a registration protocol similar to the ones used when two repositories connect to each other. During the monthly session, all transactions could be reported in a single communication and a fresh credit limit for the repository could be set.

Some security measures would be necessary. First, a personal identification code similar to those used at automatic tellers would be required before charges could be accrued. Second, all transactions would be reported by both parties; this would not prevent cheating but would require two people to collude in losing their repositories. Third, the repository itself, which is likely to be more expensive than a credit card, would require insurance to replace it. Finally, as happens with credit cards today, anyone who regularly reports the loss or theft of a repository would eventually have difficulty getting a replacement or would be forced to use a repository with more stringent security arrangements.

Petitioner Apple Inc. - Exhibit 1012, p. 1084

MSI028780

Implications and Institutional Challenges

Stakeholders in digital publication will ultimately come from many industries, walks of life, and parts of the world. For a variety of reasons, they are now accustomed to different versions of copyright law and have different conventions of what constitutes fair use of copyrighted material. As more and more kinds of publication go digital, people's different expectations are likely to create a tug of war. Digital property rights may provide a way to manage this evolving situation. Because copyrights traditionally last a long time, we need to create and shape institutions governing usage rights that will serve us well for a long time.

Usage Rights and Copyright Law

Copyright law is not static. Over time, there have been various changes. Notable copyright reforms were made as recently as 1976, and several more are currently under active discussion. Defining a few terms will bring us to the nub of many copyright issues and show how digital usage rights are relevant to them.

Copyright law has provisions for what is called *fair use*, the amount and kind of quotations from a copyrighted work that can be made without permission. In general, creators and publishers have an interest in limiting free use of their own materials under fair use so that they can require extra fees for particular uses. Consumers, librarians, and scholars, on the other hand, have an interest in ensuring that certain uses are unencumbered.

Here are some examples. A person who buys a copy of a work is permitted to use it in a variety of ways. Although making copies of the work to sell or give away is generally not legal, some copying is allowed—at least for certain kinds of works and in some contexts. For example, it is usually all right to make a copy for personal use and to quote passages from a book in a book review or scholarly work, as long as the original source is cited. As new media have become important, similar issues have arisen about fair use in quoting from recorded music and movies.

Sometimes more than one kind of use is distinguished for a work. An easily understood example is that of a play script. The usual copyright provisions govern the copying of a script. The right to create a stage production from the script and to perform it publicly for profit is not, however, covered by fair use. A public performance requires a different kind of right, a *performance right*. Similar issues arise for musical scores and recorded music. When we buy a compact disc or cassette tape of music, fair use includes playing it at home, whereas a radio transmission constitutes a public performance. Because performance rights are not included in the purchase, radio stations are supposed to pay for putting such works on the air. The small print on a compact disc generally includes the phrase "all rights reserved," the publisher's way of claiming all rights not explicitly granted.

The fair use doctrine arises when possessing a copy of a work gives a person the potential to use it in ways its creator thinks are unfair. In such cases, usage rights could provide for different kinds of uses and fees, distinguishing between copying rights, loan rights, transfer rights, play rights, broadcast rights, print rights, extract rights, embed rights, editing rights, and several others. On a trusted system, these specific rights could be granted by requiring particular digital licenses or tickets and different fees. Some kinds of digital players, for example, might have built-in licenses and codes that determine whether they can be connected to public broadcast systems or only to home systems.

In many fair use scenarios, the gap between what is fair use and what is infringement is exacerbated by the fact that there is nothing in between. Fair use costs nothing. Other uses cost fees; and even when the fees are small, the cost and bother of obtaining and accounting for them is high. The digital property rights approach, however, could permit transactions for even nominal amounts of money, changing the confrontational issue of fee versus free to a practical issue of "how much?"

Usage rights could also make it possible to grant rights to designated categories of users for social reasons. Digital certificates could be made available to librarians, library users, teachers, students, impoverished people, and so on. Some interest groups are already drafting position papers about fair use in the electronic age, spelling out certain rights that they believe should incur no fees, such as the right to print temporary paper copies for personal use. Curiously, the concept of usage rights reverses our conventional assumptions about making copies; printing a paper copy, we can now recognize, is moving digital content out of repository control. In a usage rights context, paper copies would have greater potential for unauthorized copying than digital copies would.

Petitioner Apple Inc. - Exhibit 1012, p. 1085
MSI028781

In summary, the usage-rights approach provides repository-mediated contracts to govern the various uses of digital works. It creates specific language for common kinds of uses and their fees. It is a tool never imagined by the creators of copyright law, or by those who believe laws governing intellectual property cannot be enforced. What copyright law protects is the expression of ideas. As John Perry Barlow put it, "The point at which this franchise was imposed was that moment when the 'word became flesh' by departing the mind of its originator and entering some physical object.... Protecting physical expression had the force of convenience on its side. Copyright worked well because, Gutenberg notwithstanding, it was hard to make a book.... Unlike unbounded words or images, books had material surfaces to which one could attach copyright notices, publishers marques, and price tags (*Wired*, March 1994).

The ability to attach appropriate tags proclaiming the rights and fees for different uses is exactly what repositories do for digital works. Such tags, permanently attached and honored by the trusted systems, would enable us to experience the works. With these tags, the basic concepts of copyright law seem to work just as they are. In this way, an unconventional redesign of computer operation can preserve and even improve the now conventional social contract between those who create and those who consume works of the mind.

What Repositories Can and Can't Do

Repositories cannot, of course, prevent all unauthorized copying of digital works. No technology can keep someone from reading a digital book, then laboriously typing the words verbatim at a keyboard. A plagiarizer could even use technological aids, for example, a television camera aimed at a display and feeding its output into a computer equipped with an optical text reader. Digitally published music could be played through a repository's speaker and recorded through a microphone. Recordings of interactive works such as video games are of little use; still, if a work can be experienced by the human senses, it can be recorded. Trusted systems would simply inhibit the unauthorized making of perfect digital copies.

Two things could happen when performances of digital works are re-recorded outside a repository. The first is a loss of fidelity, familiar to anyone who has made cassette-tape copies from a compact disc. The first-generation copy of a digital work re-recorded outside a repository would not be perfect, although it may be very good. Subsequent generations of uncontrolled copies would be as good as the first-generation copy. The second thing that may occur is the copying of identification information hidden on an original version. This information can be made invisible and inaudible to the human senses but detectable by special equipment. In the event that unauthorized copying is frequent enough to justify intervention, such identification information could be used to trace an illegal copy back to the repository where it was made.

In summary, repositories—like all technology—are imperfect. Yet they can make it much easier to be honest and easier for creators to make a living. Moreover, we would expect them to have other social effects in the long term. More digital works would be created because more potential authors would see a possibility of making a living creating them. That is the main effect—letting loose the light.

There are other predictable effects. With usage rights, electronic distribution of digital works would be much easier than it is now. Using computer networks and the telephone system, consumers could take immediate delivery of digital works from distributors located at great distances. Many distributors of digital works, such as digital bookstores, digital libraries, and digital music stores would serve much larger geographic areas. Consumers would be able to choose from a wide range of potential distributors and to access or purchase quality digital works at a moment's notice and at any time of the day. Distributors who add little value to the chain between producers and consumers would probably be squeezed out.

What kinds of works will first be distributed on repositories? The answer to this question, and many of the factors bearing on it, are still unknown. Repositories will be adopted first in areas where they can solve a pressing problem. In the music industry, publishers have lobbied successfully against the manufacturing of devices that can make digital recordings. There may be an opportunity in this area if the trusted systems developed give advantages to both consumers and publishers. It will probably also be easy to introduce repositories, where other technological changes are leading to system changes. In television, for example, repositories could become more viable when digital television offers fidelity that cannot be captured by the today's videotape formats.

Petitioner Apple Inc. - Exhibit 1012, p. 1086
MSI028782

The adoption of usage rights would remove many of the barriers to self-publishing and induce more creators of digital works to self-publish, offering their works for sale on computer networks and reaping the benefits of consumer-based distribution. Self-publishing would not, however, eliminate the role of digital publishers. Publishers often improve the quality of the works they publish and provide brand names recognized by the consumer as indicative of quality and style. The continued need for this kind of quality assurance will give publishers of digital works an enduring role. In fact, new publishers will probably appear. People who review works may put together collections, providing a service similar to brand-name recognition by appraising the works they offer. The net effect of these opportunities for new publishers could be the broadening of influences on popular taste.

The Digital Melting Pot

The metaphor of the melting pot has long been used to describe the culture of the United States created by blending the traditions of people from all over the world. Digital publishing, we believe, is creating a melting pot of genres. The term *multimedia* refers to the mixing of multiple kinds of media—books, newspapers, musical recordings, videos, video games, and computer software—in a single production. But the blending of forms, unlike the blending of water and oil, is creating new forms: for example, interactive movies and travel guides and annotated presentations of plays that include scripts, multiple performances, and reviews, all in a single hyperlinked work.

Some currently distinct genres may be evolving toward similar digital interactive forms. Ultimately, the form of the digital news program and the digital newspaper may be the same. Both may become a digital work broadcast in the air or by cable several times a day and laid out on multiple electronic pages. The pages will contain short film clips of anchors giving the news and, perhaps, animated advertisements and infomercials. Both versions may be interactive and playable on color screens with high-fidelity sound. Today's newspapers and television news programs are the forerunners of these future interactive news forms.

As publication forms blend, what will become of the provisions of copyright law and fair use, which today have different provisions for newspapers, videos, and computer programs? It is likely that some of today's legal distinctions will not be sustainable in the new digital forms.

In the Fall of 1993 Bruce Lehman, head of the U.S. Patent Office, conducted a public hearing on intellectual property and digital networks. The hearing was called to discuss these issues in the context of the national information infrastructure, the so-called Information Superhighway touted in the press. At this Washington meeting, representatives of the cable industry sat down the aisle from small-town librarians and civil libertarians. Representatives from the music industry rubbed shoulders with people from the computer hardware and software industries. All were aware that their own businesses and institutions were becoming more involved in digital publication and that new media were creating forms and genres that confound present definitions of fair use.

The representatives found that they had very different assumptions about the appropriate means for protecting intellectual property. The music industry uses statistical sampling of radio station broadcasts to check that royalties are properly paid, while the computer industry has no effective organization to check on copyright infringements. Paper-based publishing mostly uses the copyright clearance center, which expedites payment of copying fees. The representatives were well versed in the issues pertaining to their own businesses and recognized that the conditions for the other businesses were different. They knew that as the various media merge into new forms new ways of doing business will emerge. Whatever new rules and ways of business develop, they want to ensure that their own industry thrives.

Planning for the Generations

The laws governing the length of a copyright have changed several times. In 1978 the copyright for a work was established as the lifetime of the creator plus fifty years. Thus, the total period of a copyright may easily amount to a hundred years. In our fast-paced society, we do not often design institutions to last for hundreds of years.

Yet the long view is not unheard of. When we set aside parklands in the public trust, we are planning for the long term. Such consciousness of time is akin to that expressed by Native Americans when they speak of planning for seven generations: three past generations of parents, grand-

Petitioner Apple Inc. - Exhibit 1012, p. 1087
MSI028783

parents, and great-grandparents; the generation that makes the decisions; and three future generations of children, grandchildren, and great-grandchildren. Adapting this perspective could help us create an institution that has a lasting value for humankind.

There are many stakeholders in digital publishing, including consumers, authors, publishers, distributors, platform vendors, financial institutions, and governments. The approach based on usage rights presumes that all will share a digital property language, compatible platforms from multiple vendors, and broad general agreement about what rights mean. The details of the approach and the particular kinds of rights defined will evolve over time.

The security needs of the approach assume the existence of an authoritative institution that issues digital certificates warranting that particular platforms and software uphold and enforce the concept of usage rights. We call this institution the Digital Property Trust (DPT). Although some initial seed funding would be needed, the DPT could eventually fund its activities from a small tithe on commercial repository transactions or by renewable licenses on platforms and software.

Although planning for a DPT is tentative at this time, a few observations about its role and structure are appropriate. At present, there are many different kinds of social and international structures—government, banking, political, and standards organizations, among others—with their own bases of authority. In the future these organizations should be able to establish and publish their own digital certificates, publishers issuing their own kinds of digital licenses and authors and distributors setting whatever usage rights and fees they please. The role of the DPT would be to promote widespread commerce in digital works. To this end, it would certify and maintain the security of trusted systems and establish a common operational terminology of usage rights to meet social and economic needs.

Achieving this long-term vision for the DPT requires the wisdom and organization to appropriately balance interest groups. The DPT would need to be even-handed in its treatment of hardware providers, software designers, and publishers. Because the certification process for hardware and software would require DPT to have detailed knowledge of exactly how products work, maintaining even-handedness may be challenging. At the same time, the DPT would need the representation and support of the most powerful vendors and publishers for its decisions to carry the weight of authority.

Establishing Trusted Systems

Today's computers and installed software are not programmed to honor usage rights. This fact raises a key question: Assuming that the usage rights language is appropriate and the DPT can be established, how do we go from a world in which most systems are not trustworthy to a world populated by trusted systems? The realistic answer is that the world will not change suddenly. Rather, we need incremental approaches to establish trusted systems widely.

One incremental approach would distinguish between individual and organizational repositories, starting with institutions dealing in documents of high value and limited distribution. These might be bookstores that print documents on demand or legal offices that provide rapid access to thousands of scanned documents. Beginning with organizations like these could demonstrate the viability of usage rights without requiring tamperproof systems for authentication, authorization, and accounting.

Another incremental approach would focus on digital works in a particular market niche. For example, rather than starting with computers, it may be easier to begin with personal entertainment systems for music or video games, for these systems do not need compatibility with general-purpose application programs and operating systems.

A third avenue might be to upgrade existing computer systems by adding appropriate software and hardware. Even though such upgrades do not generally lead to high levels of security, the approach could begin with a large base of systems at low levels of security and provide incentives to upgrade them to more secure systems for works of greater sensitivity or value.

Whichever approach is taken, in the long run repositories offer advantages to both publishers and consumers. Consumers may find they have ready, quick, and cheap access to all kinds of digital works that can be delivered by telephone or computer network any time of the day. Creators may find that consumer-based distribution is a large new distribution channel; anyone who buys a digital work will be able to make a

Petitioner Apple Inc. - Exhibit 1012, p. 1088
MSI028784

copy and sell it, automatically routing compensation to its creators. The simple provisions for extracting, editing, and embedding small portions of digital work open doors to creative sampling and reuse of multimedia materials. As creators and publishers learn that safety and wider markets are possible in digital publishing, they may bring about a flowering of new works and old works in new digital form.

Repositories provide a way to let loose the light for present and future generations. There are many institutional challenges, and stakeholders need to work together to bring about the necessary changes. The popular adoption of repositories will start small. In what publishing niches will it begin, providing the sparks to ignite the bonfire of publishing?

A Glossary of Terms

Credit server A secure program and database in a repository to keep track of fees owed for the use of digital works. Typically, a credit server would have a credit limit and would need to be regularly connected to a financial clearinghouse to transfer funds to pay the bills. Like a bank automatic teller machine, a credit server would typically require the user to enter a personal identification code before using it.

Digital certificate A digital document attesting to the truth of something. Each repository would have a digital certificate certifying it as a trusted system and identifying its public key and security level. In general, digital certificates could not be transferred between repositories except by specially authorized repositories. Digital certificates are encrypted in the private key of a master repository, making them difficult to forge and providing a simple means of testing their authenticity—decrypting them by using the public key.

Digital property right or Usage right A specification of a contract to use a digital work in a certain way. Such rights would fall into several categories. Transport rights, for example, would include the right to copy, transfer, or loan a work; render rights would include playing and printing it; derivative rights would include the right to extract, embed, and edit it. Usage rights would be represented in a formal language that can be precisely interpreted by repositories. They could also be displayed to a consumer in a variety of simple ways appropriate for the situation.

Digital property rights transaction or Usage rights transaction A series of actions treated as a unit. For example, in electronic banking, a transfer of money from one account to another is a transaction that credits one account with the money at the same time that it debits the other account. Each digital property right defines a particular transaction that can be carried out. For example, a usage right to copy a digital work would cause a new copy to be made and a credit server to make a record of the required payment.

Digital Property Trust (DPT) An organization that ensures the health of digital publishing and promotes a lively international commerce in digital works. In conjunction with consumers, publishers, creators, and platform vendors, it would set the standard for the evolving digital property language and issue digital certificates to conforming platforms. It would also maintain the master repositories and perhaps ensure security and financial transactions.

Digital license A digital certificate identifying the bearer repository as licensed and thereby authorized for carrying out certain rights. For example, certain digital works might require that copies of a work could only be made and sold when the repository contains a particular digital distributor's license.

Digital ticket A digital certificate or coupon that can be used once to authorize a particular transaction. For example, a digital work may include an upgrade ticket that authorizes the user to replace the digital work with an updated version. When digital tickets are used, they would be punched by a digital ticket agent and could not be used again.

Digital work Any work that can be represented in digital form; for example, a document like a book, magazine, or newspaper. It could also be a recording of music, a movie, a computer game, or any computer program. Sometimes the word software is used in a general sense to mean a digital work.

Encryption A process of encoding a digital work by a secret code to render it unusable by anyone without the code. Decoding a work to restore it to usable form is called decryption. The preferred method of encoding is public-key encryption, in which there are two keys, a public key and a private key. When the private key is used to encrypt a work, the public key can be used to decrypt it.

Master repository A very high-level repository with the highest security level. Master repositories would be kept by the Digital Property Trust (DPT) and would be used to issue certificates. The public keys of the master repositories would be assigned to all trusted systems when they are manufactured, enabling them to exchange and identify authentic digital certificates in their transactions with other repositories.

Repository Any trusted system used for storing and playing digital works. For example, repositories could be portable entertainment de-

Petitioner Apple Inc. - Exhibit 1012, p. 1089
MSI028785

vices, laptop readers, personal computers, credit-card-sized devices, or mechanisms that fit into home entertainment equipment for controlling digital television or music. Repositories would store digital works, together with their usage rights, and include credit servers for keeping track of fees for use.

Security level Different degrees of physical security—ranging from low security to very high security—for protecting digital works against unauthorized use. Repositories for handling extremely valuable works need greater security than those for ordinary and portable use.

Shell A kind of digital container for storing digital works in the filing system of a repository. They could contain both digital works and other shells. Tags specifying usage rights and fees would be attached to each work and its shell. When someone asks a repository to use a digital work, the repository would check the rights and fees recorded on the tags.

Trusted system A system that can be relied on to follow certain rules at all times. In the context of digital works, a repository would be a trusted system that governs the uses and fees for digital works. All digital works would have tags describing uses and fees in a usage rights language; trusted systems would carry out the instructions on these tags infallibly.

Usage right See Digital property right.

Reflections

The network for digital publishing is still being invented. As its creators we will need much wisdom to guide that invention. The hundreds—if not thousands—of traditional myths about creation have tried to answer questions such as: How did the world come to be? Why are humans what they are? Where did they come from? Generally, these stories are intended to explain the actions of the gods to mortals. According to them, we were formed from the thoughts of the gods, arose out of chaos, fell from grace, or were fashioned from mud along with the animals. The myths embody stories of people searching for a land in which to live and stories about how they should live in it to keep the world in balance.

But there are few stories instructing us about how to act as able and responsible creators. Perhaps creation myths are the wrong places to look for guidance; instead we should pay attention to stories about how people in the past worked together as communities. "Letting Loose the Light" draws on those stories, on our understanding of the marketplace and on the history of intellectual property during the French Revolution.

In the past few years, several ways of governing the use of information on CD-ROMs and networks have come into use. In one version, purchasers call a telephone number to pay for keys that unlock specific software distributed on a CD-ROM. Different keys unlock different software. Because there are different versions of the CD-ROM discs, two people buying them are unlikely to be able to share keys. This approach does not, however, control subsequent redistribution of software if people have sufficient storage to copy it from a CD-ROM. Other approaches requiring special hardware and software have also been offered to meter the use of software on a CD-ROM. Efforts to control software with license servers are now widely used in organizations with closed local computer networks. They allow programs to govern the number of simultaneous users of proprietary software or data bases, making it possible, for example, for any five people of an organization of a hundred members to use a database at the same time.

Security and convenience are the key issues for approaches to digital publishing: security is an issue for publishers, and convenience is an issue for users. These concerns are often seen to be in tension. In the simple and convenient low-security approaches, users can load metering software onto existing personal computers; unfortunately, they could also load pirateware, software that defeats security measures. In many proposed systems, pirateware posted on a computer bulletin board could be used to compromise every site on a network. Fear of such attacks makes publishers reluctant to publish their works on such a network. In other approaches, works to be used must be distributed by the equipment manufacturer, which also acts as the accounting and billing company. As most publishers view control over marketing and distribution as a key to their success, they are often unwilling to engage in such arrangements. In contrast with such approaches, the digital property rights approach described in this article separates the publishing business from the financial and platform businesses. It will also require a good deal of coordination among these business sectors to make such trusted systems available.

Petitioner Apple Inc. - Exhibit 1012, p. 1090
MSI028786

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☒ OTHER: Small Print

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)

#26 Working Copy

From file history of 6,253,193

Last Edited: MJS February 8, 1995
Started: MJS December 13, 1994

Letting Loose the Light

Igniting Commerce in Electronic Publication

Copyright © 1994, 1995 by Mark Stefik.

Draft version. Please do not circulate, cite, or quote from the paper without permission of the author. Send inquiries and comments to:

Mark Stefik
Xerox PARC
3333 Coyote Hill Road
Palo Alto, CA 94304
Phone: (415) 812-4366
Fax: (415) 812-4241
email: stefik@parc.xerox.com

BEST AVAILABLE COPY

MSI028728

Petitioner Apple Inc. - Exhibit 1012, p. 1093

Introduction 2
The Origin and Rationale of Copyright 4
Why Unauthorized Copying Seems Unavoidable 6
Usage Rights on Trusted Systems 8
Attached Usage Rights 10
Transferring Digital Works 12
Rendering Digital Works 13
Making Derivative Works 15
Consumer-based Distribution 17
Licenses and Tickets 17
Foundations of Trust in Repositories 19
The Accountant Inside 22
Implications and Institutional Challenges 23
Usage Rights and Copyright Law 23
What Repositories Can and Can't Do 26
The Digital Melting Pot 28
Planning for the Generations 29
Appendix: A Glossary of Terms 32

MSI028729

Petitioner Apple Inc. - Exhibit 1012, p. 1094

Throughout the time I've been groping around cyberspace, an immense, unsolved conundrum has remained at the root of nearly every legal, ethical, governmental, and social vexation to be found in the Virtual World. I refer to the problem of digitized property. The enigma is this: If our property can be infinitely reproduced and instantaneously distributed all over the planet without cost, without our knowledge, without its even leaving our possession, how can we protect it? How are we going to get paid for the work we do with our minds? And, if we can't get paid, what will assure the continued creation and distribution of such work?
From "The Economy of Ideas" by John Perry Barlow, published in *Wired*, March 1994, page 85.

No problemo.
T-101 character played by Arnold Schwarzenegger in the movie *Terminator 2*.

It all depends on whether you really understand the idea of trusted systems. If you don't understand them, then this whole approach to commerce and digital publishing is utterly unthinkable. If you do understand them, then it all follows easily.
From a conversation with Ralph Merkle, Fall 1994.

Introduction

Across many cultures, knowledge and inner knowing are described as light. Letting loose the light refers to spreading knowledge in the world, typically as writings. Consistent with this metaphor, the period in the eighteenth century during which there began a bursting forth of writings is called the Enlightenment. Now the metaphor of knowledge as light is both poetic and physically realized. Books, pictures, movies, musical performances and other kinds of works are conveniently represented digitally. With fiber optics, digital works are actually transmitted by the shining and pulsing of light.

The digital representation of works and their nearly instantaneous transmission has profound consequences for commercial publishing. Three of the fundamental economic factors affecting the publishing industries are printing costs, inventory costs and transportation costs. Digital works can be copied at minuscule costs, stored in almost no space, and transported instantly anywhere in the world.

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1095

Best Available Copy

This portability opens up visions of a greater information age. Universal access to the world's written knowledge is a centuries old vision for libraries. Today, many libraries have services for making their catalogs accessible to anyone with a computer. Articles can be delivered electronically to anyone with a fax machine. In the technophile's idealized vision, books and magazines need never be printed on paper at all. Any digital work *could* be made available for experiencing to anyone, anytime, anywhere in the world.

However, the dream of universal access to *quality* digital works dangles just beyond reach. Quality digital works are not usually available because publishers are concerned that works will be copied without compensation, eroding their ability to make a living and infringing their copyrights. History suggests that this problem will not go away. Publishing thrives only when publishing is profitable and profitability depends on limiting uncompensated copying.

The conventional wisdom, based on the way that computers are used for word processing, electronic mail, and computer networking, is that copying digital works is easy and inevitable. Thus, there appears to be an inherent conflict between representing works digitally and honoring the commercial and intellectual property interests of the work's creators.

Fortunately, computers need not be blind instruments of copyright infringement. Properly designed, digital systems can be more powerful and flexible instruments of trade in publications than any other medium. The seeming conflict between digital publishing and commerce is merely a consequence of the way that computer systems have been conventionally designed.

The technological means for commerce in digital works are announced and described in this article. These means are new and unconventional when compared with how computers are used today. The means will enable us to buy, sell, and loan digital works much like how we buy, sell, and loan ordinary books and other published works. They will change the way that digital works get purchased and delivered. They will make it possible for consumers to access all sorts of digital works electronically any time of the day, but not necessarily for free. Consumers will be able to sample works, borrow them, rent them for nominal fees, and make copies for friends. The technological means will enable creative people to circulate their

MSI028731

Petitioner Apple Inc. - Exhibit 1012, p. 1096

works by giving them to networks of friends, and yet reliably make a living when people make copies. The means will affect everything from digital books to digital television, from digital music to digital video games. They will radically change our concepts of digital libraries, digital bookstores, digital music stores, digital newspapers, and digital television stations. Any competent technological company could implement the required systems.

Here is a road map to the story. We discuss the origins of copyright law, and why it is widely but incorrectly believed that when works are represented digitally they will be copied without permission. We then discuss the technological innovations that can enable and support commerce in digital publishing. Finally we introduce the institutional and business challenges that are ahead. What is required is the wit, will and means to create institutions that have the necessary vision, role and longevity.

The Origin and Rationale of Copyright

In copying digital works on general purpose computers, it is harder to be honest than to cheat. With most purchased computer software, the license printed on the package authorizes a buyer to load the software on one computer and to use it there. To get another legal copy for a friend involves driving to the computer store to buy it. It is much easier, faster and cheaper to simply load the same software again onto another computer. Such copying is so private and easy to do that most people do it unconsciously and without guilt.

The issue of unauthorized copying on computers is not limited to purchased software. With a few keystrokes, it is often possible to copy a paragraph, an article, a book, or a life's work without compensating the creators or publishers.

Unauthorized copying and use are not new with digital works. Anyone who ignores the FBI warning message on video tapes and makes copies for friends is infringing copyright. Similarly, people who copy compact discs onto cassettes for their friends are infringing copyright. As a practical matter, it has not been feasible to enforce copyright law in these cases. There are simply too many people with recording devices to make rigorous enforcement practical or cost effective.

Best Available Copy

MSI028732

Petitioner Apple Inc. - Exhibit 1012, p. 1097

Best Available Copy

It is widely believed that there is no viable technical solution to this problem for digital information. John Perry Barlow is a prominent spokesperson in the computer industry and co-founder and executive chairperson of the Electronic Frontier Foundation. In his article quoted at the beginning of this piece, he says that patents and copyrights need to be rethought in the digital age. According to Barlow, information cannot be contained or owned. Information wants to be free. Cyberspace is the new frontier. Its leaders and pioneers are radical thinkers about freedom of information. Barlow suggests that we abandon all notions of intellectual property ownership and market regulation.

This was tried at least once before and it didn't work. Apparently, before quality works can spread in the world, it is necessary for people to be able to make a living creating and distributing them. Barlow's arguments are reminiscent of the arguments that took place in revolutionary France. The French Revolution was accompanied by intense debates about intellectual property. A few words about this historical precedent are appropriate here.

Like John Perry Barlow, French revolutionaries argued during this period that ideas can not be owned and should not be regulated. During the revolution, many writers and underground publishers were seen as civic heroes of public enlightenment. They argued against all kinds of tyranny and for freedom of the presses. They said that revolution of the mind required dismantling the laws and institutions governing authorship, printing, publishing, and book selling. Free communication became one of the most precious rights of man. All citizens should be able to speak, to write, and crucially, to *print* freely. In the philosophical ideal, people had a will to know things. They should be allowed to read anything and to learn from what they read. The availability of books and the right to publish were seen as keys to this learning.

In 1789 the press was wholly deregulated in the expectation that the works of the great writers of the Enlightenment would be made universally and cheaply available. The writers and publishers never expected what actually happened with these changes. Instead of enlightenment, the presses mostly turned out seditious pamphlets and pornography. Printers competed with each other to bring out cheap editions of books that others spent much money developing. So little money could be made producing the best books that most editions were abridged and they contained many errors. Publisher

MSI028733

Petitioner Apple Inc. - Exhibit 1012, p. 1098

after publisher went into bankruptcy and then out of business. The disastrous nature of an unregulated press, largely unanticipated in the heat of the revolution, became blatantly obvious as the publishing industry fell into shambles. The same leaders who had clamored for the freeing of the presses came belatedly to understand the folly of their action. In the chaos of the unregulated press, even some prominent and popular writers of the period stopped publishing because they could not control the printing of their works and could not make a living by writing.

In 1793 legislation was initiated to restore order to publishing. The legislation recognized the rights of authors and grounded the publishing industry in the principles of market commerce. These principles establish the author as creator, the book as property and the reader as an elective consumer. This reflected a fundamental shift in the Enlightenment perspective: that the widespread creation and publication of creative works are better served when the creators of these works can own the products of their minds. The basic elements of modern copyright law as we know them in America derive from this period in France. An account of this period can be found in Carla Hesse's book *Publishing and Cultural Politics in Revolutionary Paris, 1789-1810.*

Why Unauthorized Copying Seems Unavoidable

Three main factors inhibit digital publishing today: (1) lack of high contrast, low power and cheap flat panel displays, (2) lack of a cheap and reliable way of handling money digitally, and (3) lack of a widely accepted means of accounting for the use and copying of digital works. The display problem will almost certainly be solved in the next five to ten years by improvements in technology. Such displays are widely thought to be crucial for portable reading of electronic books and newspapers. However, they do not matter as much for cases where desk or tabletop computer displays are satisfactory or where displays are not necessary such as for musical works. Methods for handling digital money either in the form of checks, credit cards or anonymous cash have become the subject of much field experimentation, especially over the last year. We focus on the third problem, techniques for commerce in what we call "usage rights," a generalization of the idea of copyright that distinguishes several kinds of rights besides copying.

Best Available Copy

MSI028734

Petitioner Apple Inc. - Exhibit 1012, p. 1099

For some publishers, digital copying is too big a business risk and they do not publish in digital form. Publishers of digital newspapers leave out important and high value content such as the pictures or graphics. This leaves consumers with digital newspapers of much lower quality than the paper versions, so that they do not want to pay much for them. The perception of low quality leads to a chicken and egg problem in which the publishers do not make much money and consumers have few choices. Ironically, publishers of works that need periodic upgrading, such as computer software, have found that some leakage helps to increase their customer base. However, even for computer software, it is often reported that there are more unauthorized copies in use than authorized ones. Software publishers have decided that the revenue losses of illegal copying are affordable, but they lead to billing schemes that are cumbersome. Software publishers bill all users the same amount, regardless of the use to which they will put the work, arguably over billing those who do not use the work very often.

With the proliferation of computers and computer networks, the need for a viable approach to protecting digital works is now widely appreciated. As more kinds of works are represented digitally -- such as digital music, digital video, and multimedia works that mix these forms -- people from ever wider industries are searching for solutions. Given this wide acknowledgment, why have solutions seemed so elusive? Apparently, we have been stuck assuming that things must be done the way they have always been done on computers with electronic mail, word processing, and so on.

Conventionally we use general purpose computers with general purpose operating systems and general purpose programs. The computer industry is grounded on the premise that computers can do anything that can be programmed in software. The software industry produces a wide range of programs such as word processors, spreadsheets, databases, calendars, graphics programs, and computer games. Computer manufacturers accept no liability if someone uses a computer to copy a copyrighted file. After all, one company builds the computer, another writes the software that does the copying, and both hardware and software are intended for *general* purposes. The manufacturers want no responsibility when someone uses the computer in a particular way and happens to infringe a copyright. The perpetrator of illegal copying is just the

Best Available Copy

MSI028735

Petitioner Apple Inc. - Exhibit 1012, p. 1100

consumer, who finds it easier to make an unauthorized copy than to be strictly honest.

Stuck within this framework, it is common within the community of computer users to protest against any attempt to regulate copying of digital property. If we accept this framework with all of its assumptions, then no party seems motivated and empowered to break the cycle and there is no viable way to protect digital property. Without effective property rights, the writers of words, interactive games and song are often not compensated for their work and without their works the world is a darker, poorer place. To honor creative work in the digital systems of tomorrow requires challenging the design assumptions of the systems we use today.

Usage Rights on Trusted Systems

The technical core of the approach is based on two ideas: that digital works can be bought and sold among trusted systems and that works have attached usage rights that specify what can be done with them and what it costs to exercise the rights. We now consider how it all works.

The term trusted system refers to computers that can be relied on to do certain things. For example, suppose that a particular digital work is not to be copied. A trusted system in this context would reliably and infallibly carry out its trust. No amount of shouting or coaxing would coerce it to copy the work. The trusted system might be very polite, but ultimately it would always refuse to make an unauthorized copy. Similarly, suppose that a trusted system could copy a work but only if it reliably records that a set fee should be paid when this is done. A trusted system would always record the fee whenever the work was copied. If the copying process was interrupted part way through, the trusted system would follow some standard policy. For example, it might delete the partial copy, record no fee, and note that a copying attempt was started but interrupted. Again, no amount of coaxing would change its behavior. It could be counted on to follow the rules of the trust.

A common but false analogy about why digital works cannot be protected in computers is sometimes given in terms of genies and bottles. In this analogy a valued digital work corresponds to a genie and a place to store it is a bottle. Consider the scenario where a

Best Available Copy

MSI028736

Petitioner Apple Inc. - Exhibit 1012, p. 1101

digital work is sent to a computer. For example, it may be sent in coded form so that even if the transmission is intercepted it would not be useful to a wiretapper. The argument goes on to say, however, that once someone has a copy of a digital work, they can always go on to make more copies. Since they have a key, they can just decode the work and then make copies of it. Alternatively, they copy the coded version and also give away copies of the key. Once the content genie is out of the bottle, you can't put it back in and unauthorized digital copies will circulate. This is the problem that trusted systems fix.

The important issue is not just protection and containment. The greater good is not served by just limiting the flow of information. It is served by supporting and encouraging a lively trade in information. *Rather than just confining genies to specific bottles, we want to encourage genies to travel between bottles under rules of commerce.*

A very concrete question about copying is "Why couldn't I just copy a file onto a diskette and give that away?" Unless there is permission to do so, a trusted system would never make a copy on a diskette or anywhere else. Even with permission to copy a work, a trusted system would not make a copy on a diskette because a diskette is not a trusted system. Nor are magnetic tapes, compact disks, or disk drives trusted systems. Trusted systems contain computers, have internal protected storage, and communicate by protocol. From a user's point of view, the trusted system *is* the storage device. Trusted systems only make copies of a digital work on themselves or on other trusted systems. Putting an unencrypted copy on a diskette is letting the genie out of the bottle onto an unprotected medium that could be accessed by a general purpose computer that would not honor usage rights.

There is an important issue about the perception of trusted systems. One way of looking at them is that trusted systems operate with a presumption of dishonesty of the consumer. Another way to look at trusted systems is that they are like vending machines. Trusted systems will need to offer some real advantages to consumers or they may be viewed as nuisances that complicate our lives. One advantage conferred by trusted systems is that they will make it possible to order digital works any time of the day and have them immediately delivered electronically. Faster than a phone order

Best Available Copy

Petitioner Apple Inc. - Exhibit 1012, p. 1102

pizza, a digital work can be delivered immediately over the same phone over which an order is placed.

In summary, the first key to commerce with digital works is to use trusted systems. We have spoken of these systems as computers, but they need not seem like computers. These systems could be personal entertainment devices for playing music, video game devices, laptop reading devices, personal computers, devices for playing digital movies at home, credit-card sized devices that fit in your pocket, or whatever. In the following we will refer to these trusted systems as *repositories*. Thus, the term repository is an architectural plan that can have different embodiments. Repositories communicate digitally with other repositories and not with anything else. In contrast with current passive media such as compact discs, repositories have no externally defined limits on storage capacity so that successive generations of repositories could increase in size while remaining completely compatible with previous systems. Digital works are communicated between repositories using secure coded protocols. Repositories read the rules that apply for a given digital work and follow them. This brings us to the next issue: How do repositories know what the rules are?

Attached Usage Rights

We start with an analogy. When we go to a store to buy a shirt, there are various tags attached to it. One kind of tag is a price tag. If we want to buy the shirt, we must pay the amount on the tag. Other tags give cleaning instructions. They say to wash by hand in cold water or to dry clean only. Still other tags might say something about the style of the shirt or the history of the shirt company.

This is roughly the idea for usage rights on digital works. Digital works come with tags on them. The tags are put there by the creators, publishers, and distributors. The tags describe the usage rights for the digital work -- what can be done with it and what it costs.

There are some important differences too. The first is that the tags are digital and are intended to be read and used by the repository itself. Consumers can also read the tags through the repository's user interface. The tags are written in a machine-readable language and

Best Available Copy

MSI028738

Petitioner Apple Inc. - Exhibit 1012, p. 1103

tell the repository what the rules are for using the work. The tags contain an electronic contract whose terms are enforced by the repository. The next difference is that the tags are not removable. Finally, another difference is that there can be tags attached to the parts of a work. For a shirt, it is as if there were tags on the pockets, tags on the buttons, tags on the collar, tags on the sleeves, and so on. The tags on different parts of a digital work give rights on its different parts. For example, a digital newspaper may have different rights on the local stories, photographs, wireline stories, advertisements, and so on. There can be different rights on different parts of a work.

Suppose that the digital work is a piece of music. A statement describing a right on it might say the following:

> This digital work can be played on a player of type Musica-13B. This right is valid from February 14, 1995 to February 14, 1996. The repository must have a security level of three. No other authorizations are needed. The fee for exercising this right is one cent per minute with a minimum of five cents in the first hour. Usage fees are paid to account 1997-200-567131.

Of course, such a statement internally would not be in English, but it should be in a well-defined language. Here is an example of a machine-readable statement in a usage rights language:

```
Right Code:     Play Player: Musica-13B
Copy Count:     1
Time-Spec:      From 95/02/14 Until: 96/02/14
Access-Spec:    Security-Level: 3
Fee-Spec:       Fee: Metered $0.01 per 0:1:0
                Min: $0.05 per 0/1/0
Account:        1997-200-567131
```

Computer languages are more precise than natural languages and have formal grammars. These grammars and their accompanying semantics define how to interpret each phrase in the language. Thus, computer languages are not at all poetic. They are much less ambiguous and less expressive than natural languages. The sentences of a usage rights language are parts of potential contracts between the creators of digital works and consumers. For sentences about usage rights and fees, clarity and simplicity are just what we want. Interpreting a usage rights language is quite simple. In level

Best Available Copy

MSI028739

Petitioner Apple Inc. - Exhibit 1012, p. 1104

of difficulty, it is more like reading bar codes from packages at the supermarket checkout stand than it is like reading and understanding an English sentence in a story.

Several different kinds of rights are needed in a usage rights language. The rights are mainly concerned with how the work can be transported, how it can be rendered, and whether it can be used in derivative works. There are also special rights concerned with making and restoring backup copies to protect against hardware failure. The easiest way to understand usage rights is to consider some scenarios.

Transferring Digital Works

On a general purpose computer, the copy operation increases the number of copies of a digital work, fails to compensate the work's creator, and infringes copyright. This is what happens on general purpose computers when we copy files for friends. In contrast, a repository never infringes copyright.

Our first scenario illustrates the copy and transfer rights. Suppose that Morgan buys a digital book. Perhaps he buys the digital book at the digital book kiosk at the supermarket. To buy a copy of the book, he exercises a copy right for the book and would pay a fee. Copying the book causes a transaction between the seller's repository and (say) a card-sized repository that Morgan carries with him. Alternatively, he could buy a copy of the digital book from home by phone. In either case, the digital book is delivered electronically by a communications protocol between the vendor's repository and Morgan's repository. At the end of the transaction, Morgan has spent some money and he has a copy of the digital book in his repository, which arrives with all of its usage rights attached. He can now read the digital book with a reader.

Now suppose that Morgan reads the book and is done with it. His friend Andy asks for the book. They plug their repositories together. Morgan exercises the transfer right to move the digital book to Andy's repository. For paper books, it is generally the case that once we have bought a book we can give it away or dispose of it in any way that we please. The same could be true in the usage right for Morgan's digital book. At the end of the transfer transaction, the digital book resides on Andy's repository and not on Morgan's and no

Best Available Copy

MSI028740

Petitioner Apple Inc. - Exhibit 1012, p. 1105

money has been exchanged. Andy can now read the book, but Morgan cannot. The crucial point is that the transfer transaction preserves the number of copies of the digital book.

We now consider a scenario involving a loan right. Again Morgan has a digital book. His friend Ryan wants to borrow the digital book for a week. They plug their repositories together and exercise a loan transaction. While the digital book is loaned out, Morgan cannot use it. Suppose now that Ryan goes off on vacation. He is playing volleyball on the beach thousands of miles away when the week runs out and he has completely forgotten the book. Both repositories have clocks in them. When the loan period runs out, Ryan's repository deactivates its copy. At the same time, Morgan's repository notices that the loan time is up. It marks its temporarily deactivated copy as usable again. Without any action by Morgan or Ryan or even communication between their repositories, the digital book has been returned automatically. If Ryan later tries to access the digital book, he could pay a nominal fee to rent the work or to make his own copy. Again the repositories follow rules. The rules in this case mimic and improve on the rules of loaning for paper books. The ability to automatically return loaned materials could be of wide use in digital libraries.

Rendering Digital Works

To read a digital book you have to be able to see it. To listen to digital music you have to be able to hear it. To enjoy a digital video game, you have to be able to see and hear it. We use the term *render* to mean processing a digital work so that it can be experienced. The term render has several older meanings. In art, it means to represent in a drawing or painting. It also refers to an interpretation of a musical piece.

Like copying, transferring, and loaning, rendering is controlled by usage rights. We distinguish two forms of rendering: playing and printing. To play a work is to send the digital work through some kind of transducer so that we can experience it. The term play is natural for examples like playing music or playing a movie. We also use the term play to refer to displaying part of a book, running a computer program, or running an interactive video game. The term print means to make a possibly digital copy of the work on a media

Best Available Copy

MSI028741

Petitioner Apple Inc. - Exhibit 1012, p. 1106

outside usage rights control. This includes printing on paper or writing a file to an external storage device.

Usage rights create flexibility in marketing digital works. Today when you buy a compact disc at the music store, you pay for the copy and play it for free. The same is true for a book. You buy the book and read it as often as you want. Generally, you aren't supposed to make copies of it. You can give it away.

With digital works in repositories, there is more flexibility. Suppose that Andrea is a teenager. Her mother is at the music store and does not know exactly what music Andrea wants. She transfers a selection of music to her repository. She chooses collections from a half dozen bands that she knows Andrea likes, but she does not need to pay anything for them. In this case, the right to make a copy has no fee. When she gets back home, she transfers the music to Andrea's repository. Later, Andrea checks out the music. Like all repositories, Andrea's home repository has a built-in credit server that can transfer funds electronically. Andrea can listen to short demonstration samples for free; she can listen to arbitrary pieces for twenty-five cents an hour, or she can pay for five years of unlimited playing for $10. Thus, Andrea exercises "pay for play" rather than "pay for copy." If pay for play has an infinite term, then there are no fees for later playing.

The terms and alternatives for usage rights and usage fees are set by the music's creators and distributors. What a consumer gains by this arrangement is flexibility and convenience for trying out different digital works. For example, a consumer could download music to his car repository from a music store using technology similar to a cellular telephone. He could sample music, decide what he likes, and only pay for what he wants to listen to extensively. On the other hand, a consumer could choose to pay for unlimited listening on a copy analogous to the way that music on compact discs is purchased today.

The idea of pay for play may not seem very useful for books. The typical book we may have in mind may be the paperback novel. It is cheap enough so that it does not seem worthwhile accounting for the time to read it. Besides, why should slow readers pay more to read a book than fast readers? On the other hand, consider large expensive reference works like encyclopedias. People do not casually pay out hundreds of dollars for these works. Nor do they tend to read them

Best Available Copy

MSI028742

Petitioner Apple Inc. - Exhibit 1012, p. 1107

from beginning to end. Paying a small fee for each hour of actual use may make it feasible to bring high quality digital encyclopedias into many households that could not otherwise afford them. Purchasers could decide whether to pay by the hour or to pay for large or infinite blocks of usage time.

For another example, consider a digital newspaper. In principle, a digital newspaper could be delivered by any of several ways. It could be bought at the corner newspaper stand. It could be downloaded over the telephone. It could be broadcast by a digital radio station. It could have pay for play usage rights or monthly subscriptions. We consider the issue of printing. Suppose that a particular newspaper is reluctant to allow its customers to make paper copies of the newspaper, even for a fee, out of the fear that enterprising persons would print up enough copies for the entire neighborhood and cut into newspaper circulation. If someone tried to print the newspaper, they would discover that they have no printing rights.

Suppose that a month later customers can print the newspaper without hindrance. In that variation, they can print old news but not new news. The usage right for printing has a date on it that prohibits printing until a month has passed since publication. The publisher may figure that printouts of old news are more like advertisements for the newspaper than threats to circulation. There are many variations in what the publishers may allow or encourage. The rights granted on a newspaper or on photos or whatever could become a further basis for competition among digital newspaper publishers.

Making Derivative Works

Distributors add value to products by advertising, selecting works, and presenting them to consumers. They make a living by performing these functions and they require compensation. Today bookstores and music stores work on a "pay for copy" basis. Today's copy is a hard copy such as a book or a compact disc. If pay for play became popular for digital works, how would distributors make any money? What is needed is a mechanism for paying distributors when a consumer selects pay for play. The mechanism that does this is called a shell. Shells enable distributors to modify rights and to add usage fees.

Best Available Copy

Petitioner Apple Inc. - Exhibit 1012, p. 1108

Shells can be understood by using an analogy with gift boxes of different sizes. A common and fun trick is the idea of putting a present in a small box, wrapping it, and putting that box in a bigger box, wrapping that, and putting it in a bigger box, and so on. There can be gift cards at each level.

In terms of digital works, the boxes correspond to digital containers called shells in the digital work and the gift tags correspond to attached usage rights. Putting a digital work into an empty shell or into a shell containing another digital work is called embedding. Embedding is controlled by an embed usage right.

Consider the following case. Nick has written a digital novel. He determines what he wants to charge per copy of his work and puts usage rights on the work directing that a fee should be paid to his account every time a copy is made. His publisher gets a copy of the book and agrees to publish it. The publisher puts a shell around the digital work directing that when the work is copied, an additional fee is to be paid to the publisher. The publisher may spend money on advertising and help the author in improving the book in various ways. Finally, a bookstore puts an additional shell around the publisher's shell, directing that when the kiosk makes a copy of the book, a fee should be paid to the bookstore. When a customer buys a copy of the work, a fee gets paid to the bookstore, the publisher, and to Nick. This works because the accounting system follows the instructions in every shell containing the copied work.

For another example, consider Paige, a college professor at a business school. Business schools often have classes based on case studies. A course reader is typically a collection of cases. Paige collects the cases of interest for her course as digital works with attached rights. If an interesting case has an extraction right, then Paige can remove it from its digital source. If it has qualified editing rights, Paige can make certain kinds of changes to it. If it has embedding rights, Paige can then add the work to her own collection. At each stage, the continuing rights on the work are controlled by its creator's specifications. Paige can put all of the works she has collected into a shell and add her own usage rights specifications to the shell. When anyone buys a copy of Paige's course reader, fees get paid to the creators of each of the business cases and also to Paige.

Best Available Copy

Petitioner Apple Inc. - Exhibit 1012, p. 1109

It is interesting to compare this process of controlled reuse to the existing practice where one author requests to reprint an article by another. The process of obtaining permissions is tedious and time-consuming, and often relegated to the backroom of publishing houses who do not expect to make much revenue on reprint requests. By lowering the perceived hassle and cost of reuse, usage rights may trigger a substantial increase in the commercial reuse of works.

Consumer-based Distribution

One of the most radical possibilities with digital works is the possibility of *consumer-based distribution*. With ordinary media, consumer copying and sale of works is considered a problem. Creators and publishers get no fee for such copying. In contrast, consider the scenario where Morgan makes a copy of a digital work for his friend Andy. The repositories record the transaction and bill Morgan or Andy for the copy. Depending on how the shells have been set up, fees may be collected for the original store that Morgan bought the work at, the distributor, the publisher and the creator even though none of them were present at the transaction. Every consumer is a potential salesperson.

This example is in radical contrast to the plaint by John Perry Barlow in the quotation at the front of this piece. Digital property can be any place on the planet without knowledge of the creator -- and making money for him or her whenever it is used or copied by a repository anywhere!

Licenses and Tickets

Licenses and tickets are two special kinds of digital works that have direct roles in commerce. Licenses are digital certificates that enable a possessor to exercise certain usage rights. Think of digital licenses as like driver's licenses or pilot's licenses, which authorize someone to drive a car or to fly a plane. Digital licenses authorize someone to exercise certain rights on particular works such as copying them or printing them. Digital tickets are digital certificates that enable a possessor to exercise a right exactly once. Think of digital tickets as like movie tickets or train tickets. Once you have entered the theater or boarded the train, the ticket is punched and cannot be used again.

Best Available Copy

Petitioner Apple Inc. - Exhibit 1012, p. 1110

A digital ticket is punched by a digital ticket agent, which is a program in a repository.

When an author creates a work and writes down the intended usage rights, he or she can arrange that exercising certain rights requires particular licenses or tickets. Digital licenses and tickets are essentially impossible to forge. Usage rights can be exercised in the living rooms or school dormitories anywhere, with full confidence that fees will be collected and tickets and licenses will be required as specified.

Different publishing industries have different crucial problems for which digital licenses and digital tickets offer possible solutions.

In some industries, there are advantages in assuring that digital works are sold only by authorized distributors. For example, suppose that an author of a computer game wants to ensure that his or her game will be sold only through authorized distributors, who agree to advertise, promote, and demonstrate the game. If someone without a distributor's license tries to copy and sell a copy of the game, the repository will refuse the transaction. The author specifies that the right to copy the game can only be exercised on repositories containing a certain distributor's license. By determining who gets distributor's licenses and arranging that the licenses cannot be transferred between repositories without authorization, the author maintains control over the selection of distributors. Digital licenses would also have time limits.

In the music and video industries, the creators want to limit the playing of recordings to home use. In current practice, there is no effective way to enforce this. Trusted entertainment systems could use licenses to distinguish between equipment for home use and equipment for theater or broadcast use. Different digital playing equipment would come with different licenses and have different fees for home and public use. For another example, consider the case where radio transmitters and receivers are all repositories. One station could broadcast a digital work together with a ticket for playing it once for free. Another station could broadcast digital works but require that listeners pay a nominal fee for listening to certain recordings. Trusted systems provide a basis for many different kinds of relationships between broadcasters and the public than are feasible today.

Best Available Copy

MSI028746

Petitioner Apple Inc. - Exhibit 1012, p. 1111

In the book publishing industry, it is common to offer big discounts on books if they have not sold after a period of time. Suppose that a usage right says that a copy of a digital book can be made for no fee if a certain ticket is available. Later on, a book club may offer these tickets for sale -- making it possible for a possessor to get any three digital books for three tickets. Thus, the price of the digital book on sale can be determined later by the price of tickets.

In the computer software industry, it is common that new versions of software are released to fix bugs in the initial versions. These versions are offered for free or for low prices to those who purchased copies of the original software. The problem is in making sure that the upgrade versions are not given to people who did not purchase the original software. Digital tickets offer a solution. Vendors could bundle upgrade tickets with the original works. Consumers could find copies of the upgrade versions of the software anywhere, copying them simply by using their tickets. This approach makes it possible for consumers to upgrade to new versions without necessarily going back to the dealer. Because the digital tickets get punched when they are used, the approach allows exactly one upgrade per original.

Licenses and tickets can be established for diverse categories and purposes, including social purposes. For example, a charity or governmental organization could issue poverty or inner city certificates to qualified people. Socially-conscious publishers could then offer discounts or limited free use to people with such certificates. From a profit perspective, they may assume that such offers will increase their potential base of customers by contributing to public literacy, and that no sales would be made otherwise to these consumers anyway. The same digital license mechanism could provide special rights to certified librarians, researchers, and teachers. Certificates could be dispensed at libraries to allow browsing of works for limited periods of time. One overall infrastructure for digital licenses would suffice.

Foundations of Trust in Repositories

What is it that we want to trust about repositories and what is the basis for such trust? In general, a system is trusted for something if it can be relied on to take responsibility for it.

Best Available Copy

MSI028747

Petitioner Apple Inc. - Exhibit 1012, p. 1112

In the case of digital works on repositories, the requirement for trust is that the repositories will follow the rules about how digital works are used. They must be accountable for the use of works and the money governing those uses. Responsibility is fundamentally an issue of *integrity*. The integrity of repositories has three parts: physical integrity, communications integrity, and behavioral integrity. Physical integrity refers to the soundness of the physical device itself. Communications integrity means roughly that repositories cannot be easily fooled by telling them lies. Behavioral integrity means that repositories have integrity in what they do.

Physical integrity applies both to the repositories and to the protected digital works. One kind of threat to a repository is that someone will pry open the case and thereby gain access to what is stored inside. Different repositories can have different levels of security. A repository that can be compromised with a power drill and screwdriver would have a low security level. A somewhat higher level of physical security would be a system with sensors inside its case that enable it to detect a threat and to erase certain key data. A still higher level of security, suitable perhaps for a real life James Bond, might be a system that self-destructs when it detects that it is under threat, perhaps setting off alarms and phoning for help.

Even the lowest level of security for a repository is much higher than the security for passive media, such as videotapes, compact discs, or computer diskettes. These media record their information out in the open where it can be accessed in principle by any reading device. Passive media cannot detect intrusion or take any kind of protective or evasive action. Repositories, on the other hand, never present data to any device that fails to establish itself as a bonafide and qualified repository. This brings us to communication integrity.

Communications integrity means that repositories cannot be easily fooled if they are connected to illegitimate computer systems that are designed to masquerade as repositories. When repositories connect with each other, they go through a registration process by which they identify themselves to each other and establish their bonafides. Imagine two secret agents, previously unknown to each other, meeting each other by arrangement. What's the secret word? How do I know you are who you say you are? Are we sure that nobody else is listening? These are the kinds of concerns that two

Best Available Copy

MSI028748

Petitioner Apple Inc. - Exhibit 1012, p. 1113

repositories have when they are connected. When they are connected, they put each other through a series of tests intended to weed out impostors and to protect the works that they are trusted with. When registration succeeds, they establish a trusted session.

A few words about how this works are in order. At the heart of the registration process is a security concept called public key encryption, which is a well-known and much studied system for secure and secret communication. In this approach, each repository is given a private key or code which it keeps secret and a public key. These keys are given to a repository when it is manufactured, and they are certified by a highly secure and well-known master repository. When we discuss institutional issues, one of the requirements is that there be an institution that exercises and safeguards the master repositories. Without going into the details, communications integrity is assured because all communications among repositories are in codes that are extremely difficult to break and because compromising one repository does not endanger others. Various provisions can be built into the protocols to detect attempts to tamper with communication and to isolate repositories that have been identified as compromised.

We now come to behavioral integrity. Even if the repositories have not been physically compromised and can prove their identity, how do we know that they will behave properly. In the secret agent analogy, how do we know that the other agent hasn't been turned? The behavior of computers is determined by their programing. The programs used in repositories are thoroughly tested and certified. Such thorough testing of software is a lot of work. What makes the certification task easier for repositories than computers in general is that they have limited functions. They only have to carry out a limited number of very specific operations relating to usage rights, protocol handling, and accounting. Furthermore, there are secure procedures that guarantee that all installed software is secure and not tampered with or modified.

In summary, the physical integrity, communications integrity, and behavioral integrity of a repository are the foundations for trust in it. A repository is designed with an appropriate ability to detect tampering, to detect communications errors, and to ensure certified behavior. These characteristics are easily achievable by computers today. It's just that until now, the value of these attributes has not been appreciated.

Best Available Copy

MSI028749

Petitioner Apple Inc. - Exhibit 1012, p. 1114

The Accountant Inside

When Joe makes a copy of a digital book for Bob and their repositories record the charges, what's to say that the author or publisher would ever get paid? For example, suppose that the repository is a credit-card sized device. Why not just throw it away when a large enough bill accumulates on it? Also, if repositories contain money, what is to prevent theft of that money?

There are many ways to approach these issues. Over the last year there have been a number of field experiments on national computer networks that establish digital checking accounts, digital cash, and network credit cards.

For repositories, there is a substantial advantage in enabling transactions without requiring immediate connections to financial clearing houses by phone or computer network. This is especially relevant for billing tiny amounts where the cost of a phone call or transaction could dwarf the amount of the payment. Monthly connections to a financial clearing house would be more convenient. Once a month all transactions would be reported in a single batch communication and a fresh credit limit could be set for the repository.

Some security measures are appropriate. First, a personal identification code can be required in a session before charges could be accrued. This is akin to the codes people enter at automatic tellers before making a transaction. Secondly, all transactions would be reported by both parties. This does not prevent cheating, but it does require collusion for two people to lose their repositories. Third, the repository itself is likely to be more expensive than a credit card, requiring insurance to replace it. Finally, just as with credit cards today, any party who regularly reports that his repository has been lost or stolen will eventually have difficulty getting replacements or may be forced to use a repository with more stringent security arrangements.

Best Available Copy

MSI028750

Petitioner Apple Inc. - Exhibit 1012, p. 1115

Implications and Institutional Challenges

Stakeholders in digital publication will ultimately come from many industries, walks of life, and all parts of the world. For a variety of reasons, many of these people are used to different versions of copyright law and have different expectations about what is fair. As more kinds of publication become digital, the different expectations about the law and loopholes get mixed together. Usage rights drops right into the middle of the tug of war and may provide a way to manage the evolving situation. Finally, copyrights traditionally last a long time. In creating and shaping institutions around usage rights, we need a perspective about what would serve us well over a long time.

Usage Rights and Copyright Law

Copyright law did not spring full grown from the French Revolution. Over time, there have been various changes. Some notable copyright reforms were made as recently as 1976 and several more are under active discussion now. The cases and situations are too complex to review here in detail, but defining a few terms will bring us to the nub of many of the issues and show why digital usage rights drop right into the middle of it.

Copyright law has provisions for what is called *fair use*. In general, creators and publishers have an interest in limiting what kinds of uses are permitted for free under fair use, so that they can require extra fees for particular uses. Consumers and librarians have an interest in ensuring that certain kinds of use are unencumbered.

Here are some examples. When a person buys a copy of a work, he is permitted to use it in certain ways. For example, it is generally not permitted to make further copies of the work and to sell or give those away. But at least for certain kinds of works and in some contexts, some amount of copying is permitted. For some kinds of works it is permitted to make a copy for personal use. In writing a scholarly review, it is generally permitted to lift some portions of a book and to quote them in a review. Quotations are generally marked in a way that cites the original source.

Best Available Copy

MSI028751

Petitioner Apple Inc. - Exhibit 1012, p. 1116

As new media have become important, the law has evolved to extend the doctrine of fair use. For example, books are not the only works that can be quoted. Over time practices about quoting music or quoting portions of movies have evolved.

Sometimes more than one kind of use is distinguished for a work. An easy example to understand is that of a script for a play. Simple copyright governs the right to make a copy of the script. However, the right to create a stage production from the script and to perform it publicly for a profit is not covered by fair use. A different kind of right called a performance right is required. Similar issues arise for musical scores.

Consider now a recording of music. When we buy a compact disc or cassette tape of music, we expect fair use to include playing it at home. A transmission by a radio station constitutes a public performance. That performance right is not included in the purchase and radio stations are supposed to pay to play such works on the air. If you look at the small print on a compact disc, you will generally find the phrase "all rights reserved" which is the publisher's way of claiming to withhold all rights that are not explicitly granted.

The fair use doctrine arises when possession of a work gives the copy owner the potential to use it in ways that the copy creator thinks are unfair. This is how the usage rights approach lands right in the middle of the situation. Usage rights distinguish between different kinds of uses allowing different fees and requirements for different uses. The approach distinguishes between copy rights, loan rights, transfer rights, play rights, print rights, extract rights, embed rights, editing rights, and several others. These rights can be qualified by requirements for particular digital licenses or tickets and can have different fees. For example, different kinds of digital players could have built-in licenses and codes which determine whether they can be hooked up to public broadcast systems or just to home systems.

In many fair use scenarios, the gap between what is fair use and what is infringement is exacerbated by the fact that there is nothing in between. Fair use costs nothing. Other uses cost fees, and even when the fees are small, the cost and bother of accounting for them is high. In the usage rights approach there can be transactions for nominal amounts of money. This changes the confrontational issue about fee versus free to a practical issue about "how much."

Best Available Copy

MSI028752

Petitioner Apple Inc. - Exhibit 1012, p. 1117

Usage rights also make it possible to grant rights to designated categories of users for social reasons. Digital certificates could be made available to librarians, library users, teachers, students, impoverished people, and so on. Some interest groups have been drafting position papers about fair use in the electronic age, spelling out certain rights that they believe should have no fees, such as the right to print "temporary" paper copies for personal use. Curiously, the context of usage rights changes our conventional assumptions about making copies. For example, the status of printing a copy changes because printing can now be seen as moving moves digital content out of repository control. With usage rights, paper copies have greater potential for unauthorized copying than digital copies.

In summary, the usage rights approach provides repository-mediated contracts to govern the different uses of digital works. It creates specific language for common kinds of use and and their fees. This is a tool never imagined by the creators of copyright law.

It is also a tool apparently never imagined by those who believe that laws governing intellectual property cannot work and cannot be made to work. What copyright law protects is the expression of ideas. As John Perry Barlow put it:

> The point at which this franchise was imposed was that moment when the "word became flesh" by departing the mind of its originator and entering some physical object .... Protecting physical expression had the force of convenience on its side. Copyright worked well because, Gutenberg notwithstanding, it was hard to make a book. ... unlike unbounded words or images, books had material surfaces to which one could attach copyright notices, publishers marques, and price tags. ... [*Wired*, March 1994, page 85]

The attachment of appropriate tags is exactly what repositories do for digital works. These tags proclaim the rights and fees for different uses. They are permanently attached and honored by the trusted systems that enable us to experience the works. Given these tags, the basic concepts of copyright law seem to work just as they are. In this way, an *unconventional* redesign of how our computers work can preserve and even improve the now *conventional* social contract between those who create and those who consume works of the mind.

Best Available Copy

MSI028753

Petitioner Apple Inc. - Exhibit 1012, p. 1118

What Repositories Can and Can't Do

Repositories cannot prevent all unauthorized copying of digital works. No technology can prevent someone from reading a digital book, and then laboriously typing the words verbatim at a keyboard. A plagiarizer can even use technological aids. For example, a plagiarizer may aim a television camera at a display and then feed the output of a camera into a computer that could optically recognize the text. Digitally published music could be played out a repository speaker and then recorded through a microphone. Although recordings of interactive works such as interactive video games are of little use, if a work can be experienced by the human senses a recording of it can be made. Trusted systems simply inhibit the unauthorized making of *perfect digital* copies.

When performances of digital works are re-recorded outside of a repository two things can happen. The first is the loss of fidelity, familiar to anyone who has made cassette tape copies from a compact disk. If a digital work is re-recorded outside of a repository, then the first-generation copy will not be perfect although it may be very good. Subsequent generations of uncontrolled copies would be as good as the first generation copy. The second thing that can happen is that identification information can be hidden when an original is played or printed. This information can be invisible and inaudible to the human senses but detectable by special equipment. In the event that unauthorized copying is carried to such a degree as to justify intervention, such identification information could be used to trace back to the repository where the copy was made.

In summary, repositories — like all technology — are imperfect. What they can do is make it much easier to be honest and easier for creators to make a living.

So what are the expected social effects of repositories? In the long term, more digital works will be created because more potential authors will see a possibility of making a living creating them. This is the main effect – letting loose the light.

There are other predictable effects. With usage rights, electronic distribution of digital works will be much more viable than it is now. Using computer networks and the phone system, consumers can take

Best Available Copy

MSI028754

Petitioner Apple Inc. - Exhibit 1012, p. 1119

immediate delivery of digital works from distributors that are located at great distances. Many distributors of digital works, such as digital bookstores, digital libraries, and digital music stores will serve large geographic areas. For a consumer, digital distribution will provide a wide range of potential distributors and also the convenience of being able to access or purchase digital works quickly, at a moment's notice, at any time of the day.

What kinds of works will first be distributed on repositories? The answer to this question is not known yet and there are a lot of factors that bear on it. Repositories will be adapted first in those areas where they can solve a pressing problem. In the music industry, publishers have successfully lobbied against the manufacturing of devices that can make digital recordings. There may be an opportunity in this area, if the trusted systems give advantages to both consumers and publishers.

The opportunity to introduce repositories increases when other technological changes are leading to changes anyway. For example, repositories will become more viable for television when *digital* television offers fidelity that cannot be captured by the today's videotape formats.

Usage rights remove many barriers to self-publishing and it is likely that many creators of digital works will self-publish. They may offer their works for sale on computer networks and reap the benefits of consumer-based distribution.

Self-publishing does not mean the end of a role for publishers for digital works. Quality control is part of the value added by publishers. Publishers often help to improve the quality of the works that they publish. They also provide brand names that we recognize as indicative of quality and style. Since this kind of warranting of works will continue to be important, publishers have an enduring role.

New publishers will also appear. People who review works may also put together collections and provide a function similar to brand names by giving their appraisals to works that they carry. The net effect may be increased opportunities for new publishers, so that the popular taste may be influenced by a broader set of "middlemen" than it is now.

Best Available Copy

MSI028755

Petitioner Apple Inc. - Exhibit 1012, p. 1120

The Digital Melting Pot

The metaphor of the melting pot is often used to describe the culture of the United States, where people from lands all over the world live together. It refers to the way that America blends cultures from many places.

Digital publishing is creating a melting pot of genres. Books can be published digitally and so can newspapers, musical recordings, videos, video games, and computer software. Multimedia is a term that refers to the inclusion of multiple kinds of media in a single production, such as the mixing of sound, pictures, and text. But the blending of forms is not like the blending of water and oil where the constituents separate out again. The blending is creating new forms. There are interactive movies and interactive travel guides. There are annotated presentations of plays that include scripts, multiple performances, and reviews all in a single hyper-linked work.

Some currently distinct genres may be evolving to the same digital, interactive form. For example, the ultimate form of the digital news program and the ultimate form of the digital newspaper may be the same. Both forms may evolve to become a digital work, broadcast in the air or by cable several times a day, and laid out on multiple electronic pages. The pages will contain short movies with anchors giving sound bytes. Both forms may contain animated advertisements and infomercials. Both versions may be experienced as an interactive work playable on color screens with high fidelity sound. Today's newspapers and television news programs are the present day ancestors of the future interactive news experience.

As publication forms blend together, what is to become of the provisions of copyright law and fair use, which have different provisions for today's newspapers, videos, and computer programs? Some distinctions in today's laws will probably not be sustainable in the evolving digital forms.

Public discussion about intellectual property and digital networks was invited at a public hearing in Washington in the Fall of 1993 called by Bruce Lehman, head of the U.S. Patent Office. The hearing was to discuss intellectual property and copyright issues for the national information infrastructure. This is the so-called

Best Available Copy

MSI028756

Petitioner Apple Inc. - Exhibit 1012, p. 1121

"Information Superhighway," that has been in the press. At this meeting there were representatives of the cable industry sitting down the aisle from small town librarians and civil libertarians. Representatives from the music industry were near representatives from the computer hardware and software industries. These representatives were all aware that their own businesses were becoming more involved in digital publication. They were also aware that the new media were leading to new forms and genres that confound the issues of fair use.

These representatives found that they had very different assumptions about appropriate means for protecting intellectual property. For example, the music industry uses statistical sampling of radio station broadcasts to check that royalties are properly paid. The computer industry has no effective organization to check on copyright infringements. The paper-based publishing industries mostly use the copyright clearance center, which expedites the payment for copying fees. Each industry knows the conditions of its own business and can see that the conditions for the other businesses are different. They suspect that as media merge there will be new dominant ways of doing business. Whatever the new rules and ways of business will be, they want to be sure that their business can thrive.

Planning for the Generations

The laws governing the length of a copyright have changed several times. Since 1978 the copyright for a work lasts for the lifetime of the creator plus fifty years. Thus, the total period of a copyright may easily amount to a hundred years for a single work. In our fast paced society, we do not often design institutions to last for hundreds of years.

And yet the long view is not unheard of. When we set aside park lands in the public trust, we are planning for the long term. Such consciousness of time is akin to the consciousness expressed by Native Americans who talked about planning for seven generations. Three of the generations are of the past: the parents, grandparents, and great-grandparents. One generation makes the decision. And three generations are of the future: the children, grandchildren, and great-grandchildren. Adapting this perspective can help create an institution that has a lasting value for humankind.

Best Available Copy

MSI028757

Petitioner Apple Inc. - Exhibit 1012, p. 1122

There are many stakeholders in digital publishing. These include consumers, authors, publishers, distributors, platform vendors, financial institutions, and governments.

The approach based on usage rights presumes that there is a widely used usage rights language, compatible platforms from multiple vendors, and agreement about what the usage rights mean. The approach and particular kinds of rights will need to evolve over time. The security of the approach presumes that there is an authoritative institution that issues certain digital certificates warranting that certain platforms and software uphold the meaning of the usage rights. We call it the Digital Property Trust (DPT). Although some initial funding would be needed, the DPT could eventually fund its activities from a small tithe on commercial repository transactions or by renewable licenses on platforms and software.

Although planning for a DPT is tentative at this time, a few observations about its role and structure are appropriate. For example, there are many different kinds of social and international organizations with their own bases of authority, such as government organizations, banking organizations, political organizations, and standards organizations. It is important that these different organizations should be able to establish and publish their own digital certificates, publishers should be able to establish and issue their own kinds of digital licenses, and authors and distributors ought to be able to set whatever usage rights and fees they please. The role of the DPT is in promoting widespread commerce in digital works. To this end, it would certify and maintain the security of trusted systems and establish a common operational terminology of usage rights that meets social and economic needs.

The long term vision of the DPT requires the wisdom and organization to appropriately balance interest groups. The DPT would need to be even handed in its treatment of all hardware providers, software providers, and publishers. This evenhandedness is challenging because the certification process for hardware and software requires detailed knowledge of exactly how products work. At the same time, the DPT would need the representation and support of the more powerful vendors and publishers or its decisions will carry little weight.

Best Available Copy

MSI028758

Petitioner Apple Inc. - Exhibit 1012, p. 1123

Repositories offer advantages for both publishers and consumers. Consumers may find that they have ready, quick, and cheap access to all kinds of digital works, delivered by phone or computer network, any time of the day. Creators may find that consumer-based distribution creates a large new distribution channel. Anyone who buys a digital work can also make a copy and sell it, automatically routing compensation to its creators. The simple provisions for extracting, editing, and embedding small portions of digital works opens the door to much creative sampling and reuse of multimedia materials. As creators and publishers find safety and market reach in digital publishing, there could be a flowering of new works and newly available old works in digital form. As repositories provide the flexible means for sharing, loaning, and renting digital works, consumers may find that digital access gives them easy and affordable access to the light — wonderful creations from all kinds of people and all kinds of places that they would otherwise not experience.

Today's computers and installed software are not programmed to honor usage rights. This is not a fatal flaw. The time between generations of equipment and software is two to three years for computers and perhaps ten years for home entertainment devices. In some cases, existing equipment could be upgraded to honor usage rights. These generation times are but a blink of the eye in the lifetime of a typical copyright. Furthermore, there are substantial legal and cultural differences around the world in attitudes about intellectual property. The time needed to develop worldwide understandings and agreement may be longer than the generation times of computer equipment or home entertainment equipment.

Repositories provide a way to let loose the light, for present and future generations. But there are many institutional challenges. The many stakeholders need to work together to enable the changes. The popular adoption of repositories will start from a beginning. What are the publishing niches in which the trusted systems approach can start first? Such niches may provide the sparks from which commercial digital publishing could really ignite.

Best Available Copy

Petitioner Apple Inc. - Exhibit 1012, p. 1124

credit server. A secure program and database in a repository that keeps track of the fees owed for the use of digital works. Typically, a credit server would have a credit limit and would need to be connected to a financial clearing house regularly so that funds could be transferred to pay the bills. Like a bank automatic teller machine, a credit server would typically require the entering of a personal code before it could be used.

digital certificate. A digital document attesting to the truth of something. Every repository has a digital certificate that certifies its identity as a trusted system and presents its public key and security level. In general, digital certificates cannot be transferred between repositories except by specially authorized repositories. Digital certificates are encrypted in the private key of a well-known repository. This makes digital certificates difficult to forge and provides a simple means of testing their authenticity, by decrypting them using the public key.

Digital Property Trust (DPT). The DPT would be an organization that would act to ensure the health of digital publishing, promoting a lively international commerce in digital works. In conjunction with consumers, publishers, creators, platform vendors it would set the standard for the evolution of the usage rights language and issue digital certificates to conforming platforms. It would maintain the master repositories and perhaps have an insurance function relating to security and financial transactions.

digital license. A digital certificate that identifies the bearer repository as licensed and thereby authorized for carrying out certain rights. For example, certain digital works may require that copies of a work cannot be made and sold unless the repository contains a particular digital distributor's license.

digital ticket. A digital certificate that can be used once to authorize a particular transaction. For example, a digital work may contain an upgrade ticket that authorizes the replacement of the digital work by an updated version. When digital tickets are used, they are punched by a digital ticket agent. A ticket cannot be used after it has been punched.

Best Available Copy

Petitioner Apple Inc. - Exhibit 1012, p. 1125

digital work. A digital work is any work that can be represented in digital form. For example, the work could be a document like a book, magazine or newspaper. It could also be a recording of music or a movie. It could be a computer game or any computer program. Sometimes the word software is used in a general sense to mean a digital work.

encryption. A process of encoding a digital work by a secret code to render it unusable to someone without the code. Coding a work is called encryption and decoding a work to restore it to usable form is called decryption. The preferred method of encoding is public key encryption. In public key encryption, there is a pair of keys including a public key and a private key. If one of these keys is used to encrypt a work, the other can be used to decrypt it.

master repository. A master repository is a very high level repository with the highest security level. Master repositories would be kept by the Digital Property Trust and would be used to issue certificates. The public keys of the master repositories would be given to all trusted systems when they are manufactured, to enable them to exchange and identify authentic digital certificates in their transactions with other repositories.

repository. The term repository refers to any trusted system used for storing and playing digital works. For example, repositories could be portable entertainment devices, laptop reading devices, personal computers, credit-card sized devices, or devices that fit into home entertainment for controlling digital television or music. Repositories store digital works together with their usage rights. They include credit servers for keeping track of the fees for uses.

security level. To protect digital works against unauthorized uses, repositories need different degrees of physical security. Repositories for handling extremely valuable works need greater security than ones for ordinary and portable use. The term security level refers to a sequence of levels ranging from low security to very high security.

shell. A shell is a kind of digital container for storing digital works in the file system of a repository. Shells can contain both digital works and other shells. Tags describing usage rights and fees can be attached to digital works and also to shells. When someone asks a repository to use a digital work, the repository checks the rights and fees on the digital work and on the shells in which it is contained.

Best Available Copy

MSI028761

Petitioner Apple Inc. - Exhibit 1012, p. 1126

trusted system. A trusted system is a system that can be relied on to follow certain rules. In the context of digital works, a repository is a trusted system that follows established rules governing the uses and fees for digital works. Digital works have tags on them which describe uses and fees in a usage rights language. Trusted systems are supposed to follow the instructions on those tags infallibly.

usage right. A usage right is a specification of a contract to use a digital work in a certain way. Usage rights fall into several natural categories. For example, transport rights include rights to copy, transfer, or loan. Render rights include playing and printing. Derivative work rights include rights to extract, embed, and edit. Usage rights are represented in a formal language that can be precisely interpreted by repositories. They can also be displayed to a consumer in a variety of simple ways appropriate for the situation.

usage rights transaction. A transaction refers to a series of actions that are treated as a unit. For example, in electronic banking, a transfer of money from one account to another is a transaction which credits one account with the money at the same time that it debits the other account. Each usage right defines a particular transaction that can be carried out. For example, a usage right to copy a digital work causes a new copy to be made and a credit server to make a record of the required payments.

Best Available Copy

MSI028762

Petitioner Apple Inc. - Exhibit 1012, p. 1127

THIS PAGE BLANK (USPTO)

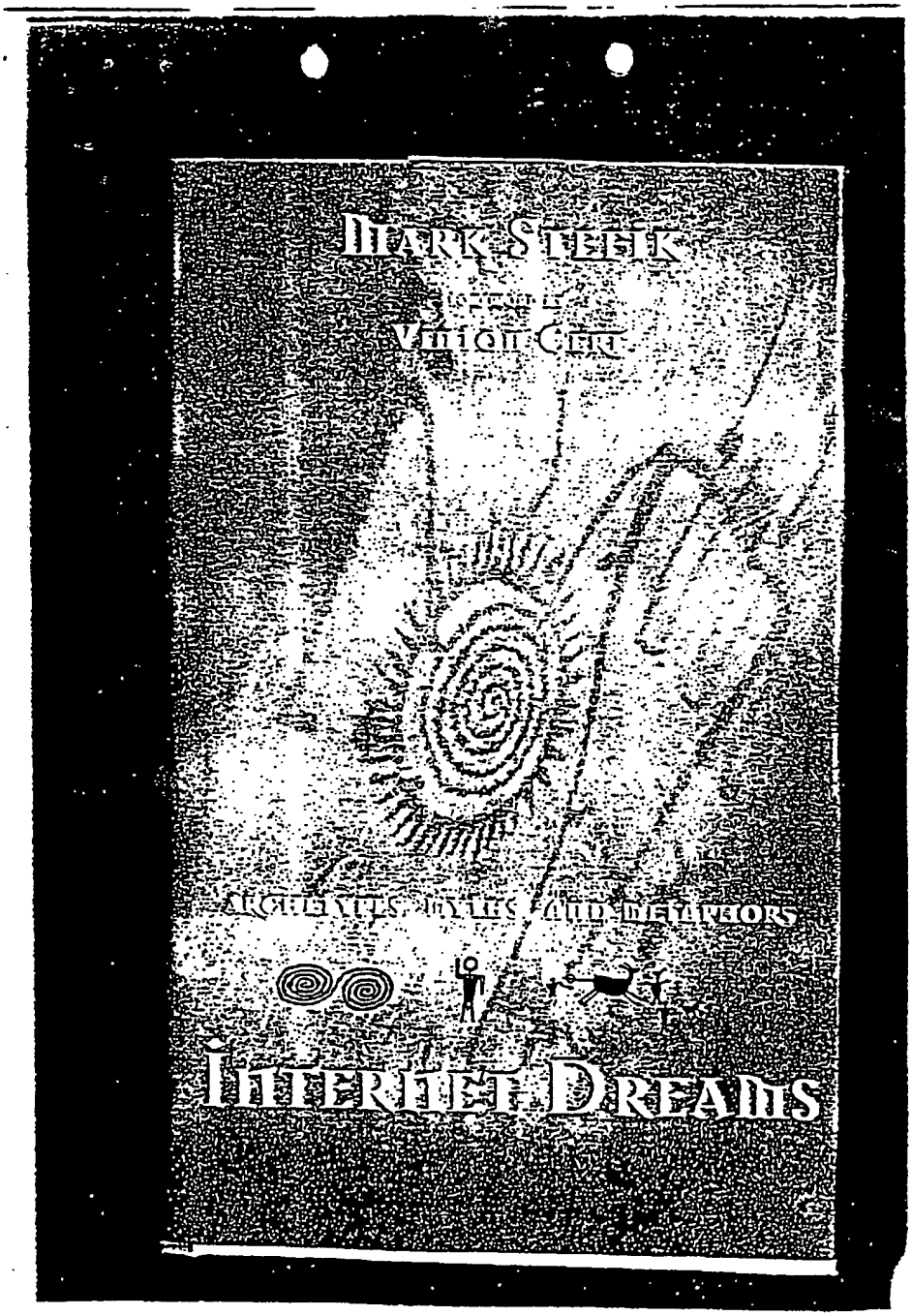
Best Available Copy

Author Biography

Mark Stefik is a principal scientist in the Information Systems and Technology Laboratory at the Xerox Palo Alto Research Center. He received his doctorate in Computer Science at Stanford University in 1980. With other colleagues at Xerox PARC, he has filed several patent applications in the area of usage rights and trusted systems for digital documents.

Best Available Copy

Best Available Copy



MSI028764

5

International
Federation of
Reproduction
Rights
Organisations

ifrro

METERING TECHNOLOGIES FOR DIGITAL INTELLECTUAL PROPERTY

A Report to the
International Federation of Reproduction Rights Organisations

Prepared by
Dr. Robert Weber, Principal
Northeast Consulting Resources, Inc.
Boston, MA USA

Commissioned by the
Committee on New Technologies

October 1994

International
Federation of
Reproduction
Rights
Organisations

The tidal waves of digital information uses are rolling into the safe harbors of copyright. Some say the harbors cannot continue to shelter information creators and vendors, and that the electronic environment requires a whole new legal regime. Others, however, predict that authors and publishers will simply sail into the wind and discover new lands of opportunity.

As the debate ebbs and flows among creators, vendors, users, governments, and experts, IFRRO has an important navigational role to play. Its members' extensive experience in the development of collective licensing systems combined with IFRRO's responsibility to facilitate the international flow of copyright rights and royalties are powerful incentives toward a major role in network licensing for RROs. But in order to be effective, IFRRO must be fully informed about the technological developments that will support its members' collective licensing programs.

IFRRO commissioned its New Technologies Committee in 1992 "to explore options and methods of collective administration in new technologies by RROs". The Committee's initial report, presented in Lugano in October, 1993, included, among others, a recommendation that IFRRO seek the assistance of an information technology professional who could, on an annual basis, provide IFRRO with a report on the state of various technological developments within the field of rights management. In May of 1994 the IFRRO Board of Directors authorized the Committee Chairman to contract with Dr. Robert Weber of Northeast Consulting Resources, Inc. (NCRI) to prepare such a summary.

NCRI is a Boston-based consulting firm that focuses on the intersection of information technology and strategic planning, with particular emphasis on identification of areas in which technology can help organizations achieve strategic goals. An NCRI principal, Dr. Weber has particular expertise in the areas of digital publishing and distribution via electronic networks. Prior to joining NCRI, he held a variety of positions in the Office of Information Technology at Harvard University.

This report focuses on commercially developed encryption and metering technologies, the two most promising technologies for copyright management. The New Technologies Committee commends Dr. Weber's comprehensive review of these technologies to the IFRRO membership with the expectation that all will find this information both informative and useful as we work together to meet the copyright challenges of national and global information networks.

Joseph S. Alen
Chairman
New Technologies Committee

Contact Information

Dr. Robert Weber
Principal
Northeast Consulting Resources, Inc.
One Liberty Square, 11th Floor
Boston, MA 02109-4825
U.S.A.
Voice: +1 (617) 654-0621
FAX: +1 (617) 654-0654
E-mail: weber@ncri.com
weber@world.std.com

Joseph S. Alen, Chairman
Committee on New Technologies
International Federation of Reproduction Rights Organisations
c/o Copyright Clearance Center
222 Rosewood Drive
Danvers, MA 01923
U.S.A.
Voice: +1 (508) 750-8400
FAX: +1 (508) 750-4343
E-mail: jalen@copyright.com

Paul Greenwood, General Secretary
International Federation of Reproduction Rights Organisations
Goethestrasse 49
80336 Munich
Germany
Voice: +4989514120
FAX: +49895141258

TABLE OF CONTENTS

1 INTRODUCTION ____ 1

2 ENABLERS OF METERING ____ 4

2.1 Changes In Information Use and Information Technology ____ 4

2.2 The Internet ____ 5

2.3 Encryption Technology ____ 6

2.4 Changes in Publishing Paradigms ____ 8

2.4.1 Publish On Demand Paradigms ____ 9

2.4.2 Multimedia Publishing ____ 9

2.4.3 Electronic Rights Are Revalued Upwards ____ 9

3 METERING TECHNOLOGIES ____ 11

3.1 CD-MAX, Inc. ____ 11

3.2 Electronic Publishing Resources, Inc. ____ 13

3.3 Infosafe Systems, Inc. ____ 16

3.4 Wave Systems Corporation ____ 19

4 MOVING FORWARD ____ 25

4.1 Publishers and Other Rightsholders ____ 25

4.1.1 New Business Models ____ 25

4.1.2. Managing Rights Proactively ____ 26

4.2 Information Consumers ____ 26

4.2.1 Will User's Accept Transaction Pricing? ____ 27

4.2.2 Corporate Policies Regarding Information Use ____ 27

4.3 Unresolved Issues ____ 28

4.3.1 Privacy Concerns ____ 28

4.3.2 U.S. Versus Global Perspectives ____ 29

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1134

1 INTRODUCTION

Powerful personal computers and global data communications networks have raised troubling issues concerning the protection of intellectual property in digital form, the collection of royalties for authorized use, and the distribution of those royalties to rightsholders. Advanced encryption technologies feature new ways to protect digital information against most forms of infringement and unauthorized use. These same encryption technologies, combined with other computer systems, will collect royalties and then return those royalties to rightsholders.

The principal purpose of this report is to provide IFRRO members and interested parties with a brief overview of emerging technologies for content control, usage metering, payments, and royalty distribution. Numerous companies and individuals are exploring metering technologies. This report does not review the numerous academic pilot projects. Nor does it address metering technologies only incorporated in the products of a single company. Those approaches are not likely to dominate the information marketplace.

Instead, this report addresses generic metering product technologies, or proposed technical architectures for metering, that have some chance of being widely adopted. This report discusses in some detail the products of four companies who are bringing to market metering technologies that have the potential to become widely adopted: CD-MAX, Inc., Electronic Publishing Resources, Inc., Infosafe Systems, Inc., and Wave Systems Corporation.

As IFRRO's very existence demonstrates, problems related to intellectual property protection are certainly global. However, this report focuses on technologies now being deployed principally in the United States. This focus is intentional and reflects the state and distribution of certain technologies destined to play important roles in the protection of intellectual property. (Also, in a few cases, developers in countries other than the USA were unwilling to disclose more than general intentions and directions.) These enabling technologies include advances in encryption technologies, advanced telecommunications technologies generally, and the significantly greater penetration of the Internet in the United States than elsewhere (although Europe and some Pacific Rim locations are catching up quickly, for example, Singapore).

What is metering? A useful first metaphor is that of cryptographic envelopes. Authors, publishers, information repackagers, and other rightsholders put content in these "envelopes" by adding certain metering control information and then encrypting the content and metering information together in a single package or envelope. In the most advanced metering systems, the control information says who is authorized to use the information, gives the prices for various uses, indicates credit card and other billing information, and indicates the clearinghouse that passes usage and financial information back to rightsholders. In some instances, the clearinghouse function is performed by the meter maker or publisher; in other cases, it will be performed by third parties.

The most advanced metering technologies will permit rightsholders to enable/disable and charge differently for a range of operations including:

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1135

- Searching. The user's application program can search the protected information to locate those portions meeting the search criteria. One would generally expect rightsholders not to charge for searching operations per se, since users typically want to do other operations once the search is complete.

- Browsing. This is the operation where a single user reads on a computer screen the content of interest. Some of what is read might have been identified by a preceding search. Browsing might also be an essential part of a multimedia application in which navigation through the content is via hypertext "buttons" or pointers rather than through formal search mechanisms. Rightsholders may or may not want to charge for browsing. If the content is generally printed after browsing, then perhaps the print operation is where charging takes place. On the other hand, browsing multimedia applications may be where value is added from the consumer's point of view and maybe this is where charging takes place.

- Modifying. In many circumstances, rightsholders will want to ensure the integrity of their information by preventing modification. In other circumstances, modifications could be enabled and charging invoked.

- Copying. There are many forms of copying. For example, making copies for backup purposes may be permitted. Other forms of copying include transmitting and excerpting.

- Transmitting. Suppose a user wants to send a copy of the information to someone else who also has the same metering technology in his/her computer. Some rightsholders might want to charge either the sender (less likely), or receiver (more likely) when the cryptographic envelope is opened for the first time, since there may be some administrative overhead in making the connection between this envelope and its contents and the usage tracking and billing system. Still, other rightsholders may elect to set the charge at zero on the theory that the recipient of the information will generate additional revenue through use by users other than the original recipient.

- Excerpting. What happens, for example, when a person wants to take a couple of paragraphs out of a document and include them as quoted material in a memo to colleagues (who also have installed the metering system)? Some metering systems (and rightsholders) will allow excerpting. In the most sophisticated metering systems, the metering control information and charging algorithms that applied to the whole document will also be applied to excerpts. This is a feature known as "property inheritance": whatever applies to the whole applies to its parts or applies to other, identical wholes. Also, metering systems differ regarding the smallest excerpt that can be tracked. Some systems can track down to a single character if that level of granularity should be desired by rightsholders.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1136

- Printing. Most rightsholders will want to charge for printing, probably on a price per page basis. Some rightsholders will set relatively high fees in order to discourage printing in the belief that, once printed, the page or pages might not be printed again. Additional copies might then be created through photocopying. Other rightsholders will set relatively low printing fees in order to encourage printing from the electronic source as a substitute for photocopying the printed pages.

- Exporting. Perhaps the highest fees will be those for exporting information beyond the boundaries of the metering system since the rightsholder would lose effective control over the exported materials. Alternatively, rightsholders can prohibit export entirely in order to ensure continuing control and revenue.

These capabilities lend themselves to a rich diversity of control and charging schemes and of publishing business models. Publishers, authors, and other rightsholders could, for example, grant perpetual licenses for a one-time fee, or they could license unlimited use (but no export) for some period of time, say a year. After the initial subscription period, users would have to pay another fee and in exchange would receive a new decryption key good for another licensing period. What seems more likely is that rightsholders will want to count various small events, the meter "clicks," to understand in detail how their information is being used, by whom, and then to charge accordingly.

Metering technologies are evolving rapidly. Consequently, this document will be inaccurate shortly after publication, and thus the information presented should not be construed as definitive in any sense. Instead, this report provides a framework that interested individuals and organizations can use as one starting point in their efforts to better understand metering. The rest of this report is organized as follows:

The next chapter answers the question, "Why is metering becoming a hot issue just now?" by reviewing key enablers in publishing, information use, and content control and metering technologies.

This report ignores limited pilot programs, some of those in academic institutions, and metering technologies incorporated only in products of a single company. We have instead chosen to highlight as examples of metering technology those companies offering products that have some potential to become widely used in a variety of settings. Consequently, this report focuses on the efforts of commercial companies with products already in the marketplace or on those who have publicly announced their intention to introduce metering systems soon. Chapter 3 reviews the metering systems and technologies of four companies: CD-MAX, Inc., Electronic Publishing Resources, Inc., Infosafe Systems, Inc., and Wave Systems, Inc.

Metering technologies will be adopted on a wide scale over the next two to three to five years in the United States. Chapter 4 discusses issues that publishers, rightsholders, and information consumers should take into account as these new technologies are deployed. This chapter also addresses several unresolved issues, such as privacy concerns and the generalizability of methods developed in the USA.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1137

2 ENABLERS OF METERING

Development and deployment of new metering technologies builds on fundamental changes in publishing paradigms, computing and communications, and information use. This chapter addresses the question, "Why has metering become a 'hot topic' at this point in time?"

2.1 Changes In Information Use and Information Technology

Chief among the changes in information use is the trend toward the personalization of information. Especially in science, medicine, engineering, the professions, business, finance, and education, users of information see value in receiving and paying for information in the right "chunks." Although it is becoming a cliché, the notion of "just-in-time" information is also relevant here too.

In industrial organizations, for example, leading edge companies want the right chunks of information delivered over wireless communications to hand-held devices on the shop floor. This information might be relevant "pages" from technical manuals for a device being built or repaired or might be information on certain toxic chemicals, their proper handling, and procedures for cleaning up hazardous spills. The technical manuals may be developed internally or provided by a publisher or information distributor. The toxic chemical information might come from an external information supplier on an "as needed" basis.

Another example might be a product manager in a technology company who wishes to write a memo; the memo includes market data from a consulting firm, parts of two other memos prepared by him/her or by his/her staff, his/her own additional comments, and two articles appended from the scientific literature. This example illustrates the need in most organizations to be able to seamlessly integrate external and internal information on the desktop. Thus, the ideal metering technologies would permit such integration while exercising control over the external information, tracking usage, and at some point providing that usage information to the appropriate billing system.

The personalization of information reflects not only changes in information use but changes in computing and communications technologies utilized by businesses as well. When the personal computer was first deployed in business, the key benefit was increases in personal productivity through use of what became common office applications, such as word processing, spreadsheets, and presentation graphics. Small groups of people with common tasks then wanted to share information and resources, such as departmental printers. Computer networks and client/server computing have become critical technologies that improve work-group productivity. (Client/server computing entails dividing an application in pieces so that part of it operates on a computer shared by several people, the server, and other parts operate on the individual's computer, the client; this scheme allows individuals to share information and computing resources more efficiently.)

Today, many businesses are leveraging their substantial investments in computer networks and client/server computing to create company-wide applications. These

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1138

are mission critical applications, such as work in progress management in manufacturing companies where the manufacturing steps are complex and may be performed at different locations as an item moves through the manufacturing process.

Thus, the extensive use of computer networks to tie all parts of companies together, to provide the "glue," enables information sharing and distribution on a company-wide scale. The tools now being deployed for information sharing and distribution help fuel demand for both information in chunks and for the integration of internal and external information on the desktop. Metering technology, which is compatible with data networks and client/server computing, will facilitate attainment of this vision while protecting rightsholders.

2.2 The Internet

At the same time businesses have been making substantial investments in computing and communications technologies, the Internet has been experiencing fantastic, unheard of growth. The Internet consists of more than 2.2 million computers in at least 74 to 90+ (accounts differ) countries. By some accounts, 10 to as many as 20 million people are reachable via the Internet.

This network is growing exponentially (that is, the rate of growth is itself increasing). Some indicators of this growth are:

- Traffic on the National Science Foundation network portion of the U.S. Internet has been growing at 6% per month compounded, or doubling every year. This is an indicator of growing research and education use.
- The number of names registered in the U.S. "commercial" domain (15,384 on June 15, 1994) is growing at about 10% per month compounded, or about 214% per year (or tripling every year). This is a crude indicator of U.S. business interests in the Internet.
- The number of networks assigned Internet addresses (57,366 as of February 14, 1994) is growing at 12% a month compounded, or about 290% per year (or nearly quadrupling every year). This is a measure of the growth in the number of computers that could be connected to the Internet (not all network addresses are used and not all networks are connected to the Internet).
- There are more networks with Internet addresses inside than outside the U.S.; however, networks with Internet addresses outside the U.S. are growing more rapidly than inside the U.S. (this reflects a smaller base and late adoption). The projected crossover point is 1996. This trend reflects the increasing globalization of the Internet.
- The number of World Wide Web servers (a globally distributed information system on the Internet) is doubling every three months or so. In March/April 1994, there were approximately

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1139

1,400 Web servers compared with nearly 3,200 near the beginning of July. This is an indicator of growth in organizations providing information via the Internet.

This explosive growth is fueled by the convergence of several key factors:

- The growth of networks within companies creates a constituency for the Internet that can speak the same networking "language" as the Internet.
- The costs of computing and network components are declining so that networking has become readily available to businesses of all sizes and to individuals.
- A critical mass of Internet capable companies and individuals who wish to communicate now exists. In short, there is someone to talk to. Increasingly, one sees Internet addresses in newspaper advertising, business cards, and corporate communications. Intel just started publication of its anonymous FTP addresses, for example.
- Fast growth of information available on the Internet, both public domain and fee-based. In addition to the large on-line services companies (for example, Mead Data Central, Dialog, CompuServe, and Dow Jones News/Retrieval), there are legions of smaller organizations and individuals providing information via the Internet.
- An emerging consensus around the standards of the Internet that determine how computers "talk" with each other as indicated by recent endorsements and adoptions of Internet standards by important vendors such as Microsoft, Novell, IBM, and Banyan.

Indeed, the Internet is so successful that some worry about future instabilities resulting from rapidly increasing complexity and size.

As metering technologies are deployed, information providers will make use of the Internet to distribute their information in protected forms and to collect usage and billing data. But deployment of metering technologies will not depend exclusively on the Internet either. Rather, the encryption technologies upon which metering is based will be useful when information is sold to individuals or organizations regardless of whether they use any network or use other distribution media such as CD-ROM or floppy disk.

2.3 Encryption Technology

Very strong public key encryption technologies were invented in the mid-1970s. These methods involve generating a pair of encryption keys with special properties. One key is made public, the other kept secret by the key owner. One person (or computer) wanting to communicate with another person (or computer) first gets that person's public key and encrypts a message with it. This encrypted message can be

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1140

decrypted only by the receiver's private key, which is never made public and carefully guarded (Figure 2.1).

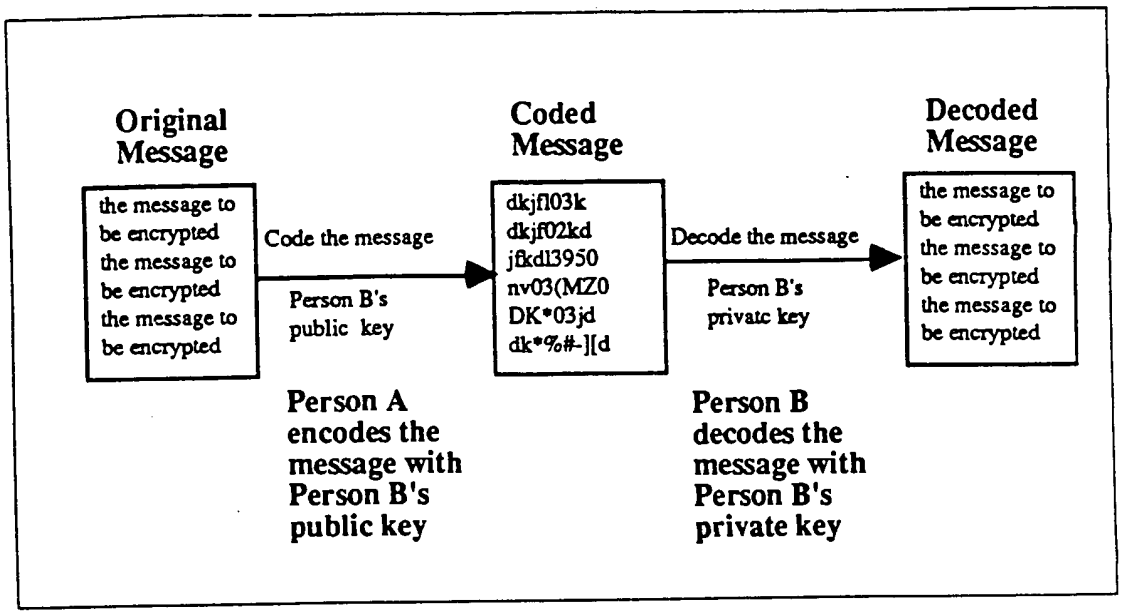


Figure 2.1 Public Key Encryption Process

Among the advantages of public key technology are that it eliminates serious problems related to safe key distribution. If there were only one key and that single key could both encrypt and decrypt a message, then it might be unsafe to transmit that key to the person with whom you want to communicate (Figure 2.2). Sending a public key entails no such problems.

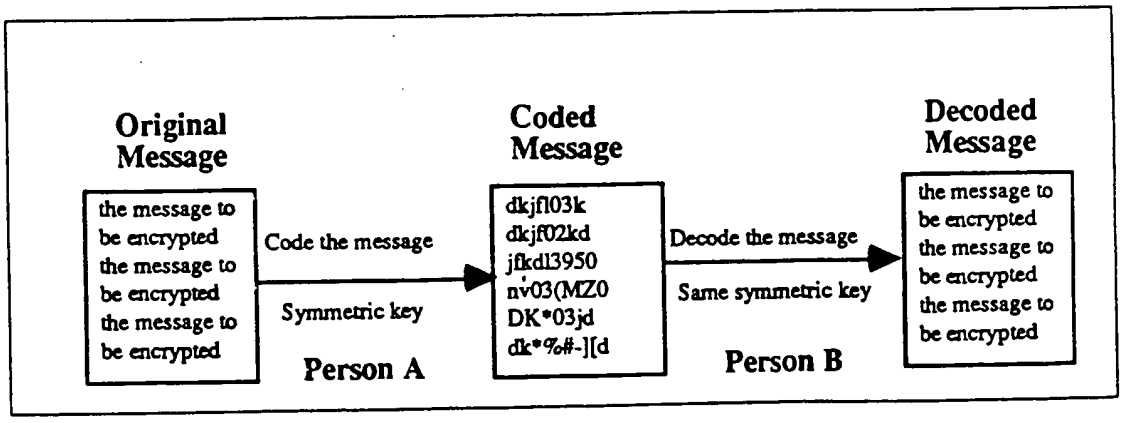


Figure 2.2 Secret Symmetric Key Encryption Process

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1141

Public key algorithms for actually encrypting information are relatively expensive in computational resources. For large amounts of information, so-called "bulk encryption ciphers" are more practical. A common bulk encryption cipher is the Digital Encryption Standard or DES. DES is a symmetric key cipher. The same key is used to encrypt and decrypt the text. Thus, a common use of the public key technology is to exchange DES keys safely.

Besides the safe exchange of encryption keys, some other uses of public key encryption are incorporated in the most sophisticated information control and metering technologies. These are digital signatures, user and computer authentication, and digital time stamps.

A digital signature does two things. First, it is an integrity guarantee. When the incoming message is decrypted, some calculations are performed in such a way that the receiver can tell immediately if the contents of the message have been tampered with. Second, a digital signature allows the receiver of the message to determine whether the person claiming to be the sender of the message is indeed the sender.

The same technology can be used to ensure that the computer claiming to have sent or received the message is actually the one that did so. For example, if someone has metering technology on a personal computer, every so often the computer will report back to the billing function how much information has been used and how it has been used since the last report. Computer authentication is one method for assuring that the usage and credit card information is being sent to the correct billing computer and not to someone else masquerading as the billing computer who wants to steal credit card information.

For some purposes, it may be important to "time stamp" a chunk of information. For example, a meter may send a cryptographic envelope back to the billing function over a network in such a way that the envelope may not be received for a day or two. The contract with the publisher may specify that billing information be returned on the last day of the month. By time stamping the cryptographic envelope, the user can prove that the cryptographic envelope was sent on the last day even though it might not have been received until the second day of the following month.

Public key technology from RSA, Inc. (named after its inventors Ron Rivest, Adi Shamir, and Leonard Adleman) is generally thought to be the leading technology of its kind. RSA has been adopted by a growing list of U.S. hardware and software vendors. RSA encryption technology is available within the U.S. and Canada and, under certain circumstances, abroad. However, it is treated as munitions by the federal government and export controls are in place. Some developers of metering technology have implemented RSA in such a way that they claim export licenses have been granted. We have not verified these claims, however.

2.4 Changes in Publishing Paradigms

The demand for personalized information is beginning to have important effects on publishers. Besides the well-known migration to digital pre-press systems, some publishers have been implementing systems that treat the content of books and journals as piece parts: discrete texts and images that can be reformatted and/or recombined in new ways. These systems lend themselves to the sale and

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1142

distribution of information in chunks such as articles, chapters, even paragraphs and single images. When metering technologies are more widely deployed, publishers and information distributors and packagers can put these chunks into cryptographic envelopes. Thus, advanced database applications for digital "chunks" strongly complement advanced metering systems.

2.4.1 Publish On Demand Paradigms

A number of publishers have implemented programs to support various versions of "publish on demand." McGraw-Hill's Primus system was an early entry. Xerox's digital copying/printing "DocuTech" technology, combined with database and distribution applications, enables local printing and binding of digital information from diverse sources. One early use of these technologies has been in the creation, printing, and sale of "coursepacks": anthologies of chapters, articles, images, or selected pages.

Metering technologies will ensure that content is controlled and royalties collected up to the point when it is put on paper. Of course, once on paper, it can be copied or scanned. But if the costs of sending the information in cryptographic envelopes and usage fees are very low—the "high volume of low priced events" model—the incentives for scanning and perhaps some photocopying might be reduced.

2.4.2 Multimedia Publishing

The multimedia market gained serious attention from publishers as the installed base of CD-ROM drives grew large and as technologies were developed to support multimedia and full motion video on computer networks. In addition to demand for textual "chunks," multimedia publishing is creating demand for image, video, and audio "piece parts."

Multimedia publishing will push metering technologies to the limit because of the internal complexity of multimedia products. However, the most powerful metering technologies that will be deployed in the next two to three years will be able to keep track of all the various pieces (now called "objects" in the computer world), incorporated in a given multimedia product if such fine granularity is desired by rightsholders. It is likely that some of the earliest deployments of advanced metering technologies will be in the entertainment rather than in the information realm.

2.4.3 Electronic Rights Are Revalued Upwards

Rightsholders will have powerful metering tools that allow them to implement a variety of business models and pricing schemes. This is completely different from the discussions of the past several years that centered on the dangers of putting information in digital form, especially the dangers of lost revenues and loss of control.

To meet market demand for personalized information, we have noted that publishers and rightsholders increasingly will provide information in chunks and protect that information with encryption-based metering technologies. A likely outcome is that the rights for intellectual property in digital format will become

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1143

increasingly valuable. But increasing value does not necessarily translate into increasing costs for information users. Most metering technologies will allow rightsholders to implement a variety of pricing schemes as discussed in the preceding chapter. While some rightsholders will choose a form of meter-enforced subscription scheme, others will choose to charge differently for different uses. Thus, browsing might be free while printing might be so much per page.

Publishers who might have sold a CD-ROM or on-line database for a lot of money (let's say $1,000) might charge no initial fee and institute modest usage charges designed to encourage higher use. The absence of high initial costs may bring many more people and organizations into the information market. Thus, metering lends itself to business models based on larger markets and higher volume aggregate use.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1144

3 METERING TECHNOLOGIES

As noted in the introduction, this report does not review the numerous academic pilot projects. Nor does it address metering technologies only incorporated in the products of a single company. Those approaches are not likely to dominate the information marketplace.

Instead, this report addresses generic metering product technologies, or proposed technical architectures for metering, that have some chance of being widely adopted in commercial settings. Consequently, this report focuses on the efforts of commercial companies with products already in the marketplace or on those who have publicly announced their intention to introduce metering systems soon.

Four companies have made public announcements of metering technologies. These are CD-MAX, Inc., Electronic Publishing Resources, Inc., Infosafe Systems, Inc., and Wave Systems Corporation.

3.1 CD-MAX, Inc.

CD-MAX, Inc. is a wholly owned subsidiary of InfoServe, Inc. with principal offices in New Jersey (219 South Street, Suite 203, Murray Hill, NJ 07974-2100, voice: (908) 771-0022, fax: (908) 771-0444, contact: David B. Boelio, Executive Vice President, Marketing, (908) 464-1878).

CD-MAX's approach to controlling content and metering begins with encrypting the content during development of the information base and before the CD-ROM is manufactured. CD-MAX provides a security program that is installed on the customer's PC. This security program transparently decrypts the information on the CD-ROM as it is accessed by the customer. A DOS version exists today (August, 1994), a Windows version is in preliminary testing, Mac and UNIX versions are anticipated, in that order.

Each file on the CD-ROM is marked with a security code and the contents encrypted with a proprietary encryption algorithm. This encryption method was designed especially for the PC environment. CD-MAX claims that the computing overhead for decryption is minimal and is not apparent to the user.

CD-MAX supplies the program that does the encryption of the content to publishers. Each program requires some modification depending on the search and retrieval software used by the publisher, so that, in effect, each program is unique.

Once processed by CD-MAX's encryption program, the files on the CD-ROM cannot be accessed except by the CD-MAX security application program running on the user's PC. The CD-MAX security program is installed from diskettes on the user's PC. A protected file is created at installation time on the user's hard disk that contains, among other things, security keys and usage information. This security system is dynamic in that it is designed to accept new keys periodically, and to prevent use when existing keys have expired. The keys are updated from diskette or by modem with a call to CD-MAX.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1145

Publishers can choose from among a number of charging options. The particular transactions that can be metered and billed include browsing, viewing, printing, and downloading. Publishers can choose a number of payment schemes, including customer prepayment or unrestricted use up to a specified credit limit. CD-MAX, Inc. processes usage data, sends bills to customers, and sends use data and royalties to the rightsholders.

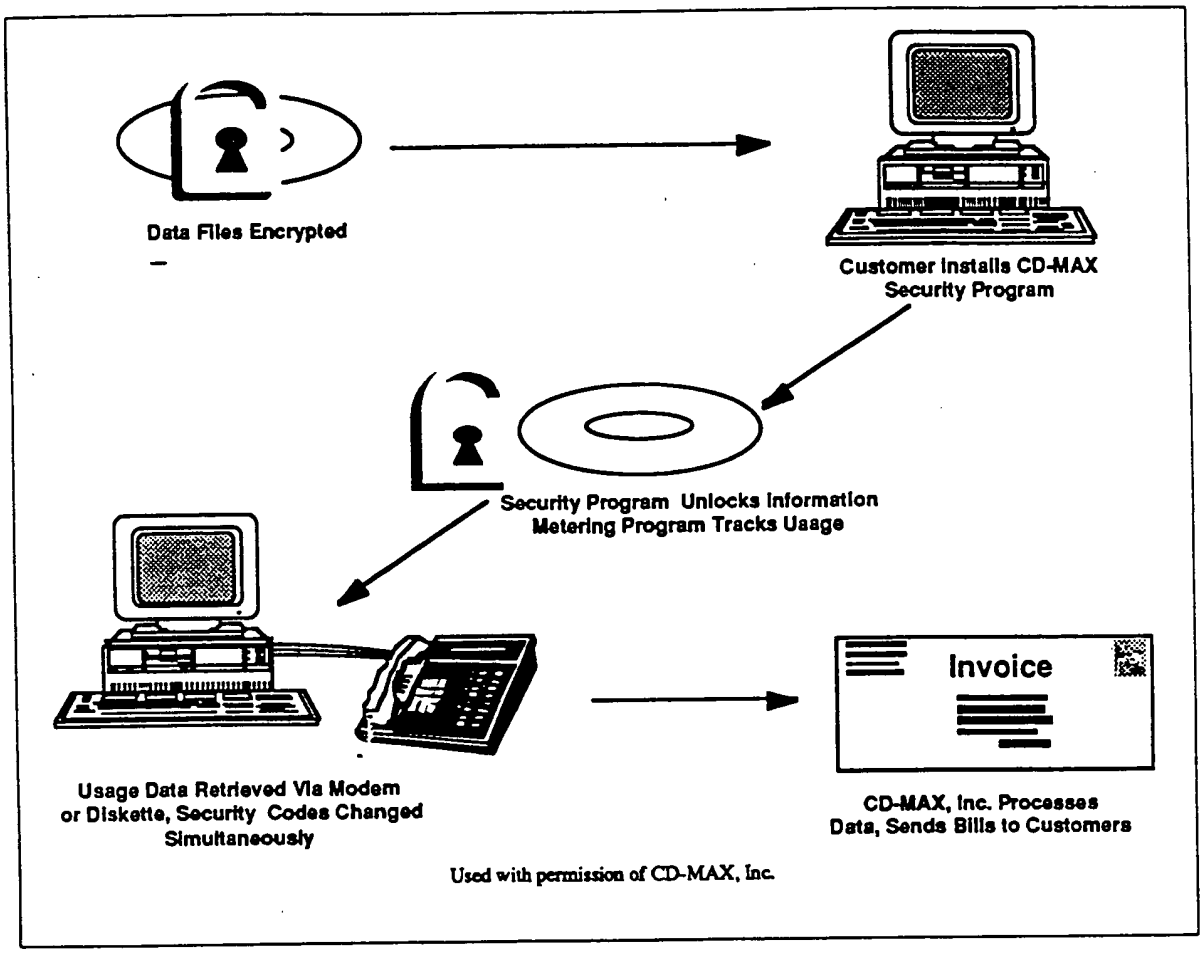


Figure 3.1 CD-MAX Process Flow

A market research function is also offered as part of the usage reports CD-MAX makes to publishers as part of its billing services.

According to CD-MAX, working demonstration systems have been installed at the National Demonstration Laboratory for Interactive Information Technologies in the Library of Congress. Visitors may see the CD-MAX's usage-tracking and billing functions in conjunction with DIALOG OnDisk® and Standard & Poor's CD-ROM. Launch of commercial versions of CD-MAX is expected in late 1994.

CD-MAX believes that software implementing their encryption algorithm can be legally exported to Canada and other countries as well, since its only practical use is for copyright protection. Modifying their software for other encryption and

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1146

decryption uses would be very difficult and probably not worthwhile. They acknowledge their responsibility to ensure that encryption export issues will not hinder their customers from pursuing sales opportunities outside the United States. However, CD-MAX acknowledges that they have not yet ascertained whether export licenses will be required or granted by the U.S. government.

Besides the advantages of metering technology generally, CD-MAX appears to provide currently encryption based security and metering technology for CD-ROM applications only. While CD-MAX is compatible with networked CD-ROM drives and databases that support multiple simultaneous users, billing and key exchange in a networked environment is addressed only in the system architecture, but has not been implemented yet. CD-MAX claims to be making extensive preparations to support these functions in a networked environment.

In its present implementation, once the user has paid for and received the decrypted information, the system provides no on-going control and usage metering capability of the digital information unless the CD-MAX system is integrated with the application being used to access the purchased information.

From information available, it seems that this approach is extensible to information stored on other media such as hard drives on file servers. CD-MAX officials stated that CD-ROM is their first and primary market, but others are envisioned later on.

CD-MAX, Inc. claims protection in part from patents granted and applied for by Dr. John David Wiedemer, a founder of the company.

CD-MAX's business model is based on performing clearinghouse functions for billing and taking a small fee for handling each billing transaction. Details of pricing and other financial information were not available.

Regarding user privacy issues, CD-MAX endorses the Information Industry Association's "Fair Information Practices Guidelines" and has implemented unspecified procedures and policies to ensure security and privacy.

3.2 Electronic Publishing Resources, Inc.

Electronic Publishing Resources, Inc. (EPR) has developed an initial implementation of a comprehensive architecture for the control of intellectual property and metered usage (Contact: Victor Shear, President, Electronic Publishing Resources, Inc., 460 Oakmead Parkway, Sunnyvale, CA, 94086, Voice: (408) 774-6100; Fax: (408) 774-6144).

EPR's technology consists, in part, of a comprehensive architecture for the control of intellectual property and support for a broad array of charging and billing schemes. Software implementing this architecture is now running. The first uses of EPR's technology are likely to be in the field of entertainment. Applications in publishing and information distribution will be announced in early 1995.

EPR's technology can be, and will most likely be deployed in many ways. Figure 3.2 shows one possible set of relationships and illustrates the power of the underlying technology.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1147

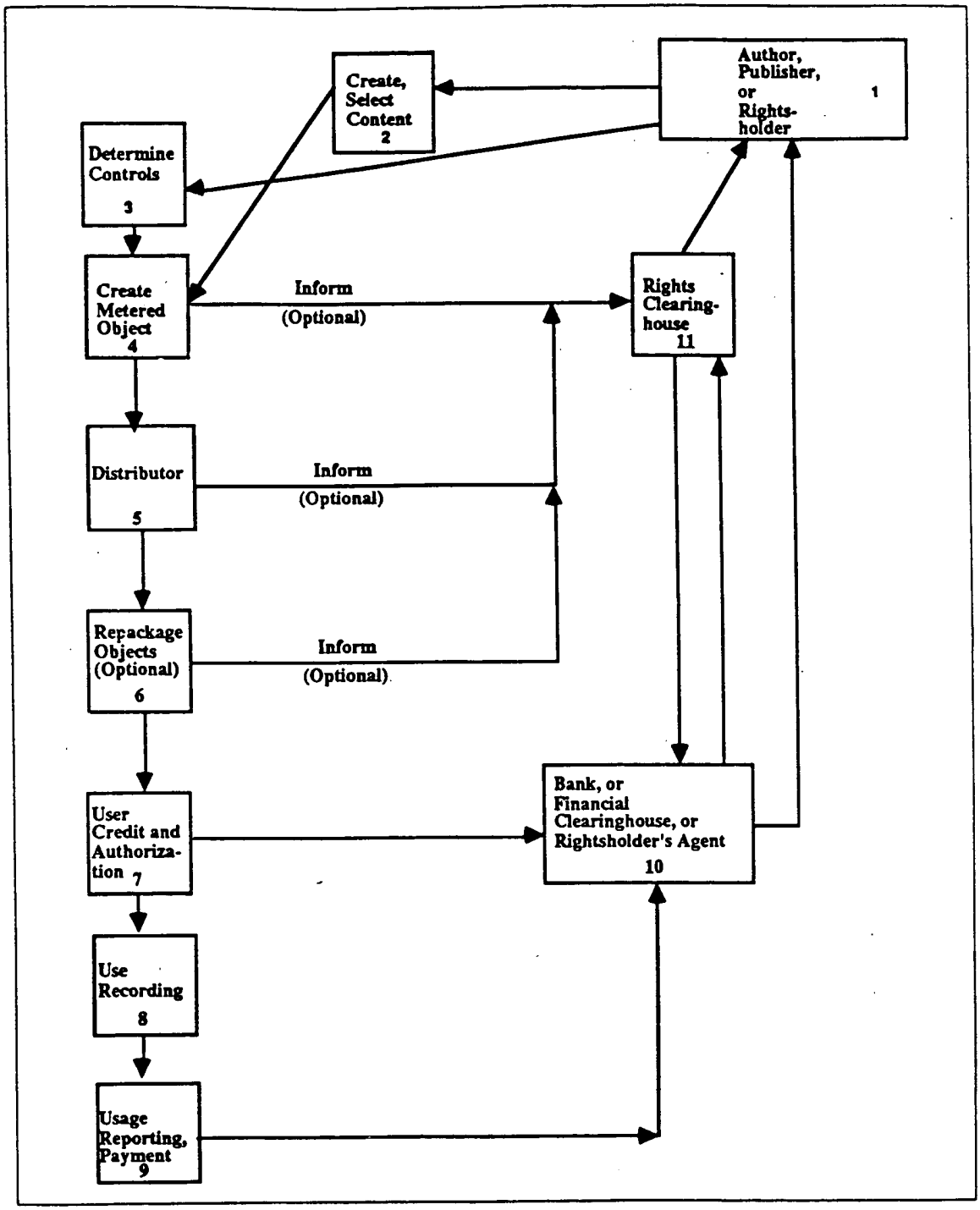


Figure 3.2. Typical EPR System Elements and Process Flow

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1148

In the description that follows, the numbers refer to the numbered boxes in Figure 3.2. An author, publisher, or other rightsholder (1) selects content to be protected by the metering system (2) and a set of controls (3) that apply to the content. Imagine for the sake of this illustration that the content is an article from a newspaper or science journal. The controls consist of information regarding authorized uses of the content, prices, ownership, and identities of various clearinghouses.

Authorized uses might include any or all of those listed in Chapter One, such as printing, excerpting, or transmitting. The prices for each authorized use are also established, for example, $X per printed page or per 2,500 characters printed (since ASCII text, for example, might not have page break information). The control information also contains points to certain operators of clearinghouse functions. If the rightsholder has established accounts at a particular bank or has nominated a financial clearinghouse or an organization such as Copyright Clearance Center to act as a rights clearinghouse, this information is also part of the controls.

The content and the controls are combined to create a metered object (4), a process referred to earlier as stuffing a cryptographic envelope. The envelope contains both the substantive content, in this example the article, and the control information. Some systems for stuffing envelopes will report this information to the rights clearinghouse (11).

Some publishers and authors may elect to distribute metered objects directly to customers; others will delegate distribution. This example shows a more complex case, specifically, where there is both a distributor or wholesaler (5) and a repackager or retailer (6). A wholesaler, in this example, might be an organization such as Dialog or Mead Data Central. A repackager or retailer might be an organization such as Individual that combines articles into newsletters personalized according to the customer's current interest profile.

Regardless of the actual distribution chain, the metered object arrives at the customer's computer. In some cases, the credit and billing information may be established with the retailer prior to receiving the object. In other cases, the credit and billing information will be established when the object (envelope) is first opened. User authorization (7) and a number of the reporting steps can happen via networks such as the Internet or by modem.

The EPR metering system keeps track of use (8) and periodically (the time intervals are set by the rightsholder, wholesaler, or retailer) the metering system reports to a financial clearinghouse (10). The financial clearinghouse may be an organization established especially for this purpose or a financial institution such as a bank or credit card company. In some instances, clearinghouse functions might be performed by others in the distribution chain, such as publishers, wholesalers or retailers. It is likely that eventually several financial clearinghouses will exist. The metering system will contact the clearinghouse via networks or modems. In turn, the financial clearinghouse will report billing or credit card information to banks and credit card companies as appropriate.

The EPR technology is capable of capturing, storing, and reporting extremely detailed use information. This detailed use information can be reported to the financial clearinghouse or aggregated by the metering technology on the user's computer. In instances where the full, detailed information is conveyed to a

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1149

financial clearinghouse, it is anticipated that the financial clearinghouse will, in turn, report the detailed usage information to a rights clearinghouse such as Copyright Clearance Center (11). In turn, the rights clearinghouse could aggregate the detailed usage information and report aggregate statistics to authors, publishers, and other rightsholders (1).

The banks and credit card companies will periodically convey the royalties to the appropriate rightsholders based on the information conveyed to them from the metering system and as set in the cryptographic envelopes.

Of the technologies investigated for this report, EPR's metering architecture and system appears to be the most comprehensive and robust. It provides a general technology not only for the control, metering, and billing of information use, but provides a basis for a complete solution to secure commercial transactions in a networked environment. Unlike the other technologies mentioned in this report, EPR's system provides for the persistent, on-going control, authorization, billing, and metering of digital information without having to integrate the EPR system into each an every application being used to access the protected information.

EPR's business model is based on a tiny part of each transaction fee plus licensing fees from computer companies and software publishers and integrators.

EPR is negotiating agreements with companies in several parts of the distribution chain, and major announcements are expected beginning in November, 1994 and continuing through 1995.

The underlying encryption technology is RSA public key, but it will work with virtually any appropriate cryptographic method. EPR believes that its technology is fully exportable.

EPR's technology is based on patents already granted and pending to Victor Shear, the founder of the company.

3.3 Infosafe Systems, Inc.

Infosafe Systems, Inc. offers a hardware based system for protecting and metering information (Contact: Thomas H. Lipscomb, President, Infosafe Systems, Inc., 342 Madison Avenue, Suite 622, New York, NY 10173, Voice: 212-867-7200; Fax: 212-867-7227).

As of this writing (the end of August, 1994), Infosafe is the only vendor with commercially available (as opposed to test or pre-release versions) metering technology. They presently have eight customers and are in full commercial operation.

Their technology is proprietary and employs both hardware and software. An external "box," the Infosafe-Mark III, is connected via an SCSI interface (Small Computer System Interface) to either an individual's computer, or to a server machine capable of supporting several users. Presently supported are Macintosh and Intel Architecture computers (DOS, Windows). Infosafe provides software to

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1150

run on the subscriber's computer; no modifications are required to the operating system that runs the subscriber's computer.

Prior to delivery to the customer, the publisher/rightsholder identifies appropriate chunks of information such as articles, paragraphs, images, and the like that would constitute a basic "packet" of information that could be priced and charged for separately. Typically, the publisher also creates a separate abstract and/or index for each packet. As part of the production process, each packet is assigned a separate encryption key, encrypted, and put on the CD-ROM or other delivery media together with the un-encrypted and hence searchable abstracts and indices. Packets may be of any size, including a single graph, photograph, article, paragraph, typeface, word, statistic, or data-point.

In a typical application, the user browses the abstracts or search results at no charge and is informed of the costs associated with purchasing the decrypted information packets. Once purchased, the information packets are decrypted and released to the user under the terms of the appropriate information provider's license agreement.

The Mark III is also equipped with a modem and a phone line that can be conveniently shared with other devices, including fax and voice calls. The modem is used by the Infosafe system to communicate with Infosafe or with an information provider's service bureau. Credit authorizations and decryption keys are sent to the Infosafe system; usage information is sent back to the publisher and/or to Infosafe, Inc. The Infosafe Mark III comes with an installed credit card reader to allow billing to credit cards instead of pre-establishing credit with the publisher and/or Infosafe.

The Infosafe system supports a wide range of charging algorithms, ranging from monthly or annual subscriptions with unlimited use, to "pay-per-view" for the smallest packet of information.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1151

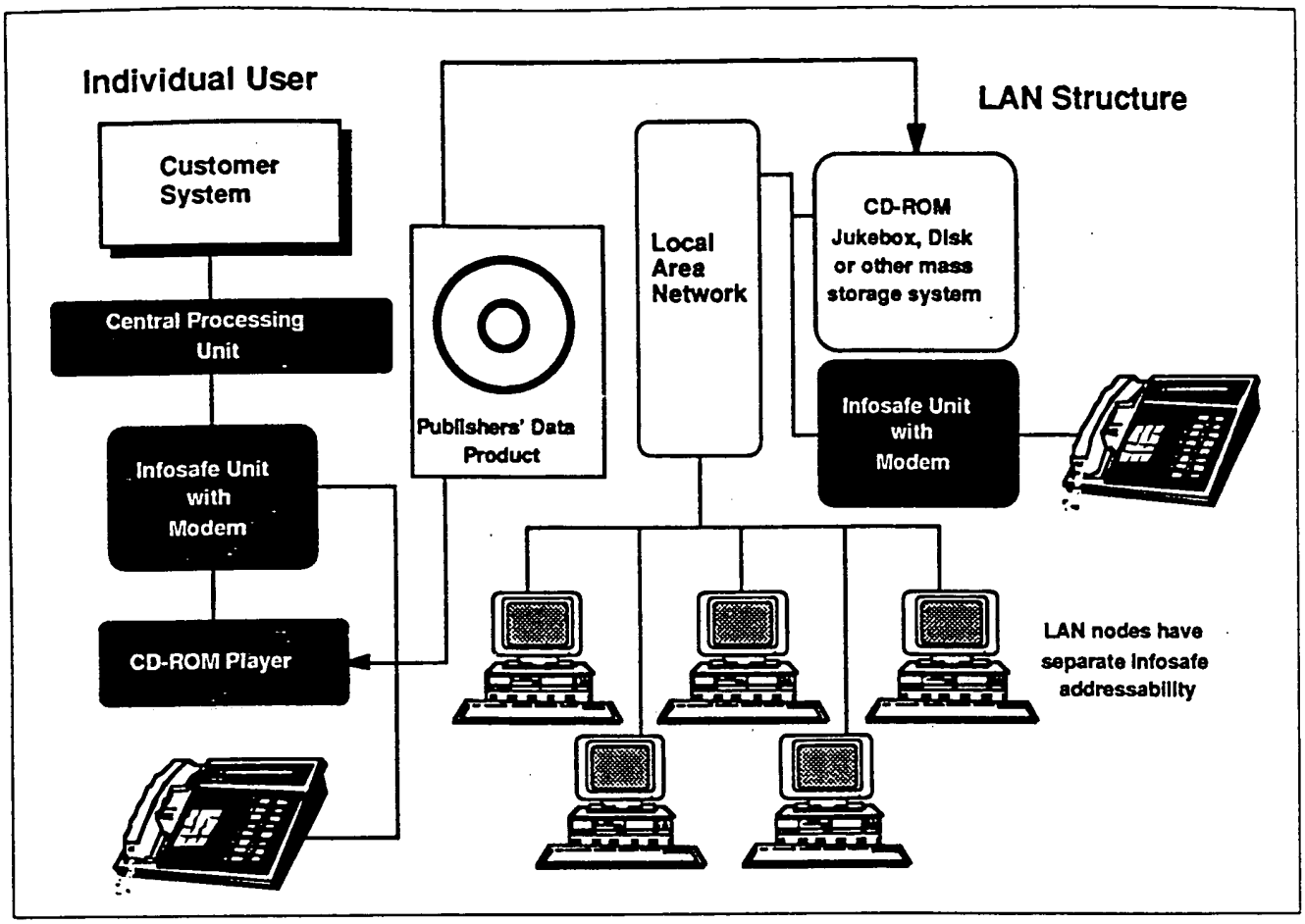


Figure 3.3 Typical Infosafe System Individual and Client/Server Configuration

The Infosafe system generally employs the widely used Digital Encryption Standard (DES) and also supports other encryption techniques, as applicable to the needs of a given customer, such as RSA public key encryption. Proprietary encryption key management techniques, plus the assignment of a different key to each packet, ensure that in the highly unlikely event of an encryption key being compromised, the loss would be a single packet rather than an entire information base. Also, each Infosafe device communicates via the modem to Infosafe Systems, Inc.'s "back office" to validate the on-going integrity of the subscriber's hardware device.

The "back office" operation consists of four major functions: (1) encryption key management and hardware services, which involve setup and support on the Infosafe system, and on-going encryption key oversight and management services; (2) subscriber support services, which involve handling or distributing customer service inquiries and user support inquiries regarding the Infosafe system or the publishers' data; (3) billing and credit services, which involve monitoring subscriber usage information, conveying electronic information regarding credit balances and requests between the subscriber and publisher, and coordinating

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1152

management of publisher mailings and processing of bills; and (4) market support services, which involve frequent communications between Infosafe Systems, Inc. and the publisher to assist the publisher in realizing the maximum return on their investment in the Infosafe system. Based on information returned from the metering device, publishers can analyze usage information to yield marketing information showing patterns of use. This allows rightsholders to re-configure or update products or change prices, either universally or at specific locations, using the memory storage available in each Mark III.

While Infosafe can perform clearinghouse operations, the Mark III is compatible with each publisher or their delegated agent performing clearinghouse functions instead. Infosafe's business model appears to be based on receiving a portion of the publisher's revenue stream from the protected data.

Additionally, Infosafe works with its clients to design, configure, and sell digital streams of information delivered through the Mark III. It charges a fee for initial configuration and software design and takes a portion of the publisher's revenue from the data it protects and delivers through the system. The size of the initial fee varies and depends in part on the extent of revenue sharing going forward. No detailed pricing information was made available by Infosafe.

The relationship between patents claimed by others and Infosafe's technology is unknown. Infosafe Systems, Inc. claims protection from patents filed, but not yet granted, and trade secrets. As of this writing, no patents are known to have been granted to Infosafe or to its principals directly related to metering.

3.4 Wave Systems Corporation

Wave Systems Corporation (WSC) (P.O. Box 610, Housatonic, MA, 02136, contact: Steven Sprague, Vice President Operations, Voice: 413-274-1400, Fax: 413-274-0290) plans both CD-ROM and networked versions of the encryption-based metering technologies.

The Wave System has five basic components: (1) the WaveMeter, a device for control and metering, (2) data preparation, (3) information delivery, (4) search and retrieval applications, and (5) WaveNet, the "back office" system. Figure 3.4 shows a typical application in which the WaveMeter is attached to a computer that acts as an information server for several other nearby computers connected through a network. Each of the major components is discussed below.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1153

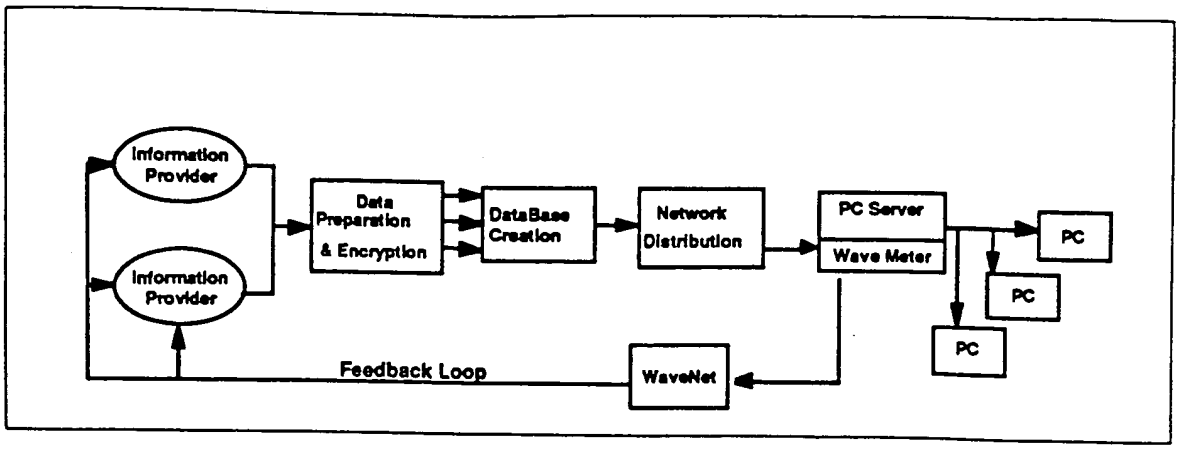


Figure 3.4 Typical WaveMeter Application

The WaveMeter is a microprocessor-based device that decrypts information and tracks usage information. It is attached to a computer or computer network. Figure 3.5 shows schematically the functions it performs, including key management, decryption, credit/debit accounting, storing pricing and tax data, and maintaining the usage log. To initialize the WaveMeter, the user starts by electronically dialing into WaveNet, a WSC operated system, using a modem and telephone lines. Once connected, the customer uses a credit card to establish a credit balance, which is automatically loaded into his/her WaveMeter. Organizations are expected to establish credit balances directly with WaveNet rather than through credit cards. Having established credit, the customer automatically receives keys for databases s/he may wish to purchase. After initializing the WaveMeter, the user can browse through and purchase information using the appropriate search and retrieval applications. For each information packet selected, a purchase price is displayed. To make a purchase, the user fills in information on the screen, including cost accounting information. The information is then decrypted by the WaveMeter and handed off to the search and retrieval application for presentation or printing. As decryption occurs, the usage information is stored within the WaveMeter.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1154

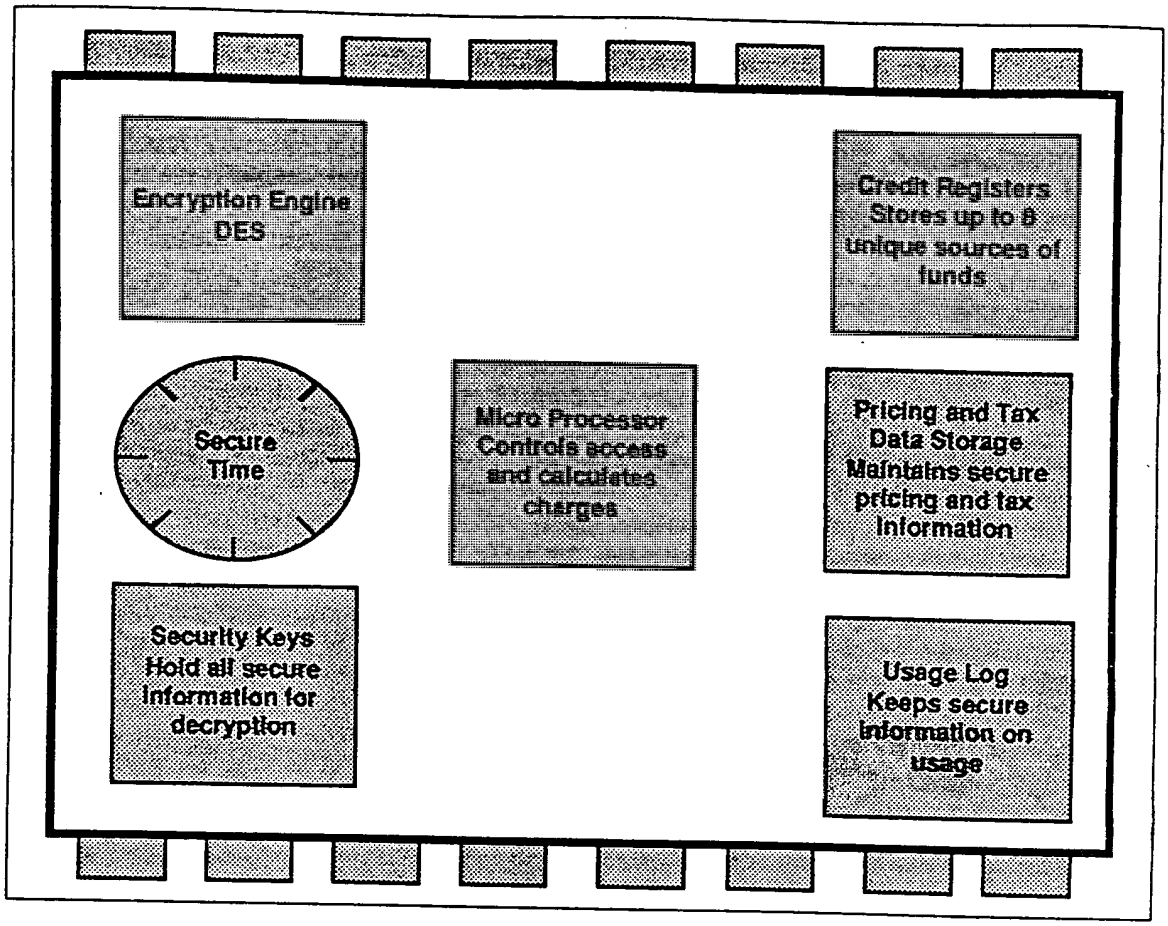


Figure 3.5 WaveMeter Functional Schematic

Data Preparation. In preparing the information to be protected by the Wave System, the publisher performs four basic tasks. First, the publisher defines logical groupings of information that can be purchased as a single item. This might be an article, a page, an entire volume or database, and so on. Next, the publisher sets the pricing for each logical unit of information such as an article and what is called the "pricing factor" for each database. The "pricing factor" is a multiplier to be applied against the prices set for each unit in the database. Pricing factors can be changed over time by the publisher. WSC provides a publisher interface to WaveNet for this purpose. The third data preparation step is to define abstracts and keywords. Wave System stores information in packets that have an encrypted part and a "clear" area in which publishers typically put abstracts and keywords that can be searched easily. The fourth and final step consists of encrypting the information to be protected. The encryption is fully automated and represents no burden to the publisher. Wave uses the Data Encryption Standard (DES).

Information Delivery. Once encrypted, the information can be delivered to customer locations by a variety of means. Early implementations of Wave System will be CD-ROM-based. Later versions are expected to use Wide Area Networks such as the Internet, satellite, or sideband FM radio broadcasting (combining text

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1155

information with FM radio broadcasts that don't interfere with the primary content of the broadcast).

Search and Retrieval Applications. WSC does not provide its own search and retrieval or other end-user applications. Instead, WSC provides what are known as Application Programming Interfaces (APIs) that define how software developers can incorporate WaveMeter functions in their applications.

WaveNet is comprised of all the "back office" data communications and information processing systems. The way to think about WaveNet is as a transaction processing system for electronic commerce. Each transaction is initiated by the user through the WaveMeter over dial-up lines to WaveNet. Each call results in one of four types of transactions: (1) registration of a new WaveMeter; (2) establishing and downloading credit; (3) downloading decryption keys for selected databases, and (4) uploading usage transaction information. (See Figure 3.6.) WaveNet also performs encryption and clearinghouse functions for publishers over electronic (modems and telephone lines) connections. The Information Management Processing Center (IMPC) component of WaveNet provides the management, control, and distribution of all encryption and decryption keys. This includes distributing encryption keys to publishers for each information packet, and managing the delivery of decryption to WaveMeters. Also, through the IMPC, publishers can establish prices on new databases, change prices on previously released databases, and change the types of transactions permitted for released databases. The IMPC also performs billing in those cases where WSC extends credit to individuals or to corporations. The IMPC also delivers usage reports to publishers and remits royalty payments regardless of whether payment was made through credit cards or through WSC.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1156

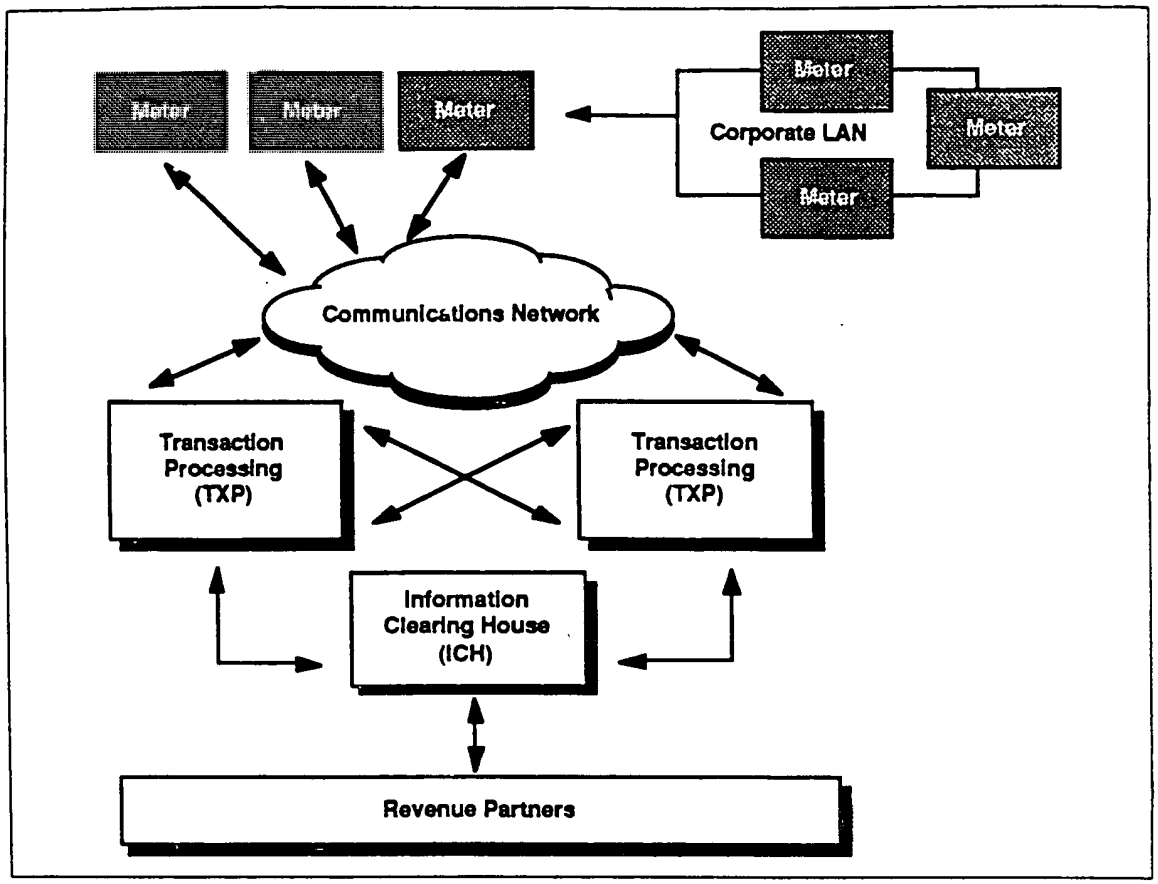


Figure 3.6 WaveNet Schematic

In its present implementation, once the user has paid for and received the decrypted information, the system provides no persistent, on-going control and usage metering capability of the digital information unless the Wave system is integrated with the application being used to access and process the purchased information.

WSC claims to have received permission from the Department of Commerce to export the WaveMeter to all non-communist countries. (This is because the user cannot control the encryption keys or the operation of the WaveMeter device; hence the WaveMeter cannot be used to encrypt data.)

The WSC business model is based on providing a set of standards for the WaveMeter and for the software that interacts with it. As noted, they also perform clearinghouse functions and retain a part of the royalty stream. No information was provided regarding the percentage retained by WSC.

Prices for the WaveMeter will vary according to how it is implemented. When built into a computer, the additional cost might be in the neighborhood of $15. A networking card version is expected to cost about $150. An external box with a SCSI interface is expected to cost about $180. At this time (September, 1994), commercial products are expected by the end of 1994 or early 1995.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1157

At this writing (October), we could not ascertain whether WSC claimed patent protection for the WaveMeter or other elements of the overall system.

Wave's success will depend on adoption of its technology by hardware manufacturers and software vendors. Publishers will be reluctant to participate until there is a sufficiently large installed base. So there is a "chicken and egg" problem that WSC has to solve. However, Personal Library Software has announced a partnership with WSC.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1158

4 MOVING FORWARD

Metering will require changes up and down the publishing and information distribution value chains. The world of metering may be so new and different that the rate of adoption will be much slower than commonly believed by metering developers and some in the rightsholder community. Radically new technology takes a while before there is a mass of adopters large enough to support commercial endeavors that turn a profit.

On the other side of the argument is the frequently heard notion that "industrial strength" metering technology would unlock the floodgates for digital content. Publishers and other rightsholders would be much more willing to distribute information in digital format that previously had been withheld for fear of infringement and loss of control on a massive scale. Many in the metering and rightsholders' communities believe the "floodgates" argument to be true. However logical, it is too early to say for sure.

4.1 Publishers and Other Rightsholders

Even though substantial deployment of metering is a few years away, it is not too soon for rightsholders and publishers to begin addressing "readiness factors," those things that publishers must address if they are to make their information available in conjunction with one or more metering systems.

4.1.1 New Business Models

One of the key issues facing publishers and other rightsholders is how to get from a print-based business to one based on electronic information and metering, or what might be called the evolution from Old World to New World publishing. New World publishing will be responsive to market demands for the personalization and customization of information and will be largely electronic. At the beginning of this decade, the term "electronic publishing" was taken by many to refer to CD-ROM publishing. At least in the U.S., electronic publishing will become largely network-based. Thus, metering allows publishers and rightsholders to distribute information over networks while retaining a fair amount of control and ensuing an on-going royalty stream.

Indeed, besides becoming substantially electronic, a key change in the evolution toward New World publishing will be a major shift in the source of revenue. In many publishing segments, revenue comes today largely from the sale of products such as books or the sale of subscriptions to periodicals. With metering, revenue will reflect use transactions, for example the broad list presented in Chapter 1. As noted earlier, some metered pricing models assume that revenue reflects a very high volume of very low priced transactions.

These kinds of pricing schemes require a substantial shift in the "mental models" of publishers and rightsholders regarding the nature of their business. This shift from products to transactions will not happen overnight. Indeed, it is much easier to identify the vision than to say how one will get there.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1159

Many close to the development of metering believe that transaction-based revenue will eventually exceed the revenue from the same traditional print products. However, to succeed, publishers may have to cannibalize existing print-based businesses in order to make a transition to metered digital information. This means that revenue from traditional print products may decline faster than the increase in revenue from metered use.

4.1.2. Managing Rights Proactively

Many publishers do not know what rights they do own, especially for backlist items. For example, consider earlier publications that are still in print and continue to sell well. In many publishing houses, the relevant contracts are in a warehouse somewhere and no one knows where the author or authors are today. Similarly, they can't find the permissions for art work or photographs. In many cases, the contracts did not anticipate the advent of the digital age and are silent on electronic rights.

Indeed, a number of U.S. author organizations have begun to demand changes in contract language so that authors retain more electronic rights, or receive a more substantial share of revenue from electronic publications.

Each individual medium and large publisher should begin building a rights management system now. A rights management system is different than a contract management system. The latter focuses on managing the creation of new contracts, their language, "boilerplate" for frequently used clauses and terms and conditions, and the like. The former is an information base that tells publishers what rights they have and don't have.

Together with digital pre-press systems, rights management systems could provide input to the systems that will actually put content into cryptographic envelopes. For example, imagine that a publisher has agreed to pay a photographer different royalties depending on the market, specifically, one set of royalties for the general public and perhaps only 25% of that amount when used for education. Tracking these details and then conveying the information to the metering system will be a major efficiency derived from rights management systems.

4.2 Information Consumers

New technologies are often used first to improve or automate what already exists. The first computers were used to automate repetitive calculations and to summarize massive amounts of data. When general purpose personal computers were introduced, they were first used for word processing, replacing both typewriters and specialized word processing computers such as those from Wang. The spreadsheet was perhaps the first new application to go beyond the typewriter and simple calculator. We forget how revolutionary VisiCalc and then Lotus 1-2-3 were when they were introduced. Since then, computers have been put to uses that were hardly envisioned 10 years ago.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1160

4.2.1 Will User's Accept Transaction Pricing?

Questions abound regarding the acceptance of real usage-based pricing by information consumers, even though metering technologies are now up to the task. Metering may evolve in a way similar to the evolution of computer use. Publishers and users may first adopt metering to add security, usage data collection, and billing to subscription and site licensing programs. By doing so, they adopt the new technology to perform familiar functions, much like using PCs for word processing.

Relating cost to perceived value will be one of the key issues that determine acceptance of transaction-based pricing. No one knows yet how information consumers will react to various charging algorithms. For example, will modest charges for printing information be accepted more easily than the sum of many tiny charges for lots of different uses, such as browsing, viewing, editing, cutting and pasting, etc.?

Information consumers generally like to have predictable costs and then be able to relate these costs to particular tasks. Imagine that a product manager sets out to create a report and to do so, s/he finds the most relevant articles in an information base, inserts the three most important quotes in a report, includes all three articles in an appendix, and modifies a spreadsheet from one of the articles by including company data, and inserts the spreadsheet in the report.

The actual cost of accomplishing these tasks will depend on the charging algorithm, the pricing established by the rightsholder, and the efficiency of the person doing the work. But will the information consumer be able to relate the bill for these activities to the task of "create a report based in part on external information?" Indeed, metering could be used by some rightsholders to prohibit all excerpting and inclusion, which would prevent creation of the report in the manner described. To gain acceptance in the market, pricing and control schemes need to be sensitive to the requirements of information users.

One "worst case" scenario is that rightsholders set pricing much too high on the theory that it is always easier to lower prices than to raise them. Today, one sees this kind of behavior in the pricing of images, audio, and video clips for multimedia products. Thus, many products never reach market or are less effective because they do not include the most relevant or best clips for the product because these were priced much too high.

Meter makers and rightsholders would do well to research thoroughly user acceptance of metering technologies and pricing and control schemes. Getting these issues wrong will delay widespread acceptance of these new paradigms.

4.2.2 Corporate Policies Regarding Information Use

There exists a wide range of formal and informal corporate policies regarding information purchasing and use. Some companies require information users to work through the corporate library or market research function. Information acquisition decisions are made as a function of internal demand and overall budget for information acquisition. Other companies decentralize such decisions, but

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1161

require business units to pay for information from their own budgets. A mixture of these models is not uncommon.

With the advent of metering, companies must now consider how their information policies need to be revised (if at all). For example, reports in electronic form may have been passed within the company without paying additional fees to the rightsholders. What happens if the recipient is in another business unit where this information use has not yet been budgeted? Should the business unit of the recipient now pay for use? The sender's business unit? Some corporate budget line? These are not insurmountable problems. But they will require some thought as metering is deployed in large companies.

4.3 Unresolved Issues

Among the unresolved issues regarding metering are public policy issues regarding user privacy and the generalizability of methods developed in the USA to the rest of the world.

4.3.1 Privacy Concerns

If all this usage information is being collected by the metering and billing system, will there be any limits on the downstream use of these transaction data? Rightsholders need to be able to assess market response to the information content itself—does anyone really want it?—and to their control and pricing schemes. Consequently, some have argued that the most detailed use transaction data should be made available to rightsholders. After all, banks and other financial institutions have handled detailed transaction data from credit card use for some time now.

Others have raised questions regarding the privacy of information consumers. They raise the specter of "Big Brother." If detailed transaction data exist, the data will fall into the wrong hands or be put to the wrong use. It is no one's business what information a given person reads or sends to whom. Still other questions relate privacy concerns to competitiveness.

For example, imagine that several semiconductor companies are engaged in a race to develop a powerful new manufacturing technology. Imagine further that several of them have installed a billing and metering system that knows which articles are being browsed, printed, transmitted to colleagues within the company, etc. This is very sensitive information. A firm's competitors would love to know what their counterparts are reading these days.

Image further that all of a sudden there is a flurry of activity and that four or five articles are widely distributed among the people working on this new silicon fabrication processes. Again, competitors would love this information, since it might show a direction that had not been considered or ruled out erroneously. And it could, of course, be a dead end (or a clever disinformation campaign).

Just as rules came into being regarding the uses and misuses of credit card and other sensitive financial transaction information, it may be that new laws will be proposed to protect the privacy of individual and organizational information consumers.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1162

Another approach, of course, is that of a third party acting as a clearinghouse for transactional data. There are numerous precedents, for example, ASCAP and BMI in the U.S. music realm or Copyright Clearance Center in the area of photocopying and more recently in corporate electronic information use.

4.3.2 U.S. Versus Global Perspectives

Metering presents new opportunities and challenges to information users, publishers and rightsholders, and, of course, to meter makers. This paper has been intentionally focused on the U.S. experience for reasons noted in the Introduction. Still, it is important to note how well and how quickly metering technologies will be adopted outside the United States. Three issues seem particularly relevant: exporting encryption technology, the installed base of computing and communications technologies elsewhere, and electronic information access and use in so-called Third World countries.

To realize scale economies, the same metering technologies must be adopted in many countries. It's not helpful if, for example, a publisher of scientific journals has to use one metering system in the U.S. and a completely different system in Europe or Japan.

Each of the profiles presented in the preceding chapter mentioned the exportability of encryption technology. All four companies profiled here claimed that their technology could be exported. Wave Systems Corporation claims to have received permission from the Department of Commerce to export, while CD-MAX, Inc., Electronic Publishing Resources, Inc., and Infosafe Systems, Inc. believe that their technology will meet U.S. government export requirements. Publishers and rightsholders should verify all claims regarding exportability.

Even if the encryption/decryption technology is exportable, the installed base of personal computers is another issue. Publishing has increasingly become a global business. Personal computers have not yet been adopted in many countries as widely as they have been adopted in the U.S. Thus, for some information of global interest, publishers may have to support both paper and electronic versions for a while longer. Even where there are personal computers in substantial numbers, the banking and credit card processing infrastructure may not yet be adequate to support widespread metering based on transaction pricing.

Finally, access to information in cryptographic envelopes may prove difficult in many of the less developed parts of the world. When metering is more widely adopted in leading commercialized countries, how will rightsholders treat, for example, the need for access to medical journals in less developed countries lacking the metering infrastructure? There are, of course, many solutions to this dilemma, but sensitivity will be required if rightsholders' interests are to be served without denying access to critical information by people who need it but may not be able to pay fees for metered usage.

© 1994 Northeast Consulting Resources, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 1163

THIS PAGE BLANK (USPTO)

Comput. & Graphics Vol. 10, No. 2, pp. 119–131, 1986
Printed in Great Britain.

0097-8493/86 $3.00 + .00
© 1986 Pergamon Journals Ltd.

DECENTRALIZED PROCESSING OF DOCUMENTS

UTE FLASCHE
Technische Universität Berlin, Franklin Str. 28–29, D-1000 Berlin 10, FRG

and

ANGELA SCHELLER
Hahn-Meitner-Institut Berlin, Glienicker Str. 100, D-1000 Berlin 39, FRG

Abstract—The term document processing covers the creation, modification, formatting, output and interchange of documents. This article describes the situation in the area of document processing today and discusses the requirements for future document processing systems. The current state of the International Standards in this area is presented.

1. DOCUMENT PROCESSING TODAY

Traditionally document processing could be divided into two different areas. One of them is the area of office documents normally processed on turn-key systems. The users of these systems do not know anything about the data structure used by the system. They type their text straight forward and use special function keys for starting a new paragraph or to center a heading. Some of these systems are able to display the content of the document with exactly the same layout as it will be printed on paper. This method is called *WYSIWYG* (What You See Is What You Get).

It is completely different from the method used in document processing systems running on normal computers. The user of these systems is a scientist or technician used to working with a computer and wants to use the same system for the processing of articles and reports (sometimes even books). He has to know the document data structure used by the system. In this area we have a great number of batch-oriented formatting systems. The user has to add specific processing instructions, e.g., for choosing fonts or defining blank space, to his machine-readable document file. Most of the systems have a macro facility. A set of processing instructions for a special purpose, like beginning a new chapter or paragraph, can be defined outside the document. Inside the document only the names of these macros are used. These keywords included in the document are called markup.

The user has to create his complete document including the markup with the normal text editor and then the formatting system prepares a file with the final formatted form (image form) of the document. This image form can be displayed on the screen or printed on paper. Even if there is only one typing mistake, the whole document has to be reformatted.

The advantages of these latter systems are the ability of typesetting any kind of difficult formulae and tables and the possibility to output the documents on high-quality devices like phototypesetters.

The disadvantage of both types of document processing systems is the different data structures used in the different systems. It is not possible to interchange documents between systems of different manufacturers.

In the future, documents will be prepared by several authors using different hardware. The different parts of the documents have to be merged together using network services. This method of document processing is called joint editing or decentralized document processing. Every author has to be able to change parts of a document created on another system. Therefore standardized document data structures are needed.

Within the last years the importance of the standardization of document interchange aspects has been identified. Without appropriate standardization framework a general approach to document interchange cannot be achieved. Various standardization committees like ISO (International Organisation for Standardization), CCITT (Commite Consultatif International Telegraphique et Telephonique) and ECMA (European Computer Manufacturer Association) are working in this area. Fortunately, during the last year, their results have been widely adapted to each other, thus avoiding the risk of the development of several incompatible standards.

The following studies the state of the document processing and interchange standards considered by the ISO and CCITT as of September 1985.

2. DOCUMENT INTERCHANGE STANDARDS

For the purpose of the standards described in this section, a *document* is an amount of text and additional control informations that can be interchanged for two major purposes:

- in image form for printing and displaying as intended by the originator
- in processable form for editing and layout revision by the recipient

Text is everything that can be presented in a two-dimensional form, for example, printed on paper or displayed on a screen. This means, text may consist of characters as well as of geometric elements and photographic elements.

In order to completely describe how documents may be interchanged between different kinds of communicating partners two aspects have to be clearly distinguished:

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1042, p. 1165

1. The administration of the document interchange, e.g., the structure of the envelope, in which the document is enclosed for its interchange and how the document is routed to the intended recipient. The communicating partners must agree on the informations to be specified for this purpose and how they are to be interpreted and processed.

2. The contents of the document. Obviously, the mechanisms for encoding the textual informations in the document must be commonly known. Nevertheless, this aspect shall not be a subject of this paper as there are many standards and recommendations on this topic, the discussion of which would fill a paper of its own.

But a document is not only a flat string of textual informations. It will consist of sections, paragraphs, figures, pages, columns and a lot of other structural units the meaning of which also must be commonly understood by the communicating partners.

Both aspects have been considered by ISO as well as CCITT and appropriate standards or recommendations, respectively have been developed. The rest of this section will briefly summarize the current state of these standards and recommendations.

2.1 *Administration of document interchange*

In order to be sent to some remote communications partner a document must be enclosed in some envelope and routed to the intended recipient. A number of administration tasks must be performed for the "real" interchange process. We will not describe how a physical communication channel can be established and how it can be made reliable, cost-effective, etc. All these aspects are discussed in a particular ISO standard, developed by ISO/TC97/SC16† as the Reference Model for Open Systems Interconnection (OSI) [1]. For the rest of this paper we will simply assume that communications connections can be established in some way on the various layers of this hierarchical architecture.

But we will discuss the additional administration tasks for the particular application of document interchange. With respect to the OSI architecture they are performed by running a particular *Application Protocol* (i.e., a protocol on the highest layer of this communication architecture). This view has also been taken by the corresponding document interchange standards.

In CCITT, the administration of document interchange has been discussed in Study Group VII and resulted in the X.400 series of Recommendations, called Message Handling Systems (MHS) [2].

In ISO, TC97/SC18 (Text and Office Systems) is responsible for this standardization area. Its working group 4 has developed a model called the Message-oriented text interchange system (MOTIS) which is strongly based on the corresponding CCITT work.

2.1.1 *CCITT/SGVII: Message Handling Systems.*

Study Group VII of CCITT has developed a set of Recommendations describing a service for interchanging documents between partners intending to communicate with each other. In its totality these MHS Recommendations are very complex, specifying different protocols, encodings procedures, conversion rules between several encoding schemes, etc.

All these Recommendations will be briefly discussed below one by one, starting with the base document X.400 (the general service description). The MHS functionality—as surveyed in Recommendation X.400—comprises a variety of features for the administration of document interchange, in particular, the following:

(a) Documents may be sent to multiple recipients of different kinds, like primary recipients, copy recipients (who just get a "copy" of the document), blind copy recipients (who are not even mentioned in the list of recipients distributed with the document), etc.

(b) If a recipient is (temporarily) unable to receive a document, an alternative recipient may be specified to which the document then is delivered. Alternatively, the document may be stored in the (message transfer) system until the recipient is available again.

(c) The time interval within which the document should be delivered may be determined, i.e., the document will not be delivered before the minimum time point and not after the maximum time point specified.

(d) Different kinds of acknowledgments can be provided if requested—including delivery notifications (indicating the delivery time) and nondelivery notifications (containing a reason code and possibly returned contents) as well as a response of the receiving user himself (perhaps by a document of its own).

(e) The repertoires used for the encoded informations of the document contents may be automatically converted by the (message transfer) system. The considered repertoires comprise TELETEX, TELEFAX, VIDEOTEX encodings, etc. This may be done either explicitly (i.e., on request by the sending user) or implicitly whenever required because the current repertoire is not supported by the intended recipient.

(f) In order to describe the kind of document to be transmitted more precisely some additional attributes may be specified, for example

- the body type of the document
- the subject of the document
- cross-referencing informations (to other documents)
- a notice that the document makes some document obsolete which was previously sent
- priority informations (normal, urgent, nonurgent)
- importance of the document
- sensitivity informations (private, personal, company-confidential)
- authorization (who is responsible for creating this document, who is responsible for sending this document)

(g) If an MHS user wants to send a document but is not sure whether its transmission will be successful, he may first send a "probe element" describing only

† After the recent ISO reorganization this subcommittee has become part of SC21 ("Open Systems").

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1166

the important characteristics of the document without its contents and await the answer of the system.

Of course, the above list shall only serve as a survey on the MHS functionality and is not intended to be complete.

As should be obvious by this list, the MHS functionality in its total is very extensive. Therefore, MHS has been decomposed into two sublayers, the *Message Transfer* sublayer, MTL, and the *Interpersonal Messaging* sublayer.

The Message Transfer sublayer is concerned with the pure document interchange functionality, like routing, timing, handling multiple or alternative recipients, delivery confirmations, communication priorities, code conversions, etc. These functionalities are performed by so-called *Message Transfer Agents*, MTAs. The collection of MTAs is called the *Message Transfer System*, MTS.

The functionality of the Interpersonal Messaging sublayer is performed by so-called *User Agents*, UAs, which are directly connected to the MHS users. Therefore UAs are responsible for that part of the MHS functionality which directly correlates to the documents themselves, like the specification of authorization, cross referencing, user responses, subject, body type, sensitivity, importance, obsolete documents, parameters, etc. In principle, the UAs shall also provide the functionality for local document processing, such as text editing, viewing, storing, etc. Nevertheless, this functionality is not specified in the MHS Recommendations, as it has only local significance and thus may be completely left to local implementations.

Figure 1 shows how a document may be moved to an intended recipient when using MHS. The sending user has access to a particular UA and may inform this UA about the document information to be sent (called the *document body*). The UA then passes the document body (together with those control informations added by the UA itself, which are called *document heading*) to the MTA which is connected to this UA. This MTA also adds certain control informations (called *document envelope*). Then the document is routed through the MTS to the MTA which is connected to the UA of the recipient. This recipient MTA interprets and removes the envelope and indicates the rest of the document to the connected UA which interprets and removes the document heading. Finally, the original document information is indicated to the recipient user. The relation between the document body, the document heading and the document envelope is also shown in Fig. 2.

The communications mechanism of the MTS is store-and-forward, i.e., no end-to-end connection (with respect to OSI) will be established. Thus, several MTAs may be involved in the interchange of a document because of necessary routing activities. This is visualized in Fig. 3.

On the two sublayers the MTA entities and the UA entities (called MTAEs and UAEs) communicate with their peers via two communication protocols (called P1 and P2) which are specified in Recommendation X.411 [3] and Recommendation X.420 [4], respectively.

An MTAE directly used by a UAE for sending or receiving a document may be, but need not be, located within the same system. In the former case the realization of the service interface between them is a local matter. In the latter case the UA will make use of the service of this MTA via an additional protocol (called the Submission and Delivery protocol, P3) which is performed by a corresponding Submission and Delivery entity (SDE). This is specified in Recommendation X.411. This protocol hierarchy is visualized in Fig. 4.

The protocol elements are encoded according to the data type description technique given by Recommendation X.409 [5]. This Recommendation defines a notation for specifying composite object types via a set of basic object types (like INTEGER, BOOLEAN, etc.) and structuring mechanisms (like SET, SEQUENCE, etc). This technique is used in X.411 and X.420 to specify the structure of the P1 and P2 protocol elements, i.e., for example the structure of the envelope parameters. As this object type notation technique is accompanied by a set of encoding rules, the concrete protocol element encoding can be derived from this (abstract) specification and need not be given explicitly.

In order to avoid interworking problems between MTAs if they would be implemented on top of different OSI communications services, one particular underlying communications service is assumed for an MTS which is specified in Recommendation X.410 [6]. This communications service (called *Reliable Transfer Server* (RTS)) is based on the OSI model and describes a particular usage of that subset of the OSI Session service which is provided by the TELETEX Session protocol (CCITT Recommendation T.62) [7].

One need not even have to have an MHS implementation in order to be able to participate in the MHS service. A TELETEX terminal without MHS software can also send documents to and receive documents from an MHS system. However, because of the lack of the MHS software, the transmission and receipt of documents must be controlled by a human user sitting in front of this TELETEX terminal. In order to be able to specify and interpret the necessary MHS administration informations of the document heading and envelope these informations must be specifiable and presentable in human-readable form at the user interface. As the X.409 encodings of the P1 and P2 protocol elements are not human-readable a conversion of the encoding must be performed when a document leaves/enters the "normal" MHS environment.

This is done by a particular gateway between the MHS world and the TELETEX world which is called TELETEX Access Unit, TTXAU. In addition, the TTXAU provides a document storage facility, by means of which received documents may be stored before they are forwarded to the TELETEX user. This might be reasonable, if the receiving TELETEX terminal is currently out of order. In this case, documents received from MHS are simply stored in the TTXAU and may be fetched by the TELETEX terminal itself

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1167

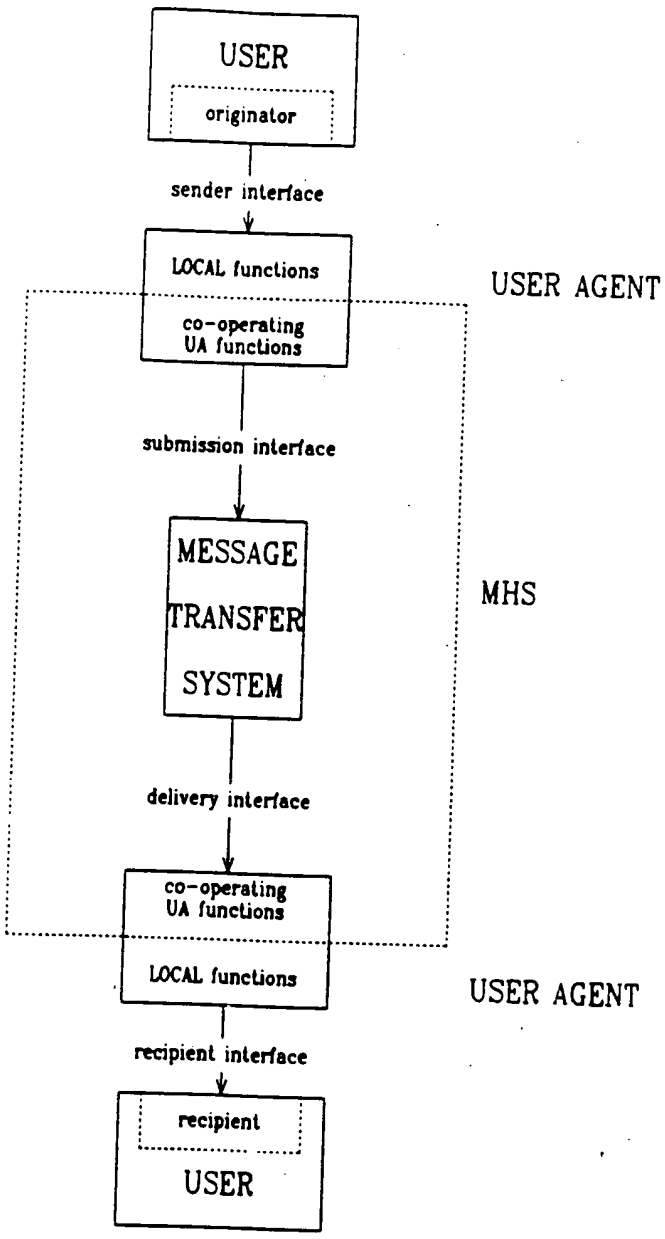


Fig. 1. Transmitting a document between two MHS users.

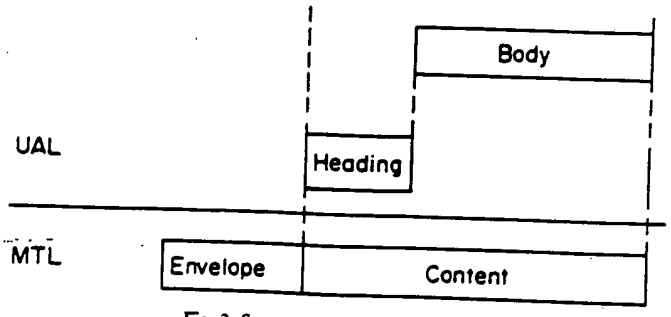


Fig. 2. Structure of an MTL message.

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1168

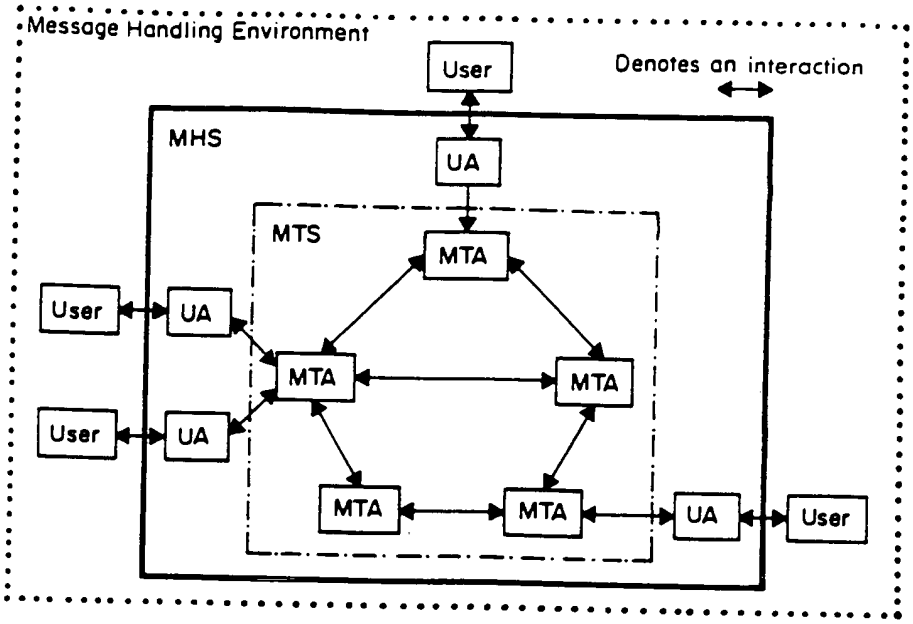


Fig. 3. Possible interactions between MHS components.

when it is available again. Accessing MHS from TELETEX terminals, as outlined here, is described in Recommendation X.430 [8].

2.1.2 *ISO TC97/SC18/WG4: Message-Oriented Text Interchange System (MOTIS).* Within ISO, SC18 has also a working group which is responsible for specifying the application protocol behaviour and encoding for document interchange applications. When this group was founded (about 3 years ago), the CCITT MHS proposal was already available in an early version. In order to achieve compatible standards, SC18/WG4 decided to use this proposal as a basis for their work on a Message-Oriented Text Interchange System (MOTIS). Only few extensions have been specified. Therefore, a precise description of the MOTIS approach need not be given here.

2.2 *Structuring the document contents*

This subsection is concerned with standards and recommendations related to the interchange of the document contents themselves.

Exchanging only the pure textual informations will not at all provide a comfortable document interchange service. The arising problems range from rather simple questions like "How to distinguish between character parts and facsimile parts?" to quite complex ones like "How can a document be modified by the recipient and still retain the characteristics of an intended layout?".

As already has been mentioned in the introduction today's local document processing systems already allow to specify certain informations (in addition to the textual parts themselves) which will structure the document in some sense (e.g., "starting a new paragraph" or "indenting the subsequent text," etc.). These additional informations will usually be interpreted by a document formatting component (which may be integrated in the editor or not). Unfortunately several different systems of this kind have been developed without being based on a common model and on a standardized encoding for these additional informations for interchange purposes.

In ISO, two working groups of SC18 (WG3 and WG5) have been working on a rather general solution of these problems for several years. A third working group (WG8) is also concerned with document structures and has developed a formal language for document markup (Standard Generalized Markup Language (SGML)). As this development was performed independently of the WG3/WG5 activities for several years† both approaches are not yet well aligned but substantial progress on this topic is expected for the near future.

As opposed to that, it is not the task of CCITT to directly support a general document model. Nevertheless, specific document interchange services have been introduced by CCITT Study Group VIII called Telematic Services. As the TELETEX and TELEFAX services only allow the interchange of homogeneous text informations they do not necessarily require an overall document model. But for the mixed-mode TELETEX/TELEFAX service an explicit distinction between character-oriented text and facsimile-oriented text is required. Therefore, the general concepts of the document model developed by SC18 have been widely adopted. This is described in CCITT Recommendation T.73 [9].

† WG8 has become a working group of SC18 only after the recent ISO reorganization.

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1169

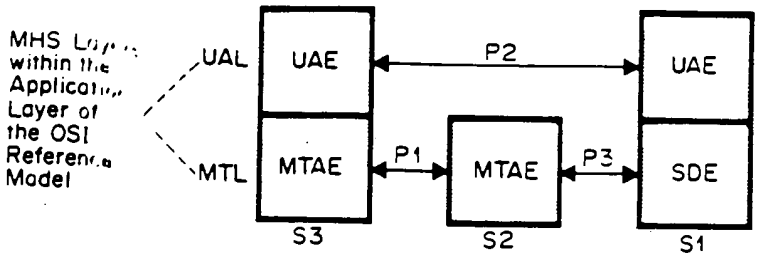


Fig. 4. Description of the MHS layering.

2.2.1 *ISO TC97/SC18/WG3 and WG5: document structures.* In order to solve the problems mentioned above WG3 and WG5 of SC18 are currently developing a ten-part standard (DP 8613) with the following structure:

1. Introduction
2. Office Document Architecture
3. Document Profile
4. Office Document Interchange Format
5. General Principles of Positioning and Imaging
6. Character Content Architectures
7. Photographic Content Architecture
8. Composite Graphic Content Architecture
9. Other Content Architectures
10. Conformance

SC18/WG3 is responsible for parts 1–4 including the necessary document common model and the document interchange format which has been derived from it.

SC18/WG5 is responsible for parts 5–9 which will further refine the characteristics of character, photographic, geometric and possibly additional categories of textual informations as far as necessary for their embedding in the general document model (and, thus, also the data stream). Of course, their work is based on the available standards and recommendations for encoding the textual informations themselves. The conformance part will be developed by both WGs.

Subsequently, the available parts of this ten-part standard will be briefly discussed—each one in a section of its own.

2.2.1.1 *SC18/WG3/DP 8613, Part 1: Introduction.* Part 1 [10] is a general introduction which need not be discussed any further.

2.2.1.2 *SC18/WG3/DP 8613, Part 2: Office Document Architecture (ODA).* Part 2 [11] of DP 8613 describes a general architectural model concerning the possible internal structures of documents the need of which has been identified above. This model is called Office Document Architecture (ODA). In order to determine the different structural elements one has to do with (and which, therefore, need to be integrated in this model), one should again take a look at usual document processing:

On the one hand, the author of a document may have it structured into chapters and sections starting with headings and consisting of a sequence of paragraphs interspersed with footnotes, figures, tables, etc.

On the other hand, a *formatter* automatically transforms this specification into a layout of this document (structuring it into pages, columns, certain blocks for figures and tables, etc.).

Thus, in fact, a document can be viewed under (at least) two completely different aspects. Obviously, both versions of the document may be subject to document interchange—simply depending on whether the document shall be modifiable at the recipient or just output.

Consequently, both kinds of document descriptions shall be considered in a general document model. Therefore the architectural model defined by SC18/WG3 clearly distinguishes between these two different internal structures of a document. In this model they are called

- the (specific) *logical structure* of the document
- the (specific) *layout structure* of the document

The elements of these structures are called (basic or composite) *logical* or *layout objects*, respectively. Basic objects are directly related to *content portions* of the document (i.e., to part of the textual information of the document). A content portion always consists of textual elements of some *content architecture*. There will be at least content architectures for character elements, photographic elements and geometric elements which are defined by WG5.

In many applications particular rules need to be applied on the internal organization and layout style of various similar documents (e.g., business letters). The publisher of an article or a book, for example, may predetermine his own layout style concerning the page format, the number and size of columns, the optimal positions and sizes of figures, the style of headings, etc. In addition the publisher may also specify rules on permitted logical structures, e.g., the maximum number of nesting levels for sections.

Thus, in the ODA approach mechanisms are provided for the specification of the characteristics of similar documents with respect to logical and layout properties. This is done by specifying a *document class* consisting of appropriate generic *logical* or *layout definitions*, respectively. They may, in particular, be used to check the specific logical structure of a document against its class definition (e.g., during editing) and for reasons of transmission and storage efficiency as these definitions need only be interchanged and stored once.

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1042, p. 1170

Common parts of document contents (e.g., a logo or a copyright sign) may already be specified in the document class and are called *common content portions*.

The subsequent paragraphs will define the characteristics of logical and layout structures and definitions more precisely.

Logical structures, for example, describe how a document may be decomposed into chapters, which are decomposed into sections, which are decomposed into subsections, etc. Therefore a *specific logical structure* is specified as a *tree* structure of logical objects (although some relations, e.g., references between chapters, are not expressible by a pure tree). Relations of this kind as well as other additional characteristics of logical objects may be specified as *attributes* of these logical objects. An example of a tree representing a specific logical structure is shown in Fig. 5.

Generic logical definitions describe for all documents of a document class the general (hierarchical) structure: the possible sequences and repetitions of the "branches" of the permitted tree structures; the types of logical objects within this tree (called *object classes*), including the specification of the predefined or default values of relations to other "nodes" and of other attributes; and common content portions.

An example of a graph representing generic logical definitions is shown in Fig. 6.

A *specific layout structure* mainly describes the (positioning) interrelations between the parts of an image of a document and the visual attributes of these image parts. It will be specified as a tree structure of layout objects (although some relations, e.g., flow links, cannot be expressed by a pure tree). The possible layout objects are called page sets, pages, frames and blocks and provide different kinds of representatives for the parts of the document image. All these containers are rectangular and parallel to each other. *Page sets* describe a set of correlated *pages* with similar layout characteristics, e.g., a set of table of contents pages. *A block* is directly related to a content portion of the document. Blocks have to be positioned either directly onto a page, or, alternatively, one (or more) intermediate level(s) may be inserted in the tree structure, which are called *frames*. Frames describe predefined boundaries of the page layout, e.g., the columns of a page. Blocks may be transparently or opaquely overlaid with other blocks. An example of a tree representing a specific layout structure is shown in Fig. 7.

Generic layout definitions describe for all documents of a document class the rules for establishing their layout structures, the predefined or default relations and other attributes of the layout objects and the common portions of contents. An example of a graph representing generic layout definitions is shown in Fig. 8.

As already has been mentioned above, the components of the logical and layout structures of a document may have *attributes*. In particular, it has to be distinguished between logical attributes, layout attributes and attributes of the content portions. Particular kinds of logical attributes are the *logical-layout relations* and the *layout directives* which describe how the logical objects have to be related to layout objects. Relations may either be specified by certain rules (e.g., indentation) or by explicitly naming the layout object into which this logical object has to be placed. Attributes of layout objects are, in particular, positioning and rendition attributes which have been determined by SC18/WG5. Content attributes specify the content type, the coding type and alternative graphic representations. The elements constituting the office document architecture model are summarized in Fig. 9.

Fig. 10 shows how the various elements of the ODA model may be integrated into the process of document production, formatting and rendition.

2.2.1.3 *SC18/WG3/DP8613, Part 3: document*

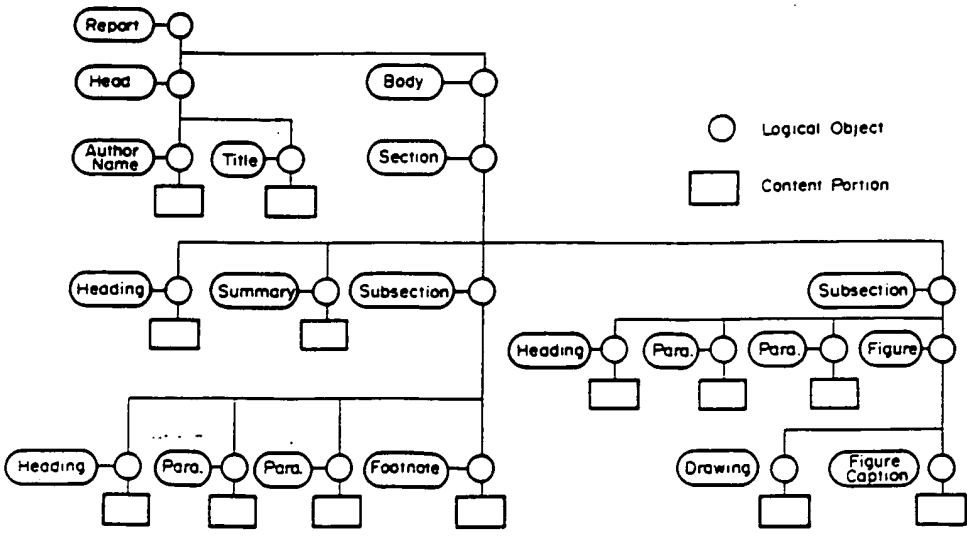


Fig. 5. Example of a specific logical structure of a *report*.

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 217

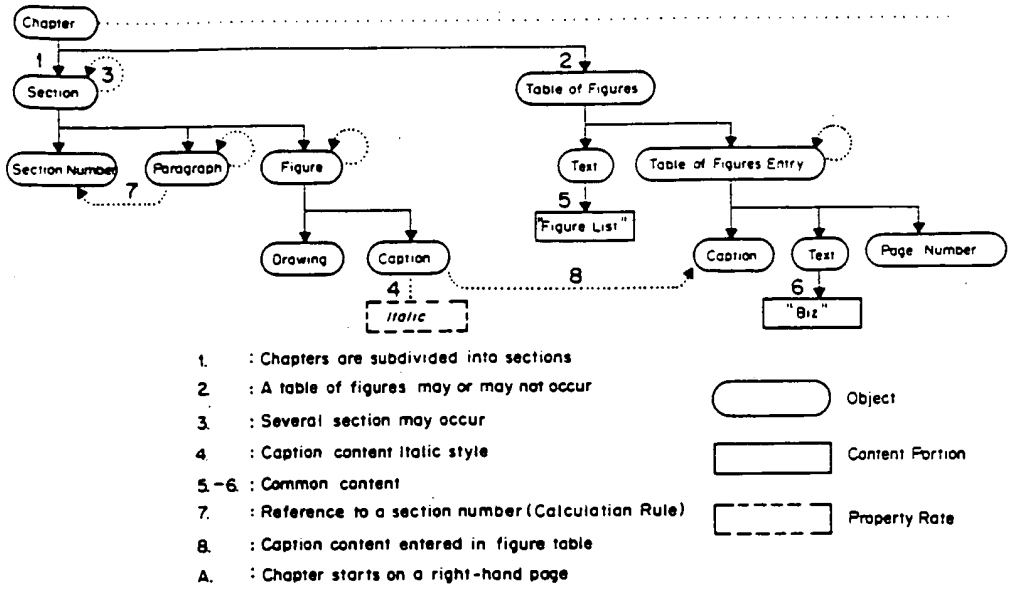


Fig. 6. Example of a set of generic logical definitions.

profile. Part 3 [12] contains the specification of the *document profile*, which describes attributes of documents considered as a whole (like originator, title, dates and times, comments, cross referencing, keywords, security informations, etc.). In principle, these informations constitute some kind of document heading and thus have a close relationship to the MHS environment. In fact, some of these attributes can also be found in MHS, because both proposals have been developed independently.

2.2.1.4 *SC18/WG3/DP8613, Part 4: office document interchange format (ODIF)*. This part [13] describes the mechanisms for exchanging documents structured according to the ODA philosophy. The interchange of a document is performed by first transferring the document profile and then the document body. For interchange purposes the document body is structured into so-called *descriptors* (each specifying a generic/specific logical/layout object) and *text units* (each specifying a content portion). Each element of

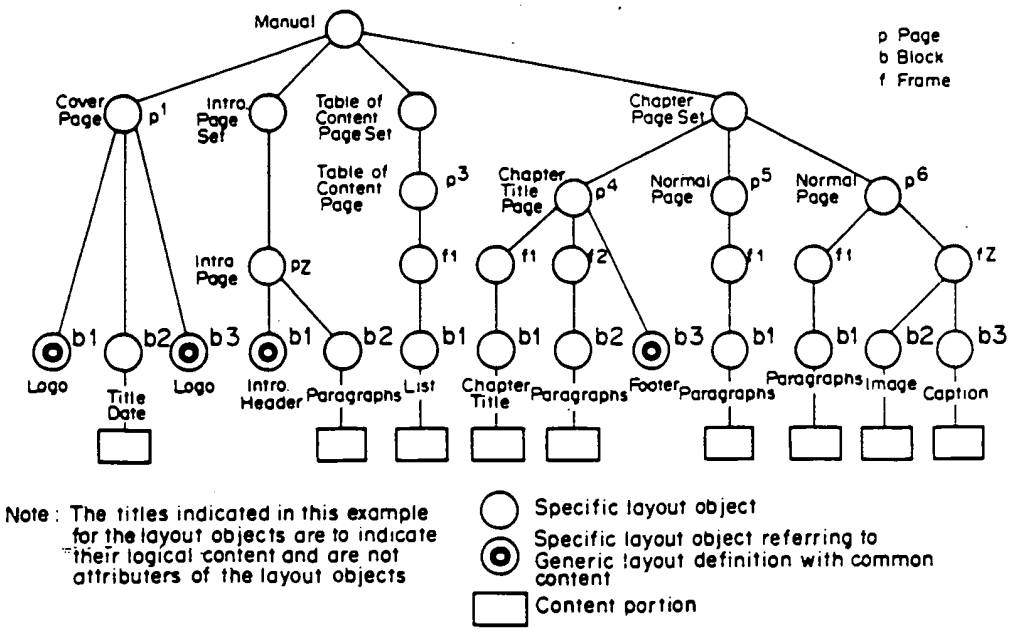


Fig. 7. Example of a specific layout structure of a *manual*.

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1172

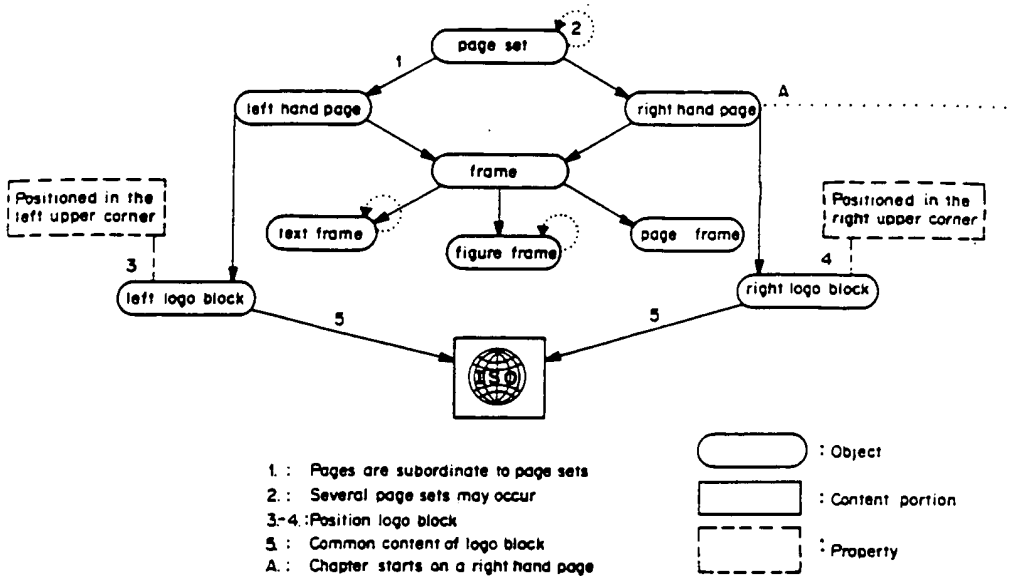


Fig. 8. Example of a set of generic layout definitions.

the data stream may be related to other elements by referring to their identifier attribute values.

The descriptors and text units may be interchanged in two different orders, specifying two different possible data streams:

Data Stream A. This kind of data stream may be always used and results in the subsequent order of elements:

1. Document profile
2. Descriptors of generic layout definitions
3. Descriptors of generic logical definitions
4. Text units for common content portions
5. Descriptors of specific layout objects
6. Descriptors of specific logical objects
7. Specific text units

Within each part of this data stream the order of elements is arbitrary.

Data Stream B. This data stream may be used if only the layout part or only the logical part of a document specification is to be exchanged. In this case, the descriptors and text units are given in the subsequent order:

1. Document profile
2. Generic "tree"
3. Specific "tree"

Each of the two tree structures is exchanged in prefix order. Each text unit is directly inserted after the descriptor of the basic object to which it is related. Because of this natural transmission order the specification of part of the object identifiers and relations between objects may be left away in the data stream.

The interchange formats defined in part 4 are described by using the X.409 [5] notation and are transmitted by using the X.409 encoding rules.

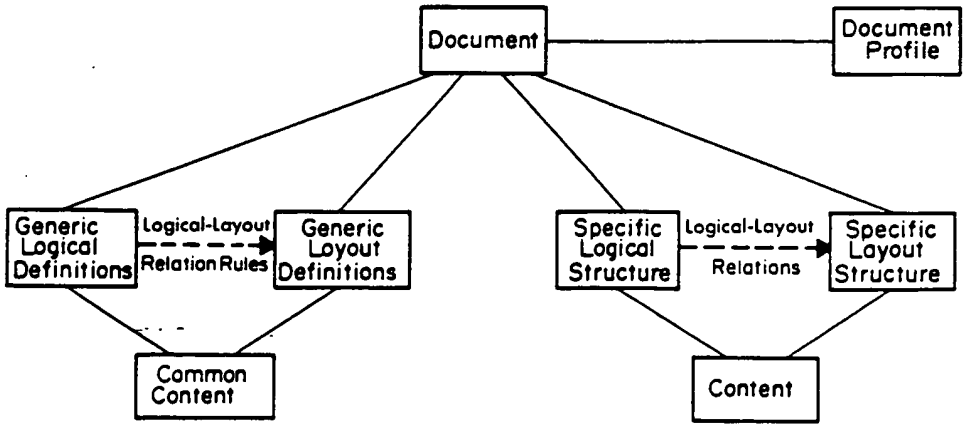


Fig. 9. Office document architecture model.

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1173

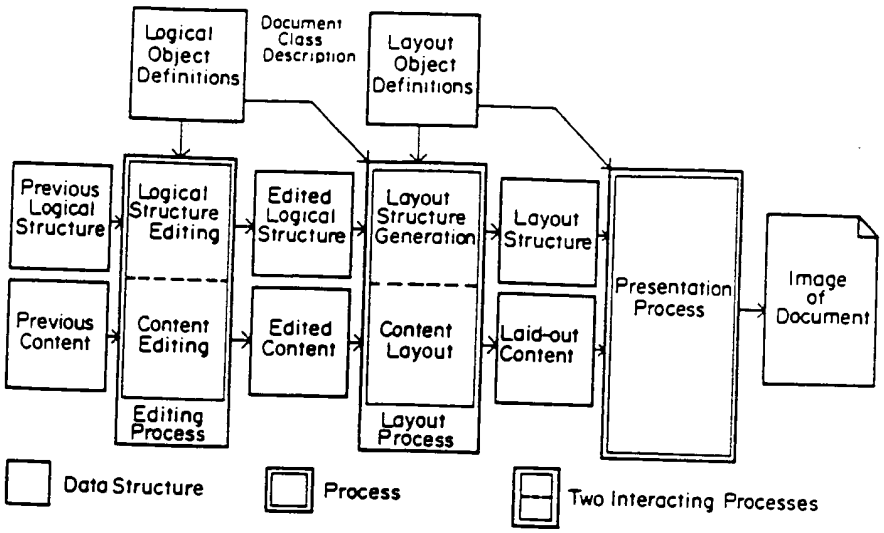


Fig. 10. Text processing model.

In principle—although not explicitly identified in part 4 of this standard—documents may be interchanged in three kinds of interchange formats:

- text-image format (TIF)
- text-processable format (TPF)
- formatted-processable format

A TIF only describes an image of a text, i.e., the TIF describes only the layout part of this text. Thus, if only the TIF of a text is exchanged, this text can no longer arbitrarily be manipulated by the communications partner.

A TPF describes a text in its original form, i.e., only the logical structure and the corresponding layout directives are exchanged. Thus, the text can still be manipulated by the communications partner, but must be formatted remotely in order to obtain an image of it.

A "formatted-processable format" contains both the logical part and the layout part of the document. Thus, the document may be modified by the recipient as well as directly presented on some output medium.

2.2.1.5 *SC18/WG5/DP8613, Part 5: general principles of positioning and imaging.* Part 5 [14] of the standard defines the rules for positioning and imaging layout objects on presentation surfaces—independent of the concrete content architectures used in the related content portions.

Layout objects have a rectangular shape. For each layout object an orthogonal co-ordinate system is defined. The origin of each of these co-ordinate systems is at the top left corner of the object. The horizontal (x) axis corresponds to the top edge, and the vertical (y) axis corresponds to the left edge of this layout object. Horizontal positions are measured from the vertical axis to the right, and vertical positions are measured from the horizontal axis downwards. All positions and dimensions are specified as integral multiples of a *basic measurement unit* (BMU). The BMU is defined as 1/1200 of an inch.

The objects immediately below the level of the page are positioned in absolute page co-ordinates, while all objects subordinate to that level are positioned relative to the object immediately superior to them. Each subordinate object is contained entirely within the area of its superior object.

Within a page, frames and blocks may be positioned in such a way that they intersect partially or fully. The principles for intersecting layout objects are based on a sequential layout order specified in the standard (layout objects later in the sequence are said to overlay objects earlier in the sequence), and an attribute called *transparency*: Two values of this attribute are possible, opaque and transparent. If an opaque block overlays another layout object, any content of the underlying object is not imaged in the area of intersection. If a transparent block overlays another layout object the image of the underlying object is combined with the image of this block.

Monochrome imaging is the default method for imaging text. The background colour is implementation-dependent, and the foreground is a contrasting colour. A single colour system is specified as being applicable to text interchange. It has the capability of imaging eight colours. As an alternative, it may be used with colour tables to provide the possibility of altering the colours in an image of some text without altering the colour specification in the document. The concrete coded representations of the colour system and the possible provision of other colour systems have to be specified in the various content architectures.

2.2.1.6 *SC18/WG5/DP8613, Part 6: Character Content Architectures.* Part 6 [15] of the standard defines the Character Content Architectures. Therefore, this part must determine the particular characteristics of basic logical and layout objects related to content

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1174

priate parameters incorporated in the protocol elements of the underlying OSI Session protocol.

2.2.3 *ISO TC97/SC18/WG8*: text processing languages. Initially this working group (former SC5/WG8) planned to prepare a multipart standard entitled "Computer Languages for the Processing of Text CLPT" dealing with all areas of document processing, except interchange. This means that CLPT deals with the structure and the contents of a document but not with its envelope. The multipart standard was planned to consist of the following parts:

1. General Introduction
2. Vocabulary
3. Programming Language
4. Entry and Editing Functions
5. Formatting and Composition Functions
6. Document Markup Metalanguage (SGML)
7. Markup Support Functions
8. Binding to the Graphical Kernel System
9. Application to WYSIWYG Processing
10. Registration Procedures

Part 6 was the major part of this multipart standard. It has reached the status of a Draft Proposal whereas there were not even first working drafts for the parts 7–10. Therefore SC18 decided to have a single standard SGML with the original ISO number of the multipart standard DP 8879 [17]. SGML is expected to become an International Standard in August 1986. The work on some of the other parts (e.g., part 3 and part 8) has been suspended. The rest has been rearranged and some new work items have been defined. The following list gives an overview on the actual working plan of SC18/WG8:

- *SGML Support Facilities*

1. Introduction—This part will give an overview on the other parts of this multipart standard.
2. Parser Function Requirements—This part of the standard will support the implementation of an SGML parser interpreting documents structured according to DP 8879.
3. Context-sensitive Data Entry—This part will define editor functions sensitive for the elements of a document defined according to DP 8879.
4. Formatting Functions—The purpose of this part of the standard is to describe the formatting functions needed for systems handling documents according to DP 8879.

- *SGML Document Interchange Format*. This standard dealing with the interchange of SGML documents will be based on ODIF. There are some features in SGML which cannot be handled with the current version of ODIF. Therefore this standard has to be a superset of ODIF.
- *Procedure for the Registration of Markup Constructs*. For the interchange of SGML documents there has to be an agreement about the elements used in a special document class because the definition of the document class does not contain any semantics. A proposal for the registration of standard elements like "paragraphs" and "headings" is being prepared by the American Association of Publishers.
- *Procedure for the Registration of Fonts*. Considering the number of fonts available today and the expected increase in their numbers, a registration procedure similar to that of books (ISBN) is proposed. The identifier of a font has to contain font characteristics of the font such that a recipient of a document is able to select a "good font" as a substitute for that used by the sender, when the latter is not available at the recipient site. This standard will contain rules for specifying font identifiers.

In addition to these standards, two technical reports will be prepared:

- Vocabulary for Computer-Assisted Publishing.
- SGML Support Facility—Interface with Text Entry Systems. This technical report will define how SGML can be integrated into existing text processing systems.

First proposals for most of these work items are expected in September 1985. The following section contains a detailed description of the functionality and the syntax of SGML.

The Standard Generalized Markup Language SGML (formerly Generic Document Representation Specification) provides a formal grammar for specifying a generic logical definition of a document. In SGML this is called Document Type Definition. The type definition includes a specification which elements (objects in terms of ODA) and attributes can occur in a document and in what order.

It also defines a special markup language for this document type. This markup language is used in the specific logical structure of a document structured according to the generic logical definition. The markup language defines a syntax, but no semantics. The processing instructions associated with the markup are collected outside the document in so-called procedures. For different applications, different procedures can be associated with the elements and attributes without changing the markup of the document. Documents which exist only in final formatted form are not within the field of application of this standard.

The following paragraphs describe the functionality and syntax of SGML guided by some examples.

In terms of SGML a document consists of different elements. The structure of a document is specified in its type definition by using a notation similar to that used in regular expressions. This notation includes operators to indicate sequential ordering, repetition, optionality, alternative choice and required appearance. The notation for syntax productions is as follows:

Occurrence of syntactic tokens:

? Optional (0 or 1 time)
+ Required and repeatable (1 or more times)
* Optional and repeatable (0 or more times)

Ordering and selection of syntactic tokens within a parenthesized group:

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 3 of 15

portions of some character content architecture, and the precise character elements making up character-oriented content portions.

There are three types of attributes defined for basic objects related to character-oriented content portions:

- Layout attributes (e.g., Initial Offset)
- Logical attributes (e.g., Widow Size)
- Shared attributes (e.g., Background Colour, Line Spacing)

Obviously, for some attributes it is difficult to decide to which category they shall belong.

Some of these attributes are used for positioning character elements in a basic layout object. Characters are positioned in so-called *character boxes* which are laid out sequentially (and in some specified orientation) along a *character path* making up a *line* of characters. According to the value of the line progression attribute the basic layout object is sequentially filled with lines of this kind.

The colour system used in the character content architectures is compatible to the colour system defined in part 5. It provides three colour imaging attributes:

- Background colour, used for a basic object as a whole
- Fill-in colour, used as an alternate background colour for single character boxes
- Foreground colour, used for the shape of the characters

Other attributes of basic objects which are related to character-oriented content portions are responsible for determining the emphasis and font of the character elements of this content portion. Possible values of emphasis are underlining, intensity, blinking, inverse image, italicized, crossed-out.

The content of a basic object structured according to a character content architecture is a character string consisting of a combination of graphic characters, certain control functions and space characters. Any sets of graphic characters may be used in character-oriented content portions if they are only aligned to the code extension techniques defined in ISO 2022 [16]. Control functions can be briefly categorized into format effectors (e.g., cursor control functions), interim formatting functions, presentation control functions (e.g., for distinguishing between different fonts, styles, renditions) and code extension control functions. There are three types of control functions:

- Layout control functions (e.g., Set Justification Space)
- Logical control functions (e.g., No Break Here)
- Shared control functions (e.g., Background Colour, Line Spacing)

Seven different concrete character content architectures are defined in the standard which may be used for different kinds of applications (thus, subsets of the overall functionality have been specified for, e.g., TELEX and TELETEX applications). These character content architectures are further categorized into three classes: one for image form, one for processable form, and one for formatted processable form documents. For each of the defined character content architectures the attributes and control functions which shall be provided are specified.

2.2.2 *CCITT/SG VIII/T.73: document interchange protocol for the telematic services.* CCITT has no Study Group which is directly responsible for a general model for office document architecture. But, with respect to its mixed-mode TELETEX/TELEFAX service some requirements for document structuring have been identified. In its first version (about 3 years ago), the Study Group VIII responsible for the TELETEX/TELEFAX service has developed a proposal of its own for specifying an interchange format for mixed-mode documents—mainly including features clearly distinguishing between the character-oriented and the facsimile-oriented parts of the text and for allocating appropriate attributes to them.

Fortunately, in sight of the development of the ODA model by ISO/TC97/SC18 this proposal has been dropped in favour of the ODA approach.

But—as only a small subset of the ODA model is necessary for and directly applicable to the current mixed-mode service—only that subset has been described in more detail in the corresponding Recommendation T.73 [9]. All other features are marked as being for further study. This small subset is widely compatible to the respective ODA features and is briefly introduced below.

Currently, the T.73 approach makes only use of document profiles and of generic layout definitions and specific layout structures (i.e., the logical part and the specification of its relationship to the document layout have been left out). With respect to layout structures two different levels of support are specified:

1. On the one hand, an interchange format for quite general layout definitions/structures is specified in this Recommendation—again in X.409 notation and using the ODIF data stream B. It comprises, in principle, a rather large subset of the layout attributes which can be used in ODA documents.

2. On the other hand, only two small subsets of this general interchange format shall be really used currently, between which one may choose before the transmission of each document:

- TIF.0: Facsimile group 4, describing a document as a number of facsimile encoded pages, and
- TIF.1: Mixed-mode TELETEX/TELEFAX, describing a document as a number of either character- or facsimile-encoded blocks on a sequence of pages.

Only a subset of the general layout attributes of T.73 is available for the TIF.0 and TIF.1 applications. Two kinds of TIF.0 and TIF.1 can be distinguished:

- the basic TIF.0/TIF.1, which shall be supported by all T.73 implementations, and
- the extended TIF.0/TIF.1, which comprises additional (i.e., optional) parameter values.

Optional features must be explicitly negotiated with the corresponding communications partner by appro-

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1176

, All must occur, in the order shown
& All must occur, in any order
| One and only one must occur

The occurrence indicators are applied first, then the ordering connectors. Parentheses can be used as in mathematics to change these priorities.

The following example defines an element "chapter" which consists of a required element "heading" followed by any number of paragraphs and list in any order:

⟨!ELEMENT chapter (heading, (paragraph|list)*)⟩

So called markup tags are used to map specific document text or other visual information to logical document elements. Markup consists of start- and end-tags indicating the start respectively the end of a particular element. An example for markup is

⟨par⟩ This is paragraph text ⟨/par⟩

Characteristics of specific document elements can be described with the help of attributes. Attributes can be provided in the definition of the element. Actual values for attributes can then be supplied as part of the document markup. For example, an attribute indicating the major language of a chapter of a multilingual document could be defined in the following way:

⟨!ELEMENT chapter (heading, paragraph +)
language (German|English|French) German⟩

Corresponding markup may look like this:

⟨chapter language = English⟩

Text and character substitution is implemented in SGML by means of entities. This serves the purpose of handling unkeyable or otherwise confusing characters (for example the German ä, ü, ö or ß). It also provides an abbreviation facility. An example of an entity definition is:

⟨!ENTITY OSI "Open Systems Interconnection"⟩

The reference to this entity could appear embedded in text:

SC16 developed a Reference Model for &OSI;.

Its expansion would be:

SC16 developed a Reference Model for Open Systems Interconnection.

Full-scale SGML markup can be detrimental to document readability and cause unnecessary keying effort. SGML offers several features to allow for leaving away markup when the markup rigor is not affected. For example, the end-tag of an element need not appear when the start-tag of the next element implies the element end. The minimization features are extremely important for user acceptance.

REFERENCES

1. ISO 7498, Open system interconnection, basic reference model. International Organization for Standardization, Geneva (April 1982).
2. CCITT Draft Recommendation X.400. Message Handling Systems: system model—service elements CCITT Draft Recommendation. X.401: Message Handling Systems: basic service elements and optional user facilities. CCITT Draft Recommendation X.408: Message Handling Systems: information type conversion rules.
3. CCITT Draft Recommendation X.411. Message Handling Systems: message transfer layer.
4. CCITT Draft Recommendation X.420. Message Handling Systems: message transfer layer.
5. CCITT Draft Recommendation X.409, Message Handling Systems: presentation transfer syntax and notation.
6. CCITT Draft Recommendation X.410. Message Handling Systems: remote operations and reliable transfer server.
7. CCITT/SG VIII, Recommendation T.62, Control procedures for teletex and Group 4 facsimile services (June 1983).
8. CCITT Draft Recommendation X.430. Message Handling Systems: access protocol for teletex terminals.
9. CCITT/SG VIII: T.73, Document interchange protocol for the telematic services (October 1983).
10. ISO DP8613, Part 1: Introduction. International Organization for Standardization, Geneva (March 1985).
11. ISO DP8613, Part 2: office document architecture. International Organization for Standardization, Geneva (March 1985).
12. ISO DP8613, Part 3: document profile. International Organization for Standardization, Geneva (March 1985).
13. ISO DP8613, Part 4: office document interchange format. International Organization for Standardization, Geneva (April 1985).
14. ISO DP8613, Part 5: positioning and imaging. International Organization for Standardization, Geneva (April 1985).
15. ISO DP8613, Part 6: character content architecture. International Organization for Standardization, Geneva (March 1985).
16. ISO DIS 2022, Information processing—ISO 7-bit and 8-bit coded character sets—code extension techniques. International Organization for Standardization, Geneva (April 1982).
17. ISO DP8879, Standard generalized markup language (SGML). International Organization for Standardization, Geneva (September 1985).

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1177

THIS PAGE BLANK (USPTO)

BEST AVAILABLE COPY

XP 000159229

THE TRANSACTIONS OF THE IEICE, V E73(1990)July, No.7, Tokyo, JP
2334 The Transactions of the Institute of Electronics, Information and Comm. Engineers
H04L 23/06
1133
E p. 1133-1146
PAPER <Special Issue on Cryptography and Infomation Security>
G06F1/00N
G07F17/16
G07F7/00C

Superdistribution : The Concept and the Architecture

Ryoichi MORI† *and* Masaji KAWAHARA††, *Members*

SUMMARY Superdistribution is an approach to distributing software in which software is made available freely and without restriction but is protected from modifications and modes of usage not authorized by its vendor. By eliminating the need of software vendors to protect their products against piracy through copy protection and similar measures, superdistribution promotes unrestricted distribution of software. The superdistribution architecture we have developed provides three principal functions: administrative arrangements for collecting accounting information on software usage and fees for software usage; an accounting process that records and accumulates usage charges, payments, and the allocation of usage charges among different software vendors; and a defense mechanism, utilizing digitally protected modules, that protects the system against interference with its proper operation. Superdistribution software is distributed over public channels in encrypted form. In order to participate in superdistribution, a computer must be equipped with an S-box —a digitally protected module containing microprocessors, RAM, ROM, and a real-time clock. The S-box preserves secret information such as a deciphering key and manages the proprietary aspects of the superdistribution system. A Software Usage Monitor insures the integrity of the system and keeps track of accounting information. The S-box can be realized as a digitally protected module in the form of a three-dimensional integrated circuit.

1. Introduction

Superdistribution is an approach to distributing software in which software is made available freely and without restriction but is protected from modifications and modes of usage not authorized by its vendor. Superdistribution relies neither on law nor ethics to achieve these protections; instead it is achieved through a combination of electronic devices, software, and administrative arrangements whose global design we call the "Superdistribution Architecture". The concept was invented by Mori in 1983; it was first called the "Software Service System"[1],[2]. Since 1987, work on superdistribution has been carried out by a committee of the Japan Electronics Industry Development Association (JEIDA), a non-profit industrywide organization. That committee is now known as the Superdistribution Technology Research Committee.

Superdistribution of software has the following novel combination of desirable properties:

(1) Software products are freely distributed without restriction. The user of a software product pays for using that product, not for possessing it.

(2) The vendor of a software product can set the terms and conditions of its use and the schedule of fees, if any, to be charged for its use.

(3) Software products can be executed by any user having the proper equipment, provided only that the user adheres to the conditions of use set by the vendor and pays the fees charged by the vendor.

(4) The proper operation of the superdistribution system, including the enforcement of the conditions set by the vendors, is ensured by tamper-resistant electronic devices such as digitally protected modules.

From a different viewpoint, the needs of users and the needs of vendors have until now been in irreconcilable conflict because the protective measures needed by vendors have been viewed by users as an intolerable burden. The superdistribution architecture provides a resolution to that conflict that serves the interests of both parties. Wide distribution benefits vendors because it increases usage of their products at little added cost and thus brings them more income. It benefits users because it makes more software available and the lower unit costs lead to lower prices. It also creates the possibilities of additional value-added services to be provided by the software industry. Moreover, users themselves become distributors of programs that they like, since with superdistribution there is absolutely nothing wrong with giving a copy of a program to a friend or colleague.

It might seem at first that publicly distributed software such as freeware and shareware already solves the problem addressed by superdistribution. But the likelihood of the authors being paid is too small for public for public domain software to play a leading role in the software industry. Superdistribution software is much like public domain software for which physical measures are used to ensure that the software producer is fairly compensated and that the software is protected against modification. While public domain software might achieve the aims of superdistribution in an idealized world where all users paid for software voluntarily and none of them abused it, we see little hope that such an

Manuscript received February 14, 1990.
Manuscript revised April 17, 1990.

† The author is with the Institute of Information Sciences and Electronics, University of Tsukuba, Tsukuba-shi, 305 Japan.
†† The author is with Master's Degree Program in Sciences and Engineering, University of Tsukuba, Tsukuba-shi, 305 Japan.

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1179

Table 1 Levels of software protection technology.

level	key concept	remarks
4	superdistribution	SdA(Superdistribution Architecture) 1983 R.Mori(University of Tsukuba)
3	execution privileges	"Right-To-Execute":ABYSS(A Basic Yorktown Security System) 1987 S.R.White(IBM)[3]
2	customizing software with a computer ID	customizing deciphering key (software is common) 1986 A.Herzberg PPS(Public Protection of Software)[4] 1984 D.J.Albert (Enciphering and key management)[5] 1982 G.B.Purdy SPS(Software Protection Scheme)[6]
		customizing each copy of the software
1	hardware protection	controling execution: hardware key, e.g., ADAPSO Key-ring[7]
		inhibiting duplication: copy protection, noncompatible ROM
0	no physical protection	laws & ethics

idealized world will ever come to exist.

Table 1 describes a hierarchy of levels of software protection[3]-[7]. The previous work most similar to superdistribution is the ABYSS architecture[3],[6] developed by White, Comerford, and Weingart at the IBM Thomas J. Watson Research Center in Yorktown Heights, New York. ABYSS is based on the notion of a use-once authorization mechanism called a "token" that provides the "right to execute" a software product. All or part of the software product is executed within a protected processor, and is distributed in encrypted form. Physical security for an ABYSS processor is provided by a dense cocoon of wires whose resistance is constantly monitored by the processor. A change in resistance indicates a likely attempt to penetrate the system. The chief difference between superdistribution and the ABYSS scheme is that superdistribution does not require the physical distribution of tokens or anything else to users of a software product. In other words, ABYSS requires that software be paid for in advance while superdistribution does not.

2. The Superdistribution Architecture

The superdistribution architecture we have developed provides three principal functions:

(1) Administrative arrangements for collecting accounting information on software usage and fees for software usage.

(2) An accounting process that records and accumulates usage charges, payments, and the allocation of usage charges among different software vendors.

(3) A defense mechanism, utilizing digitally protected modules, that protects the system against interference with its proper operation.

In order to participate in superdistribution, a computer must be equipped with a device known as an *S-box* (Superdistribution Box)†. An S-box is a protected module containing microprocessors, RAM, ROM, and a real-time clock. It preserves secret information such as a deciphering key and manages the proprietary aspects of a superdistribution system. An S-box can be installed on nearly any computer, although it must be specialized to the computer's CPU type. It is also possible to integrate the S-box directly into the design of a computer. We call a computer equipped with an S-box an *S-computer*.

Programs designed for use with superdistribution are known as *S-programs*. They can be distributed freely since they are maintained in an encrypted form.

In order to make it acceptable to users, software vendors, and hardware manufacturers, the superdistribution architecture has been designed to satisfy the following requirements:

(1) The presence of the S-box must not prevent the host computer from executing software not designed for the S-box. The presence of the S-box must be invisible while such software is active.

(2) The modifications needed to install an S-box in an existing computer must be simple and inexpensive.

(3) The initial investment required to make S-programs generally available must be small.

(4) The execution speed of an S-program must not suffer a noticeable performance penalty in comparison with an ordinary program.

(5) The S-box and its supporting protocols must be unobtrusive both to users and to programmers.

(6) The S-box must be compatible with multiprogramming environments, since we anticipate that such environments will become very common in personal computers.

In our current design a program can be written without considering the S-box, but the program must be explicitly encrypted before it is distributed if it is to gain the protections of superdistribution. This encryption can be done by a programmer, using the S-box itself.

† The S-box is unrelated to the S-boxes used in the Data Encryption Standard.

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1180

The design of a superdistribution architecture can be decomposed into four tasks:

(1) Design of the superdistribution network.
(2) Logical design of the S-box and its interfaces.
(3) Design of the supporting software and file structures, including appropriate cryptographic protocols and techniques.
(4) Design of the protection for the S-box.

Technology for accomplishing each of these tasks is now nearly within to the state of the art. In the rest of this paper we describe our approach to these tasks. We have already designed and constructed two prototype S-computers with their supporting software. Prototype II, the version we are now working with, satisfies the six requirements stated above.

3. Design of the Superdistribution Network

The technical innovations that we describe here are best understood in the context of a network that provides superdistribution of S-programs and the files needed in a user's computer in order to support the use of the superdistribution services. We emphasize, however, that distributing the S-software itself is not a function of the network since a user can obtain that software by any convenient means — from a bulletin board, making a copy of a friend's program, or perhaps purchasing a collection of S-programs at a nominal price. S-programs are stored and transmitted in encrypted form, so the transmission paths need not be protected in any way.

Figure 1 illustrates a typical software distribution system that utilizes the superdistribution architecture. Each S-computer — that is, an end-user computer supporting superdistribution — is equipped with an S-box. The S-box contains a metering program, the Software Usage Monitor (SUM), that enforces the terms set by each software vendor for executing that vendor's products and keeps track of how much the user owes to each vendor. The S-box generates a payment file that contains this information. The fees charged for software usage are measured in units that we call *S-credits*. Payment files are encrypted and transmitted to the collection agency through the network as shown in the figure.

The collection agencies receive the payment files from users, process those files, and transmit payments to vendors — both the authors of the S-programs and the manufacturers of the S-boxes. Each collection agency has an S-box in its computer. The payment files are decrypted and processed under control of this S-box so as to ensure the integrity of payments to the vendors of S-programs and of the supporting hardware as well.

The clearinghouse keeps track of funds transfers engendered by superdistribution. The clearinghouse can be either a new organization or an existing one, e. g. a credit card company, that is prepared to provide the necessary services. The advantage of creating a new organization is that it provides additional degrees of freedom in the systems design. The disadvantage is that it requires a large initial investment. Using an existing organization as the clearinghouse not only saves that investment but also gives that organization the opportunity to enlarge its market.

Identification numbers (ID's) are essential to this arrangement. Each user, each software vendor, each S-box manufacturer, and each collection agency has a unique ID. In addition, users can also have ID's, either as individuals or as organizations. The ID of a user is usually in a different name space than the ID of that user's machine. User ID's provide a convenient mechanism for establishing credit, since they are associated with the individual or organization who is actually

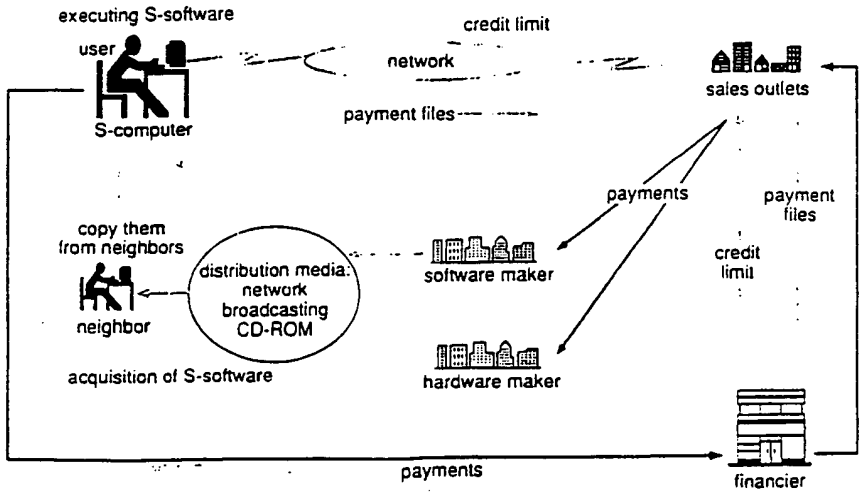


Fig. 1 Example of software distribution system utilizing the superdistribution architecture.

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1181

paying for the software. (An organization or even an individual may have more than one machine.) On the other hand, a software distribution system based purely on S-box ID's can provide a high degree of privacy for users.

Requiring prepayment for software usage avoids any risk of default, but such a requirement is unattractive to users and negates the social benefits that we hope to see provided through superdistribution. It is easy to understand why this should be so if we consider how people would react to being required to pay for all their water and electricity in advance.

The superdistribution scheme does not provide any absolute guarantee that users will pay what they owe, or even that they will return the necessary payment files to the collection agents. However, the S-box, which contains a real-time clock, will suspend its services (other than transmitting payment files) if the conditions, which are specified by the vendor or the system, are not met. Transmission can be either over a telecommunication link or with a memory card. In the event that a user transmits the payment files but does not remit the corresponding payment, a collection agent can apply appropriate sanctions.

Superdistribution does not rely on the honesty or goodwill of the manufacturer of the S-box. It is even possible to protect software designed for the S-box against attacks perpetrated by the manufacturer of the S-box. However, the methods of providing such protection are beyond the scope of this paper.

To join the system, a user need only insert an S-box, most likely in the form of a coprocessor chip, into his or her own personal computer. A collection agency can join the system in the same way. The collection agency needs a slightly different form of S-box, one that contains the software for decoding and processing the payment files. Processing at and between the collection agencies and the clearinghouse can be conveniently handled by a Credit Authorization Terminal (CAT) very similar to the ones now in use in many retail establishments.

3.1 Usage of the S-Box

Suppose that I am interested in using some S-programs. I obtain an S-box from an agent either in person or by mail. My agreement with the agent includes a credit authorization or a prepayment of, say, $100. I can now use up to $100 worth of S-programs. When I obtain the S-box, I can also obtain a memory card for it. The memory card is used to record accounting information that describes my usage of S-programs as well as the balance in my account.

To renew my usage, I must communicate the accounting information to the agent. I can do this either by establishing modem communication with the agent or by physically presenting the memory card (if I have one) to the agent. Suppose I use a modem. Then I transmit a message specifying my usage to date of each S-program that I have run. This message is generated by the S-box and enciphered so that it cannot be tampered with by anyone. The agent charges my credit card account for that usage and credits the vendors of the software that I have used. He then transmits back to me an enciphered message that resets my authorization to $100.

On the other hand, suppose that I physically present the memory card either in person or by mail. I can either have it renewed on the spot or (if I choose to mail it in) can have a second card sent to me in advance so that I am never without a card.

3.2 Customer Support and Manuals in Superdistribution

Superdistribution can also be helpful in conjunction with forms of support for users of S-programs that are not yet provided electronically.

Superdistribution changes the environment for telephone support. First, superdistribution eliminates the need to discriminate illicit and authorized users, because the incidence of illicit usage can be kept reasonably low. Second, superdistribution provides a way of charging for telephone support fairly. An S-program can generate a code number, with internal checking, and charge the user for that code number. The user then calls the vendor, asks his questions, and provides the code number. The vendor validates the code number.

Superdistributed software can be supported by hypertext and other forms of electronic documentation, but such documentation is still unlikely to replace printed manuals entirely. Currently, manuals serve both to educate the user and to provide an additional safeguard for the vendor against piracy (since a user can't buy the manuals separately from the software). With superdistribution, the safeguarding function is unnecessary and paper manuals can be sold as freely as books. In particular, a user can obtain several copies of the printed manuals if he wishes, and can even purchase the manuals without purchasing the software at all. Similar remarks apply to manuals distributed on CD-ROMs, which could be used to generate customized versions of the printed manual for particular configurations of the software, the hardware, or other aspects of the working environment.

4. Design of the S-Box and Its Interfaces

The function of the S-box is to execute the Software Usage Monitor in a secure way. The S-box also contains the cryptographic keys that ensure the integrity of the system. These keys are kept secret by storing them within a digitally protected modules (see Sect. 6).

An S-box can be added to an existing computer in any of several ways:

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1182

(1) Attaching it to an I/O port.
(2) Connecting it to the bus.
(3) Placing it between the CPU and the bus.
(4) Placing it on the same chip as the CPU or inside the CPU.

Methods (1) and (2) require no modification to the computer; our Prototype I used method (1). This method has the disadvantage that it introduces significant overhead in a multiprogramming environment. Method (4), though more difficult to implement initially, offers the best performance and the lowest cost. Because methods (3) and (4) require modifying the computer, we chose to use method (2), connection to the bus, for Prototype II.

This connection is best realized by making the S-box a coprocessor and using an existing coprocessor socket. Our current implementation uses a second computer connected to the coprocessor socket of the first one; our goal is to fabricate the S-box as a single chip that can be placed in that coprocessor socket. We are using an MC68020-based computer because of its compatibility with other equipment in our laboratory, but adapting the design to other types of processors is not difficult.

All the protection needed to ensure the integrity of the payment files and of the software is concentrated in the S-box. There is no need to protect any of the communication paths shown in Fig. 2. The signals sent over the communication paths are all encrypted, so dedicated networks are not necessary to ensure the security of the system. Any public network can be used, and the added cost of a dedicated network can be avoided. In fact, since the communications links need not be kept constantly active the system is even suitable for use with portable personal computers.

The S-box provides a limited form of protection against viruses, in that programs that are specifically designed to work with the S-box cannot be modified at the user's computer and so cannot be disabled or otherwise taken over by a virus. However, the S-box does not protect against programs, distributed through superdistribution or otherwise, whose effect is on parts of the system unrelated to the S-box.

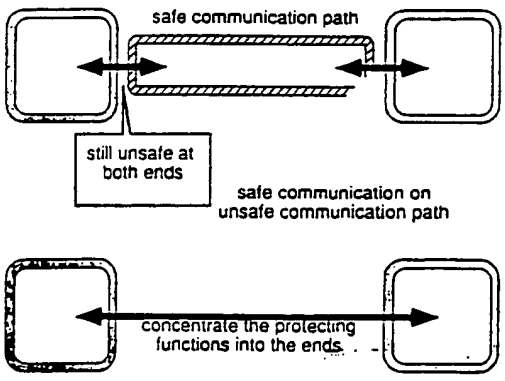


Fig. 2 No protection of communication paths results better performance/cost.

Some of the functions called for may appear to be expensive—in particular, the ability to provide the necessary physical protection and to erase the cryprographic keys recorded in the S-box in the event of an attack. However, these functions can be achieved at reasonable cost if the S-box is mass-produced as a single IC chip (or a small group of such chips).

The workings of the S-box, which we describe below, depend on the existence of cryptographic keys within the S-box. A potential problem could arise were the equipment manufacturing the S-box to be disabled and the values of the keys to be lost. This problem can be solved, although it requires the use of a different kind of protected module.

We have considered but rejected the idea of using simpler memory cards, similar to the farecards used in some transit systems, that would merely record an account balance. There are two problems with such cards. First, separate mechanisms would still be needed to record and transmit the accounting information described above. Second, the devices generally available for reading and writing such cards are insufficiently secure. A cheater could obtain such a device and modify the data on the card without using the S-box at all.

4.1 The Software Usage Monitor

The Software Usage Monitor is executed in the S-box. It performs the following functions:
(1) It monitors the execution of an S-program in order to make sure that it is only executed in the manner intended by its vendor.
(2) It encrypts and decrypts S-programs and other necessary information.
(3) It maintains an account of the charges associated with the execution of an S-program.

An S-program can issue instructions to the Software Usage Monitor. These instructions are realized as extended instructions of the CPU.

In Prototype II we have implemented the Software Usage Monitor through an emulation of the coprocessor functions. We have used an MC68020 board fitted with an MC68881 coprocessor socket, connecting a second computer (the emulator) to that socket through an interface circuit as shown in Fig. 3. The current implementation does not provide for multiprogramming because the Apple Macintosh we are using, to which an MC68020 board is plugged in, does not yet have that capability.

Further limitations on Prototype II are that it does not provide encryption and that it is not encapsulated as a digitally protected module. We consider those limitations acceptable because the purpose of our experiments at this stage is to validate the execution control and

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1183

charge control functions of the Software Usage Monitor.

4.2 Architecture of Prototype II

Figure 4 shows a conceptual diagram of the architecture of Prototype II.

- The MC68020 processor executes the S-program and communicates with the coprocessor. The coprocessor ensures the legitimacy of the execution.
- The interface section communicates with the MC68020 according to the standard MC68020 coprocessor protocol[9],[10].
- The processing section interprets and executes the coprocessor commands issued by the MC68020.
- The execution control section monitors the execution of the S-program.
- The accounting buffer contains pricing information for each currently executing S-program as well as accumulated usage information. The pricing information in the accounting buffer is a subset of the information in the tariff section of an S-program (see Sect. 5.1).
- The payment file contains a record of payments.
- The charge control section updates the S-credit balance, utilizing the information in the accounting buffer and the payment file. It also keeps a record of access violations and halts execution of the S-program if the number of violations exceeds some threshold. (Our experience suggests that access violations occasionally happen by accident, so this threshold should be nonzero). The charge control section also implements functions required to support the user utility program.
- The cryptography section performs three functions:
(1) It decrypts the information in the tariff section of the S-program and enters that information into the accounting buffer. It does this as part of the process of loading an S-program into the S-box. Either a public-key or secret-key cryptosystem methods can be used.
(2) It decrypts the encrypted portions of the S-program itself, using in this case a high-speed conventional cryptosystem.
(3) It encrypts arbitrary programs upon request. This facility is necessary so that a programmer can create new S-programs without outside assistance. In particular, no assistance is needed from the manufacturer of the S-box.

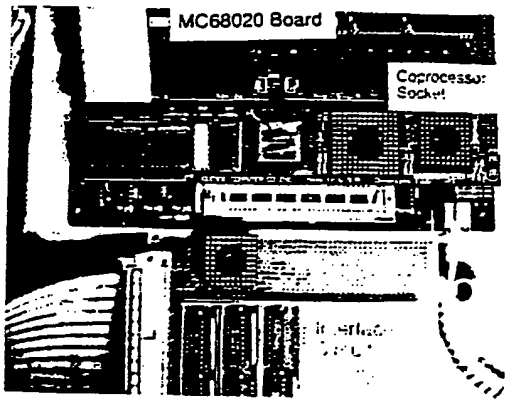


Fig. 3 Implementation of Prototype II.

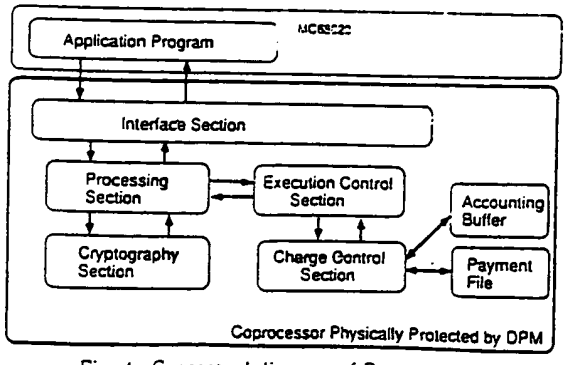


Fig. 4 Conceptual diagram of Prototype II.

5. Design of the Supporting Software and File Structures

5.1 Structure of an S-Program

The structure of an S-program as implemented in Prototype II is shown in Fig. 5. The pricing information for a S-program is contained in its tariff section. When execution of the S-program is initiated, the coprocessor verifies the information in the tariff section and copies the pricing information into the accounting buffer of the S-box. A verification routine, described below, is embedded in the body of the S-program. Execution is aborted if the verification routine detects any inconsistency in the tariff section.

The tariff section includes the following:
(1) Software ID: an identifier unique to the S-program.
(2) Access control key: A key used by the authentication routine in the S-program body. This key is checked by the coprocessor.

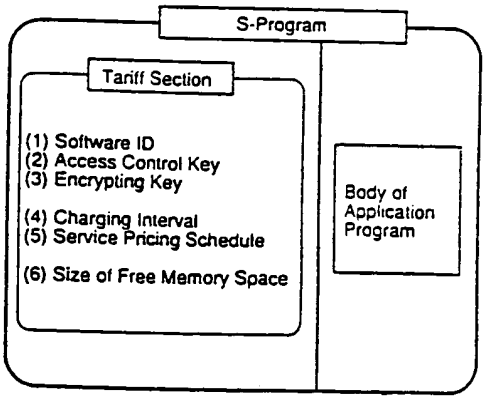


Fig. 5 Structure of S-program.

BEST AVAILABLE COPY

(3) Encrypting key: A key used to encrypt the machine instructions in the body of the S-program. An encrypted block of instructions is transferred to the coprocessor, where it is decrypted using this key and then executed.
(4) Charging interval: the length of execution time for which a single S-credit is charged to the user.
(5) Service pricing schedule: the number of S-credits charged to the user each time a particular software service, e. g. saving a file, has been rendered and successfully completed.
(6) The amount of memory required within the coprocessor for executing the S-program.

Note that items (4) and (5), which together constitute the pricing information, allow for two styles of charging: per unit of time (by setting (5) to zero) or per execution (by setting (4) to zero). Combinations of the two styles are also possible.

5.2 Execution of an S-Program

Execution of an S-program is monitored by the program and the coprocessor working together. The coprocessor halts execution whenever it detects a protocol violation. For proper protection, the S-software must be structured so that analysis of it by an intruder is not possible. Some methods of achieving this are:
(1) The coprocessor receives a number from the S-software and compares it with an encrypted value, returning the result of the comparison.
(2) The coprocessor receives data from the S-software and returns a jump address.
(3) The coprocessor verifies that a particular message is sent by the S-software within a prescribed period.
(4) The coprocessor receives a block of encrypted MC68020 instructions and executes them, placing the results of the execution in the registers and/or the memory of the MC68020.

These methods can be used individually or in combination.

The sequence of events that takes place as an item of S-software is executed is as follows:

- Initialization. The pricing information is sent to the coprocessor by the initialization routine when execution of the S-software commences. This can be done using general purpose coprocessor instructions[9],[10]. S-credits are then decreased periodically until execution of the S-software is terminated.
- Execution. The check routine in the software body is executed, and execution of the software is aborted if the prescribed protocol is not satisfied. Methods (1)-(3) of execution control as described above have been implemented. The implementation techniques are as follows:

—For (1), the software ID, the access control key, and a random number are sent to the coprocessor. The random number can be encrypted, although we have not yet done this. The result of comparing the random number with a known value is then returned to the processor.
—For (2), we transfer a jump address table to the coprocessor during initialization. This table can subsequently be referenced by the S-software. The coprocessor then returns the appropriate jump address.
—For (3), the access control key, the range of acceptable response times, and a random number are sent to the coprocessor. The range is represented as a lower limit and an upper limit. The coprocessor then checks that the time of the next message is within the limits. If it is not, the coprocessor aborts execution of the S-software by interrupting the main processor.

- Termination. The coprocessor is informed when the S-software has completed execution. This can be implemented using general purpose coprocessor instructions. At this time the payment file is updated to account for the usage.

5.3 Supporting Files

The *payment file* keeps track of S-credits that are owed as the result of software usage. Each record in a payment file ordinarily contains three fields: a payer, a receiver, and an amount. The collection of payment files is an essential function in a superdistribution system in order to make sure that revenues are properly distributed to the providers of services.

The *privilege file* records a user's privileges with respect to software usage. For example, if a user has purchased a program then the user has the privilege of using it thereafter without paying any additional fees. Another kind of privilege is a volume discount: after a certain amount of usage, the charging rate is decreased.

Carryover is a form of discount in which the money that a user pays for usage of a program is deducted from its purchase price if the user chooses to purchase the program at some later time. Carryover can be accommodated by associating a carryover parameter c with a particular program, where c is no greater than 1. Should the user decide to purchase the program, a credit of c times the accumulated usage charges is deducted from the purchase price. If a vendor chooses to set c to 1 for a particular program, then a user of that program need not make any decision as to whether or not to purchase the program. Carryover, if provided, is also recorded in the privilege file.

Some forms of superdistribution can be realized without having a privilege file. In these forms the charges are based on services provided, e. g. 10 credits for each program execution, 2 credits for each file save, 5 credits per printout, and 1 credit per 18 seconds of execution time.

The privilege file grows with time, since information is added to it but is rarely if ever deleted. Moreover

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1185

it must be preserved indefinitely. It is ordinarily the obligation of a software vendor to provide backup for the portion of the privilege file pertaining to that vendor's software.

A record in the privilege file is ordinarily generated at the same time as a record in the payment file and stored in the user's machine. In some environments in which users send payments separately, the vendor may generate records to be placed in the privilege file, but this arrangement is usually less convenient for users.

The portion of the privilege file pertaining to a particular vendor's software can be kept either in the user's machine or by the vendor. If privilege records are generated in one place and stored in another, then the superdistribution system must make allowances for delays in transmission and in confirmation.

If a superdistribution system provides for trial usage of software either free or at a discount, it must keep records of that usage in a *trial usage file*. Otherwise a user could use software indefinitely on a trial basis. These records need to be backed up, although backup is less critical than it is for the privilege file. The reason is that trial usage is not an obligation but rather a gratuity on the part of a vendor, and a vendor can reserve the right to cancel the privilege of trial usage at any time.

The *benefit file* keeps track of special benefits granted to the user by various vendors. The benefit file differs from the privilege file in that the information in the benefit file has no direct correspondence to the information in the payment file and is unaffected by what software is used or how much it is used. Examples of information in the benefit file are a certification entitling the user to educational discounts or a secret number entitling the user to run a certain program not available to the general public.

The *account file* is an aggregation of the particular files we have just discussed: the payment file, the privilege file, the trial usage file, and the benefit file.

A superdistribution system needs to provide secure backup for its accounting files and for the privilege file in particular. It need not make any special provision for backing up software since a user can back it up by any convenient means or get another copy without cost if the original copy is lost.

The backup requirements for the privilege file depend on whether or not privileges can decrease with time. If not, it suffices to ensure that the process of restoring the privilege file from its backup cannot generate additional privileges. This requirement can be met by associating an ID and a randomly generated validation number with each privilege file and encrypting the file before backing it up. The restoration process checks to make sure that the decrypted validation number is correct and that the backup file is indeed a proper one.

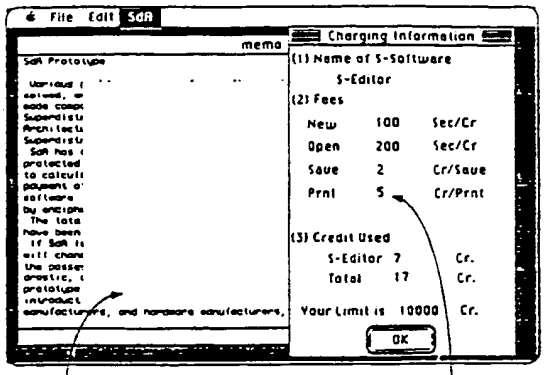


Fig. 6 Example of execution of user utility program.

5.4 Implementation of the User Interface

Since a user of an S-computer should be able to ascertain the status of his account at any time, we have built a user interface for retrieving and displaying that information. The user interface program provides two functions:

(1) Transmitting the payment file

(2) Displaying the accumulated charges for S-programs.

In Prototype I we implemented the user interface within the Software Usage Monitor; in Prototype II we have implemented it as a separate program. By making it a separate program we reduce the size and complexity of the software that needs to be permanently resident in the S-box. Prototype I allowed a great deal of flexibility in the way that usage was charged; Prototype II has adopted a simpler system based on a combination of charges for performing specific actions, e.g. opening a file, and charges per unit of time.

An example showing the execution of the user utility program is shown in Fig. 6. The user can inspect the record of software charges, the remaining credit balance, etc., through this program. Although Prototype II does not have a general multiprogramming capability, it does allow the user utility program to be executed while an application program is also executing.

6. Digitally Protected Modules

6.1 Design of the Digitally Protected Module

A protected module (PM) is a container for information that protects that information from attacks intended to read or write it in an unauthorized manner. Protected modules have also been described in the literature as "tamper resistant modules" or "protected processors". We prefer "module" to "processor" because we

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1186

are not concerned with protecting the hardware itself, but only with protecting the information being processed by the hardware.

The design presented here assumes that the S-box is implemented as a digitally protected module — that is, a module whose protective logic is based on digital technology. We plan to use three-dimensional integrated circuit technology, since we believe that a high level of physical protection can eventually be achieved by applying fabrication methods such as chip bonding to three-dimensional circuitry.

Increasingly effective levels of protection are possible :

(1) A protective method may rely on the ignorance or lack of resources of the attacker. For example, software can be stored in ROM in a form where access is difficult and does not follow the usual conventions of the computer to which it is attached.

(2) A protective method may rely on keeping a permanent record of attacks rather than on withstanding those attacks. If the proprietor of a protected module can retrieve this record, then attackers will be dissuaded by the knowledge that their activities will be discovered. Examples of devices using such methods are the counters on rented copying machines, the odometers on rented automobiles, and the electric meters placed on the main power lines of buildings.

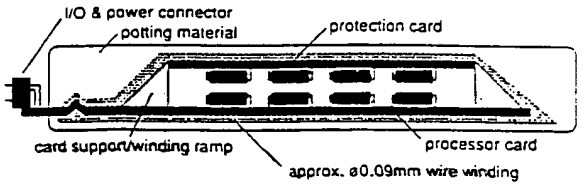
(3) A protective method may be designed to defend a protected module even when the proprietor of the module has no access to it, either physically or logically. Since no physical device can be expected to resist destruction indefinitely when the attacker has sufficient time and resources, a device using methods of this kind must be able to detect attacks and erase its contents before the attacker can retrieve them. Then an attacker is simply left with a broken module and has gained nothing.

(4) A protective method may be designed to defend a protected module even from attacks by its manufacturer. Since in some cases a protected module may contain information that the module's manufacturer is not authorized to access, this case is also of interest.

The device we discuss in this article is intended to achieve the third level of protection above, although we believe that it is even possible to achieve the fourth and highest level of protection.

Most earlier research on protected modules has either been theoretical in nature or has been subject to military classification. The μABYSS module[8] is an exception. Using this approach, an entire circuit board is enclosed in a cocoon of nichrome wire of approximately 0.09 mm diameter. Several windings, each having thousands of turns, are used. The circuit board records the protected information. The resistance of the windings is monitored in analog fashion to detect attacks (see Fig. 7).

In μABYSS, a 5 % change in resistance of the wire is taken as a threshold to determine whether an attack is taking place. This comparison is made with the original resistance value. A change of at least 1 % from the most recently measured value is also taken as an indication of an attack.



Source: Steve H. Weingart, IBM Thomas J.Watson Research Center

Fig. 7 Physical structure of μABYSS.

6.2 Operation of the Digitally Protected Module

One of our approachs is illustrated in Fig. 8. The protective mechanism consists of a random access memory (RAM) containing a great number of closely-spaced microscopic one-bit detectors. The DPM contains one or more layers of these detectors, packed tightly so as not to leave enough room for penetration between them. Layers of detectors can be staggered so as to increase the effective density. The memory can be implemented using either IC's or printed circuits. With these technologies the center-to-center distance of adjacent detectors can be made as small as 3 μm. The detectors are individually addressable, and each one can be read or written. A possible attack is indicated when any detector is found to have lost its normal operating functions.

The testing method is simple: write a random value into the detector and read it back. Then write the complement of that value into the detector and read it back. The element is considered to be working if and only if the retrieved values agree with the written values. If the values do not agree, a possible attack is indicated. We call this event an exception.

If an exception occurs, the microprocessor examines the faulty detector several more times. Repeating the test provides protection against random transient failures such as might be caused by alpha rays. The probability of such a failure and the consequent change of state is proportional to the time between writing and reading. If a detector is read immediately after it is written, the probability becomes very small. In some environments the probability of transient errors may be low enough so that transient errors can be disregarded altogether.

If an exception is judged not to be a transient error, then the DPM can test other detectors in the physical vicinity of the erroneous one. The number of faulty elements can then be compared to a threshold. If that threshold is exceeded, we assume that the DPM has been attacked. The threshold test reduces the chance of a

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1187

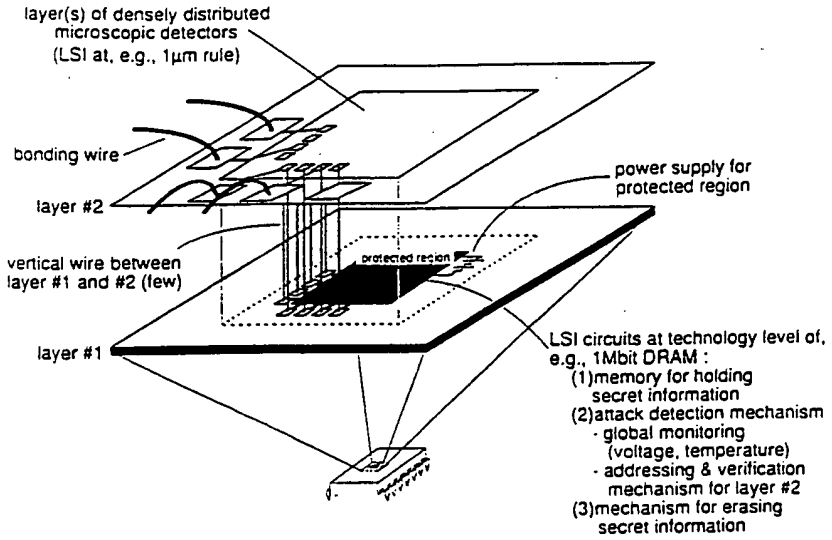


Fig. 8 Three-dimensional IC implementation of a digitally protected module.

false alarm.

Techniques that apply to RAM used in other applications can also be used for the DPM. For instance, the microprocessor can be provided with a list, resembling the list of bad tracks on a disk, that indicates elements known to be faulty. Similarly, it is possible to read and write blocks of several bits in parallel instead of operating on a single bit with each test. However, some economies are possible for the DPM that are not possible in general. For instance it is not necessary to refresh the memory because it can hold its state for at least ten milliseconds without being refreshed. That interval is much greater than the interval between writing and reading a bit. Such economies can help to reduce the cost of manufacturing the DPM.

The design of any type of protected module must address an inherent conflict. In order to make the device more likely to detect an attack it must be made more sensitive; but the more sensitive it is, the greater the likelihood of a false alarm. The more information that can be gotten about a presumed attack, the easier it is to resolve this conflict.

The digital design can provide more information than an analog design in the event of a fault because the digital design has more discrete components. In an analog design such as μABYSS there are relatively few windings. If a resistance measurement is off, there is no way to localize the fault further. In a digital design it is possible to check the detectors in the vicinity of the faulty one. The analog design can be brought closer to the digital one by using many small windings, but the control logic then becomes far more complex and it becomes much harder to manufacture the device.

We next consider various kinds of potential attacks on a digitally protected module and the protection against them:

(1) An attacker might attempt to separate the detecting layer and the protected region. Such an attack can be detected by monitoring the continuity of the interlayer wires.

(2) An attacker might aim at the detection mechanism itself rather than at the information being protected. This strategy can be foiled by placing the detection mechanism in the protected region.

(3) An attacker might attempt to manipulate the wires that connect the circuitry to the outside world. Such attacks can be prevented by a structure where the wires pass through the detecting layer, as described in the next section.

(4) It is possible to reuse a digitally protected module that has erased its cryptographic keys in response to an apparent attack, but caution is necessary in order to guard against Trojan horses or other attempts at subversion of the logical protection.

The protective capability of any protected module cannot be regarded as permanent. Once a module has been installed the hardware implementation of its defensive technology is fixed, even though the technology of attack advances continually. With time it becomes easier and easier to find ways of bypassing or otherwise neutralizing whatever defenses the module utilizes. Thus the useful life of a protected module is determined by the progress of the technology of attacks. A useful life of five years is probably not difficult to achieve. Twenty years would be desirable; ten years is probably about the longest time that we would consider practical. However, it is likely that the state of the art in attacking protected modules would be known to their proprietors, and the modules could be replaced when they are known to have become vulnerable.

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1188

6.3 Realization of Digitally Protected Modules

Three-dimensional large-scale integrated circuits[11], possibly manufactured using chip-bonding methods, provide an excellent method of realizing digitally protected modules. We have assumed such an implementation in Fig. 8.

Layer 1 consists of a protected region where the information to be protected is stored. The memory for the information can be implemented using technology at the level of 1 Mbit DRAMs. The protected region either has its own power supply or uses an external power supply. It is possible that there is more than one power supply. The protected region also contains circuitry whose function is to erase the information if an attack is detected. The erasure is accomplished by cutting off the power to Layer 1.

An attack might involve making holes in the device, etching it, or subjecting it to electro-optical reading. Layer 2 is made of devices and wirings designed to detect these kinds of attacks. It will be constructed using a technology such as 1-2 μm rule semiconductor devices.

The distance between Layer 1 and Layer 2 can be made sufficiently small, on the order of 3 μm, so that an attacker will not be able to penetrate between the layers. An attack from below Layer 1 is not feasible because any attempt to reach the components from that direction will cause the components to lose their charge. Should penetration from below be a concern, it is possible to place a layer of detectors there too, thus enclosing the protected region in a sandwich of detectors.

The wires between the two layers serve two purposes: to provide signal paths between the circuitry in the layers and to provide signal paths from the protected layer to the outside world. These wires are connected to small pads on the inner surface of each layer. They cover the entire perimeter of the DPM. Any disruption of their signals will have the same effect as a disturbance to the detectors, so they provide an additional level of protection to the device.

The larger pads on the upper surface of the detecting layer are bonding pads like those of a conventional IC. Their purpose is to provide connections for external wiring. Although external connections are logically necessary only for the protected circuits in Layer 1, the wires are routed via Layer 2 in order to prevent an attacker from gaining access to the protected region via the external connections.

The DPM can be encapsulated using an appropriate resin, preferably one that is not transparent. By mixing a substance such as alumina with the resin we can increase the resistance of the device to attacks using mechanical or chemical methods, or even attacks using lasers or plasmas. Simpler measures may, however, suffice for some environments.

The RAM in Layer 1 depends on a continuous supply of power to maintain its state. If the protective logic of the DPM concludes that an attack has taken place, it grounds the power supply and erases the secret information in the protected region. It is pointless for an attacker to disrupt the power supply because the effect of doing that will be to erase the protected information.

The DPM is not a demanding application of three-dimensional IC technology. The number of lines of inter-layer wiring is small, particularly in comparison with typical applications of three-dimensional IC's. For example, an image processor would usually require several interlayer connections for each pixel. An image processor capable of handling large images would thus need thousands of inter-layer lines. Far fewer lines are needed for the DPM: power supplies, inputs, outputs, and addresses.

Furthermore, the DPM is a general-purpose device that will be produced in quantity. Mass production of DPM's will lead to economies of scale, just as it has with memories, microprocessors, and personal computers.

6.4 How to Detect Attacks

A likely form of attack is to attempt to make a hole in the device. Because of the spacing of the detectors, a hole whose diameter is as small as ten microns will still destroy at least one detector, and a hole not larger than twenty microns will destroy at least four. The design of the DPM makes it possible to determine not only that four detectors are faulty, but that the four are all in the same region.

The DPM has several different memories, and these memories have distinct purposes. The memory in Layer 1, the protected region, stores the information that is to be protected. The memory in Layer 2 is devoted to detecting attacks.

The order in which the detectors are tested is arbitrary, but the total test duration must be kept short. The detectors can be tested individually or in groups. Group testing helps to keep the testing interval short because the detectors in a group can be tested in parallel.

If we have a million elements and test one element every microsecond, then it will take just one second to test all the elements. If we test in parallel, the testing time can be made much less than that. The time required to erase the protected information is negligible by comparison.

There are at least three levels of protection that can be provided for the information in the protected region:

(1) The lowest level of protection is provided by using the same physical structure in every DPM. The protected information is represented by the presence or absence of electrical charges at particular physical locations in the structure.

(2) The second level of protection is provided by

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1189

storing the protected information in a way that is different for each individual DPM. One way of doing this is as follows: Each module contains a random number, which is generated independently for each module. The information is encoded in such a way that it can be decoded by using the random number. Full cryptographic protection is not necessary for this encoding; even such a simple method as exclusive or'ing the stored information with the random number is sufficient.

(3) The third level of protection is provided in a similar way as the second, but the random number and the decoding function change with time and are not always stored in the same location.

The choice among these levels should be made according to the defensive strength that is required and the cost that is acceptable.

In some applications a less effective method of protection may suffice. The protected information is kept on a mask ROM, and the chip containing the ROM is encapsulated in resin. For applications in which the attackers are not expected to be sophisticated, or in which the protecting device can be inspected by the owner of the protected information, this method may be appropriate since it is simpler and cheaper. Further discussion of it, however, is outside of the scope of this article.

6.5 The Protected Region

Layer 1 of the DPM is the protected region. Layer 2 of the DPM covers the protected region.

The purpose of the detectors is to insure that nobody can physically invade the protected region without destroying one of the detectors. However, if it is known that physical invasion will not result in the theft of the protected information, the invasion can be tolerated.

It is highly desirable to use RAM rather than EPROM for the memory in the protected region, at least in the initial stage of commercial production of the DPM. The advantage of RAM over EPROM is that RAM can be erased almost instantaneously by cutting off its power. EPROM retains its information even when it is not powered.

Near-instantaneous erasure is particularly important because the protected information typically includes an encryption key, and that key will be common among many DPM's. If the key in one DPM is stolen then the information in any device using the same type of DPM becomes vulnerable. Because the rewards of a successful attack are so great, we can expect the DPM to be subject to thorough, well-planned, and prolonged attacks. The explicit action required to erase EPROM makes it far more susceptible to attack.

At very low temperatures, a RAM may hold an electrical charge for some length of time even without power. Therefore the protected region can contain a monitoring circuit that will erase the secret information should the temperature drop below a specified threshold.

The DPM requires a continual supply of electrical power, whether it is constructed using RAM or EPROM. Once the DPM has been loaded with its protected information, power is needed for the memory that contains the secret information, the addressing logic, and the testing circuitry.

6.6 The Power Supply

Maintaining the power supply is not necessary for protection, since if the power is disrupted the device simply loses its information. It is necessary, however, to insure that in the event of a power loss the protected information is erased before the protective mechanism itself fails. This can be achieved by having the protective mechanism monitor the power supply and grounding it entirely if its voltage is not within acceptable limits.

Nevertheless it is very important to protect the device against accidental loss of power, since such an event can lead to the loss of cryptographic keys, and will be a great inconvenience to the user. Thus it is very desirable that the protected region have its own power supply. Using current CMOS and battery technology, we can build power supplies that have a lifetime of ten years. As we noted above, the useful lifetime of the DPM is unlikely to be longer than that because of the progress we can anticipate in the technology of attacks.

However, it is also possible to use an external power source provided certain precautions are taken. An external backup battery must be connected at all times once the device has been loaded with its information. It is possible to safeguard against momentary power loss by attaching a condenser to the power line. This condenser can be integrated into the device or external to it.

It will still be necessary occasionally to replace the backup battery. A device such as an electromagnetic plunger can be used to prevent the backup battery from being removed accidentally when the external power line is not connected.

7. Current Status and Future Plans

Prototype I (Fig. 9)[2] has been operating in our laboratory for three years and is available for demonstration. The S-box of Prototype I is connected to a NEC 9801 personal computer through an RS232C interface, but any other personal computer could be used. Prototype I was constructed when we were using the "Software Service System" name for these ideas.

Prototype II (Fig. 10) is now working. We expect to fabricate the S-box chip during 1990. We further plan to demonstrate the chip and distribute a limited number of copies of it to groups that will test it. We then hope

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1190

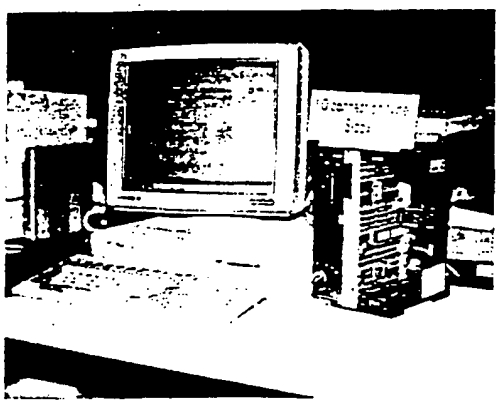


Fig. 9 Prototype I for superdistribution architecture.

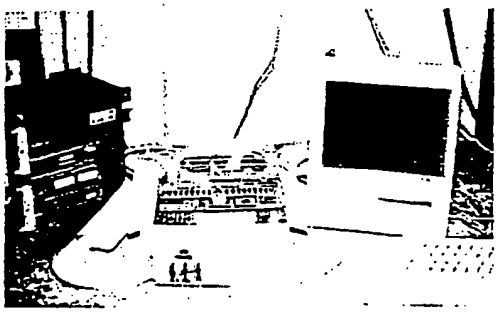


Fig. 10 Prototype II for superdistribution architecture.

to make available sufficient technical information so that others can design and produce S-boxes with the same function and purpose as ours. These S-boxes would be coprocessors for the 68020, 68030, 80286, and 80386 chips. The coprocessor implementation is clearly superior to the free-standing implementation because it has less overhead, would make multitasking possible, and is nearly invisible to users.

Prototype II does not provide encryption, nor does it physically protect the coprocessor against attacks. However, we anticipate no difficulty in using existing ASIC technology as embodied in encrypting units using established cryptographic technology to satisfy all the requirements of Section 1 of this paper.

The accounting algorithms of Prototype II are simple—simpler, even, than those of Prototype I. We are now investigating methods by which various charging methods, e. g. outright purchase and free trials, can be gotten by having a collection agent process the payment files.

The extension of these methods to multiprogramming is not difficult, given appropriate hardware. The MC68020 coprocessor interface has save-restore instructions for the coprocessor status, and these can be adapted to halt or resume processes within the coprocessor. It is also possible to disable interrupts in the main processor while the coprocessor is executing instructions, provided that the coprocessor can return control within a suitably short period of time. The time can be kept short because it usually requires only one general purpose coprocessor instruction to carry out the authentication required by the checking routine.

We have implemented Prototype II using the MC68020, but the interface section of Fig. 4 is the only part of the system that depends on the coprocessor interface of the MC68020. Thus our architecture can be adapted to other MPU's just by changing the interface.

Our work on Prototype II has verified that superdistribution can be achieved without a large initial investment, and reinforces our belief that a production system will be feasible in the near future. Our future plans include the following:

(1) Investigating the details of integrating the entire system.

(2) Systematic investigation of the software for the emulating computer.

(3) Fabrication of the coprocessor chip that provides encryption and decryption functions using ASIC technology.

(4) Distributing the coprocessor chips to other experimenters in order to verify that the system functions as expected and to learn from the experiences of others.

Although we have directed our work towards superdistribution of computer software, our architecture can be applied to other forms of digital information as well. One example is music in the forms that it is recorded on digital audio tapes.

8. Conclusions

We have developed an implementation for one step in the realization of a superdistribution architecture. This implementation has been achieved by inserting an emulated coprocessor containing the Software Usage Monitor into the coprocessor socket of an existing computer. Most personal computers already have such a socket in order to support a floating point coprocessor. It is possible to construct a single chip that combines the S-box with a floating point coprocessor, thus avoiding conflicts over the use of the socket. For those computers lacking a coprocessor socket, a special-purpose board inserted into an expansion slot can be used instead. In this case software is needed that simulates the coprocessor interface, but the overhead is not excessive.

Although we have described our system in terms of application programs, it can also be applied to system programs as well. Our methods, moreover, can be adapted to a virtual computer system that supports multiple operating systems, an arrangement that is likely to be supported in personal computers of the future.

Containers for tangible items reflect the value and importance of their contents. No similar containers have existed for digital information despite the progress of microelectronics and communications networks. The lack of such containers has invited problems such as

BEST AVAILABLE COPY
Petitioner Apple Inc. - Exhibit 1012, p. 1191

computer viruses and software piracy.

Digitally protected modules promise to provide such containers and thus to become one of the most fundamental applications of integrated circuits in the information society. We have viewed them as a fundamental support for our work on superdistribution, which aims to provide unrestricted distribution of commercial software.

Acknowledgement

We wish to thank Dr. Paul Abrahams, Consulting Computer Scientist, Deerfield Massachusetts and Professor Takashi Tokuyama, University of Tsukuba for their advice on this paper.

References

(1) R. Mori and S. Tashiro: The concept of 'Software Service System (SSS)'", Trans. IEICE, J70-D, 1, pp. 70-81 (Jan. 1987).
(2) S. Tashiro and R. Mori: "The implementation of a small scale prototype for Software Service System (SSS)", Trans. IEICE, J70-D, 2, pp. 335-345 (Feb. 1987).
(3) S. R. White: "ABYSS: A trusted architecture for software protection", Proc. 1987 IEEE Symp. on Security and Privacy, Oakland, CA, pp. 38-51 (April 1987).
(4) A. Herzberg and G. Karmi: "Public protection of software", in Advances in Cryptology; Proc. Crypto 85, ed. H. C. Williams, p. 158 (1986).
(5) D. J. Albert and S. P. Morse: "Combating software piracy by encryption and key management", IEEE Computer, pp. 68-73 (April 1984).
(6) G. B. Purdy, G. J. Simmons and J. A. Studier: "A software protection scheme", Proc. 1982 Symp. on Security and Privacy, Oakland, CA, pp. 99-103 (April 1982).
(7) "Proposal for software authorization system standards", Ver. 0.30, ADAPSO, Association of Data Processing Service Organization, (1985).
(8) S. H. Weingart: "Physical security for the μABYSS system", Proc. 1987 IEEE Symp. on Security and Privacy, Oakland, CA, pp. 52-58 (April 1987).
(9) MC68020 32-Bit Microprocessor User's Manual, Motorola Inc. (1986).
(10) MC68881 Floating-Point Coprocessor User's Manual, Motorola Inc. (1988).
(11) Y. Akasaka and T. Nishimura: "State of the art of three dimensional ICs", J. IEICE, 72, pp. 1417-1421 (1989).

Ryoichi Mori was born in 1929. He received the B. E. and Ph. D degrees from The University of Tokyo in 1953 and 1962, respectively. In 1959 he joined ETL, MITI then moved to the Institute of Information Sciences and Electronics, University of Tsukuba, in 1978, where he is a professor. He has been a Chairman of the Microcomputer Technology Committee of the Japan Electronic Industry Development Association since 1974. He is a Director of Euromicro. He received the Silver Core from IFIP in 1986.

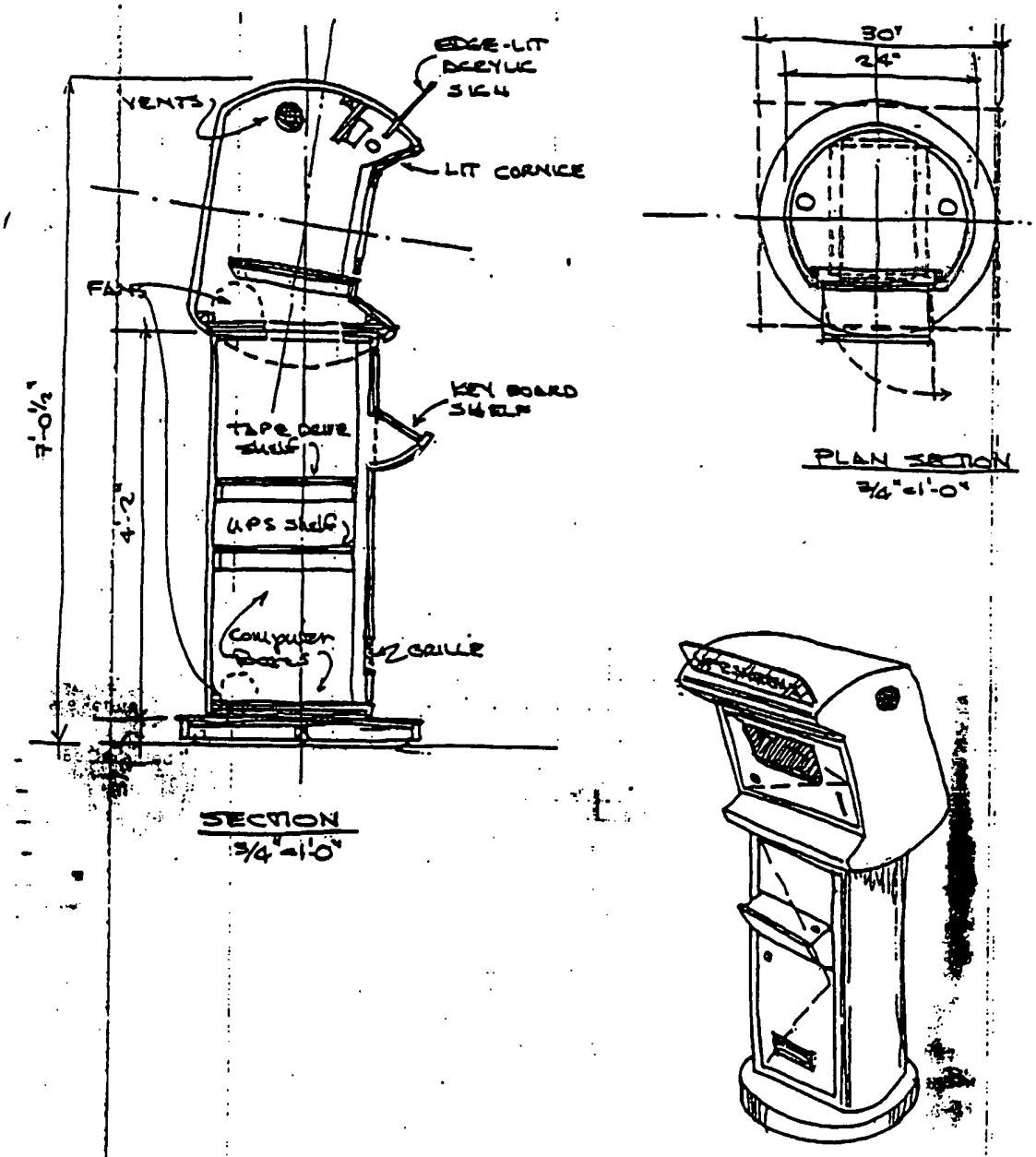
Masaji Kawahara was born in Kagawa, on April 9, 1962. He received the B. S. degree from University of Tsukuba, Tsukuba, Japan, in 1985. From 1985 to 1988, he joined Fujitsu Program Laboratory Ltd., Japan. He is now the first year graduate student of the master cource of University of Tsukuba.

BEST AVAILABLE COPY

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1192

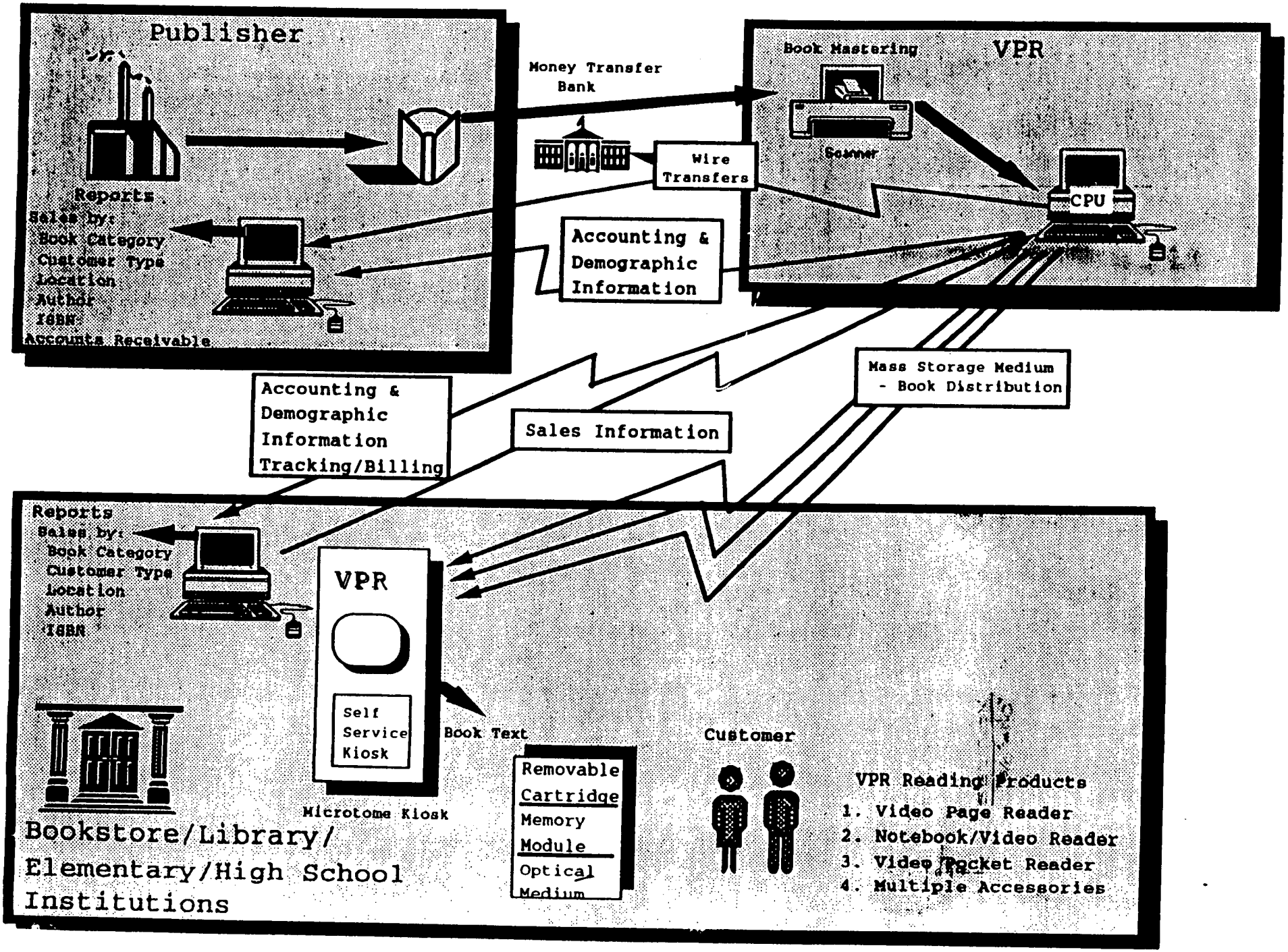
WELCOME TO THE WORLD OF MICROTOME™



MONITOR PROTOTYPE FOR V.P.R. SYSTEMS LTD.

CUBICON CORPORATION · P.O. 28745 · ST. LOUIS · MO · 63146 · (24) · 314 · 567-0662

Petitioner Apple Inc. - Exhibit 1012, p. 1193

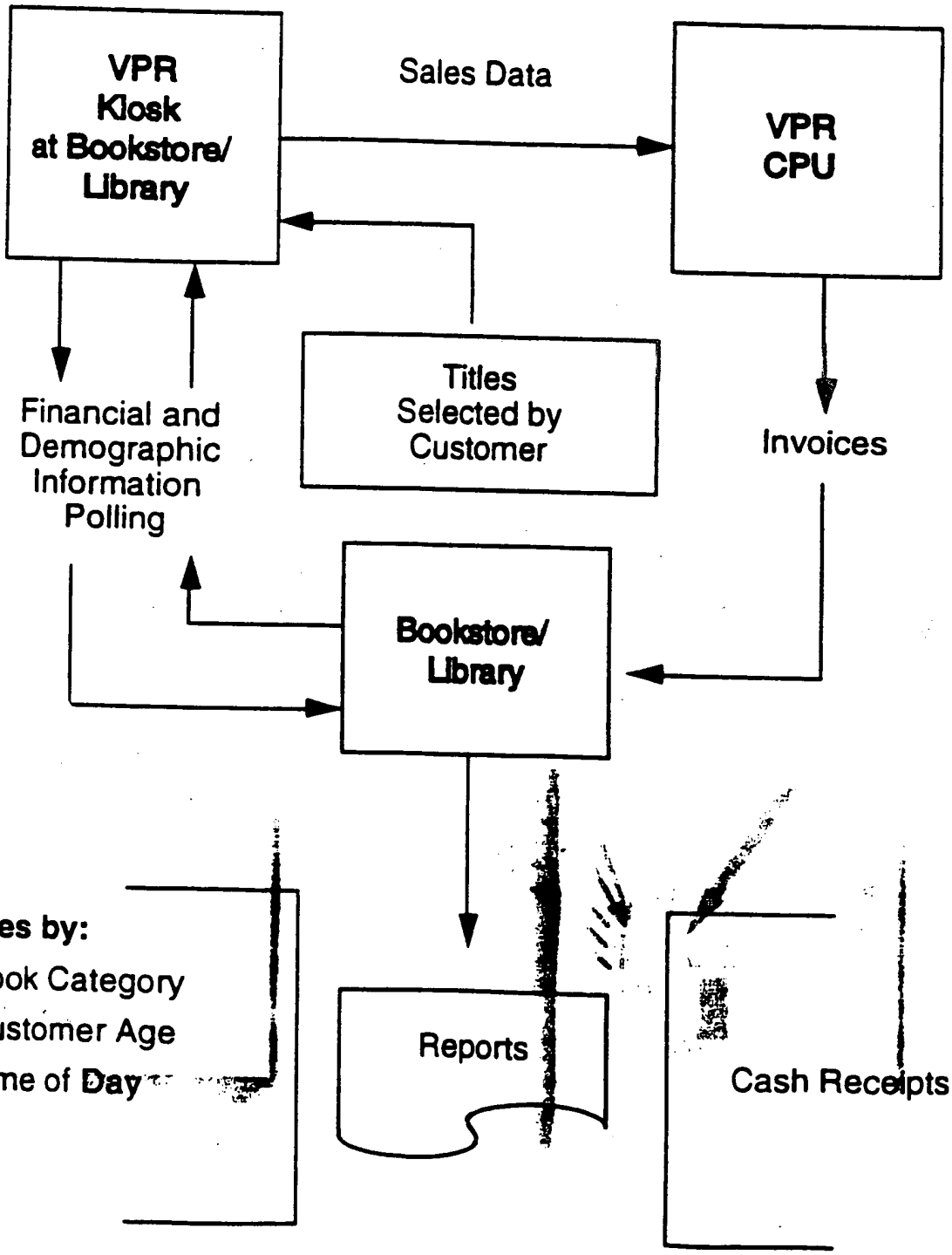


Petitioner Apple Inc. - Exhibit 1012, p. 1194

KPMG Peat Marwick
Management Consultants

VPR Systems, Ltd.

Bookstore/Library System



The Natural Evolution of Reading

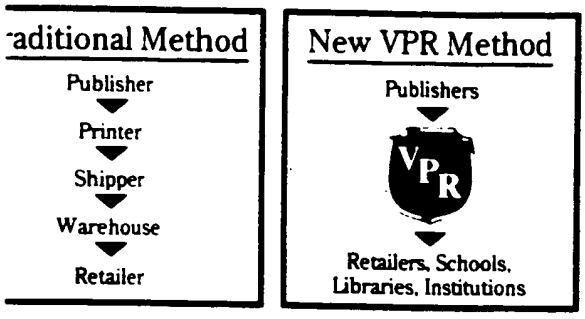
"The VPR System offers the University Bookstore an opportunity to be profitable ... every university will welcome the system with open arms."

Jackie Klotzer
Supervisor of Textbook Dept.
University of Missouri-St. Louis

"The VPR System will allow professors the ability to customize text books in accordance to their specific needs and still protect publisher revenue sources."

Paul Bueneman
Instructor

:TTING BOOKS TO THE PUBLIC



"The VPR System will create a universal availability of reference material, it will eliminate out of print problems. The fact that the programmed book checked out is automatically erased is incredible."

Martha Smart
Library Director

"The the last dozen years a vast variety of high tech products have been introduced. Very few, however, have the capacity to profoundly impact the culture. VPR readers are among the few. When it reaches full potential, it will change the way in which we access and transmit information, at the same time protecting intellectual rights as well as the environment. And best of all it will eliminate "out-of-stocks" and returns for the publisher/bookseller channel."

Paul Scheffel
Director of Stores
Washington University

"The technology is exciting and will help solve many of our problems."

Vice-President
Major Publishing Company

"The VPR System is excellent and perhaps even phenomenal ... the prospects will reshape the concepts of the mainstay supply of materials and text books."

Dr. Earl Hobbs
Superintendent
Clayton School District

"The System provides a solution for storage problems, recycling waste and tightening budget constraints. Electronics are fascinating to students and will greatly increase learning ... the students should adapt easily."

Dr. Mitchel W. Hensen
Assistant Superintendent
Ferguson School District

"The VPR should receive viable universal acceptance."

Allen Mittleman
President, Library Ltd., Retail Trade Store

VPR SYSTEMS, LTD.
525 North Laclede Station Road
St. Louis, Missouri
63119

(314) 962-5089
FAX (314) 962-4387

sized screen on a tablet and is held and read like a clipboard.

To get books, customers use the VPR "Microtome," a self-service, computer-driven kiosk that transfers books onto a mass storage cartridge contained in one of the three consumer reading products. The user inserts a special VPR information card, similar to a credit card, which identifies the book. The cards will be found in pockets beside the shelf tags that identify the hardbound book. The Microtome kiosk is expandable to six "ports"—much like a hexagonal freestanding cluster of six automated teller machines—to accommodate the traffic during rush.

The VPR "Link" is the latest but perhaps most crucial addition. At first glance, it's a lightweight, notebook PC with a detachable screen connected by a retractable cord. Normal PC operating systems and software applications can run on the unit, but it also accepts VPR mass storage cartridges for use as a VPR electronic book. Users may detach and hold the screen and its reading controls while reading, then re-connect the screen to its base for computer processing tasks. The Link will be price-competitive with a 80386 notebook PC with SuperVGA graphics.

VPR devices will allow users to enlarge the type size of the text being read. Readers can also highlight material, search for specific pages or words, or place a "bookmark." Each device will have a unique "signature" or code which will not allow the user to read cartridges other than his or her own. Eventually, VPR hopes to introduce color readers for color text and even a pen interface.

The system could very well revolutionize the content of books and the tools of the book business much like ATMs have changed banking. Accounting data like sales, store billings, copyright fees for anthologized texts, and author royalties would be available instantaneously. Funds would transfer with similar speed. Publishers may choose to make chapters of books available at prorated costs, allow professors to download free copies, or even allow users to print or copy certain sections of text, such as forms or study guides. Other changes could include the elimination of printing and binding, understocks, overstocks, freight, returns, shrinkage, damaged books, used books, the resale of comp copies, copyright violation, and deforestation.

And the eventual elimination of the college store? Not likely, says Saigh. The college store "remains a completely logical location for Microtome kiosks." Stores will, as today, receive a percentage of each sale of each book. Libraries, too, can have Microtome kiosks, but books from those machines will "erase" themselves after a predetermined period. Saigh anticipates a far smaller charge for a borrowed book than a purchased one, thus providing a cost recovery mechanism for libraries as well as an incentive for publishers to brings books to libraries via VPR.

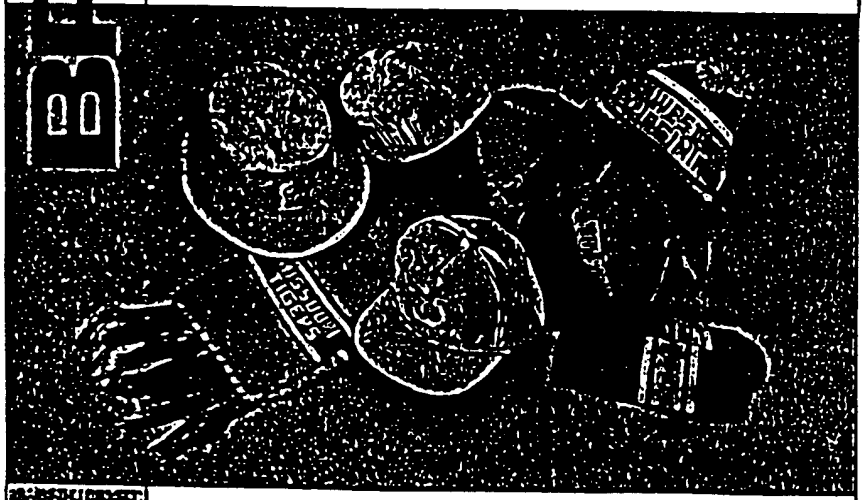
"VPR, in essence, is a conduit for publishers," says Saigh. "We're neutral. Our business mission is not to be 'a publisher' but rather to provide book dissemination for publishers. Our goals are to make and save money for publishers, for stores, and for readers in general. Our focus is on reading and books."

Having displayed prototypes of the VPR Mentor, VPR Scholar, and VPR Link at CAMEX 1992 in New Orleans, VPR Systems, Ltd. will undergo the first phase of their rollout in January 1993 with a test market of four or five campuses. In September of that year, the company hopes to be at the college stores and libraries of approximately 250 colleges and universities. CSJ

BRONER

SHOW YOUR CLASS!

For 1992, Broner Inc. will offer you the largest assortment of exciting headwear and handwear styles for your college store.



Our new state-of-the-art embroidery capabilities provide you with new exciting looks in headwear. Broner has something new for you! Get ready for 1992!

359 Robbins Drive · Troy, Michigan 48083
1·800·543·4482 fax 313·583·7724

Petitioner Apple Inc. - Exhibit 1012, p. 1197

Tony Ramos,
Contributing Editor

Making Book On Electronic Books

Wagering on the future of electronic books? Don't hedge your bets as much as you used to.

An article from the September, 20, 1991 edition of *Campus Marketplace* posed the question "Is The Campus Ready For Electronic Books?" The news was that the pace of the field was quickening, but no one had emerged as the hands-down winner. Electronic books faced marketing hurdles which were as high as—if not higher than—the technical ones.

But news changes quickly. Consider these recent items:

• Franklin Electronics, the electronic reference device veteran, is moving ahead with its late-1993 launch plans for an electronic book with interchangeable cartridges. The company now has over 20 different models of machines, ranging from a $39 spelling checker to a nearly $400 encyclopedia. Rebounding from a sluggish 1991, Franklin's first quarter 1992 earnings were 67% higher than the same period last year, says Publishers Weekly. Franklin believes the growth comes from increased consumer awareness and acceptance of the [illegible] Recently signed agreements with Bantam, McGraw-Hill, and [illegible] medical reference titles due for [illegible] Franklin's lead in several niche markets, including medical reference, language reference, and bibles.

• The Voyager Company, a Santa Monica, CA-based software publisher, is enjoying much attention for its Expanded Books, as the company calls them. Current titles on floppy diskette include Douglas Adams' *The Hitchhiker's Guide to the Galaxy*, Martin Gardners' annotated version of *Alice in Wonderland*, and Michael Crichton's *Jurassic Park*. Among the advantages of electronic versions are the ability to compile an index, mark and search text, type notes in margins of the text, change type size, view moving graphics, or even hear sound on an Apple Powerbook or any large-screen Macintosh. Retail prices are between $20 and $25.

• Random House and Voyager will introduce ten literary classics of its Modern Library unit on diskette this winter. For the 75th anniversary of the historic imprint, Random House is relaunching the line in hardcover while simultaneously introducing electronic versions with the help of Voyager. *The Picture of Dorian Gray* and *The Invisible Man* will be the first diskettes out, followed by *Moby Dick, Crime and Punishment*, and others. Prices for Modern Library Expanded Books are expected to be between $20 and $25.

• The Sony Data DiscMan hit the North American market in November last year. It reads special 8 cm (3.14") [illegible] from Sony Electronic Publishing, the new publishing arm of [illegible] electronics giant which [illegible] business, and home [illegible] for the pocket-sized reader. Publishers Weekly said that [illegible] producer Brilliance Corp. have developed Talking Type, a new audio form of electronic books for use with the Data DiscMan. These new discs will sell for less than $40 and are expected to debut this year.

• In addition, Sony is preparing the Data DiscMan's larger, MS-DOS-driven sibling for a late 1992 or early 1993 release. Code-named BookMan, this unit will use IBM PC-compatible processing power to display images and sounds from "extended architecture" (XA) compact discs, which are expected to store a much richer array of text, sound, and graphics than today's CD-ROMs. The BookMan is not quite a portable multimedia PC, but it will offer a QWERTY keyboard, LCD screen, cursor controls, and 640K of RAM in a 7" x 2" x 6" package. Heaviest use will likely be for those who need access to large amounts of data while away from their desks. (Microsoft is cooperating with Sony to provide third parties with tools to make multimedia applications in CD-ROM XA. You can bet that traditional books from those third parties are sitting in your text and trade book sections right now.)

VPR: Beyond Gadgetry

Names like Sony and Franklin are today more widely known than VPR Systems, Ltd., but what boosts the odds for this growing, St. Louis-based start-up is that the company holds firmly to the idea that the bookstore—indeed, the college bookstore—can and will play a pivotal role in the distribution of digitized text.

"The VPR is not so much an electronic device as it is a conduit for publishers," says Michael Saigh, co-inventor of what has now become a system of products and processes. Developing radically new technology is not as important to VPR as is the development of radically new uses of largely existing technology.

The VPR "Mentor," is a pocket-sized double display—that is, two display screens facing each other with a hinge down the middle—and reads like an opened book. Users can choose to display text vertically or horizontally. The VPR "Scholar," offers a larger, page-

Petitioner Apple Inc. - Exhibit 1012, p. 1198

VIDEO POCKET/PAGE READER
SYSTEMS LTD

Knowledge is Sacred

THE VPR SYSTEM

HOW THE SYSTEM WORKS

The VPR System represents a complete point-of-purchase book distribution network for publishers.

VPR Systems installs a self-service hexagonal "Microtome™ Book Bank" or Microtome™ wall mounted "ATM" style unit in college and trade bookstores, libraries, schools and institutions. The Microtome™ Book Bank is volume expandable up to six book transfer ports which can service thousands of users per day with unlimited publishers' book titles.

BOOK STORE BOOK TRANSFER PROCEDURE

A customer hands a scannable book information card to the cashier for payment. After payment, the customer receives the now activated card and takes it to the Microtome™ Book Bank which automatically transfers the purchased book(s) to the small removable mass storage medium. Next, the customer inserts the VPR mass storage medium into the Video Reader (see VPR Consumer Products) for viewing. All publishers' book sales are automatically tracked and accounted for by the VPR central CPU (see Publisher excerpt for details). The VPR System is a new, more efficient, more effective and therefore a more profitable dawn for the publishing and book marketing industry.

For more information please call:
1-800-READ VPR
1-800-732-3877

or write to:
VPR Systems Ltd.
525 North Laclede Station Road
St. Louis, MO 63119 USA

Patents Pending
United States & International

© Copyright 1992
by VPR Systems, Ltd.

VIDEO POCKET PAGE READER
SYSTEMS LTD

Knowledge is Sacred

VPR CONSUMER PRODUCTS

THE WEIGHT IS OVER!

We are a family of products that are designed specifically to enhance reading. These products interface with the Microtome™ book point-of-purchase distribution system at bookstores, schools, libraries, and institutions to facilitate knowledge transfer for all users.

VPR LINK™	A combination of a notebook size computer and basic book reader that offers multi-faceted options.
VPR SCHOLAR™	A page size display book reader.
VPR MENTOR™	A folding pocket sized double display reader.

FEATURES

- Variable speed scrolling.
- Word search and retrieval.
- Index and page retrieval access.
- Automatic patented erasure mechanism utilizing a real time clock.
- Direct page access.
- Text highlighting and retrieval.
- Built-in bookmark.
- Type size enlargement.
- Multiple uses.
- High resolution display screen.
- Durable solid state.
- Backlighting & contrast control.
- Easy to use.
- Portable.
- Rechargeable battery.
- Multiple accessory interface availability.

Extended warranty options.

Financing available.

To obtain more information call:
1-800-READ VPR
1-800-732-3877

or write to:
VPR Systems Ltd.
525 North Laclede Station Road
St. Louis, MO 63119 USA

Patents Pending
United States & International

© Copyright 1992
by VPR Systems, Ltd.

VIDEO POCKET/PAGE READER
SYSTEMS LTD

Knowledge
is Sacred

THE VPR SYSTEM ELIMINATES

~~USED BOOK DISTRIBUTORS~~

~~COPYRIGHT VIOLATIONS~~

~~PRINTING AND BINDING~~

~~TRANSPORTATION COSTS~~

~~BOOK WHOLESALERS~~

~~DEFORESTATION~~

To obtain an application or for more information call:
1-800-READ VPR
1-800-732-3877

or write to:
VPR Systems Ltd.
525 North Laclede Station Road
St. Louis, MO 63119 USA

Patents Pending
United States & International

© Copyright 1992
by VPR Systems, Ltd.

VIDEO POCKET/PAGE READER
SYSTEMS LTD

Knowledge is Sacred

PUBLISHERS

VPR will be the conduit that provides publishers' books to the market place via the Microtome™ Kiosk. More specifically, we will not take possession or title to books. This Microtome™ point-of-purchase Kiosk disseminates publishers' books to consumers who utilize various VPR readers.

- Contracts provided for scanning and digitizing textbook material.
- VPR system used to provide professors free desk copy distribution.
- Custom publishing on demand available.
- Information system within Kiosk houses consumer database information.
- Accounting package will allow automatic funds transfer.
- Publisher accounts receivable administration reduced by automatic customer billing.
- All book sales automatically tracked and accounted for by the VPR central CPU.
- ISO Standard Generalized Markup Language (SGML) accepted.
- Additional revenue from library circulations provided.
- Increased sales by eliminating the used book market.
- Warehousing costs eliminated are:
  - No inventory or excess inventory returns
  - No shipping
  - No printing
  - No binding
  - No stockouts
- Built-in copyright safeguards through encryption.
- Positive environmental impact.
- Point-of-sale transfer.

For more information call:
1-800-READ VPR
1-800-732-3877

To obtain a publisher contract write to:
VPR Systems Ltd.
525 North Laclede Station Road
St. Louis, MO 63119 USA

© Copyright 1992
by VPR Systems, Ltd.

VIDEO POCKET PAGE READER
SYSTEMS, LTD

Knowledge
is Sacred

MICROTOME™ KIOSK LIBRARIES

The Microtome™ Kiosk is a stand-alone hexagonal or wall mounted information dissemination machine which is volume expandable up to six information transfer ports. The Microtome™ Kiosk can service thousands of users per day with unlimited publishers' book titles available for circulation through the library patrons' personal VPR reader.

Library patrons will interface the Microtome™ Kiosk in order to select book(s) by title, subject, author, or ISBN number. After book(s) are chosen, the library patron will insert a special VPR mass storage cartridge to transfer selected book(s). Library patrons will use a personalized VPR debit card to check out books on the VPR System. The debit card provides revenue generating, labor free book circulation. This VPR cartridge will then be inserted into the personal VPR reader for viewing. The special library cartridge includes a patent pending erasure mechanism utilizing a real time clock that will **automatically remove all** information on the cartridge in a time period prescribed to by the publisher and library administration.

Customers of libraries can now check out reference books, journals, as well as regularly circulated books. In fact, a Harvard library can now be stored in a very small area.

The VPR System can enhance cash flow by providing additional revenues and reduced operating costs for the libraries.

An 800 trouble line is available and repairs are guaranteed within eight (8) hours.

For more information call:
1-800-READ VPR
1-800-732-3877

or to obtain a leasing application write to:
VPR Systems Ltd.
525 North Laclede Station Road
St. Louis, MO 63119 USA

Patents Pending
United States & International
© Copyright 1992
by VPR Systems, Ltd.

VIDEO POCKET PAGE READER
SYSTEMS LTD

Knowledge is Sacred

LIBRARIES

The VPR system provides access to thousands of reference books as well as professional plus technical journals and other regularly circulated books through the Microtome™ Kiosk (see Microtome™ Kiosk-Libraries). Library patrons will be able to transfer their chosen circulated material and read the material through their own VPR reader. The book(s) then will **automatically erase** at a predetermined time.

BENEFITS

- Enhanced Cash Flows Through:
  - Generating income for every book checked out.
  - No book wear and tear.
  - No labor for restocking returned books.
  - No shortage of inventory.
  - No capital investment in inventory.
  - No book theft.
- Elimination of unreturned books. A patented erasure feature utilizing a real time clock will **automatically remove all** books and/or journals at a predetermined time established by publishers and libraries.
- Provides access of a Harvard library in a very small area.
- Saves or eliminates expensive book stocking requirements.
- Builds repeat business.
- Provides immediate point of distribution circulation.
- Provides accounting, tracking, and book circulation analyses.

For more information call:
1-800-READ VPR
1-800-732-3877

or write to:
VPR Systems Ltd.
525 North Laclede Station Road
St. Louis, MO 63119 USA

Patents Pending
United States & International

© Copyright 1992
by VPR Systems, Ltd.

VIDEO POCKET/PAGE READER
SYSTEMS, LTD

Knowledge
is Sacred

Patents Pending
United States & International

© Copyright 1992
by VPR Systems, Ltd.

MICROTOME™ KIOSK TRADE BOOKSTORES

The Microtome™ Kiosk is a stand-alone hexagonal or wall mounted point-of-purchase machine which is volume-expandable up to six book transfer ports. The Microtome™ Kiosk can service thousands of users per day with unlimited publishers' book titles.

Credit card size VPR information vouchers containing book title information, publisher name, author(s), ISBN identification, edition, copyright date, UPC code, etc. will be contained in pockets located next to the hard copy of the book. Bookstore patrons will choose the book(s) they desire to purchase by simply selecting the appropriate information voucher card. They will bring this card to the cashier for payment . Following payment, the cashier will activate the card at the checkout station. The buyer then takes the activated card and inserts it into the Kiosk. The card will automatically select the ISBN purchased and transfer the book to the buyers' VPR storage medium. The cartridge is removed and the buyer can access the book through their own VPR Reader (see consumer products).

An 800 trouble line is available and repairs are guaranteed within eight (8) hours.

To obtain an application or for more information please call:
1-800-READ VPR
1-800-732-3877

or to obtain a leasing application write to:
VPR Systems Ltd.
525 North Laclede Station Road
St. Louis, MO 63119 USA

VIDEO POCKET PAGE READER
SYSTEMS LTD

Knowledge is Sacred

TRADE BOOKSTORES

The VPR system will provide access to an unlimited number of publishers' titles through the Microtome™ Kiosk (see Microtome™ Kiosk-Trade Bookstores). Now reference, professional, trade, and religious books will be able to be transferred and read by the consumer, utilizing their own VPR reader. The consumer can build his or her own personal customized library.

BENEFITS

- Enhances Cash Flow Through:
  - No payments until book is sold.
  - No capital tied up in inventory.
  - No stockouts.
  - No shipping costs.
  - No book theft.
- Increases sales revenue for VPR reading products.
- Saves valuable shelf space for diversification.
- Builds repeat business.
- Provides immediate point of purchase distribution.
- Provides accounting and sales analyses.

For more information call:
1-800-READ VPR
1-800-732-3877

oe write to:
VPR Systems Ltd.
525 North Laclede Station Road
St. Louis, MO 63119 USA

Patents Pending
United States & International
© Copyright 1992
by VPR Systems, Ltd.

VIDEO POCKET PAGE READER
SYSTEMS. LTD

Knowledge is Sacred

COLLEGE BOOKSTORES

The VPR System gives college bookstores access to thousands of books ready for instant distribution.

Bookstores taking advantage of the point-of-purchase distribution system (see Microtome™ Kiosk - College Bookstores) will realize immediate bottom line savings with respect to textbook sales.

BENEFITS

- No textbook orders to be placed.
- No textbooks to be received and unpacked.
- No textbook stocking.
- No textbook pricing.
- No freight costs in or out.
- No returns to be packed.
- No stockouts.
- No second day air shipments.
- Reduces immediate costs of generations of anthologies.
- Eliminates costs of late adoption orders.
- Special orders eliminated.
- Immediate point of sale distribution.
- Perpetual inventory.
- Saves valuable shelf space and facilities diversified merchandising.
- Eliminates Text theft.
- **Enhances Cash Flow. No payment until books are sold.**

ACCOUNTING/SALES IMPACT

All sales will be recorded within the Kiosk at the book store via the VPR CPU. Each book store will receive only one invoice for multiple publishers.

For more information please call:
1-800-READ VPR
1-800-732-3877

or write to:
VPR Systems Ltd.
525 North Laclede Station Road
St. Louis, MO 63119 USA

Patents Pending
United States & International
© Copyright 1992
by VPR Systems, Ltd.

VIDEO POCKET/PAGE READER
SYSTEMS, LTD

Knowledge
is Sacred

MICROTOME™ KIOSK
COLLEGE BOOKSTORES

The Microtome™ Kiosk is a stand-alone hexagonal or wall mounted point-of-purchase machine which is volume-expandable up to six book transfer ports. The Microtome™ Kiosk can service thousands of users per day with unlimited publishers' book titles.

Credit card size VPR information vouchers containing book title information, publisher name, author(s), ISBN identification, edition, copyright date, UPC code, etc. are contained in pockets located next to the hard copy of the textbook. Students can choose the book(s) they desire to purchase by simply selecting the appropriate information voucher card. They will bring cards to the cashier for payment. Following payment, the cashier will activate the card at the checkout station. Buyers then take the activated cards and insert them into the Kiosk. The card will automatically select the ISBN number purchased and transfer the book to the students' VPR storage medium. The cartridge is removed and the students can access the books through their own VPR reader.

An 800 trouble line is available and repairs are guaranteed within eight (8) hours.

To obtain an application or for more information please call:
1-800-READ VPR
1-800-732-3877

or to obtain a leasing application write to:
VPR Systems Ltd.
525 North Laclede Station Road
St. Louis, MO 63119 USA

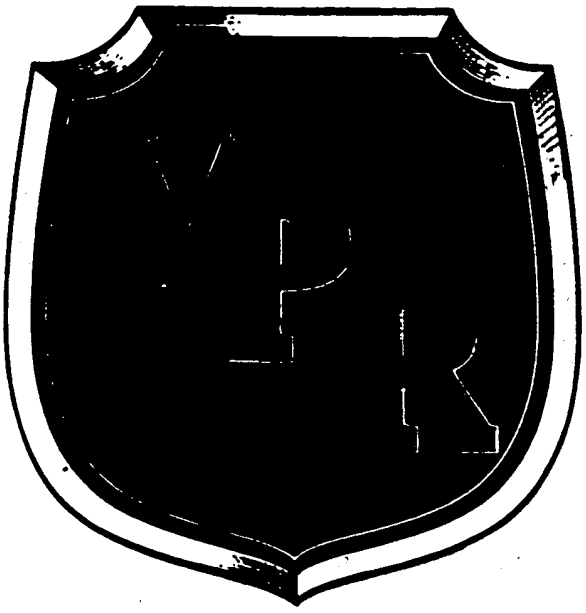
Patents Pending
United States & International
© Copyright 1992
by VPR Systems, Ltd.

DR. WILLIAM K. SAIGH
C.E.O.

525 North Laclede Station Rd.
St. Louis, MO 63119
314-962-5089
FAX 314-962-4387

"KNOWLEDGE IS POWER"

Knowledge Is Sacred



VIDEO POCKET/PAGE READER

SYSTEMS, LTD.

Petitioner Apple Inc. - Exhibit 1012, p. 1210

From / To | JERRY RACHFAL

Date 11/6/92

Tom Kailath / C. Levitt
Michigan State / FBI Wash DC
Lieff
new address

Jay Lees received this letter
at Knox - Here some information
on the product - Copies if you
want this permanently please have
Susie copy - for you.

Regards
Jay

☐ Please Re...
☐ May Be...
For ...

...OX

Petitioner Apple Inc. - Exhibit 1012, p. 1212

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- [x] BLACK BORDERS
- [x] IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- [ ] FADED TEXT OR DRAWING
- [ ] BLURRED OR ILLEGIBLE TEXT OR DRAWING
- [ ] SKEWED/SLANTED IMAGES
- [ ] COLOR OR BLACK AND WHITE PHOTOGRAPHS
- [ ] GRAY SCALE DOCUMENTS
- [ ] LINES OR MARKS ON ORIGINAL DOCUMENT
- [ ] REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- [ ] OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

THIS PAGE BLANK (USPTO)

DEPOSIT, REGISTRATION AND RECORDATION

IN AN ELECTRONIC COPYRIGHT MANAGEMENT SYSTEM

by

Robert E. Kahn

Corporation for National Research Initiatives
Reston, Virginia

August 1992

Summary

This document proposes the development of a testbed for deposit, registration and recordation of copyright material in a computer network environment. The testbed will involve the Library of Congress and provide for electronic deposit of information in any of several standard formats, automated submission of claims to copyright, notification of registration and support for on-line clearance of rights in an interactive network. "Digital signatures" and "privacy enhanced mail" will be used for registration and transfer of exclusive rights and other copyright related documents. Electronic mail will be used for licensing of non-exclusive rights with or without recordation. Verification and authentication of deposits can be carried out within the testbed using the original digital signatures. A system of distributed redundant "Repositories" is assumed to hold user deposits of electronic information. The testbed provides an experimental platform for concept development and evaluation, a working prototype for system implementation and a basis for subsequent deployment, if desired.

© CNRI 1992

1.0 Introduction and Background

Deposit, registration and recordation of copyright material and its associated claims to rights have generally been handled manually. Over the past two decades, the economics of information technology has enabled an electronic foundation for such material and claims. The key elements of this foundation are the personal computers, workstations, computer networks and peripheral devices such as scanners, printers and digital storage systems which have now become sufficiently powerful and cost effective to be put into widespread use. It is now essential that the underlying systems used to manage copyright be conformed to be compatible with the promise of this new computer networking environment. This paper addresses several essential steps that should now be taken to facilitate that process.

In the current manual system, claims to copyright are registered with the Copyright Office, Library of Congress. Deposits are accepted and stored in physical form including tapes and diskettes as well as paper and other substances. Notification of registration is also made in physical form. In addition, documents transferring copyright ownership and other documents pertaining to copyright may be submitted to the Copyright Office for recordation. While an on-line record of recent registrations and recordations may be accessed at the Copyright Office, there is only limited external dissemination of this information in

Petitioner Apple Inc. - Exhibit 1012, p. 1216

electronic form for access at remote sites.

This approach requires considerable physical storage at the Library of Congress for deposited materials which can only increase over time. Materials stored in physical form will slowly degrade unless deposited in digital media in which case the contents may be reproduced subsequently without loss of information but at some cost for duplication. Even if it is available digitally, much, if not most, of this material will not generally be accessible on-line from any source. Rights to use the information in a computer network environment cannot usually be acquired easily or quickly, even if the identity of the rightsholder is accurately known. Fortunately, these limitations can also be overcome with the use of information technology and only minor modification to the current manual system.

2.0 Components of the Proposed System

This document proposes building a testbed to develop and evaluate key elements of an electronic copyright management system. These elements include:

a. Automated copyright registration and recordation
b. Automated transactional framework for on-line clearance of rights
c. Privacy enhanced mail and digital signatures to facilitate

Petitioner Apple Inc. - Exhibit 1012, p. 1217

on-line transactions

d. Methodology for deposit, registration, recordation and clearance

Current registration and recordation activities of the Library of Congress would be maintained and enhanced in the proposed testbed. It provides for repositories and recordation systems both within and without the Library of Congress, which would serve as agents for authors and other copyright owners which seek to register works with the library. In addition, the testbed provides for automated rights clearance, outside of but linked to the library, which would accelerate permissions and royalty transfers between users and rightsholders.

2.1 Electronic Copyright Management Testbed

A testbed is proposed to develop and evaluate these concepts and to obtain experience in the implementation and operation of an experimental system (see Figure 1). The proposed testbed consists of a Registration and Recording System (RRS), a Digital Library System (DLS) and a Rights Management System (RMS). The RRS will be operated by the Library of Congress and will permit automated registration of claims to copyright and recordation of transfer of ownership and other copyright related documents. The RRS would also provide evidence of "chain of title." The DLS will be a distributed system involving authors, publishers, database

Petitioner Apple Inc. - Exhibit 1012, p. 1218

providers, users, and numerous organizations both public and private. It will be a repository of network accessible digital information and contain a powerful network based method of deposit, search and retrieval. The RMS will be an interactive distributed system that grants certain rights on-line and permits the selective use of copyright material on the network.

Information may be stored in the DLS, located within the DLS and retrieved from the DLS using any of several mechanisms such as file transfer, electronic mail or agents such as Knowbot programs. Material may be imported into the DLS from other independent systems, from paper and other sources or exported from the DLS to other independent systems, to paper or to other materials such as CD-ROM, DAT, and microcassettes. The electronic copyright management system described in this document would be directly linked to the DLS.

The testbed would contain a digital storage system connected to an applications gateway (which is, in turn, connected to multiple communication systems including the Internet) to which documents would be submitted. The storage system would constitute an experimental repository for information. The applications gateway would be designed to support multiple access methods including direct login. The RRS and RMS would be servers connected to the Internet. Initially, they would be on a common machine, but they could later be easily separated. After development, the RRS would

Petitioner Apple Inc. - Exhibit 1012, p. 1219

be relocated to the Library of Congress or its designated agent prior to being placed in operation. After initial implementation, the repository and the RMS would be replicable at other sites.

2.2 Electronic Bibliographic Records

An electronic bibliographic record (EBR) is created by the user for each digital document submission and supplied with the document for registration. The EBR is also suitable for use in cataloging and retrieval. The EBR may be supplied to other systems without the actual document but with a pointer to it. The EBR must contain a unique name for the document per author. If a name is provided that has already been used by the same author, it will be rejected with an explanation. An acknowledgement of deposit will be returned to the user along with a unique numerical identifier and a retrieval pointer to the document, and, in the event of a claim to copyright, a certificate of registration from the RRS.

2.3 Claims Registration

When the EBR indicates a claim to copyright, the RRS will be supplied a copy of the EBR by the repository along with a digital signature (to be described shortly) that can be used to verify the accuracy of a deposit at a later time. The actual work would remain in the repository. The digital signature consists of a few

Petitioner Apple Inc. - Exhibit 1012, p. 1220

hundred bytes of data and is approximately the size of the EBR. It should allow the authenticity of the retrieved document to be formally established at any time for legal and other purposes.

2.4 Repositories

The RRS need not be colocated with a repository. It is expected that an operational RRS would be operated by the Library of Congress. The repositories would be operated by the Library of Congress as well as other organizations or individuals. Deposits in certain qualified repositories will constitute deposit for public record purposes. The Library of Congress will maintain its own repository of selected deposits.

Although a set of distributed repositories is envisioned for a widely deployed system, the proposed testbed will only have a single repository for experimentation. The repositories would be established in such a way as to insure the survival of the deposited information with perhaps different degrees of confidence (much like the treasury, banks and brokerage houses, for example). Certain information would probably not be deposited for purposes of registration and might be stored at the users local site or in a commercial repository. Highly valued information could be stored in rated repositories (5-star down to 1-star) with varying degrees of backup and corresponding costs. The most critical information, as determined by Copyright Office

Petitioner Apple Inc. - Exhibit 1012, p. 1221

regulations, might be stored at the Library of Congress or the National Archives as a safeguard. The structure of such a system of repositories should be developed as part of the project.

The advantages of a distributed repository system are:

1. Large amounts of physical storage is not required to be made available at the Library of Congress.

2. Access to the original documentation is guaranteed by the DLS to the confidence level selected by the user's choice of repository (again like the banks).

3. Repositories serve as interfaces to the users, thus offloading and insulating any central servers and systems such as the RRS from potentially large user loadings and specialized customer service requests.

4. Access to the RRS in transaction mode is available only to authorized repositories and RMSs that are qualified to use the RRS in that mode. An individual author, a collective licensing organization, a government or corporate entity or others may run an RMS. Authors and other copyright owners, as well as users may also connect directly to the RRS through a separate interactive user interface.

Petitioner Apple Inc. - Exhibit 1012, p. 1222

2.5 The Computer Network Environment

There are three specific actions of concern in a network environment. One is the movement of information already contained in a computer network environment thereby greatly facilitating the creation of multiple copies in multiple machines in fractions of a second. The second is the importation of external information, such as print material or isolated CD-ROM based material, which must first be scanned or read into the system before it can be used. The third is export of internal network based information to paper using digital printers or facsimile machines or copied to separable media such as tape or DAT for external transport to others. Some of these actions, such as local use on paper in very small quantities, may or may not be covered by fair use provisions. However, non fair use actions would require approval of rightsholders.

In addition to the above three actions, there is a fourth action that is facilitated by the computer network environment. Information in digital form has the property of being easily manipulated on a computer to produce derivative works. Such derivative works can also be easily moved about in a computer network environment and be subject to further manipulation by other parties. The technology makes it possible for parallel and concurrent manipulation of such information to result in an exponential proliferation of such derivative works.

Petitioner Apple Inc. - Exhibit 1012, p. 1223

2.6 Rights Management System

The four actions described above form a basis for a rights management system. In general, there will be many such systems operated by rightsholders or their agents for required permissions on either an exclusive or non-exclusive basis for a given type of action. To locate an RMS, a user requires the existence of a domain server that knows about the network names and addresses of all RMS servers. Transactions involving rights may be handled by direct exchange on-line between the user system and the corresponding RMS. Typically, this exchange would occur rapidly on-line, and we refer to this as the interactive clearance of rights. Privacy enhanced electronic mail would be available for exclusive licenses and other transfers of rights. Non-exclusive licenses might be handled by regular electronic mail.

Transfer of copyright ownership would usually involve recordation in the RRS and could conceivably be handled automatically by the RMS on behalf of the rightsholder and the user to facilitate matters. The confirmation from the RRS would also be passed back to the rightsholder and user directly or via the RMS using privacy enhanced mail. Various enabling mechanisms in the normal screen-based computer interface could be developed and invoked by a user to achieve rapid clearance. If included in the user

Petitioner Apple Inc. - Exhibit 1012, p. 1224

interface, this capability would have the effect of creating an instant electronic marketplace for such information.

Recordation is defined to mean the official keeping of records of transfers of copyright ownership and other documents pertaining to copyright by the Copyright Office, Library of Congress. For legal purposes, proof of official registration of claims and recordations will be provided by the Copyright Office (via the RRS). Other registrations (at repositories) and non-exclusive licenses (via RMSs) will be certified by privacy enhanced mail. It will be up to the parties to such registrations and recordations to maintain electronic records of their transactions. These could also be stored within the DLS.

2.7 Identification Systems

The electronic copyright management system actually requires several types of domain servers. First, documents can be easily retrieved via the DLS if the citation is accurately known or through one or more search and browsing processes otherwise. However, the mapping of a bibliographic pointer (to the designated repository) into its network name and address may require a separate server. Second, the above mentioned domain server for RMSs is needed. Third, the date and time that transactions have been requested and taken may need to be formally validated. An electronic notary and time server would

Petitioner Apple Inc. - Exhibit 1012, p. 1225

provide such a capability as part of the privacy enhanced mail system.

2.8 Retrieval, Appearance and Submission of Documents

Retrieval of documents from the DLS is generally a two-step process. The initial step is to identify the document and to retrieve its EBR. This record will also identify the rightsholder and any terms and conditions on the use of the document or a pointer to a designated contact for rights and permissions. Rules would have to be formulated and posted to inform clearly what obligations a user incurs when accessing the system. For example, it may be specified that a submitted request with a valid EBR will then be taken to mean acceptance of the terms and conditions, including any implementation and usage restrictions or payment requirements. The rightsholder may also wish to place restrictions on the appearance of documents for certain uses.

As part of the process of document submission, a valid EBR will have been produced which can be used in the author's system. Each author or other owner of copyright (or such owner's successor in title or duly authorized agent) will maintain his or her own collection of EBRs. Searches and requests will typically be made to the user's home system unless the rights have been transferred or delegated elsewhere (e.g. to a publisher, agent, or database provider). In applying for registration of claims to copyright at

Petitioner Apple Inc. - Exhibit 1012, p. 1226

the Copyright Office, a user could be required to certify that he or she has the rights to the material and sign the submission digitally.

3.0 Privacy and Authentication Technology

This section briefly describes several key technologies to handle privacy and authentication in the digital network environment. Four such technologies are described below, namely: 1) Public Key Cryptography, 2) Digital Signatures, 3) Privacy Enhanced Mail, and 4) Notarization.

3.1 Public Key Cryptography

In conventional cryptography, a mathematical function and a "secret key" are shared by parties who wish to communicate confidentially. Each message to be sent is "encrypted" using the function and key and the recipient(s) "decrypt" it using the same function and key. This may be thought of as sharing a locked box in which several individuals have the key and any of them can lock or unlock the box at will.

In the late 1970's, two Stanford University researchers, Martin Hellmann and Whitfield Diffie speculated that it might be possible to devise paired cryptographic functions which had the interesting property that one function would encrypt and the

Petitioner Apple Inc. - Exhibit 1012, p. 1227

other would decrypt. In fact, the concept was slightly more sophisticated in that any message encrypted with either one of the functions could only be decrypted by the other. In other words, having access to the function which did the encrypting does not help when it is time to decrypt. Using the box analogy, the public key cryptography system would be like having a box with a two-key lock. If one of the keys is used to lock the box, the other must be used to unlock it. A person holding a key used for locking could not use it for unlocking.

One of the biggest problems with conventional cryptography is that the keys must be kept secret and must be distributed by secure means. The notions of Hellman and Diffie opened up a new way of thinking about key management. One key could be made public (e.g. the one to be used for encryption) and the other kept private. Anyone knowing the public part of a pair of keys could use it to prepare a message which would remain confidential until the person knowing the private key used it to decrypt the message. The public keys could be listed in public directories without any special protection since knowing them did not help anyone decrypt messages encrypted using the public key. This feature makes it far simpler to manage key distribution since the public part need not be protected.

Three researchers at MIT, Rivest, Shamir and Adelman developed a pair of functions meeting the requirements specified by Diffie

Petitioner Apple Inc. - Exhibit 1012, p. 1228

and Hellman. These functions are now known as the RSA algorithms (from the last names of the inventors).

3.2 Digital Signatures

Since either key of a public key cryptography pair can be used to perform the initial encryption, an interesting effect can be achieved by using the secret key of the pair to encrypt messages to be sent. Anyone with access to the public key can decrypt the message and on doing so successfully, knows that the message must have been sent by the person holding the corresponding secret key. The use of the secret key acts like a "signature" since the decryption only works with the matching public key. Buyers could send digitally signed messages to sellers and the sellers could verify the identity of the sender by looking up the public key of the sender in a public directory and using it to verify the source of the message by successfully decrypting it.

3.3 Privacy-Enhanced Mail (PEM)

Public key cryptography can be combined with electronic mail to provide a flexible way to send confidential messages or digitally signed messages or both. In actual practice, a combination of public key, conventional secret key and another special function called cryptographic hashing is used to implement the features of privacy-enhanced mail. The public key algorithms require a

Petitioner Apple Inc. - Exhibit 1012, p. 1229

substantial amount of computing power compared to conventional secret key algorithms. The older secret key algorithms, such as the Data Encryption Standard (DES) developed by the National Institutes of Standards and Technology (NIST), are much more efficient. Consequently, confidential messages are typically encrypted using a conventional secret key which, itself, is sent, encrypted in the public key of the recipient. Thus, only the recipient can decrypt the conventional secret key and, eventually, decrypt the message.

To send digitally-signed messages, each message is run through a "hashing" algorithm which produces a compressed residue which is then encrypted in the private key of the sender. The message itself is left in plain text form. The recipient can apply the same hashing algorithm and compare the compressed residue against the one that was sent (after decrypting it with the sender's public key).

One of the basic problems with this application of public key cryptography is knowing whether the public key found in the directory for a given correspondent is really that correspondent's key or a bogus one inserted by a malicious person. The way this is dealt with in the Privacy-Enhanced Mail system is to create certificates containing the name of the owner of the public key and the public key itself, all of which are digitally signed by a well-known issuing authority. The public

Petitioner Apple Inc. - Exhibit 1012, p. 1230

key of the issuing authority is widely publicized so it is possible to determine whether a given certificate is valid. The actual system is more complex because it has a hierarchy of certificate issuers, but the principles remain the same.

3.4 Notarization

Using digital signatures, it is possible to establish an on-line notarization service which accepts messages, time-stamps them and digitally signs them, then returns them in that form. If the person desiring notarization digitally signs the message at the time it is sent to the notarizing service, then it will be possible, later, to establish that the person requesting the notarizing had the document/message in question at the time it was notarized. One can imagine that the originator of a message might have it notarized for the record and the recipient might independently do so. By this means, for instance, evidence of a contract's existence in the hands of each party at particular times might be established.

4.0 Verification, Authentication and Certification

The verification process uses stored digital signatures to ascertain whether a given copy is identical to the version which was originally deposited. If any portion of the copy differs from the original, the verification process will fail.

Petitioner Apple Inc. - Exhibit 1012, p. 1231

Authentication or formal certification of deposits may be provided to a requesting party in traditional ways or via electronic mail. Privacy enhanced mail would be used to certify the authenticity of a deposit, as well as to certify registration and recordation records, for legal purposes.

5.0 Conclusion

The deployment of an electronic deposit, registration and recordation capability for use in a computer network environment would greatly facilitate and accelerate the move to a network base for information creation and dissemination. The system would be compatible with the current manual system and would support the ability of the Library of Congress to provide automated registration and recordation services. It would provide a foundation for straightforward and easy expansion and evolution and provide a direct linkage for the Library of Congress to the DLS. It would provide a prime working example for all other kinds of activities where claims registration and rights management come into play. Verification and authentication of copies of deposits may be performed electronically using digital signatures. Formal certification of deposits, as well as registration and recordation records, using privacy enhanced mail may be provided for legal purposes. A testbed which demonstrates the relevant concepts and ideas can be implemented within a two to three year period with initial limited use within a year.

Petitioner Apple Inc. - Exhibit 1012, p. 1232

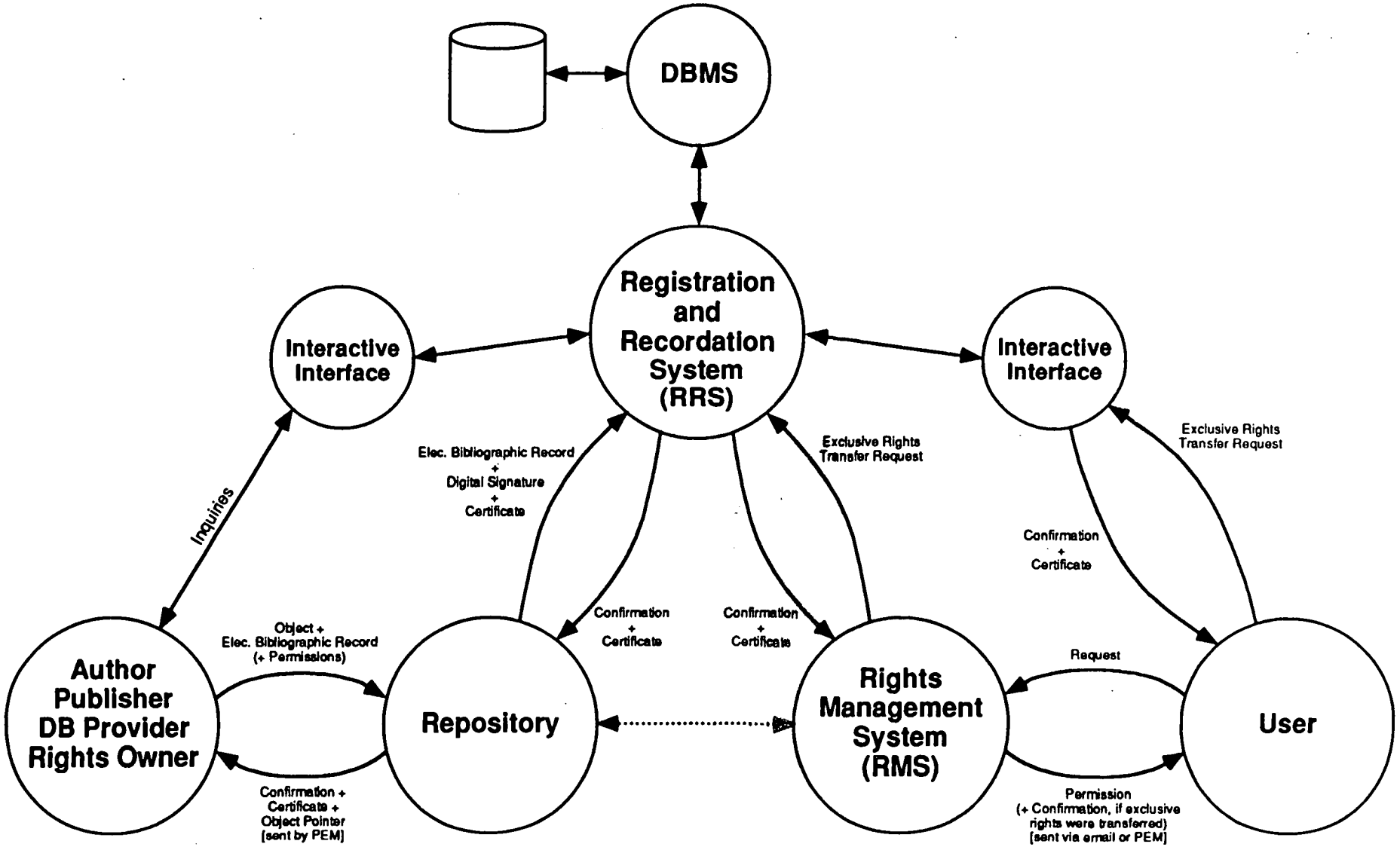


Figure 1. System Components and Information Flow.

Petitioner Apple Inc. - Exhibit 1012, p. 1233

THIS PAGE BLANK (USPTO)

OIPE JC98 SEP 27 2002 PATENT & TRADEMARK OFFICE

PRIORITY OCT 02 2002

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: Mark J. Stefik et al.)
Serial No. 10/015,951)
Filed: 12/17/2001)
For: DIGITAL WORKS HAVING USAGE RIGHT AND METHOD FOR CREATING THE SAME)
)
)

Examiner: Unassigned
Group Art Unit: 2161

RECEIVED
OCT 0 1 2002
GROUP 3600

INFORMATION DISCLOSURE STATEMENT

Commissioner of Patents
Washington, D.C. 20231

Sir:

In accordance with the duty of disclosure as set forth in 37 C.F.R. §1.56, Applicants hereby submit the following information in conformance with 37 C.F.R. §§ 1.97 and 1.98. Pursuant to 37 C.F.R. § 1.98, a copy of each of the documents cited is enclosed.

The documents are being submitted within three (3) months of the filing of this application or entry into the national stage of this application, or before the first Office Action on the merits, whichever is later, therefore no fee or certification is required under 37 C.F.R. § 1.97(b).

It is requested that the accompanying information disclosure statement be considered and made of record in the above-captioned application. To assist the Examiner, the documents are listed on the attached form PTO-1449. It is respectfully requested that an Examiner initialed copy of this form be returned to the undersigned.

The Commissioner is hereby authorized to charge any fees connected with this filing which may be required now, or credit any overpayment to Deposit Account No. 19-2380.

Respectfully submitted,

By: Marc S. Kaufman
Registration No. 35,212

NIXON PEABODY LLP
8180 Greensboro Drive, Suite 800
McLean, Virginia 22102
Telephone: (703) 770-9300

Form PTO-1449 (Rev. 8-83)	U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-88	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT		Applicants: Stefik et al.	
		Filing Date: December 17, 2001	Group Art Unit:

OIPE
SEP 27 2002
PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date (if appropriate)
	4,796,220	01/03/1989	Wolfe			

FOREIGN PATENT DOCUMENTS

RECEIVED
OCT 01 2002
GROUP 3600

Examiner Initial	Document Number	Date	Country	Class	Subclass	Translation Yes	Translation No
	0 715 241	06/05/1996	JP			Full Eng	
	04-369068	12/21/1992	JP			Eng Abst	
	05-268415	10/15/1993	JP			Eng Abst	
	06-175794	06/24/1994	JP			Eng Abst	
	06-215010	08/05/1994	JP			Eng Abst	
	07-084852	03/31/1995	JP			Eng Abst	
	07-200317	08/04/1995	JP			Eng Abst	
	07-244639	09/19/1995	JP			Eng Abst	
	62-241061	10/21/1987	JP			Eng Abst	
	64-068835	03/14/1989	JP			Eng Abst	
	WO 94/01821	01/20/1994	PCT			Full Eng	
	WO 96/24092	08/08/1996	PCT			Full Eng	
	WO 97/48203	12/18/1997	PCT			Full Eng	
	WO 98/11690	03/19/1998	PCT			Full Eng	
	WO 98/42098	09/24/1998	PCT			Full Eng	

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

Examiner Initial	
	Henry H. Perritt, Jr., "Technological Strategies for Protecting Intellectual Property in the Networked Multmedia Enviroment", April 2-3, 1993, Knowbots, Permissions Headers & Contract Law

Examiner	Date Considered

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this formwith next communication to applicant.

Requested Patent: WO9401821A1

Title:

SECURE COMPUTER NETWORK USING TRUSTED PATH SUBSYSTEM WHICH ENCRYPTS/DECRYPTS AND COMMUNICATES WITH USER THROUGH LOCAL WORKSTATION USER I/O DEVICES WITHOUT UTILIZING WORKSTATION PROCESSOR ;

Abstracted Patent: US5596718 ;

Publication Date: 1997-01-21 ;

Inventor(s):

BOEBERT WILLIAM E (US); HANSON MARK H (US); MARKHAM THOMAS R (US) ;

Applicant(s): SECURE COMPUTING CORP (US) ;

Application Number: US19920911900 19920710 ;

Priority Number(s): US19920911900 19920710 ;

IPC Classification: G06F15/17 ;

Equivalents: AU4672693, AU663406, EP0649546 (WO9401821), JP7509086T ;

ABSTRACT:

A method and apparatus for ensuring secure communication over an unsecured communications medium between a user working on an unsecured workstation or computer and a host computer. A secure user interface is created by inserting a trusted path subsystem between input/output devices to the workstation and the workstation itself. Data transferred from the input/output devices is intercepted, encrypted and transmitted in packets to the host computer. Packets of screen display data from the host computer are decrypted and presented within a user-defined screen overlay.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 5 : G06F 12/14, 1/00 — A1

(11) International Publication Number: **WO 94/01821**

(43) International Publication Date: 20 January 1994 (20.01.94)

(21) International Application Number: PCT/US93/06511

(22) International Filing Date: 9 July 1993 (09.07.93)

(30) Priority data:
07/911,900 10 July 1992 (10.07.92) US

(71) Applicant: SECURE COMPUTING CORPORATION [US/US]; 2675 Long Lake Road, Roseville, MN 55113-2536 (US).

(72) Inventors: BOEBERT, William, E. ; 4915 DuPont Avenue South, Minneapolis, MN 55409 (US). HANSON, Mark, H. ; 3560 Baltic Avenue, Eagan, MN 55122 (US). MARKHAM, Thomas, R. ; 709 River Lane, Anoka, MN 55303 (US).

(74) Agent: BRUESS, Steven, C.; Merchant, Gould, Smith, Edell, Welter & Schmidt, 3100 Norwest Center, 90 South Seventh Street, Minneapolis, MN 55402 (US).

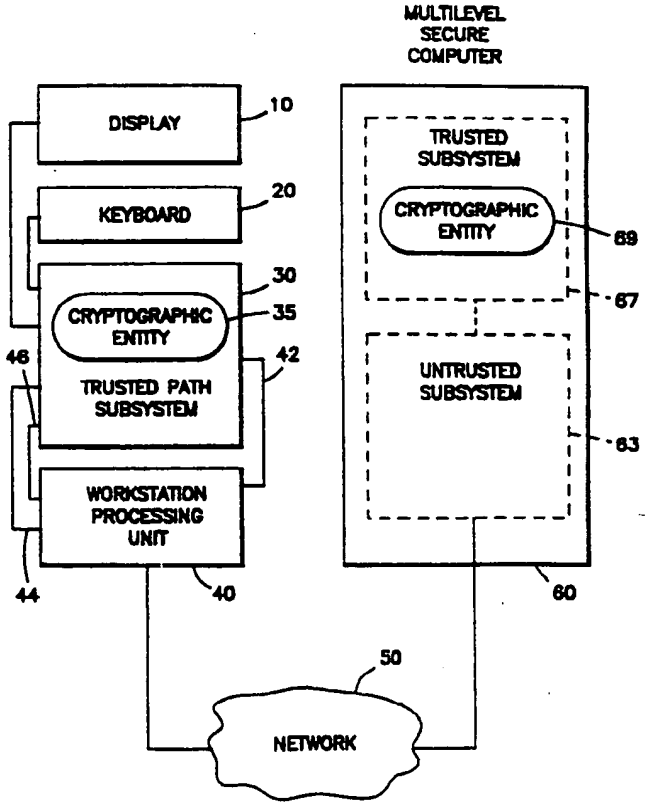
(81) Designated States: AT, AU, BB, BG, BR, BY, CA, CH, CZ, DE, DK, ES, FI, GB, HU, JP, KP, KR, KZ, LK, LU, MG, MN, MW, NL, NO, NZ, PL, PT, RO, RU, SD, SE, SK, UA, VN, European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: TRUSTED PATH SUBSYSTEM FOR WORKSTATIONS

(57) Abstract

A method and apparatus for ensuring secure communication over an unsecured communications medium between a user working on an unsecured workstation or computer and a host computer. A secure user interface is created by inserting a trusted path subsystem between input/output devices to the workstation and the workstation itself. Data transferred from the input/output devices is intercepted, encrypted and transmitted in packets to the host computer. Packets of screen display data from the host computer are decrypted and presented within a user-defined screen overlay.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AT	Austria	**FR**	France	**MR**	Mauritania
AU	Australia	**GA**	Gabon	**MW**	Malawi
BB	Barbados	**GB**	United Kingdom	**NE**	Niger
BE	Belgium	**GN**	Guinea	**NL**	Netherlands
BF	Burkina Faso	**GR**	Greece	**NO**	Norway
BG	Bulgaria	**HU**	Hungary	**NZ**	New Zealand
BJ	Benin	**IE**	Ireland	**PL**	Poland
BR	Brazil	**IT**	Italy	**PT**	Portugal
BY	Belarus	**JP**	Japan	**RO**	Romania
CA	Canada	**KP**	Democratic People's Republic of Korea	**RU**	Russian Federation
CF	Central African Republic			**SD**	Sudan
CG	Congo	**KR**	Republic of Korea	**SE**	Sweden
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovak Republic
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LU**	Luxembourg	**TD**	Chad
CS	Czechoslovakia	**LV**	Latvia	**TG**	Togo
CZ	Czech Republic	**MC**	Monaco	**UA**	Ukraine
DE	Germany	**MG**	Madagascar	**US**	United States of America
DK	Denmark	**ML**	Mali	**UZ**	Uzbekistan
ES	Spain	**MN**	Mongolia	**VN**	Viet Nam
FI	Finland				

TRUSTED PATH SUBSYSTEM FOR WORKSTATIONS

Background of the Invention

Field of the Invention

The present invention relates to an apparatus and method for providing a trusted computer system based on untrusted computers, and more particularly to an apparatus and method for providing a trusted path mechanism between a user node based on an untrusted computer or workstation and a trusted subsystem.

Background Information

Advances in computer and communications technology have increased the free flow of information within networked computer systems. While a boon to many, such a free flow of information can be disastrous to those systems which process sensitive or classified information. In response to this threat, trusted computing systems have been proposed for limiting access to classified information to those who have a sufficient level of clearance. Such systems depend on identifying the user, authenticating (through password, biometrics, etc.) the user's identity and limiting that user's access to files to those files over which he or she has access rights. In addition, a trusted path mechanism is provided which guarantees that a communication path established between the Trusted Computer Base (TCB) and the user cannot be emulated or listened to by malicious hardware or software. Such a system is described in U.S. Patent Nos. 4,621,321; 4,713,753; and 4,701,840 granted to Boebert et al. and assigned to the present assignee, the entire disclosures of which are hereby incorporated by reference.

The last decade has marked a shift in the distributing of computational resources. Instead of connecting a large number of relatively "dumb" terminals to a mainframe computer, the automatic data processing

environment has gradually shifted to where a large number of current systems are file server systems. In a file server system, relatively low cost computers are placed at each user's desk while printers and high capacity data storage devices are located near the server or servers. Files stored in the high capacity data storage devices are transferred to the user's computer for processing and then either saved in local storage or transferred back to the storage devices. Documents to be printed are transferred as files to a print server; the print server then manages the printing of the document.

An even more loosely coupled distributed computing approach is based on the client-server paradigm. Under the client-server paradigm, one or more client processes operating on a user's workstation gain access to one or more server processes operating on the network. As in file server systems, the client processes handle the user interface while the server processes handle storage and printing of files. In contrast with file server systems, however, the client processes and the server processes share data processing responsibilities. A more complete discussion of distributed computing is contained in "Client-Server Computing" by Alok Sinha, published in the July 1992 issue of *Communications of the ACM*.

Both the file server and the client-server paradigms depend heavily upon the availability of low-cost computer systems which can be placed at each user's desk. The low-cost systems are then connected through a network such as a LAN or a WAN to the server systems. Such a networked system is illustrated in the block diagram shown in Fig. 1.

In Fig. 1, a workstation processing unit 40 is connected through a network 50 to a host computer 60. Workstation unit 40 is also connected through video port

44 and keyboard port 46 to display unit 10 and keyboard 20, respectively.

In a typical distributed computer system, the workstations 40, the host computers 60 and the connecting networks 50 are all at great risk of a security breach. Trusted computer systems based on host computers such as the Multilevel Secure (MLS) Computer 60 shown in Fig. 1 make security breaches at the host computer more difficult by partitioning the system to isolate security critical (trusted) subsystems from nonsecurity critical (untrusted) subsystems. Such computers do little, however, to prevent security breaches on network 50 or at user workstation 40.

A Multi-Level Secure (MLS) Computer such as is shown in Fig. 1 is capable of recognizing data of varying sensitivity and users of varying authorizations and ensuring that users gain access to only that data to which they are authorized. For example, an MLS computer can recognize the difference between company proprietary and public data. It can also distinguish between users who are company employees and those who are customers. The MLS computer can therefore be used to ensure that company proprietary data is available only to users who are company employees.

Designers of MLS computers assume that unauthorized individuals will use a variety of means, such as malicious code and active and passive wiretaps, to circumvent its controls. The trusted subsystem of an MLS computer must therefore be designed to withstand malicious software executing on the untrusted subsystem, to confine the actions of malicious software and render them harmless. One mechanism for avoiding malicious software is to invoke a trusted path, a secure communications path between the user and the trusted subsystem. A properly designed trusted path ensures that information viewed or sent to the trusted subsystem is not copied or modified along the way.

Extension of the trusted path through the network to the user is, however, difficult. As is described in a previously filed, commonly owned U.S. patent application entitled "Secure Computer Interface" (U.S. Patent Application No. 07/676,885 filed March 28, 1991 by William E. Boebert), "active" and "passive" network attacks can be used to breach network security. Active attacks are those in which masquerading "imposter" hardware or software is inserted into the network communications link. For example, hardware might be inserted that emulates a user with extensive access privileges in order to access sensitive information. "Passive" network attacks include those in which a device listens to data on the link, copies that data and sends it to another user. A system for ensuring secure data communications over an unsecured network is described in the above-identified patent application. That application is hereby incorporated by reference.

Active and passive attacks can also be used to breach computer security through software running on an untrusted user computer, an untrusted host or in the untrusted subsystem of a Multilevel Secure Computer. For example, malicious software running in the workstation could present itself to an authorized user as the trusted subsystem, and cause that user to enter highly sensitive data, such as a password. The data is then captured and given to the attacker. Under a passive software attack, data which is intended for one user could be copied and sent to a user who is not authorized to work with it.

Systems for ensuring secure communications over an unsecured network have been limited to date to scrambling devices which encrypt data written to the network and decrypt data received from the network. Such systems are limited in that they provide no assurance that the user's computer is secure or that the user has, in fact, established a trusted path to the

trusted subsystem. Therefore, despite the fact that the communications link is secure, it is possible for a user on the computer to be misled into believing that a program executing on his computer is actually running on the host computer.

What is needed is a mechanism for extending the trusted path from the trusted subsystem of the host computer to the user of an untrusted computer or workstation. Such a method should provide access to the workstation for normal workstation activities while shielding confidential data so that it cannot be read by software executing on the unsecured workstation.

Summary of the Invention

The present invention provides a method and apparatus for ensuring secure communication over an unsecured communications medium between a user working on an unsecured workstation or computer and a host computer. A secure user interface is created by inserting a trusted path subsystem between input/output devices to the workstation and the workstation itself. Data transferred from the input/output devices is intercepted, encrypted and transmitted in packets to the host computer. Packets of screen display data from the host computer are decrypted and presented within a user-defined screen overlay.

According to another aspect of the present invention, a method is disclosed for ensuring secure file transfers between an unsecured workstation and a host computer. A file to be transferred is downloaded to a trusted path subsystem inserted between the workstation and its keyboard and display device. The trusted path subsystem presents a representation of the file on the display device where the user can verify that the file is as expected. The verified file is then encrypted and transferred as packets to the host computer.

Brief Description of the Drawings

FIG. 1 is a system level block diagram representation of a networked computer system.

FIG. 2 is a system level block diagram representation of a secure networked computer system according to the present invention.

FIG. 3 is a block diagram representation of a user node including a trusted path subsystem according to the present invention.

FIG. 4 is a block diagram representation of a user node including a different embodiment of a trusted path subsystem according to the present invention.

FIG. 5 is an electrical block diagram representation of one embodiment of the trusted path subsystem according to the present invention.

FIG. 6 is a representation of a secure window overlay according to the present invention.

Detailed Description of the Preferred Embodiments

In the following Detailed Description of the Preferred Embodiments, reference is made to the accompanying Drawings which form a part hereof, and in which are shown by way of illustration specific embodiments in which the invention may be practiced. It is to be understood that other embodiments may be utilized and structural changes may be made without departing from the scope of the present invention.

The present invention provides a method and apparatus for ensuring secure communication over an unsecured communications medium between a user working on an unsecured workstation or computer and a host

computer. A secure user interface is created by inserting a trusted path subsystem between input/output devices to the workstation and the workstation itself. Data transferred from the input/output devices is intercepted, encrypted and transmitted in packets through the workstation to the host computer. Packets of screen display data from the host computer are decrypted and presented within a user-defined screen overlay.

Cryptographic entities in the trusted path subsystem and the host computer apply end-to-end encryption to confidential data transferred to and from the network. End-to-end encryption is a technique whereby data is encrypted as close to its source as possible and decrypted only at its ultimate destination. This technique differs from link encryption, in which data is decrypted, then encrypted again as it moves from the sender to the receiver.

The present invention extends the notion of end-to-end encryption by performing the encryption/decryption closer to the originator and receiver than prior systems. In the present invention, the encryption/decryption is performed as the data enters and leaves the input/output device. The data is therefore protected from malicious software which might be operating on the workstation and from active or passive attacks on the network.

A secure networked computer system constructed according to the present invention is illustrated generally in Fig. 2. In Fig. 2, a workstation processing unit 40 is connected through a network 50 to a host computer 60. Workstation 40 can be any computer, workstation or X terminal which has a separate data path for communication between a trusted path subsystem 30 and the workstation. For instance, workstation 40 can be a commercially available workstation such as the UNIX workstations manufactured by Sun Microsystems, Mountain

View, California, an IBM PC compatible such as those available from Compaq, Houston, Texas or an X terminal such as Model NCD19g from Network Computing Devices, Inc, Mountain View, California.

Trusted path subsystem 30 is connected to workstation 40 (through auxiliary data port 42), keyboard 20 and display 10. Trusted path subsystem 30 includes cryptographic entity 35 for encrypting and decrypting information transferred between display 10, keyboard 20 and workstation 40.

Host computer 60 is a Multi-Level Secure computer which includes a trusted subsystem 67 and an untrusted subsystem 63. Trusted subsystem 67 includes a cryptographic entity 69 for encrypting and decrypting data transferred between trusted subsystem 67, untrusted subsystem 63, and network 50. In another embodiment of the present invention, host computer 60 is a computer running a trusted subsystem software package. In that embodiment, cryptographic entity 69 would be implemented in software.

In the embodiment shown in Fig. 2, all communication between trusted path subsystem 30 and host computer 60 is done via workstation 40. In one such embodiment, auxiliary data port 42 is an RS-232 line connecting workstation 40 and subsystem 30. Communications software running on workstation 40 receives encrypted packets from the trusted path subsystem and sends them to the host computer. In a like manner, encrypted packets from host computer 60 are received by workstation 40 and transferred to subsystem 30 for decrypting. This type of interface is advantageous since a standard communications protocol can be defined for transfers between subsystem 30 and host computer 60. Workstation 40 then implements the standard protocol for the communications media connecting it to host computer 60.

Network 50 can be implemented in a wide range of communications protocols, from FDDI to a simple telecommunications line between two modems. In a network implementation, subsystem 30 provides only the encrypted file; workstation 40 provides the layers of protocol needed for reliable communication on network 50.

Fig. 3 provides more detail of trusted path subsystem 30. Trusted path subsystem 30 consists of a processor 31 connected to a keyboard manager 37, a video manager 38 and cryptographic entity 35. Trusted path subsystem 30 operates in normal mode and in trusted path mode. When in normal mode, workstation trusted path subsystem 30 is transparent to workstation 40. Logical switches 37 and 38 are in the UP position, connecting workstation processor 40 directly to keyboard 20 and display 10. This permits the free transfer of information from keyboard 20 to workstation 40 and from workstation 40 to display 10. In normal mode, workstation processor 40 runs software and communicates with host computer 60 via network 50.

When the user invokes trusted path mode, however, workstation processor 40 is disconnected from keyboard 20 and display 10 by logical switches 37 and 38, respectively. Keyboard 20 and display 10 are then connected to their respective managers in workstation trusted path subsystem 30.

As is shown in Fig. 6, while in trusted path mode, video manager 34 creates a trusted window 82 which is overlaid on the screen display 80 generated by workstation 40 for display 10. Since window 82 is created outside of workstation 40, by trusted elements, it is not possible for malicious software in workstation 40 to control any of the video in trusted window 82. In the preferred embodiment the size of trusted window 82 can vary; if sufficient video RAM is present, window 82 may be as large as the entire display screen.

In a like manner, while in trusted path mode, keyboard manager 36 intercepts keyboard data intended for workstation 40. The data is then routed to cryptographic entity 35, where it is encrypted before being passed over auxiliary port 42 to workstation processing unit 40. Thus, keyboard inputs are protected from eavesdropping and undetected modification until they are decrypted by cryptographic entity 69 on host computer 60.

In one embodiment of the trusted path subsystem of Fig. 3, cryptographic entity 35 uses a pair-wise key to encrypt data to be transmitted from keyboard 20 to host computer 60. At the same time, cryptographic entity 35 decrypts data transmitted from host computer 60 to display 10. The encryption and integrity mechanisms protect the data from eavesdropping and undetected modification as it is passed through workstation processor 40, network 50 and host computer untrusted subsystem 63. Other types of symmetric encryption algorithms such as the Data Encryption Standard (DES) and asymmetric cryptographic techniques such as public key can also be used. Furthermore, the encryption algorithm can either be implemented in software, programmable hardware, or custom hardware.

Trusted path mode can be invoked in a number of ways. In one embodiment, a switch on trusted path subsystem 30 can be used to manually activate trusted path mode. A second method would be to invoke trusted path mode by a combination of keys pressed simultaneously on keyboard 20 (like the control/alt/delete key sequence on a PC-compatible computer). A third embodiment would require that the user insert some sort of token device into subsystem 30. A token device might range from a smart card to a cryptoignition key. In the preferred embodiment, subsystem 30 would also have a feedback mechanism such

as a light to notify the user that subsystem 30 was in trusted path mode.

The trusted path mode, used in conjunction with cryptographic entity 69 on host computer 60, provides security services such as user authentication, data confidentiality, data integrity and data origin authentication and confinement of malicious software. The user is authenticated to trusted path subsystem 30 and this authentication is securely passed to trusted subsystem 67 in MLS computer 60. Data passed between cryptographic entities 35 and 69 is protected from unauthorized disclosure and undetected modification. Cryptographic entities 35 and 69 also assure that the data was sent from one cryptographic entity to its peer cryptographic device. In addition, malicious software on workstation 40, network 50 or untrusted subsystem 63 is confined so that it cannot dupe the user or trusted subsystem 67 into performing an insecure action.

The user can be authenticated to the trusted computing system by either authenticating himself directly to trusted path subsystem 30 or by going through subsystem 30 to host computer 60. In the first method, the user can authenticate himself to subsystem 30 via such means as a personal identification number (PIN), a password, biometrics or a token device such as a smart card or a cryptographic ignition key. Once the user has authenticated himself to subsystem 30, subsystem 30 relays the authentication to trusted subsystem 65. The step of relaying authentication can be done by either automatically entering trusted path mode as part of the authentication process or by having subsystem 30 relay the authentication data at a later time.

A second method for authenticating a user would be to first enter trusted path mode and then authenticate the user directly to host computer 60.

This approach would reduce the processing power needed on subsystem 30.

In its simplest form, trusted path subsystem 30, in conjunction with workstation 40, display 10 and keyboard 20, forms an assured terminal. Data typed on keyboard 20 or extracted from a pointing device such as a mouse is encrypted and transferred over network 50 to host computer 60. Screen display data transferred from host computer 60 is decrypted and displayed within trusted window 82. Such a terminal might be implemented as a relatively dumb terminal such as a VT100, or it could be implemented as a X Windows terminal. The X Window embodiment would be useful since it would allow the creation of multiple trusted windows 82 and would permit the assigning of a different security level to each window. Such a mechanism would permit qualified users to cut information from a document of one sensitivity and paste it into a document of a different sensitivity.

An assured terminal is especially useful in an environment where you are trying to maintain a number of security levels despite having a workstation which will only operate at one level. An example is a trusted computing system mixing single level secure workstations with a multi-level computer with three security levels: unclassified (least sensitive), secret (much more sensitive), and top secret (most sensitive). Trusted path subsystem 30 can be used to expand the capabilities of the single level workstation since subsystem 30 allows the user to essentially disable subsystem 30, do all his work at the level permitted by the workstation (say, secret) using all the capabilities of his workstation and whatever facilities are available on the multilevel computer. Then, if the user has a small amount of work that he or she needs to do at top secret, the user can invoke trusted mode in subsystem 30, isolate their workstation, its processor memory and

storage devices, and he has, in effect, a keyboard and a terminal connected to a secure communications device through a multilevel host. The user can then do the operations required at top secret.

The cryptographic techniques applied in subsystem 30 will ensure that none of the top secret information going to or from the multilevel secure computer is linked to files within workstation 40 or is captured and copied on the network.

Likewise, if a user had to do a small amount of unclassified work, he could put the workstation into trusted path mode using subsystem 30. The user could, through a trusted path, invoke an unclassified level and again the cryptographic techniques applied at each end of the link would prevent secret information from being mixed in with the unclassified information. The system essentially provides a pipe to keep data from one security level from being mixed into data at a different security level.

Trusted subsystem 30 is not, however, limited to a role as an assured terminal. In a file server application, files stored at host computer 60 or within workstation 40 could be transferred to subsystem 30 for data processing tasks such as editing, reviewing the file or transferring it as electronic mail. In a client server application, processor 31 could execute one or more client processes such as an editor or a communications process. Software and firmware which could be implemented inside trusted path subsystem 30 would be limited only by the amount of storage within subsystem 30 and the review and approval process required to provide clean software.

Trusted path subsystem 30 has access not only to files on host computer 60 but also on workstation 40. Files transferred from either computer 60 or workstation 40 can be manipulated and transferred to other computers or workstations. For example, a secure electronic mail

system could be implemented in which trusted path subsystem 30 is used for reviewing, reclassifying, and electronically signing messages. A document file from computer 60 or workstation 40 can be displayed and reviewed. If appropriate, the user may downgrade its sensitivity level by attaching a different security level to the document. The finished file can then be sent via electronic mail to other users.

In one embodiment of such an electronic mail function, subsystem 30 would go out on the network to the directory server to retrieve the names, electronic mail addresses and public key information of the intended recipients. The directory server could be implemented as either a trusted or an untrusted process on host computer 60 or on another network computer. Subsystem 30 would then attach the addresses to the file, affix a digital signature, encrypt the final product and send it through host computer 60 to the designated addresses.

In another embodiment of such a function, in a system without a MLS computer, secure electronic mail is possible by first establishing a trusted path from the user to processor 31. The user then accesses files of workstation 40 (or on other network computers), displays and reviews the file, accesses an unsecured directory server to retrieve the names, electronic mail addresses and public key information and sends the encrypted message via electronic mail to its recipient.

Processor 31 can also be used to control video manager 34 in order to implement and control the user interface. Such an approach would permit the use of a graphical user interface (GUI) within trusted window 82 that would reduce the amount of screen information transferred by host computer 60. This approach also permits the user to implement, through processor 31, multiple trusted windows 82 at the user node in order to perform the cut-and-paste function referred to above.

In the preferred embodiment, subsystem 30 is a modular design in which processor 31 and cryptographic entity 35 are kept constant and video manager 34 and keyboard manager 36 are designed so that they can be replaced easily to handle different displays and keyboards. In one embodiment, subsystem 30 is designed to be portable. A portable subsystem 30 can be used to turn any modem equipped computer with the requisite auxiliary data port into a secure data terminal or computer.

Fig. 4 is a block diagram representation of an alternate embodiment of trusted path subsystem 30. In Fig. 4, processor 31 is connected through network interface 39 to network 50 and through communication port 48 to workstation 40. In the embodiment shown in Fig. 4, workstation processing unit 40 is isolated from the network. This approach allows the encryption of all network traffic associated with the user node. In the embodiment shown in Fig. 4, communication port 48 can be a communication medium ranging from RS0232 to an unsecured Ethernet.

A more detailed representation of one embodiment of trusted path subsystem 30 is shown in Fig. 5. In Fig. 5, keyboard logical switch 37 receives data from keyboard 20 and routes it to processor 31. During normal mode, processor 31 then sends the received keyboard data directly over keyboard port 46 to workstation 40.

In contrast, in trusted path mode, processor 31 captures the received keyboard data and sends it to cryptographic entity 35 for encrypting. No information is sent over keyboard port 46 to workstation 40. The resulting encrypted keyboard data is instead sent through auxiliary data port 42 to workstation 40 and from there to computer 60.

Video data from workstation 40 is transmitted from video port 44 to video manager 34. During normal

mode, the video data is sent through to display 10 without modification. During trusted path mode, however, the video data transferred from video port 44 is overlaid, at least in some part, by video data generated by video manager 34.

A representative video manager 34 is shown generally in Fig. 5. Video manager 34 consists of video synchronization hardware 72, video RAM 74, video driver 78 and video multiplexer 76. Video synchronization hardware 72 receives synchronization signals from video port 44 and uses the signals to coordinate the display of data from video RAM 74 with the display generated by workstation 40. During normal mode data from video RAM 74 is not used; video is transferred directly from workstation 40 through video multiplexer 76 to display 10. When, however, trusted path subsystem 30 is placed into trusted path mode, video data stored in video RAM 74 is used instead of the normal video stream to create trusted window 82.

In one embodiment synchronization hardware 72 uses the synchronization signals received from workstation 40 to control the reading of data from video RAM 74 and the conversion of that data into a video signal by video driver 78. The output of video driver 78 is then used to drive video multiplexer 76. Synchronization hardware 72 controls video multiplexer 76 in order to switch between the video generated by workstation 40 and the video being read from video RAM 74. The output of video multiplexer 76 is driven through video amplifiers to display 10.

The design of the video hardware needed to overlay one display on top of another is well known in the art. Window 82 can be synched up to the video going to display 10. Typically, if window 82 is not full screen, video synchronization hardware 72 counts the number of lines to the first line of window 82, counts in the number of pixels, and inserts the video at that

point. Trusted path video data is then written for the desired number of pixels and video multiplexer 76 is switched back to normal video for the remainder of the video line. This mechanism provides flexibility in placement and sizing of window 82 on screen 80.

Video multiplexer 76 can be built using a crosspoint video switch such as the MAX456 manufactured by Maxim Integrated Products. Video data to and from the crosspoint video switch can be buffered using the MAX457 by Maxim Integrated Products. Video RAM 74 can be any commercial video RAM. A typical video RAM is the MT42C8256 manufactured by Micron Technologies Inc. It should be obvious that the given design can be easily adapted for either a color or a black and white display or even for a black and white overlay of a color display.

In one embodiment, host computer 60 transmits, as encrypted packets, video data to be displayed within trusted window 82. The encrypted packets are passed to processor 31 by workstation 40 and then on to encryption device 35. Encryption entity 35 decrypts the video data and places it into video RAM 74. Synchronization hardware 72 then activates video multiplexer 76 and video RAM 74 in order to display the decrypted secure video data.

In a second embodiment (not shown), processor 31 creates the video overlay data and writes that data to video RAM 74. Display of the data is as above.

A trusted computing system based on unsecured, commercially available, workstations, trusted path subsystems and multilevel secure computers provides a powerful, highly secure computing environment. The ability of such a system to compensate for unsecured workstations allows the designers of such systems to use the latest versions of commercially available hardware and software without compromising the security of the system.

For instance, a user of a workstation may wish to edit a secret document and reclassify the edited document as unclassified. The document can be loaded into the workstation, edited with the user's favorite word processing software package, and saved. Then, in order to classify the document as unclassified, the user would invoke trusted path mode, the trusted window would be displayed and the user could review the revised document to verify that no additional information had been attached to the file. The reviewed document could then be released as an unclassified document and the user would then returns to normal mode.

The unique placement of cryptographic entity 35 relative to workstation 40 allows a single workstation to be used at different levels of security sensitivity. Therefore, instead of systems in which a workstation is required for each level of security sensitivity, in the present system a single commercial workstation may be used to protect and access a range of security levels.

Finally, the end-to-end characteristic of the encryption permits secure communication without the need to perform costly analysis of complex elements such as network controllers. The invention also allows use of commercial off-the-shelf workstations and network components and can be used with a variety of keyboards and displays.

Although the present invention has been described with reference to the preferred embodiments, those skilled in the art will recognize that changes may be made in form and detail without departing from the spirit and scope of the invention.

What is claimed is:

1. A secure computing network, comprising:

a network computer, wherein the computer comprises

a trusted subsystem; and

encryption means for encrypting and decrypting data transferred to and from the trusted subsystem;

communications means, connected to the network computer, for permitting data transfer between the network computer and other computers;

an input/output device;

a workstation comprising:

first communications interface means, connected to the communications means, for transferring data between the workstation and the network computer;

input/output device interface means for transferring data between the workstation and the input/output device; and

second communications means for transferring data between the workstation and another processor; and

trusted path means, inserted between the input/output device and the input/output device interface means and connected to the second communications means, for intercepting data transfers between the input/output device interface means and the input/output device, wherein the trusted path means comprises encryption means for encrypting and decrypting the data transfers and for routing such transfers over the second communications means to the trusted subsystem.

2. The secure computing network of claim 1 wherein the network computer is a multilevel secure computer capable of recognizing data of varying sensitivity and users of varying authorizations.

3. The secure computing network of claim 1 wherein the input/output device comprises a keyboard.

4. The secure computing network of claim 1 wherein the input/output device comprises a display device.

5. The secure computing network of claim 1 wherein the input/output device comprises a pointing device.

6. A secure computing network, comprising:
a network computer, wherein the computer comprises
a trusted subsystem; and
encryption means for encrypting and decrypting data transferred to and from the trusted subsystem;
communications means, connected to the network computer, for permitting data transfer between the network computer and other computers;
an input/output device;
a workstation comprising:
input/output device interface means for transferring data between the workstation and the input/output device; and
workstation communications means for transferring data between the workstation and another processor; and
trusted path means, inserted between the input/output device and the input/output device interface means and connected to the workstation communications means, for intercepting data transfers between the input/output device interface means and the input/output device, wherein the trusted path means comprises encryption means for encrypting and decrypting the data transfers and network interface means, connected to the communication means, for transferring

the encrypted data transfers between the trusted path means and the trusted subsystem.

7. The secure computing network of claim 6 wherein the network computer is a multilevel secure computer capable of recognizing data of varying sensitivity and users of varying authorizations.

8. The secure computing network of claim 6 wherein the input/output device comprises a keyboard.

9. The secure computing network of claim 6 wherein the input/output device comprises a display device.

10. The secure computing network of claim 6 wherein the input/output device comprises a pointing device.

11. A trusted path subsystem capable of being connected between an input/output device and a processor of a workstation in order to provide secure communication with a multilevel secure computer network server, the subsystem comprising:

input/output manager means for selectively intercepting, under user control, data transferred from the input/output device to the processor and from the processor to the input/output device;

encryption means for encrypting the intercepted data before transferring the encrypted data to the processor; and

decryption means for decrypting the intercepted data before transferring the decrypted data to the input/output device.

12. The trusted path subsystem according to claim 11 wherein the input/output manager means comprises keyboard manager logic, wherein the keyboard manager logic comprises:

a keyboard interface which captures information generated by a keyboard; and

processing means for transferring the captured information to a workstation processor, wherein the processing means transfers the captured information on a first path when in a first mode and on a second path when in a second mode.

13. The trusted path subsystem according to claim 11 wherein the input/output manager means comprises a video manager which can be used to generate a trusted window overlay on a video screen, wherein the video manager comprises:

a video multiplexer having first and second input ports and an output port, wherein the first input port can be connected to an external video signal and wherein the output port can be connected to a video display;

a video data memory;

converter means, connected to the video data memory and the second multiplexer input port, for converting data read from the video data memory into a trusted video signal representative of that data and for applying the trusted video signal to the second video multiplexer input port; and

video synchronization means, connected to the video data memory and the video multiplexer, for controlling the video data memory and the video multiplexer so as to insert the trusted video signal into the video signal generated at the video multiplexer output port.

14. A method of securely transferring data in a network comprising an unsecured workstation connected to a multilevel secure computer server, wherein the workstation comprises a processor and an input/output device and wherein the multilevel secure server comprises a trusted subsystem and encryption means for encrypting and decrypting data transferred to and from

the trusted subsystem, the method comprising the steps of:

providing trusted path means for providing a user selectable secure communications path between the input/output device and the trusted subsystem; and

inserting the trusted path means between the input/output device and the processor.

15. A method for providing secure file transfer capability on an unsecured workstation connected over a network to a second computer, wherein the workstation comprises a workstation processor and an input/output device and wherein the second computer comprises a trusted subsystem and encryption means for encrypting and decrypting data transferred to and from the trusted subsystem, the method comprising the steps of:

providing means for creating a trusted path between the input/output device and a trusted subsystem, said trusted path means including a trusted processor capable of executing a secure electronic mail program;

inserting the trusted path means between the input/output device and the workstation processor;

downloading from the workstation processor to the trusted processor a file to be transferred to the second computer;

displaying, on the input/output device, a representation of the file to be transferred;

if the file is as expected, transferring the file to the second computer; and

if the file is not as expected, generating an error message.

16. The method according to claim 15 wherein the step of generating an error includes allowing secured processing on the file.

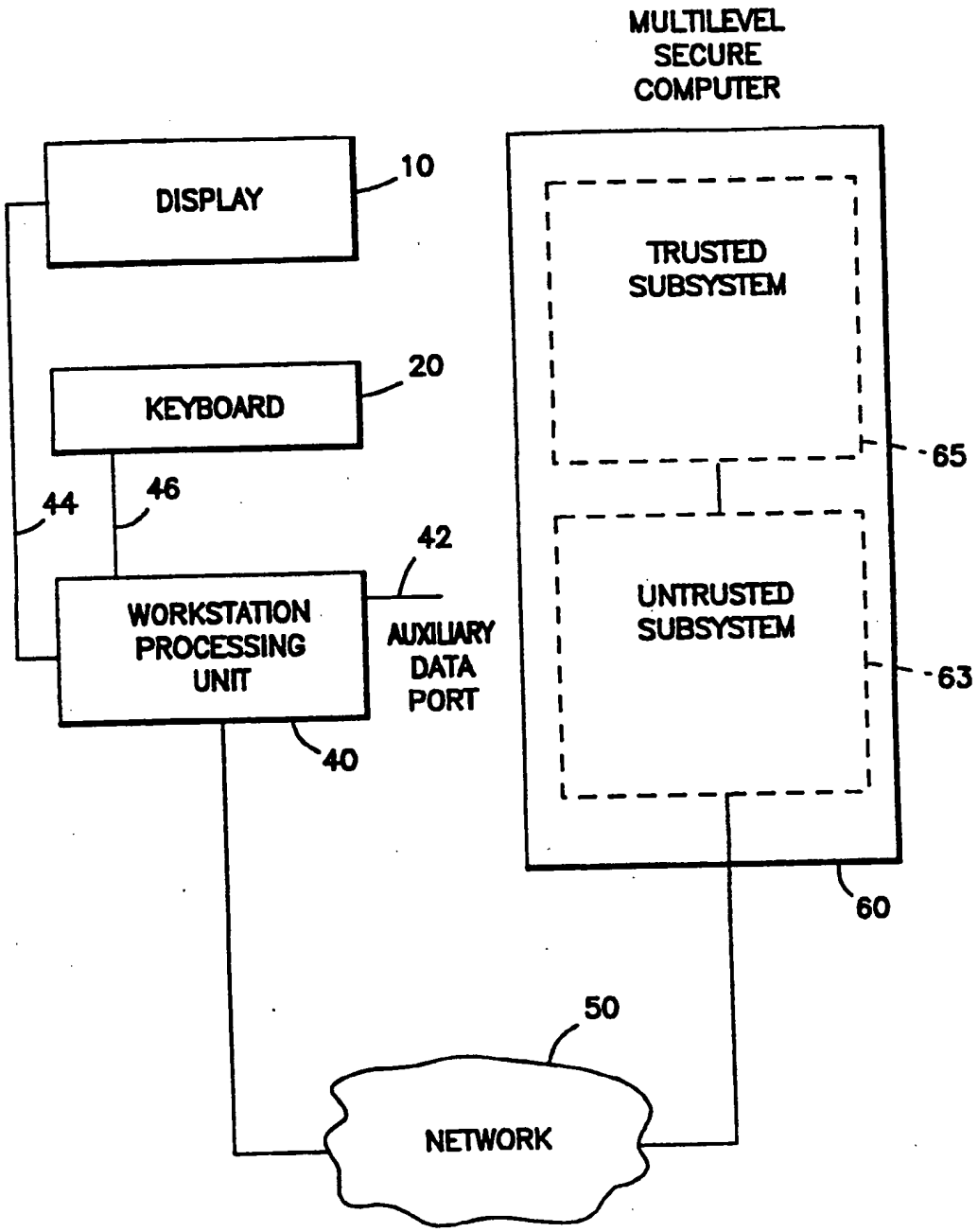


FIG. 1
PRIOR ART

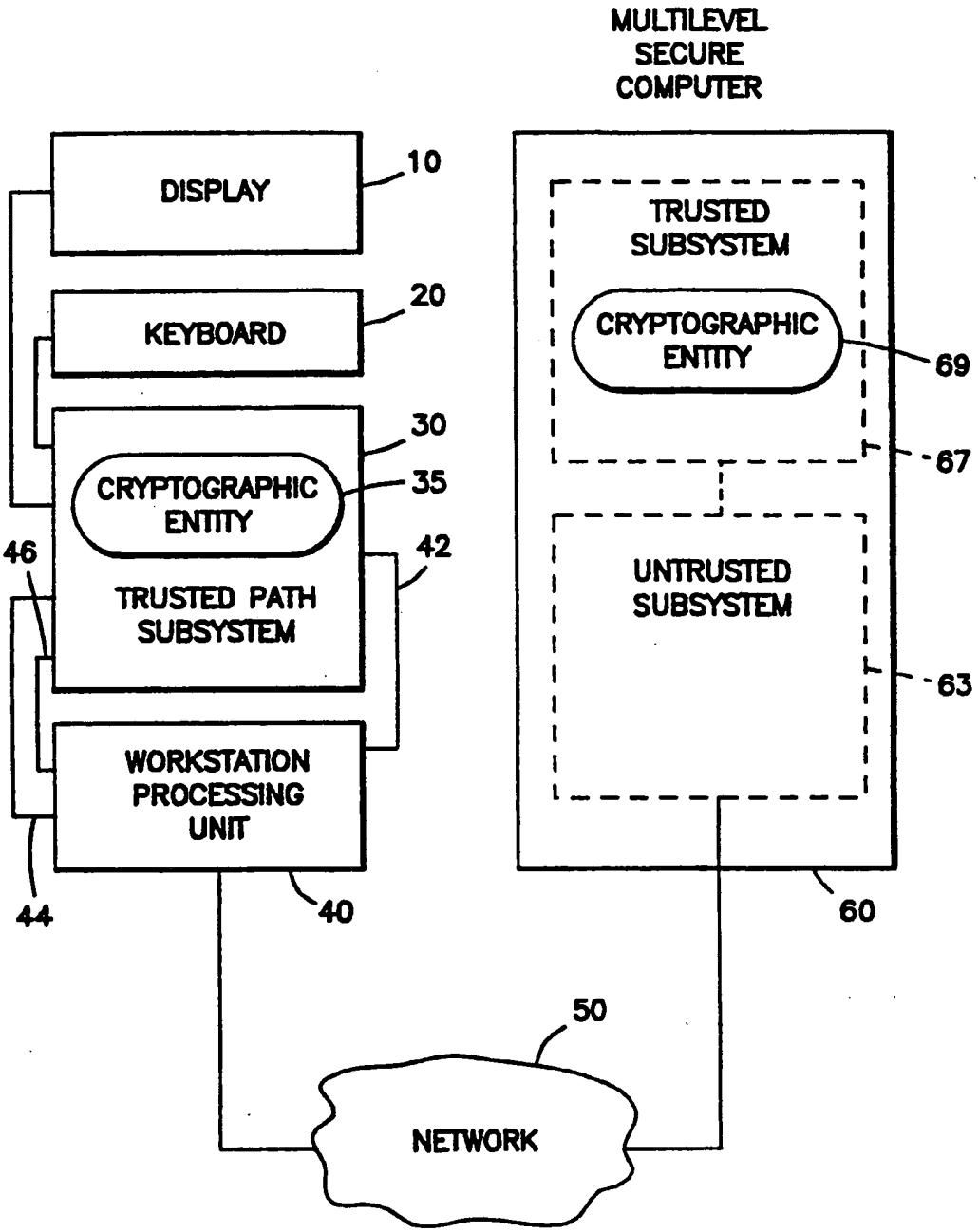

MULTILEVEL SECURE COMPUTER
DISPLAY
10
KEYBOARD
20
CRYPTOGRAPHIC ENTITY
30
35
TRUSTED PATH SUBSYSTEM
42
46
WORKSTATION PROCESSING UNIT
44
40
TRUSTED SUBSYSTEM
CRYPTOGRAPHIC ENTITY
69
67
UNTRUSTED SUBSYSTEM
63
60
50
NETWORK

FIG. 2

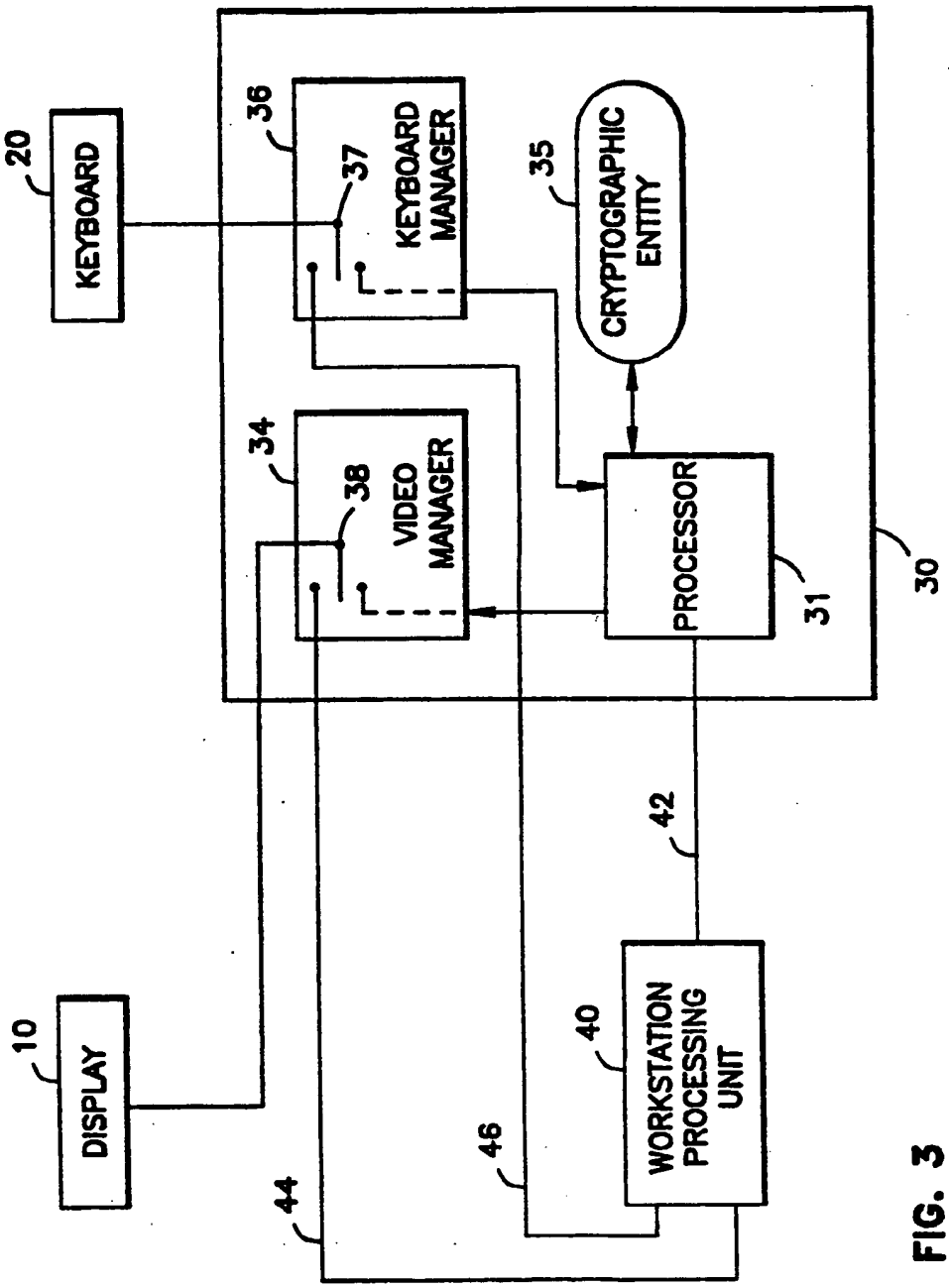

20
KEYBOARD
36
37
KEYBOARD MANAGER
35
CRYPTOGRAPHIC ENTITY
34
38
VIDEO MANAGER
PROCESSOR
31
30
42
10
DISPLAY
40
WORKSTATION PROCESSING UNIT
46
44

FIG. 3

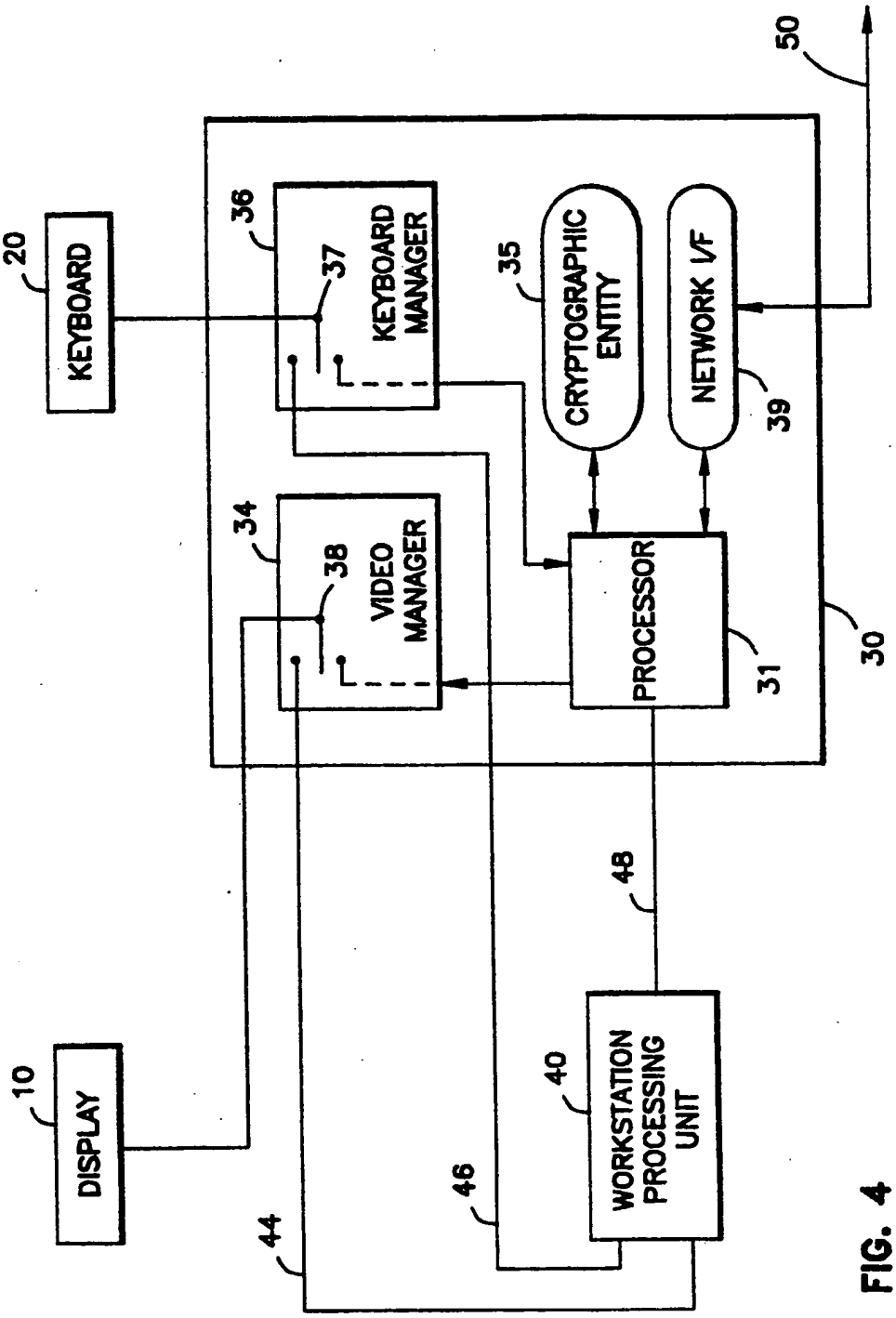

50
20
KEYBOARD
36
37
KEYBOARD MANAGER
35
CRYPTOGRAPHIC ENTITY
NETWORK I/F
39
34
38
VIDEO MANAGER
PROCESSOR
31
30
48
10
DISPLAY
40
WORKSTATION PROCESSING UNIT
46
44

FIG. 4

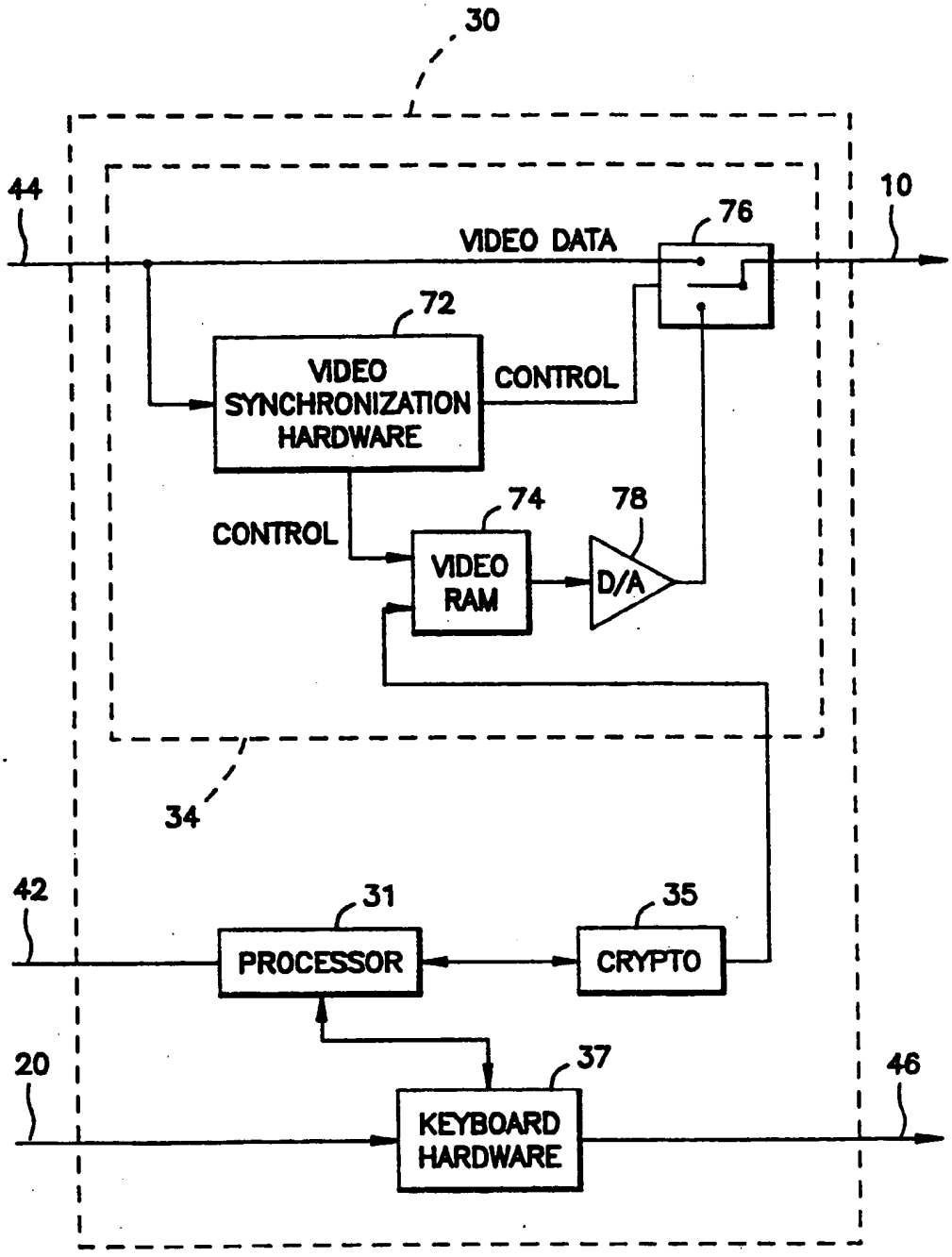

30
44
10
VIDEO DATA
76
72
VIDEO SYNCHRONIZATION HARDWARE
CONTROL
CONTROL
74
78
VIDEO RAM
D/A
34
42
31
35
PROCESSOR
CRYPTO
20
37
46
KEYBOARD HARDWARE

FIG. 5

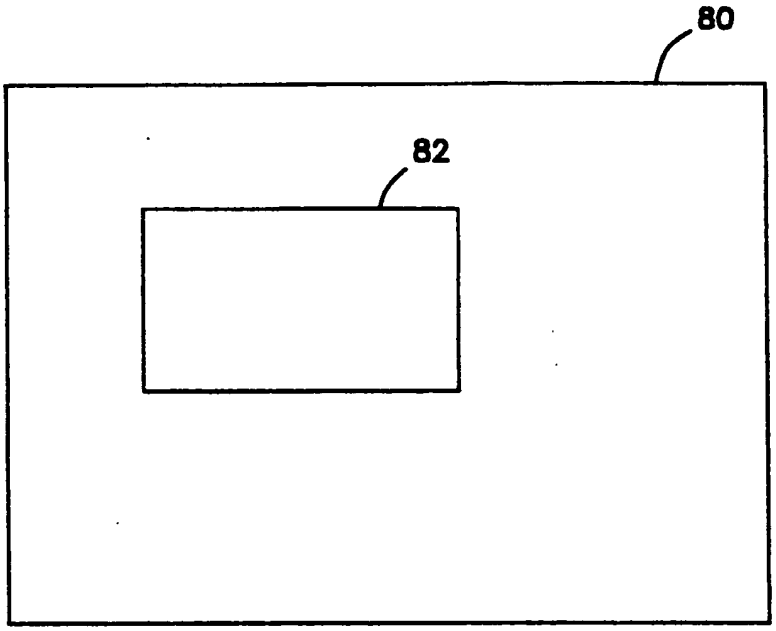


FIG. 6

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 93/06511

A. CLASSIFICATION OF SUBJECT MATTER
IPC 5 G06F12/14 G06F1/00

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
IPC 5 G06F

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	EP,A,0 192 243 (HONEYWELL) 27 August 1986 cited in the application see abstract; figures 3,4 see page 18, line 16 - page 21, line 14 see claims 1-10	1-16
P,Y	WO,A,92 17958 (SECURE COMPUTING TECHNOLOGY) 15 October 1992 cited in the application see abstract; figure 1 see page 3, line 35 - page 6, line 16 see page 7, line 22 - page 10, line 35	1-16

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
23 November 1993	07. 12. 93

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+ 31-70) 340-2040, Tx. 31 651 epo nl, Fax (+ 31-70) 340-3016	POWELL, D

Form PCT/ISA/210 (second sheet) (July 1992)

Petitioner Apple Inc. - Exhibit 1012, p. 1269

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	IEEE SYMPOSIUM ON SECURITY AND PRIVACY, 4 May 1992 , OAKLAND, US; pages 226 - 239 J.EPSTEIN ET AL 'Evolution of a Trusted B3 Window Prototype' see figure 3 see page 229, left column, line 1 - page 230, right column, line 5 see page 231, right column, line 23 - page 232, left column, line 32 see page 233, left column, line 5 - page 234, left column, line 15 ---	3-5,8-13
Y	PROC. FALL JOINT COMPUTER CONF., 25 October 1987 , DALLAS, US; pages 411 - 420 J.PICCIOTTO ET AL 'Privileges and Their Use by Trusted Applications' see page 415, left column, line 23 - page 419, left column, line 18 ---	15,16
A	EP,A,0 096 628 (DIGITAL EQUIPMENT CORPORATION) 21 December 1983 see abstract; figure 1 ---	13
A	EP,A,0 443 423 (DIGITAL EQUIPMENT CORPORATION) 28 August 1991 see abstract; figures 4A,4B -----	15,16

Petitioner Apple Inc. - Exhibit 1012, p. 1270

INTERNATIONAL SEARCH REPORT

information on patent family members

International Application No
PCT/US 93/06511

Patent document cited in search report	Publication date	Patent family member(s)		Publication date
EP-A-0192243	27-08-86	US-A-	4713753	15-12-87
		CA-A-	1252907	18-04-89
		JP-A-	61195443	29-08-86
WO-A-9217958	15-10-92	AU-A-	1576792	02-11-92
EP-A-0096628	21-12-83	US-A-	4498098	05-02-85
		AU-A-	1501683	08-12-83
		CA-A-	1185377	09-04-85
		JP-C-	1628356	20-12-91
		JP-B-	2052911	15-11-90
		JP-A-	59057279	02-04-84
EP-A-0443423	28-08-91	AU-A-	7103191	15-08-91

Petitioner Apple Inc. - Exhibit 1012, p. 1271

Requested Patent: JP1068835A

Title: SOFTWARE RIGHT MANAGEMENT CONTROL METHOD ;

Abstracted Patent: JP1068835 ;

Publication Date: 1989-03-14 ;

Inventor(s): MORI RYOICHI; others: 01 ;

Applicant(s): RYOICHI MORI ;

Application Number: JP19870227106 19870910 ;

Priority Number(s): ;

IPC Classification: G06F9/06 ;

Equivalents: JP2723231B2 ;

ABSTRACT:

PURPOSE:To perform the right management superior in maintainability and flexibility in the environment of multiprogramming by individually assigning the key, with which ciphered instructions are deciphered, to a program or a program group as the right management object and switching the deciphering keys by a right management interrupt.

CONSTITUTION:A right management interrupt generating mechanism 13 which controls the change related to the right management state is provided independently of the supervisor interrupt which starts the processing function of an operating system or the like. When the right management interrupt is generated by the right management interrupt generating mechanism 13, the right management state is saved to a right management table 17 and a current right management ID 16 of a program status word 15 is changed by a right management state change processing 14, and the key with which instructions are deciphered is switched. Thus, right management in the environment of multiprogramming is possible.

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭64－68835

⑤1Int.Cl.⁴	識別記号	庁内整理番号	④3公開　昭和64年(1989)3月14日
G 06 F 9/06	330	A－7361－5B	

審査請求　未請求　発明の数 1　（全13頁）

⑤4発明の名称　ソフトウエア権利管理制御方法

②1特　願　昭62－227106
②2出　願　昭62(1987)9月10日

⑦2発明者　森　亮一　東京都文京区白山1－24－12
⑦2発明者　田代　秀一　千葉県柏市松葉町1－12－20－2
⑦1出願人　森　亮一　東京都文京区白山1－24－12
⑦4代理人　弁理士　小笠原　吉義　外2名

明　細　書

1．発明の名称　ソフトウエア権利管理制御方法

2．特許請求の範囲

（1）暗号化された命令を，命令フェッチ時に復号化して実行するデータ処理装置におけるソフトウェア権利管理制御方法であって，

権利管理状態の変更に関する割込みを制御する権利管理割込み発生機構(13)を設け，

権利管理対象となるプログラムまたはプログラム群に対し，暗号化された命令を復号化する鍵を個別に割り当て，

上記権利管理割込みにより，上記復号化する鍵を切り換える(14)ことを特徴とするソフトウェア権利管理制御方法。

（2）上記権利管理対象となるプログラムまたはプログラム群は，許諾条件プログラム，該許諾条件プログラムによって実行を制御されるソフトウェア本体，またはそれらの組み合わせであることを特徴とする特許請求の範囲第（1）項記載のソフトウェア権利管理制御方法。

3．発明の詳細な説明

〔概要〕

個々の権利対象ソフトウェア毎に，ソフトウェアの使用許諾，使用記録情報の収集などを，他のソフトウェアによる影響および干渉を受けずに行うことができるようにしたデータ処理装置におけるソフトウェア権利管理制御方法に関し，

マルチプログラミングの環境における権利管理の実現に適した制御方法を提供することを目的とし，

暗号化された命令を，命令フェッチ時に復号化して実行するデータ処理装置におけるソフトウェア権利管理制御方法であって，権利管理状態の変更に関する割込みを制御する権利管理割込み発生機構を設け，権利管理対象となるプログラムまたはプログラム群に対し，暗号化された命令を復号化する鍵を個別に割り当て，上記権利管理割込み

Petitioner Apple Inc. - Exhibit 1012, p. 1273

により，上記復号化する鍵を切り換えるように構成する。

〔産業上の利用分野〕

本発明は，個々の権利対象ソフトウェア毎に，ソフトウェアの使用許諾，使用記録情報の収集などを，他のソフトウェアによる影響および干渉を受けずに行うことができるようにしたデータ処理装置におけるソフトウェア権利管理制御方法に関する。

半導体技術の進歩によって，計算機ハードウェアの価格低下，小型化，高機能化が急速に進みつつある。ハードウェア機能の高度化は，ソフトウェアの高度化を要求し，結果として，ハードウェア開発者，ソフトウェア開発者，利用者の明確な分業化が促進されている。

しかしながら，ソフトウェア流通の環境は，現在，混乱した状況にあるといってよく，その環境を改善するために，ソフトウェア権利者の保護と利用者の便利さとを両立させるシステムであって，

上記(3)は，バックアップがとれなくなるという問題や，複製不能にしている手段を調べ，それを回避することにより複製可能となるという問題があり，上記(4)は，特定計算機を識別するために，ソフトウェアの販売時などに特殊化処理が必要となり，自由なソフトウェアの流通が阻害されるという問題がある。

これらの問題を解決するものとして，本出願人は，ソフトウェア権利者の権利と，利用者の自由と，流通の容易性の3つを同時に満たすソフトウェアサービスシステム（ＳＳＳ）の基本構想を提案している。〔森亮一："ソフトウェアサービスシステム"，電子通信学会誌，Vol.67，No.4，pp.431-436（Apr.1984）〕

ここで提案されたソフトウェアサービスシステムの基本は，

(1) ソフトウェアは，いかなる条件が成立した場合に，その実行を許すかの許諾条件を内部に持つべきである。

(2) 計算機内部には，利用者の持つ権利を記述し

ソフトウェアの自由な大量流通を支援するシステムを構築することが望まれている。

〔従来の技術〕

ソフトウェアの開発には，大量の人員および時間を要するにもかかわらず，利用者または第三者は，完成したソフトウェアを複製して，全く同じものを作成することが比較的容易にできる。そのため，ソフトウェアを開発した権利者（ソフトウェア権利者）は，開発コストの回収が不能になるケースが多く，これに対して，(1)ソフトウェア製品の価格を盗用による損失分を上乗せした値とする，(2)契約によって無断複製を禁止する，(3)ソフトウェアを複製不能な媒体に封入して流通させる，(4)計算機のシリアルナンバーなどにより使用可能な装置を限定する，などによって対処することが行われている。

しかしながら，上記(1)は，正当な利用者に過度の負担を与え，上記(2)は，繁雑な契約手続きが必要になると共に，それによる効果が充分でなく，

た権利記録があるべきである。これには，共通クレジット，買い取り記録，試用記録，特別許諾コード等が有り得る。

(3) 計算機は，上記(2)の権利記録が上記(1)の許諾条件を満足した場合にのみ，ソフトウェアの利用を許す実行管理機構を持つべきである。

(4) 権利者が，ソフトウェアの利用状況を把握できるように，計算機は，回収用作業記録を持つべきである。利用者に特別な面倒を与えることなく，この作業記録を回収する電子的手段が有り得る。

…というものである。

ところで，このソフトウェアサービスシステムの提案とは別に，暗号化された命令およびデータを主記憶にロードし，命令フェッチ時に，計算機のシリアルナンバーなどの復号鍵によって復号して実行する計算機アーキテクチャが知られている。

〔発明が解決しようとする問題点〕

上記ソフトウェアサービスシステムを，マルチプログラミングの環境下で実現する場合，複数の

Petitioner Apple Inc. - Exhibit 1012, p. 1274

ソフトウェア権利者に係る複数のプログラムが，時分割的に同時に計算機資源を利用して，走行することになる。この場合，第１に，権利の管理に係るハードウェア機構を制御する主体を，いかにして許諾条件をチェックするプログラム（以下，許諾条件プログラムという）に限定するか，第２に，マルチプログラミングの環境において，許諾条件プログラムと，それによって実行を制御されるソフトウェア本体との対応関係をいかにして保つか，第３に，オペレーティング・システムに対し，スワッピングやプロセス・スイッチを行うためのアクセス権を認めつつ，許諾条件プログラムの内容を改ざんしたり，権利管理のための流れを乱したりすることがないように，いかにしてアクセス権を制限するか，といったことに対する考慮が重要となる。従来，このような権利管理に対する適切な計算機の実行制御を行う機構はなかった。

本発明は上記問題点の解決を図り，マルチプログラミングの環境における権利管理の実現に適した制御方法を提供することを目的としている。

〔問題点を解決するための手段〕

第１図は本発明の原理説明図である。

第１図において，１０は権利管理の単位となる権利管理対象プログラム，１１は許諾条件をチェックしソフトウェア本体の実行を制御する許諾条件プログラム，１２はワープロソフト，コンパイラなどの利用者の使用目的に応じた処理を行うソフトウェア本体，１３は権利管理状態の変更に関する割込みを制御する権利管理割込み発生機構，１４は権利管理割込みによって権利管理状態を変更する権利管理状態の変更処理，１５はプログラムステータスワード（ＰＳＷ），１６は権利管理対象プログラム１０を識別する権利管理ＩＤ（ＰＭＩＤ），１７は権利管理対象プログラム１０の暗号化された命令を復号化する鍵を権利管理ＩＤ１６毎に記憶管理する権利管理テーブル，１８は暗号化された命令をその命令のフェッチ時に復号化する復号化回路を表す。

権利管理対象プログラム１０は，例えば許諾条

件プログラム１１とソフトウェア本体１２との対によって構成される。これらの全部または一部は，権利管理対象プログラム１０毎に定められた１または複数の暗号鍵によって予め暗号化されている。

権利管理対象プログラム１０のロード時に，暗号化された命令を復号化する鍵情報が，その権利管理対象プログラム１０に対してシステムでユニークに割り当てた権利管理ＩＤ１６と共に，権利管理テーブル１７に書き込まれる。

プログラムステータスワード１５は，カレントの権利管理ＩＤ１６が設定されるフィールドを持っている。プログラム実行時に，プログラムステータスワード１５に設定されている権利管理ＩＤ１６により，権利管理テーブル１７の該当エントリがアクセスされ，そのエントリ中の復号鍵（ＫＥＹ）が読み出されて，復号化回路１８へ送られる。復号化回路１８は，暗号化された命令をフェッチしたときに，権利管理テーブル１７から読みだした復号鍵によって復号し，その復号した命令を計算機の命令実行ユニットへ送る。

本発明では，オペレーティング・システム等の処理機能を起動するスーパバイザ割込みなどとは別に，権利管理状態に関する変更を制御する権利管理割込み発生機構１３を設ける。そして，権利管理割込み発生機構１３により，権利管理割込みが発生した場合に，権利管理状態の変更処理１４によって，権利管理テーブル１７への権利管理状態の退避やプログラムステータスワード１５のカレントの権利管理ＩＤ１６の変更などを行う。これにより，命令などを復号化する鍵を切り換える。

〔作用〕

本発明によれば，割込みが，オペレーティング・システムによる資源管理などに関連する従来の割込みと，権利管理状態を制御するための権利管理割込みの２系統に分離されることになる。

権利管理割込みが発生したときに，権利管理状態の変更処理１４によって，権利管理テーブル１７に基づく権利管理状態を変更するので，権利管理に係るハードウェア機構を制御することができ

Petitioner Apple Inc. - Exhibit 1012, p. 1275

る主体を，特定の許諾条件プログラム１１などに個別的に限定することができる。また，個々に復号鍵が管理されるので，ある許諾条件プログラム１１に対応した権利管理テーブル１７中のエントリ等，権利管理に関する情報を，他の権利管理対象プログラム１０などによって，改ざんされることを防止することができる。

また，割込みが，少なくとも従来の割込みと権利管理割込みの２系統になるので，オペレーティング・システムによる権利管理に対する望ましくない関与も，防止することが可能となる。

〔実施例〕

第２図は本発明を用いたソフトウェアの流通形態の例を説明するための図，第３図は本発明による権利管理の説明図，第４図は権利管理状態の状態遷移図，第５図は本発明に用いるハードウェア構成例，第６図は権利管理対象となるソフトウェアの構成例，第７図は権利管理テーブルの構成例，第８図はＰ割込み要求テーブルの構成例，第９図

はＳ割込み制御の例，第１０図はＳ割込みからの復帰制御の例，第１１図は本発明の一実施例におけるスタックの使用例，第１２図は本発明の一実施例における空間と鍵の関係説明図を示す。

本発明は，ソフトウェアの保護と利用促進のため，例えば第２図に示すようなソフトウェアの流通形態を採用する場合に用いることができる。

① ソフトウェアを開発したソフトウェア権利者は，そのソフトウェアを流通させる場合，ソフトウェアの利用者に対して要求する条件を記述した許諾条件プログラムを作成し，それを開発したソフトウェア本体と結合して，暗号化し，電波による放送も含めた自由な媒体により，ソフトウェアを配布する。

② ソフトウェアを利用したい利用者は，例えば予め共通クレジット（ＣＣ）を自動販売機などのベンディングマシンにより購入する。この共通クレジットの内容は，例えばＩＣカードによる媒体を介して，データ処理装置２０に入力できるようになっている。

③ 利用者は，共通クレジットの内容が記録されたＩＣカードを，本発明に係るソフトウェア権利管理制御機能を持つデータ処理装置２０に装着し，適当な流通路から入手したソフトウェアを，データ処理装置２０上で動作させる。これにより，そのソフトウェアの許諾条件プログラムが復号化されて動作し，ＩＣカードへのアクセスにより，共通クレジット情報に関連するチェックなどを行う。必要に応じて共通クレジットに記録されている料金の減算を行う。チェックに合格した場合にのみ，必要なソフトウェア本体の実行を可能とする制御を行う。そのとき，その利用に関する作業記録情報を蓄積しておき，その作業記録（ＡＲ）を適当な時期にＩＣカードへ転記する。

④ ＩＣカードに書き込まれた作業記録は，例えば共通クレジットを継続使用するために，新たな料金の支払いにより共通クレジットの内容を再設定するときに，ベンディングマシンに読み取られ，収集される。この作業記録情報を参照することにより，ソフトウェア利用状況の統計をとり，それに基づいて複数のソフトウェア権利者間で妥当な料金の分配を行うことができる。

第２図に示したソフトウェア流通形態は，一例であり，本発明は，共通クレジットではなく，各ソフトウェア個別の利用資格情報を管理する流通形態をとる場合にも採用することができる。また，ＩＣカード以外の媒体を用いることも可能である。

本発明による場合，データ処理装置２０は，複数の独立したソフトウェアを，マルチプログラミングによって並列動作させることができる。

本発明による権利管理は，概念的には，第３図に示すようになる。

マルチプログラミングの環境では，オペレーティング・システムが，入出力装置の割り当て，プロセッサの割り当てなどの計算機ハードウェア資源の管理を行っている。この場合，誤ったプログラムの実行などによって支障をきたさないようにするために，また計算機の資源を多く利用しようとする利用者によって，資源が恣意的に用いられることを防ぐために，計算機の実行状態をユーザ

Petitioner Apple Inc. - Exhibit 1012, p. 1276

状態と，スーパバイザ状態に分けることが広く行われている。

利用者のプログラムは，ユーザ状態で実行され，資源管理用のオペレーティング・システムは，通常，スーパバイザ状態で実行される。そして，利用者による資源の濫用を防止し，また利用者が勝手に実行状態を変更できないようにするために，ユーザ状態からスーパバイザ状態へと状態を変更する手段を，割込み（割出しを含む）に限ることによって，両状態の分離を図っている。

ここで，第２図で説明したような許諾条件プログラムの復号化や，共通クレジットの読み書きなどに関連する権利管理を，スーパバイザ状態のもとで，オペレーティング・システムにより制御するとすれば，利用者が自己の都合のよいように内部を改変したオペレーティング・システムをロードすることに関して，抵抗力を持たない。これに対し，オペレーティング・システムをファームウェア化して，内容の変更を困難にするという対応策も考えられるが，オペレーティング・システムのバージョンアップが不可能になるなどの他の問題が発生する。

そこで本発明では，スーパバイザ状態とは異なる権利管理状態という特別な実行状態を新設している。権利管理状態は，ソフトウェアをできるだけ無料で実行したいと考える利用者があり得る環境の中で，利用者の故意または過失による介入を避けつつ，外部から供給されたソフトウェアの権利に関する管理を行うためのプログラムを実行可能とする状態である。

権利管理状態は，他の状態からそこへ状態を変更する手段を割込みに限っている点および他の状態では実行できない命令を持つ点で，スーパバイザ状態に類似しているが，暗号の応用と鍵の管理とによって不正なアクセスの防止を図る点が，スーパバイザ状態と大きく異なる。

第３図に示すように，オペレーティング・システムが，スーパバイザ状態のもとで，資源管理を行うのに対し，権利管理対象となっているプログラムの各許諾条件プログラム１１Ａ，１１Ｂ，…

は，個々の権利管理状態のもとで，ソフトウェア本体１２Ａ，１２Ｂ，…の実行を監視することによって，権利管理を行う。以下，許諾条件プログラムと，それによって制御されるソフトウェア本体とを合わせて権利管理対という。

権利管理状態を設けることにより，本発明に係るデータ処理装置は，例えば第４図に示すような状態遷移を行う。ユーザ（ＵＳ）状態，スーパバイザ（ＳＶ）状態，権利管理（ＰＭ）状態があり，スーパバイザ状態は，さらにＳＶｐ状態とＳＶｕ状態とに分かれる。ＳＶｐ状態とＳＶｕ状態とは，使用できる命令，アクセス権等に関しては全く同様であるが，割込みからの復帰命令を実行した場合に，ＰＭ状態に復帰するかＵＳ状態に復帰するかの点が異なる。

以上の４つの状態（ＳＶｐ，ＳＶｕ，ＰＭ，ＵＳ）は，独立した２つの状態ビットにより表現される。その１つは，プログラムステータスワード１５中に置くＳビットであり，他の１つは権利管理テーブル１７中に置くＰビットである。

Ｓビットの変化に伴う状態遷移は，スーパバイザ状態で実行するプログラム，即ち，オペレーティング・システムの制御に関係するものであり，Ｐビットの変化に伴う状態遷移は，ＰＭ状態で実行されるプログラム，即ち，許諾条件プログラムの制御に関係するものである。

これら２系統の状態遷移を直交した関係におき，互いに他の系統の状態遷移には直接影響を及ぼさないようにしているので，資源管理と権利管理との制御機構の分離が図られている。

以下，Ｓビットに関連する従来の割込みをＳ割込みといい，Ｐビットに関連する本発明に係る権利管理割込みをＰ割込みという。

本発明に用いるハードウェア構成は，例えば第５図に示すようになっている。

第５図において，第１図と同符号のものは，第１図に示すものに対応する。３０は命令実行ユニットである演算／制御部，３１はＩＣカードインタフェース，３２はＩＣカードから入力された共通クレジット情報を記憶する共通クレジットレジ

Petitioner Apple Inc. - Exhibit 1012, p. 1277

スタ（ＣＣＲ），３３はソフトウェア買い取り情報などの個々のソフトウェアに特有な権利管理情報を持つ個別権利メモリ（ＳＲＭ），３４はソフトウェアの利用実績情報が記録される作業記録メモリ（ＡＲＭ）である。

共通クレジットレジスタ３２，個別権利メモリ３３，作業記録メモリ３４は，不揮発メモリによって構成される。

３５は許諾条件プログラムまたはソフトウェア本体の全部または一部をＤＥＳ方式により復号化するＤＥＳ暗号機構，３６はＰ割込みの要因などの制御情報を記憶するＰ割込み要求テーブル（ＰＩＴ），３７は権利管理対象となるソフトウェアをロードする際に後述するキー格納部の復号化を行う公開鍵暗号機構である。

第５図に示す装置が扱うソフトウェアの構造は，例えば第６図に示すようになっている。キー格納部，許諾条件プログラム１１，ソフトウェア本体１２の３つの部分からなる。

本実施例では，許諾条件プログラム１１を，権

利者が任意に与える鍵（ＫＥＹ１）によって，いわゆるＤＥＳ方式で暗号化する。また，ソフトウェア本体１２の少なくとも一部を，やはり権利者が任意に与える鍵（ＫＥＹ２）によってＤＥＳ方式で暗号化する。なお，ＤＥＳ方式については，例えば「一松信監修："データ保護と暗号化の研究"，日本経済新聞社〔1983〕」に記述されている。

キー格納部には，このソフトウェアを識別するユニークな権利番号（ＰＮ）と，個別権利記録（ＳＲ）に対するアクセスを管理するための非公開のＳＲアクセスキーと，許諾条件プログラム１１，ソフトウェア本体１２を復号化するためのＫＥＹ１，ＫＥＹ２とが設定されるようになっている。キー格納部は，例えば公開鍵暗号方式のひとつであるＲＳＡ法により暗号化される。なお，このＲＳＡ法も，例えば上記"データ保護と暗号化の研究"の著書などにより知られている。公開鍵暗号方式は，暗号化に用いる鍵を知っていても，秘密鍵である復号化鍵を知っていないと，暗号を

解くことができないという特徴がある。もちろん他の暗号方式を用いても，同様に本発明を実施することは可能である。

このキー格納部を復号化するための鍵は，ハードウェア製造時に，第５図に示す公開鍵暗号機構３７の内部に封入しておく。このソフトウェアを主記憶上にロードする際に，公開鍵暗号機構３７によってキー格納部を復号化し，その復号結果を権利管理テーブル１７に設定する。

権利管理テーブル１７は，例えば第７図に示すような権利管理に関する情報を持つ。

権利管理テーブル１７中のレコードは，このレコードに対応する権利管理対を識別するためのＰＭＩＤ，権利番号（ＰＮ），ＳＲアクセスキー，許諾条件プログラムを実行するために必要なＤＥＳ鍵（ＫＥＹ１），ソフトウェア本体を実行するために必要なＤＥＳ鍵（ＫＥＹ２），ＫＥＹ２の有効／無効を示すビット（Ｋ２Ｆ），許諾条件プログラムによる権利管理状態か否かを表すＰビット，対応する権利管理対がロードされた直後であ

ることを表すイニシャルビット，およびスタックの正当性を確認するためのスタックチェックコードの９つのフィールドからなる。

システム中に同時に存在し得る権利管理対の数は，権利管理テーブル１７のレコード数に等しい。複数のレコードのうち，ＰＳＷ中のカレントＰＭＩＤの値と一致したＰＭＩＤを持つレコードを，カレントＰＭＴレコードと呼び，権利管理テーブル１７のレコードに対するアクセスは，通常の場合，このカレントＰＭＴレコードに対して行われる。

第５図に示すＰ割込み要求テーブル（ＰＩＴ）３６は，権利管理割込み（Ｐ割込み）発生機構１３が使用するテーブルであり，例えば第８図に示すような構成になっている。ＰＩＴ３６中の各レコードは，Ｐ割込みを要求する権利管理対のＰＭＩＤ，そのＳＲアクセスキーを記憶するフィールド，要求するＰ割込みの要因を記述するフィールド（Ｐ－Reason），Ｐ割込み発生時の飛び先アドレスを記述するフィールド（New-PC），Ｐ割込み

Petitioner Apple Inc. - Exhibit 1012, p. 1278

要求の要因に対するパラメータを記述するフィールドの５つのフィールドからなる。

ＰＩＴ３６中のレコードは，ＰＭ状態でしか使用できない特権命令によってのみ，生成／消去が可能にされ，また，ＳＲアクセスキーを用いたアクセス権のチェックにより，正当な権利者以外の許諾条件プログラムからは，既に存在するＰＩＴレコードの書き換えや消去ができないようになっている。

Ｐ割込みの要因には，例えばＵＳ状態におけるＰ割込み命令の実行，タイマー割込み，ＵＳ状態における特定命令の実行（命令トラップ）がある。タイマー割込みに対しては，パラメータとして割込み発生の時間間隔を与えることができ，命令トラップに対しては，任意の命令コードをパラメータとして与えることができる。これにより，許諾条件プログラムは，必要に応じてソフトウェア本体の実行制御を行い，またソフトウェア本体の実行に関する作業記録をとる契機を得ることができるようになっている。

トＰＭＴレコードから取り出した旧スタックチェックコード１，２の４ワード（６４bit）をＫＥＹ１で暗号化し，スタックへストアする。

(e) 新スタックチェックコード１，２を，カレントＰＭＴレコードへストアする。

(f) ＰＩＴの飛び先アドレス（New-PC）を，プログラムカウンタにセットする。そして，(h)の制御へ移る。

(g) Ｐビットが０の場合には，割込みベクタをプログラムカウンタにセットする。

(h) ＰＳＷ，プログラムカウンタ，スタックフォーマットコードをスタックへストアする。

(i) ＰＳＷのＳビットを"１"にし，オペレーティング・システムの割込み処理ルーチンへ制御を移す。

なお，この例では，Ｓ割込み時における飛び先アドレス，即ち，プログラムカウンタに設定する新しい値を，いわゆる割込みベクタテーブルからロードする方式を用いている。

スーパバイザ状態において，ＲＳＥ（Return

第５図に示すＰ割込み発生機構１３は，許諾条件プログラムがＰＩＴ３６に指定した要因が発生したときに，自動的にＰ割込みを起こす機構であるが，その内部の回路構成等については，従来技術と同様な一般的な割込み技術を用いて実施可能であるので，これ以上の説明を省略する。

Ｓ割込みとＰ割込みとを独立させるために，Ｓ割込みが発生した場合におけるプロセッサの動作は，例えば第９図に示す(a)～(i)のようになる。

(a) Ｓ割込みが発生した場合，ファームウェアなどにより，カレントＰＭＴレコードのＰビットの０／１をチェックし，０であれば(d)へ制御を移す。

(b) Ｐビットが１であれば，現在のＰＳＷ及びプログラムカウンタの値から，１６bit のサイクリックコードを生成し，新スタックチェックコード１とする。

(c) １６bit の乱数を生成し，新スタックチェックコード２とする。

(d) 新スタックチェックコード１，２及びカレン

from S-Exception）命令を実行することにより，ＰＭ状態またはＵＳ状態のいずれかへ遷移する。そのときのプロセッサの動作は，例えば第１０図に示す(a)～(g)のようになる。

(a) カレントＰＭＴレコードのＰビットの０／１をチェックする。それが０であれば，(f)へ制御を移す。

(b) スタックから，スタックチェックコード１，２および旧スタックチェックコード１，２を取り出し，それらをＫＥＹ１で復号化してプロセッサ内に保持する。

(c) スタックのＰＳＷ及びプログラムカウンタの値から，１６bit のサイクリックコードを生成し，上記(b)で取り出したスタックチェックコード１と比較する。不一致であれば，エラーとして処理する。即ち，ＰＭ状態への遷移などを防止する。

(d) 次に，カレントＰＭＴレコードのスタックチェックコード２と，上記(b)で取り出したスタックチェックコード２とを比較する。不一致であ

Petitioner Apple Inc. - Exhibit 1012, p. 1279

ればエラーとして処理する。

(e) 旧スタックチェックコード1，2をカレントPMTレコードへストアする。

(f) PSWのSビットを"0"に戻す。

(g) スタックにストアされているプログラムカウンタの値を，プログラムカウンタにセットする。そして，割込み発生直前に実行されていたルーチンへ復帰する。

PM状態からS割込みによりSVp状態へ遷移する際に，例えば第11図（a）に示すようなスタック情報が，プロセッサによってスーパバイザ空間に退避される。スタックチェックコードは，スタックに退避された情報が，オペレーティング・システムによって書き換えられることを防止するために使用されるコードである。

スタックチェックコード1は，第9図で説明したように，スタックに退避されるPSW及びプログラムカウンタの値から生成するサイクリックコードであり，スタックチェックコード2は，16bitの乱数である。これらは，スタックに退避されると同時に，カレントPMTレコードにも格納され，後にスタックの情報を取り出す際にチェックされる。これにより，スタック内容が書き換えられたことを検出できるようになっている。

旧スタックチェックコード1，2は，割込みがネストされた場合に，古いスタックチェックコードを記録するためのものである。

US状態からSVu状態へ遷移する場合には，第11図（b）に示すデータがスタックに退避される。また，SV状態時におけるS割込み発生時には，第11図（c）に示すデータがスタックに退避され，US状態時におけるP割込み発生時には，第11図（d）に示すデータがスタックに退避される。なお，SV状態においては，P割込みはマスクされる。

本実施例では，SV，PM，USの各状態毎に，プログラムのアクセスできる空間およびハードウェアによって自動的に使用される暗号の鍵が決められる。第12図は，その空間と鍵の関係を示している。

PM状態におけるプログラムの実行は，以下のとおりである。

PM状態において，命令フェッチ，データのロード／ストア，サブルーチン呼び出し，割込み発生時におけるプログラムカウンタのスタックへの退避など，主記憶に対するあらゆる書き込み，読み出しの際に，カレントPMTレコード中のKEY1を用いた自動的な暗号化および復号化が，第5図に示すDES暗号機構35によって行われる。PM状態で使用するアドレス空間は，US状態の空間と全く同一であり，区別されてない。これらは，鍵の管理によってのみ隔離されている。

オペレーティング・システムといえども，鍵を知らない限り，許諾条件プログラムを一時停止，強制終了させること以外，その動作に不正に介入することはできない。

PM状態からUS状態への戻りは，RPE（Return from P-Exception）命令の実行によって行われる。

US状態においては，命令フェッチ時に限り，カレントPMTレコードのKEY2を用いた復号化を行う。ただし，復号化による命令実行速度の低下を軽減するために，プログラムのすべての部分を暗号化するのではなく，暗号化する範囲を任意に指定できるようにする方式をとることが望ましい。そのため，US状態で，カレントPMTレコードのK2Pビットをコントロールする命令が用意され，K2Pビットが"1"の間だけ，命令フェッチ時に，KEY2による復号化を自動的に行うようになっている。

オペレーティング・システムは，以下の処理を行う。

① 権利管理対象のソフトウェア全体を，暗号化されたまま主記憶へロードする。

② 次に，権利管理テーブル17内に新しいレコードを生成する命令を発行する。この命令では，これから実行しようとする権利管理対に与えるPMIDの値と，ロードしたソフトウェアのキー格納部の先頭論理アドレスとをパラメータとする。PMIDの値は，システム内部においてユニーク

Petitioner Apple Inc. - Exhibit 1012, p. 1280

であれば，任意でよい。この命令によって，ハードウェアは，ソフトウェアのキー格納部を復号化し，その情報を権利管理テーブル１７に格納して新しいＰＭＴレコードを作成する。同時に，ＰＳＷのカレントＰＭＩＤのフィールドを，これから実行しようとする権利管理対のＰＭＩＤの値にセットする。権利管理テーブル１７のイニシャルビットおよびＰビットを"１"にセットする。

③　ＲＳＥ命令を実行する。カレントＰＭＴレコードは，新しく生成されたレコードであり，このイニシャルビットが"１"である場合に，ＲＳＥ命令が実行されると，プロセッサの状態はＰＭ状態に遷移し，許諾条件プログラムに実行制御が渡される。同時に，イニシャルビットはクリアされ，以後，オペレーティング・システムから許諾条件プログラムへ制御を移す手段は，Ｓ割込みに対するＲＳＥ命令の実行以外に存在しなくなる。

④　上記③までで，権利管理対が生成され，許諾条件プログラムの先頭から実行が開始される。許諾条件プログラムの先頭部分には，利用者との会話を行うプログラム，ソフトウェア本体の実行時間等の計量を開始するために，Ｐ割込み要求テーブルに割込み要求を書き込むプログラム等を置くことができる。その後，ソフトウェア本体に制御を移す命令を発行する。この命令では，Ｐビットのクリアが行われる。

以後，Ｐ割込みとＲＰＥ命令によって，ＵＳ状態とＰＭ状態とを間を行き来しながらプログラムの実行がなされる。権利管理対の実行を終了する場合，オペレーティング・システムは，消去したい権利管理対のＰＭＩＤをパラメータとするＰＭＴ消去命令を発行する。これにより，ハードウェアによって，権利管理テーブルの対応するレコードおよびＰＩＴの該当エントリが消去される。

権利管理に関する命令について，例えばいかなる命令を用意すればよいかについては，以上の実施例の説明で明らかであるが，各命令の機能変更，拡張は任意になし得る。

〔発明の効果〕

以上説明したように，本発明によれば，マルチプログラミングの環境において，保全性，柔軟性に優れた権利管理を行うことが可能になり，ソフトウェアを自由に大量に流通させ，かつソフトウェアの保護が充分であるシステムを構築できるようになる。

4．図面の簡単な説明

第１図は本発明の原理説明図，

第２図は本発明を用いたソフトウェアの流通形態の例を説明するための図，

第３図は本発明による権利管理の説明図，

第４図は権利管理状態の状態遷移図，

第５図は本発明に用いるハードウェア構成例，

第６図は権利管理対象となるソフトウェアの構成例，

第７図は権利管理テーブルの構成例，

第８図はＰ割込み要求テーブルの構成例，

第９図はＳ割込み制御の例，

第１０図はＳ割込みからの復帰制御の例，

第１１図は本発明の一実施例におけるスタックの使用例，

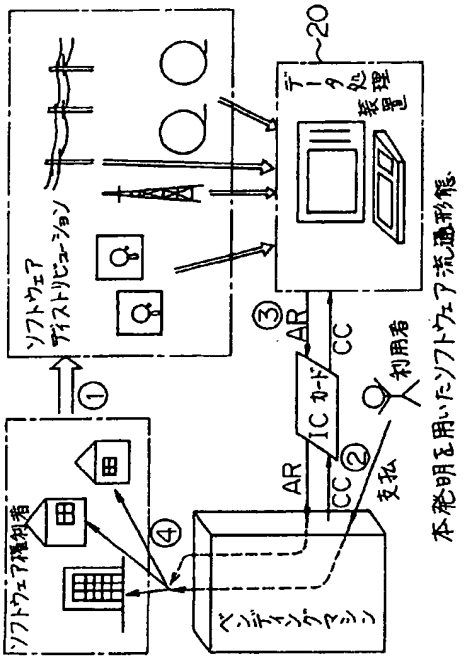
第１２図は本発明の一実施例における空間と鍵の関係説明図を示す。

図中，１０は権利管理対象プログラム，１１は許諾条件プログラム，１２はソフトウェア本体，１３は権利管理割込み発生機構，１４は権利管理状態の変更処理，１５はプログラムステータスワード，１６は権利管理ＩＤ，１７は権利管理テーブル，１８は復号化回路を表す。

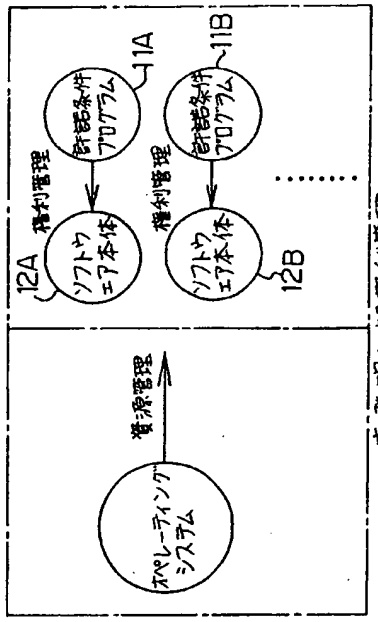
特許出願人　　森　亮一

代理人　弁理士　　小笠原　吉義（外２名）

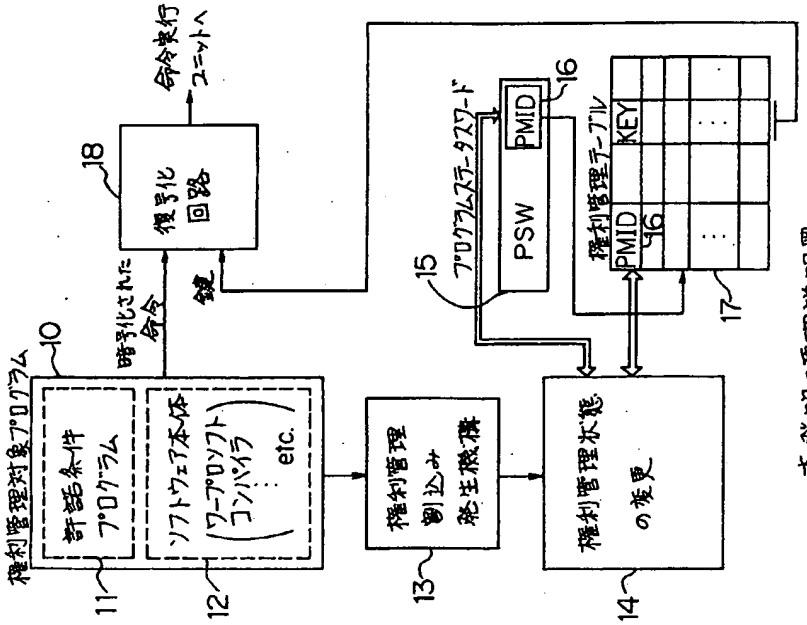
Petitioner Apple Inc. - Exhibit 1012, p. 1281



本発明を用いたソフトウェア流通形態
第２図

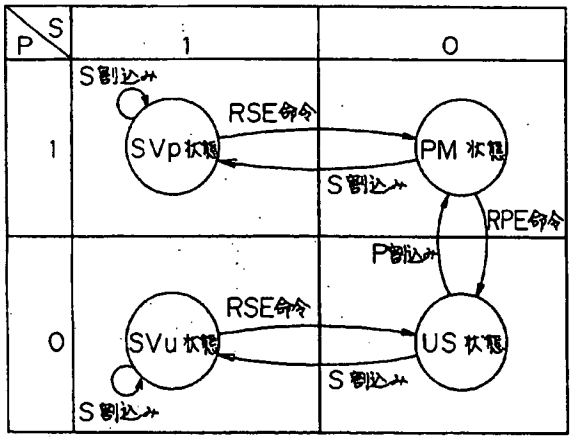


本発明による権利管理
第３図



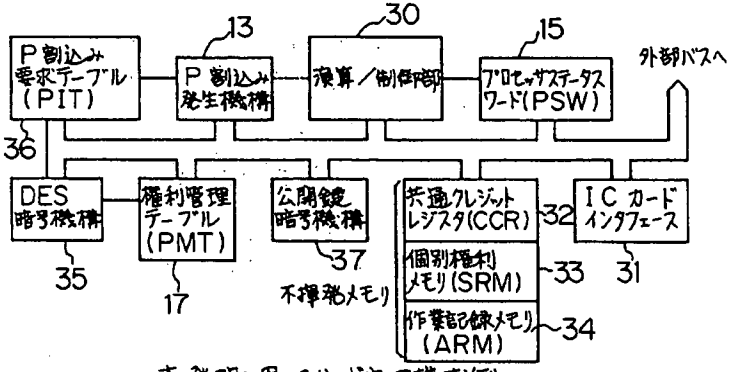
本発明の原理説明図
第１図

Petitioner Apple Inc. - Exhibit 1012, p. 1282



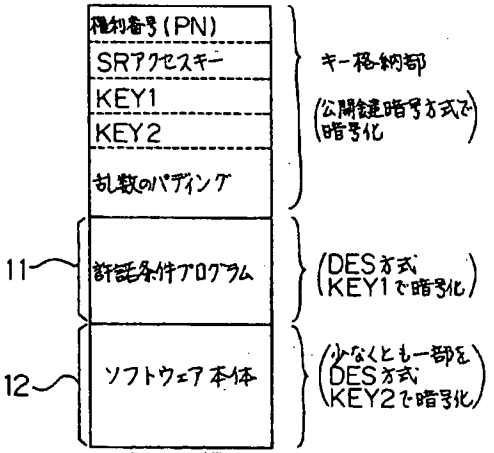
状態遷移図

第 4 図



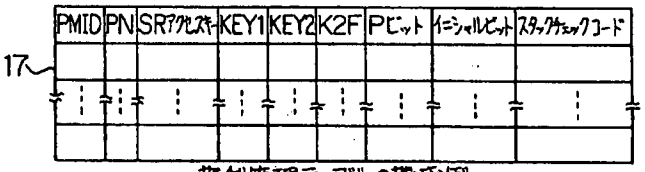
本発明に用いるハードウェア構成例

第 5 図



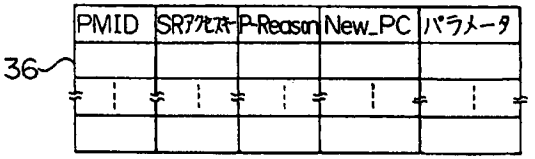
ソフトウェアの構成例

第 6 図



権利管理テーブルの構成例

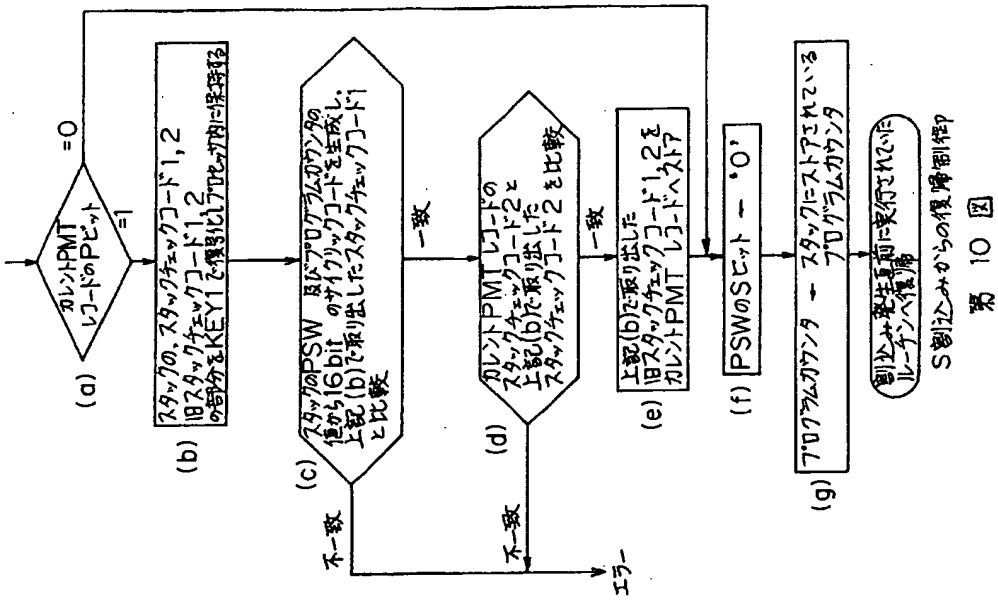
第 7 図



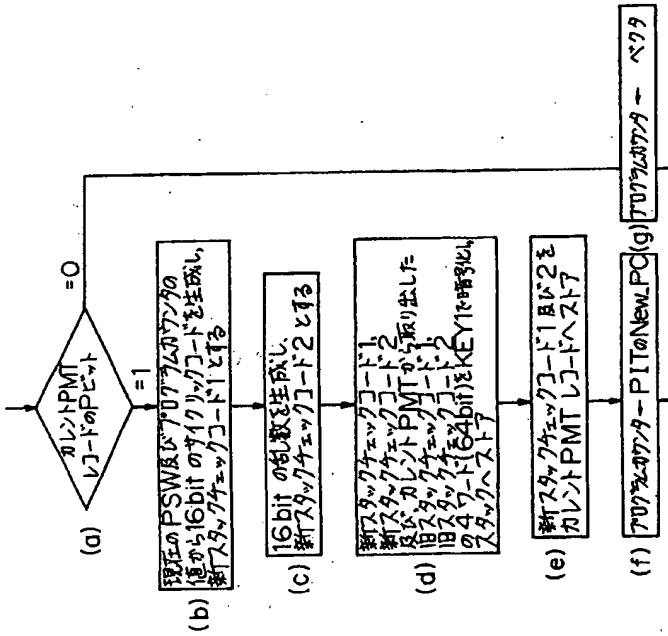
P割込み要求テーブルの構成例

第 8 図

Petitioner Apple Inc. - Exhibit 1012, p. 1283

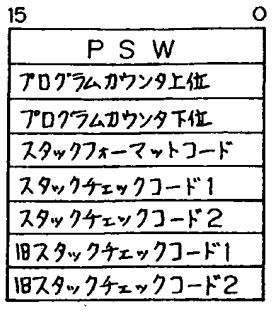


第 10 図

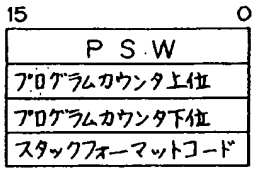


第 9 図

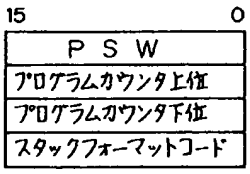
Petitioner Apple Inc. - Exhibit 1012, p. 1284



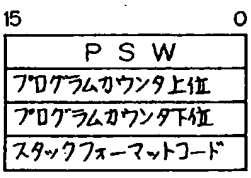
(a) PM状態時におけるS割込み発生時



(b) US状態時におけるS割込み発生時



(c) SV状態時におけるS割込み発生時



(d) US状態時におけるP割込み発生時

スタックの使用例

第 11 図

	SV状態	PM状態	US状態
空間	スーパバイザ空間	ユーザ空間	
鍵	—	カレントPMTのKEY1	カレントPMTのKEY2

空間と鍵の関係

第 12 図

Petitioner Apple Inc. - Exhibit 1012, p. 1285

Requested Patent: JP62241061A

Title: INFORMATION ACCESS MANAGEMENT SYSTEM ;

Abstracted Patent: JP62241061 ;

Publication Date: 1987-10-21 ;

Inventor(s): SHIMOSATO MASAO ;

Applicant(s): NEC CORP ;

Application Number: JP19860083842 19860411 ;

Priority Number(s): ;

IPC Classification: G06F15/16; G06F12/00 ;

Equivalents: ;

ABSTRACT:

PURPOSE:To eliminate the need for changing access rights for reference and updating required for each change in constituent members, by registering not only the names of the users who can refer to and update the information stored in a file area but also their hierarchical positions, etc.

CONSTITUTION:A register means 1 registers the access right management information including the accessible hierarchy information showing the hierarchical positions of the users who can refer to and update the information stored in a file and the file name and then stores the information in an access right memory means 2. A request accepting means 4 accepts file access requests for reference/updating of the information stored in the file from users and judges these request via a deciding means 3 based on user organization information informed via an organization information transmitting means 6 and the access right management information stored in the means 2. Based on the judgement result of the means 3, the permission or rejection of the file access request is informed in reply to the user who had file access through an answer means 5.

⑲日本国特許庁（JP）　⑪特許出願公開

⑫公開特許公報（A）　昭62－241061

⑤Int.Cl.⁴	識別記号	庁内整理番号	㊸公開　昭和62年(1987)10月21日
G 06 F 15/16		Z－2116－5B	
12/00	302	6711－5B	

審査請求　未請求　発明の数 1　（全7頁）

㊹発明の名称　情報アクセス管理方式

㉑特　願　昭61－83842

㉒出　願　昭61(1986)4月11日

㉒発明者　下郷　昌夫　東京都港区芝5丁目33番1号　日本電気株式会社内

㉑出願人　日本電気株式会社　東京都港区芝5丁目33番1号

㉔代理人　弁理士　河原　純一

明　細　書

1．発明の名称

情報アクセス管理方式

2．特許請求の範囲

単一ないしはネットワークで結ばれた複数の電子計算機システムの主記憶装置ないしは補助記憶装置上に確保されたファイル領域に格納されている情報を参照、更新ないしは参照および更新するファイルアクセス権を管理するファイルアクセス管理システムにおいて、

前記電子計算機システムのファイルに格納されている情報を参照、更新ないしは参照および更新できる利用者の組織階層の階層位置ないしは上下位置関係を示すアクセス可能階層情報と前記情報が格納されているファイルを識別するファイル名とから構成されるアクセス権管理情報を登録する登録手段と、

この登録手段から供給される前記アクセス権管理情報を記憶するアクセス権記憶手段と、

前記電子計算機システムの利用者からのファイルに格納されている情報を参照ないしは更新するファイルアクセス要求を受け付ける要求受付け手段と、

前記電子計算機システムの利用者の利用者名と利用者の組織階層の階層位置情報とで構成される利用者組織情報を通知する組織情報通知手段と、

前記要求受付け手段から供給される前記ファイルアクセス要求の正当性を前記組織情報通知手段によって通知される前記利用者組織情報と前記アクセス権記憶手段によって記憶されている前記アクセス権管理情報とに基づいて判定する判定手段と、

この判定手段からの判定結果に基づき前記ファイルアクセス要求の許可ないしは拒否をファイルアクセスを要求した前記利用者に応答する応答手段と、

を含むことを特徴とする情報アクセス管理方式。

3．発明の詳細な説明

〔産業上の利用分野〕

本発明は情報アクセス管理方式に関し、特に単

Petitioner Apple Inc. - Exhibit 1012, p. 1287

一ないしはネットワークで結ばれた複数の電子計算機システムの主記憶装置ないしは補助記憶装置上のファイルに格納されている情報を参照、更新ないしは参照および更新するファイルアクセス権を管理するファイルアクセス管理システムにおける情報アクセス管理方式に関する。

（従来の技術）

不特定多数の利用者により利用される単一ないしはネットワークで結ばれた複数の電子計算機システムにおいては、電子計算機システム内の情報を第三者の参照ないしは更新から保護することが必要である。

従来、電子計算機システムにおいて、情報は主記憶装置ないしは補助記憶装置上に確保されたファイルと呼ばれる領域に格納され、第三者からの情報の参照ないしは更新の保護管理は情報が格納されているファイルへのアクセス権として管理され、各ファイルごとにアクセス権を持つ単一ないしはネットワークで結ばれた複数の電子計算機システムの利用者の一人ないしは複数の利用者名を指定せしめ、指定されていない利用者がファイルにアクセスすることを拒絶することにより、主記憶装置ないしは補助記憶装置上に格納されている情報を第三者の参照ないしは更新から保護している。

（発明が解決しようとする問題点）

不特定多数の利用者により利用される単一ないしはネットワークで結ばれた複数の電子計算機システムのファイル内に格納されている情報を複数の利用者間で参照ないしは更新する利用形態において、ファイルにアクセスできる利用者の範囲は、

① 範囲を限定しない、

② 特定個人に限定、

③ 複数人に限定

の3レベルに分類される。

①のレベルは、誰でもがアクセスできるレベルであるので、誰でもアクセス可能と指定せしめることにより従来技術によって実現されうる。

②のレベルは、ファイルごとにファイルをアクセスできる利用者名を設定せしめることにより従来技術によって実現されるが、情報を参照ないしは更新する利用者が少なく情報と情報を参照ないしは更新する利用者との関係が長期間固定しているような場合には余り問題にはならないが、情報を参照ないしは更新する利用者数が多いと情報が格納されているファイルに対応したファイルへのアクセス権を持つ利用者名数が非常に多くなり、また情報と情報を参照ないしは更新する利用者との関係が度々変わるような場合には、情報と情報を参照ないしは更新する利用者との関係が変わるごとに影響をうける各ファイルすべてのファイルへのアクセス権を持つ利用者名を変更しなければならないという欠点がある。

③のレベルは、複数の利用者名を指定せしめることにより従来技術でも実現されえないことはないが、利用者が多いと情報が格納されているファイルに対応したファイルへのアクセス権を持つ利用者名数が非常に多くなり、また情報と情報を参照ないしは更新する利用者との関係が度々変わるような場合には、情報と情報を参照ないしは更新する利用者との関係が変わるごとに影響をうける各ファイルすべてのファイルへのアクセス権を持つ利用者名を変更しなければならないとい欠点がある。

多数の利用者で情報を参照ないしは更新するのは、たとえば会社などの階層的組織がほとんどである。会社などの階層的組織では、組織内での階層位置ないしは階層の上下関係により情報へのアクセス権が決まり、各個人が誰であるかは問われない情報と個人のみで参照ないしは更新する情報とが大部分であり、特定の複数者のみ参照ないしは更新する情報は少ない。

本発明の目的は、上述の点に鑑み、階層的組織では組織内のかなりの情報が組織内での階層位置ないしは階層の上下関係により情報へのアクセス権が決まり各個人が誰であるかは問われない性格を持っていることに着目して、階層的組織の構成員の変動の度ごとに各情報が格納されているファイルの参照ないしは更新のためのアクセス権を変更する必要のない情報アクセス管理方式を提供す

Petitioner Apple Inc. - Exhibit 1012, p. 1288

ることにある。

〔問題点を解決するための手段〕

本発明の情報アクセス管理方式は、単一ないしはネットワークで結ばれた複数の電子計算機システムの主記憶装置ないしは補助記憶装置上に確保されたファイル領域に格納されている情報を参照、更新ないしは参照および更新するファイルアクセス権を管理するファイルアクセス管理システムにおいて、前記電子計算機システムのファイルに格納されている情報を参照、更新ないしは参照および更新できる利用者の組織階層の階層位置ないしは上下位置関係を示すアクセス可能階層情報と前記情報が格納されているファイルを識別するファイル名とから構成されるアクセス権管理情報を登録する登録手段と、この登録手段から供給される前記アクセス権管理情報を記憶するアクセス権記憶手段と、前記電子計算機システムの利用者からのファイルに格納されている情報を参照ないしは更新するファイルアクセス要求を受け付ける要求受付け手段と、前記電子計算機システムの利用者の利用者名と利用者の組織階層の階層位置情報とで構成される利用者組織情報を通知する組織情報通知手段と、前記要求受付け手段から供給される前記ファイルアクセス要求の正当性を前記組織情報通知手段によって通知される前記利用者組織情報と前記アクセス権記憶手段によって記憶されている前記アクセス権管理情報とに基づいて判定する判定手段と、この判定手段からの判定結果に基づき前記ファイルアクセス要求の許可ないしは拒否をファイルアクセスを要求した前記利用者に応答する応答手段とを含む。

〔実施例〕

次に、本発明について図面を参照して詳細に説明する。

第1図は参照すると、本発明の一実施例は、登録手段1、アクセス権記憶手段2、判定手段3、要求受付け手段4、応答手段5および組織情報通知手段6から構成されている。

第2図を参照すると、登録手段1における処理は、ファイルアクセス権情報登録要求受付けステップ21および登録情報通知ステップ22からなる。

第3図を参照すると、アクセス権記憶手段2における処理は、登録情報受付けステップ31および登録情報記憶ステップ32からなる。

第4図を参照すると、判定手段3における処理は、ファイルアクセス要求情報受付けステップ41、アクセス権情報取得ステップ42、組織情報取得ステップ43、正当性判定ステップ44、正当通知ステップ45および不当通知ステップ46からなる。

第5図を参照すると、要求受付け手段4における処理は、ファイルアクセス要求受付けステップ51およびファイルアクセス要求情報通知ステップ52からなる。

第6図を参照すると、応答手段5における処理は、判定結果取得ステップ61、判定結果比較ステップ62、要求許可通知ステップ63および要求拒否通知ステップ64からなる。

第7図を参照すると、組織情報通知手段6における処理は、取得要求受付けステップ71、組織情報取得ステップ72および組織情報通知ステップ73からなる。

第8図を参照すると、アクセス権管理情報80は、ファイルを識別するファイル名81と、そのファイルに格納されている情報を参照ないしは更新できる利用者の組織階層の階層位置ないしは上下位置関係を示すアクセス可能階層情報82とから構成されている。

第9図を参照すると、利用者組織情報90は、利用者の利用者名91と、利用者の組織階層の階層位置情報92とから構成されている。

ここで、組織の階層位置とは、会社の部とか課とか研究所のグループなどの階層的な組織の組織単位であり、上下位置関係とは、その階層の課長とか部長とかグループ長などの役職の上下関係のことである。

次に、このように構成された本実施例の情報アクセス管理方式の動作につい説明する。

まず、利用者は、情報を作成すると、作成した

Petitioner Apple Inc. - Exhibit 1012, p. 1289

情報を格納するファイルを電子計算機システムの主記憶ないしは補助記憶装置上に確保して情報を格納する。このとき、利用者は、情報を格納したファイル名８１に対応して格納情報を参照ないしは更新できる利用者の組織階層の階層位置ないしは上下位置関係を示すアクセス可能階層情報８２を指定して登録手段１を動作させる。

登録手段１は、ファイルアクセス権情報登録要求受付けステップ２１でこの登録要求を受け付け、登録情報通知ステップ２２でこの登録情報をアクセス権記憶手段２に通知する。

アクセス権記憶手段２は、この登録情報を登録情報受付けステップ３１で受け付け、登録情報記憶ステップ３２でこの登録情報であるアクセス可能階層情報８２と作成した情報を格納したファイルを識別するファイル名８１とがアクセス権管理情報として記憶されて動作が停止される。

次に、利用者は、ファイルに格納されている情報を参照ないしは更新するというファイルアクセス要求を行い、要求受付け手段４を動作させる。

要求受付け手段４は、このファイルアクセス要求をファイルアクセス要求受付けステップ５１で受け付け、ファイルアクセス要求情報通知ステップ５２で参照ないしは更新要求するファイル名と要求利用者名とで構成されるファイルアクセス要求情報を判定手段３に通知する。

判定手段３は、このファイルアクセス要求情報の通知をファイルアクセス要求情報受付けステップ４１で受け付け、アクセス権情報取得ステップ４２でこの受け付けたファイルアクセス要求情報のファイル名に対応するファイルのアクセス権記憶手段２によって記憶されたアクセス権管理情報８０が取得され、さらに組織情報取得ステップ４３でファイルアクセス要求情報の利用者名に対応する利用者の利用者組織情報９０を通知するように組織情報通知手段６に要求する。

組織情報通知手段６は、この要求を取得要求受付けステップ７１で受け付け、組織情報取得ステップ７２で要求された利用者名に対応する利用者組織情報９０を取得し、組織情報通知ステップ７３で判定手段３に通知する。

判定手段３は、この通知された利用者組織情報９０を組織情報取得ステップ４３で取得し、この利用者組織情報９０とアクセス権管理情報８０とから正当性判定ステップ４４で利用者のファイルアクセス要求の正当性が判定される。この判定結果が正当であれば、正当通知ステップ４５で正当という判定結果が応答手段５に通知される。判定結果が不当であれば、不当通知ステップ４６で不当という判定結果が応答手段５に通知される。

応答手段５は、この判定結果通知を判定結果取得ステップ６１で取得し、判定結果比較ステップ６２で取得された判定結果が正当であるか不当であるかを比較によって判定し、比較結果が正当であれば要求許可通知ステップ６３で利用者に許可が通知されて動作が停止される。比較結果が不当であれば、要求拒否通知ステップ６４で利用者に拒否が通知されて動作が停止される。

次に、判定手段３における判定処理について具体例を用いて説明する。ここでは、第１０図（ａ）で示される階層の組織において、第１０図（ｂ）で示されるアクセス可能階層情報８２が登録されているファイルに格納されている情報をアクセスする場合を例にとって説明する。

第１０図（ａ）は、組織階層の一例を示し、Ａ～Ａａａａｃｂはその組織の階層位置を示す。

第１０図（ｂ）は、ファイルに対応したアクセス可能階層情報８２の一例を示す。

第１０図（ｃ）は、第１０図（ａ）で示される組織において、第１０図（ｂ）で示されるアクセス可能階層情報が登録されているファイルにアクセスできる階層位置のリストを示す。ここで、参照可能階層位置リストのＡａａａａ，Ａａａａｂ，ＡａａａｃおよびＡａａａｄは、第１０図（ｂ）の参照アクセス可能階層情報の同階層という登録情報から、ＡａａａおよびＡａａは直上２階層までという登録情報から、ＡａａｂおよびＡａａｃは直上２階層下の直下１階層という登録情報からそれぞれ導かれる。また、更新可能階層位置リストのＡａａａは、第１０図（ｂ）の更新アクセス

Petitioner Apple Inc. - Exhibit 1012, p. 1290

可能階層情報の直上1階層という登録情報から導かれる。

例えば、Aaaaaの階層位置の利用者のファイルに格納されている情報への参照アクセス要求は、第10図(c)に示される参照可能階層位置リストに利用者のAaaaaという階層位置が含まれているので正当と判定されるが、更新アクセス要求は第10図(c)に示される更新可能階層位置リストにAaaaaという階層位置が含まれていないので不当と判定される。また、Aaaaの階層位置の利用者の参照アクセス要求は、第10図(c)に示される参照可能階層位置リストに利用者のAaaaという階層位置が含まれているので正当と判定され、更新アクセス要求も第10図(c)に示される更新可能階層位置リストにAaaaという階層位置が含まれているので正当と判定される。

しかしながら、AaaacaやAabなどの階層位置の利用者の参照アクセス要求ないしは更新アクセス要求は、第10図(c)に示される参照可能階層位置リストにも更新可能階層位置リストにもAaaacaおよびAabという階層位置は含まれていないので、両方とも不当と判定される。

〔発明の効果〕

以上説明したように本発明には、主記憶装置ないしは補助記憶装置上に確保されたファイル領域に格納されている情報を参照、更新ないしは参照および更新できる1人ないしは複数の利用者名だけでなく、組織階層の階層位置ないしは上下位置関係を各ファイルに対して登録できるようにすることにより、単一ないしはネットワークで結ばれた複数の電子計算機システムの情報を複数の利用者で参照ないしは更新する利用形態において、組織構成員が絶えず変動しても、組織階層の階層位置ないしは上下位置関係を指定されたファイルにおいては、ファイルへのアクセス権はアクセス要求者の組織階層の階層位置ないしは上下位置関係により決まり、要求者個人の利用者名には依存しないので、構成員の変動の度ごとに各情報が格納されているファイルの参照ないしは更新のためのアクセス権を変更する必要がなくなるという効果がある。

4. 図面の簡単な説明

第1図は本発明の一実施例を示す構成図、

第2図は第1図中に示した登録手段における処理を示す流れ図、

第3図は第1図中に示したアクセス権記憶手段における処理を示す流れ図、

第4図は第1図中に示した判定手段における処理を示す流れ図、

第5図は第1図中に示した要求受付け手段における処理を示す流れ図、

第6図は第1図中に示した応答手段における処理を示す流れ図、

第7図は第1図中に示した組織情報通知手段における処理を示す流れ図、

第8図はアクセス権管理情報の構成を示す図、

第9図は利用者組織情報の構成を示す図、

第10図(a)～(c)は階層組織の一例を示す図、アクセス可能階層情報を示す図およびアクセス可能階層位置のリストである。

図において、

1・・・・・登録手段、

2・・・・・アクセス権記憶手段、

3・・・・・判定手段、

4・・・・・要求受付け手段、

5・・・・・応答手段、

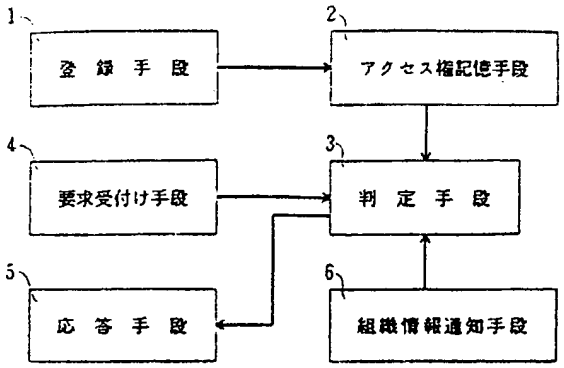
6・・・・・組織情報通知手段である。

特許出願人　日本電気株式会社

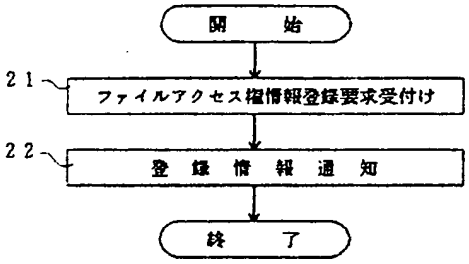
代理人　弁理士　河原純一

Petitioner Apple Inc. - Exhibit 1012, p. 1291

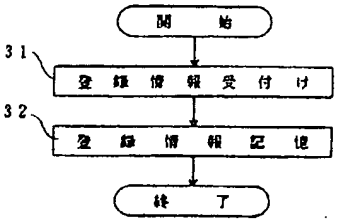
第 1 図



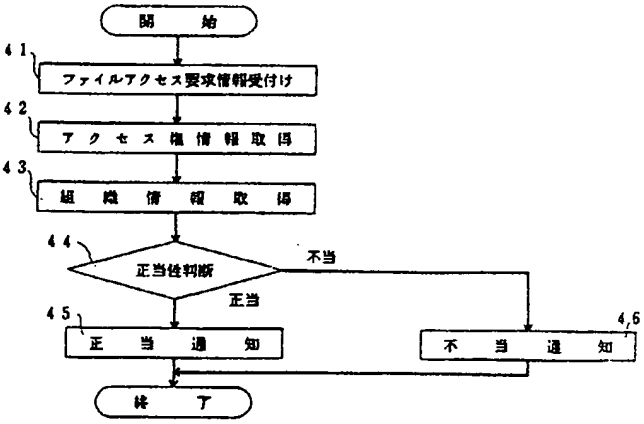
第 2 図



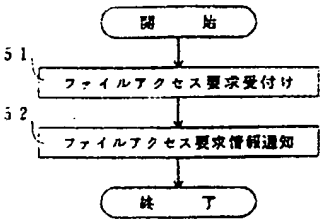
第 3 図



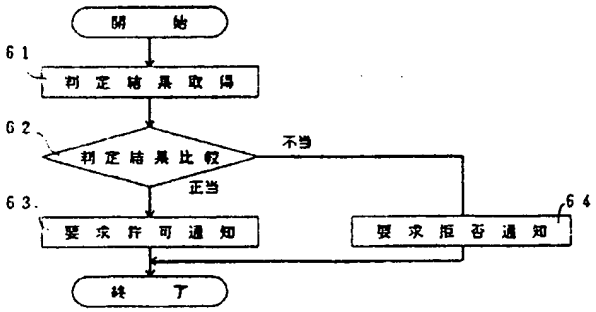
第 4 図



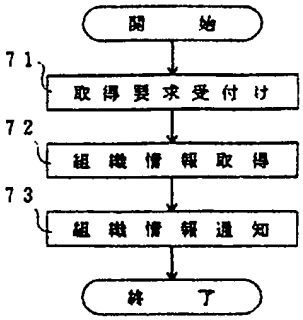
第 5 図



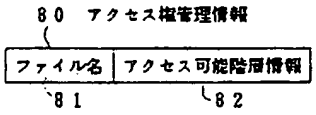
第 6 図



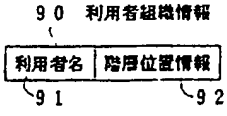
第 7 図



第 8 図

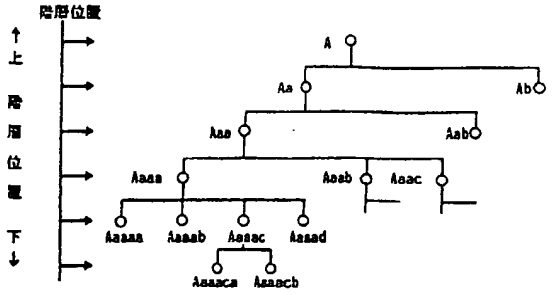


第 9 図



Petitioner Apple Inc. - Exhibit 1012, p. 1292

第 10 図 （a）



第 10 図 （b）

	登録情報
階層基準階層位置	A a a a b
参照アクセス可能階層	同階層，直上2階層まで，直上2階層下の直下1階層
更新アクセス可能階層	直上1階層

第 10 図 （c）

アクセス種別	アクセス可能階層位置リスト
参照	A a a a a，A a a a b，A a a a c，A a a a d，A a a a，A a a，A a a b，A a a c
更新	A a a a

Petitioner Apple Inc. - Exhibit 1012, p. 1293

Knowbots, Permissions Headers and Contract Law

paper for the conference on

Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment

April 2-3, 1993 with revisions of 4/30/93

Copyright 1993
Henry H. Perritt, Jr.
Professor of Law
Villanova Law School
Villanova, PA 19085
(215) 645-7078
FAX (215) 645-7033, (215) 896-1723
Internet: perritt@ucis.vill.edu

Introduction

One of the ways to protect intellectual property on the NREN is through a digital library concept. Under this concept, a work would have attached to it a "permissions header," defining the terms under which the copyright owner makes the work available. The digital library infrastructure, implemented on the NREN, would match request messages from users with the permissions headers. If the request message and the permissions header match, the user would obtain access to the work. This concept encompasses major aspects of electronic contracting, which is already in wide use employing Electronic Data Interchange ("EDI") standards developed by ANSI Committee X12.1

This paper explains the relationship between the digital library concept and EDI practice, synthesizing appropriate solutions for contract law, evidence, and agency issues that arise in electronic contracting. The question of how electronic signatures should work to be legally effective is an important part of this inquiry. The paper also defines particular types of service identifiers, header descriptors, and other forms of labeling and tagging appropriate to allow copyright owners to give different levels of permission, including outright transfer of the copyright interest, use permission, copying permission, distribution permission, display permission, and permission to prepare derivative works.The paper considers how payment authorization procedures should work in conjunction with a permissions header and digital library concept in order to integrate the proposed copyright licensing procedures with existing and anticipated electronic payment authorization systems. The paper necessarily considers whether existing standards approaches related to SGML and X12 are sufficient or whether some new standards development efforts will be necessary for implementation of the concepts. The paper considers the relationship between technology and law in enforcing intellectual property, and emphasizes that the traditional adaptation of legal requirements to levels of risk is appropriate as the law is applied to new technologies.

There are certain common issues between the intellectual property question and other applications of wide area digital network technology. The question of signatures and writings to reflect the establishment of duties and permissions and the transfer of rights is common to the intellectual property inquiry and to electronic commerce using EDI techniques. There also are common questions involving rights to use certain information channels: First Amendment privileges, and tort liability. These are common not only to technological means of protecting intellectual property but to all forms of wide area networking.

The problem

The law recognizes intellectual property because information technology permits one person to get a free ride on another person's investment in creating information value. Creative activity involving information usually is addressed by copyright, although patent has a role to play in protecting innovative means of processing information.2

Intellectual property arose in the context of letterpress printing technology. Newer technologies like xerography and more recently small computer technology and associated word processing and networking have increased the potential for free rides and accordingly increased the pressure on intellectual property.

The concern about free ride potential is especially great when people envision putting creative works on electronic publishing servers connected to wide area networks intending to permit consumers of information products to access these objects, frequently combining them and generally facilitating "publishing on demand" rather than the well known publishing just in case, typified by guessing how many copies of a work will sell, printing those in advance, and then putting them in inventory until someone wants them.

The concern is that it will be too easy to copy an entire work without detection and without paying for it. Worse, it will be easy to copy an entire work and resell it either by itself or as a part of a new derivative work or collection.

But technology is capable of protecting investment in new ways as well as gaining a free ride. Computer networks make it possible to restrict access and to determine when access occurs. Depending on how new networks are designed, they may actually reduce the potential for a free ride. The digital library is one way of realizing that potential. Professor Pamela Samuelson has observed that the digital library model replaces intellectual property with a system of technological controls.3

Digital Library Concepts

Basic Concepts

A digital library is a set of information resources ("information objects") distributed throughout an electronic network. The objects reside on servers (computers with associated disk drives connected to the network). They can be retrieved remotely by users using "client" workstations.

Origin of Concepts

The phrase "digital library" and the basic concept was first articulated in a 1989 report growing out of a workshop sponsored by the Corporation for National Research Initiatives.4 From its inception, the digital library concept envisioned retrieval of complete information resources and not merely bibliographic information.5

The technologies of remote retrieval of complete information objects using electronic technologies is in wide use through the WESTLAW, Dialog, LEXIS, NEXIS, and National Library of Medicine databases. These remotely accessible databases, however, unlike the digital library involved a single host on which most of the data resides. The digital library concept envisions a multiplicity of hosts (servers).

Recent Developments

The remotely accessible database host concept is converging with the digital library concept as more of the electronic database vendors provide gateways to information objects actually residing on other computers. This now is commonplace with WESTLAW access to Dialog, and Dialog's gateways to other information providers.

The most explicit implementation of the digital library concept is the Wide Area Information Service ("WAIS"), which implements ANSI standard Z.39.6 WAIS permits a remote user to formulate a query that is applied to a multiplicity of WAIS servers each of which may contain information responsive to the query. The WAIS architecture permits search engines of varying degrees of sophistication, resident on WAIS information servers to apply the query against their own information objects, reporting matches back to the user.7 Future implementations of WAIS permit automatic refinement of searches according to statistical matching techniques.

The Corporation for National Research Initiatives has proposed a test bed for an electronic copyright management system.8 The proposed system would include four major elements: automated copyright recording and registration, automated, on line clearance of rights, private electronic mail and digital signatures to provide security. It would include three subsystems: a Registration and Recording System (RRS), a Digital Library System (DLS), and a Rights Management System (RMS). The RRS would provide the functions enumerated above and would be operated by the Library of Congress. It would provide "change of title" information.9 The RMS would be an interactive distributed system capable of granting rights on line and permitting the use of copyrighted material in the Digital Library System. The test bed architecture would involve computers connected to the Internet performing the RRS and RMS functions.

Digital signatures would link an electronic bibliographic record with the contents of the work, ensuring against alteration after deposit.10 Multiple RMS servers would be attached to the Internet. A user wishing to obtain rights to an electronically published work would interact electronically with the appropriate RMS. When copyright ownership is transferred, a message could be sent from the RMS to the RRS11 - creating an electronic marketplace for copyrighted material.

The EBR submitted with a new work would "identify the

rights holder and any terms and conditions on the use of the document or a pointer to a designated contact for rights and permissions."12 The EBR, thus, is apparently equivalent to the permissions header discussed in this paper. Security in the transfer of rights would be provided by digital signatures using public key encryption, discussed further, infra in the section on encryption.

Basic Architectural Concepts

The digital library concept in general contemplates three basic architectural elements: a query, also called a "knowbot" in some descriptions; a permissions header attached to each information object; and a procedure for matching the query with the permissions header.

Two kinds of information are involved in all three architectural elements: information about the content of information objects desired and existing, and information about the economic terms on which an information object is made available. For example, a query desiring court opinions involving the enforcement of foreign judgments evidencing a desire to download the full text of such judicial opinions and to pay up to $1.00 per minute of search and downloading time would require that the knowbot appropriately represent the subject matter "enforcement of foreign judgments." It also requires that the knowbot appropriately represent the terms on which the user is willing to deal: downloading and the maximum price. The permissions header similarly must express the same two kinds of information. If the information object to which the permissions header is attached is a short story rather than a judicial opinion, the permissions header must so indicate. Or, if the information object is a judicial opinion and it is about enforcement of foreign judgments, the permission header may indicate that only a summary is available for downloading at a price of $10.00 per minute. The searching, matching, and retrieval procedure in the digital library system must be capable of determining whether there is a match on both subject matter and economic terms, also copying and transmitting the information object if there is a match.

Comparison to EDI

Electronic Data Interchange ("EDI") is a practice involving computer-to-computer commercial dealing without human intervention. In the most widespread implementations, computers are programmed to issue purchase orders to trading partners, and the receiving computer is programmed to evaluate the terms of the purchase order and to take appropriate action, either accepting it and causing goods to be manufactured or shipped or rejecting it and sending an appropriate message. EDI is in wide use in American and foreign commerce, using industry-specific standards for discrete commercial documents like purchase orders, invoices, and payment orders, developed through the American National Standards Institute.

There obviously are similarities between the three architectural elements of the digital library concept and EDI. There is a structured way of expressing an offer or instruction, and a process for determining whether there is a match between what the recipient is willing to do and what the sender requests.

There is also, however, an important difference. In the digital library concept, a match results in actual delivery

of the desired goods and services in electronic form. In EDI practice, the performance of the contractual arrangement usually involves physical goods or performance of nonelectronic services.

Nevertheless, the digital library and EDI architectures are sufficiently similar and, it turns out the legal issues associated with both are sufficiently similar to make analogies appropriate.

Elements of Data Structure

For purposes of this paper, the interesting parts of the data structure are those elements that pertain to permission, more than those elements that pertain to content of the information object to which the header is attached. Accordingly, this section will focus on only permissions-related elements, after noting in passing that the content part of the header well might be a pointer to an inverted file to permit full text searching and matching.

The starting point conceptually for identifying the elements of the permissions header are the rights exclusively reserved to the copyright owner by 106 of the copyright statute. But these exclusive rights need not be tracked directly because the owner of an information object free to impose contractual restrictions as well as to enjoy rights granted by the Copyright Act. Accordingly, it seems that the following kinds of privileges in the requester should be addressed in the permissions header:

outright transfer of all rights

use privilege, either unrestricted or subject to restrictions

copying, either unlimited or subject to restrictions like quantitative limits

distribution, either unlimited or subject to restrictions, like geographic ones or limits on the markets to which distribution can occur

preparation of derivative works

Display and presentation rights, separately identified in 106 would be subsumed into the use element, because they are particular uses.

The simplest implementation would allow only binary values for each of these elements. But a binary approach does not permit the permissions header to express restrictions, like those suggested in the enumerated list. Elements could be defined to accept the most common kinds of restrictions on use, and quantitative limits on copying, but it would be much more difficult to define in advance the kinds of geographic or market-definition restrictions that an owner might wish to impose with respect to distribution.

In addition to these discrete privileges, the permissions header must express pricing information. The most sensible way of doing this is to have a price associated with each type of privilege. In the event that different levels of use, copying, or distribution privilege are identified, the data structure should allow a price to

be associated with each level.

A complicating factor in defining elements for price is the likelihood that different suppliers would want to price differently. For example, some would prefer to impose a flat fee for the grant of a particular privilege. Others might wish to impose a volume-based fee, and still others might wish to impose a usage or connect-time based fee. The data structure for pricing terms must be flexible enough to accommodate at least these three different approaches to pricing.

Finally, the data structure must allow for a specification of acceptable payment terms and have some kind of trigger for a payment approval procedure. For example, the permissions header might require presentation of a credit card number and then trigger a process that would communicate with the appropriate credit card database to obtain authorization. Only if the authorization was obtained would the knowbot and the permissions header "match."

There is a relationship between the data structures and legal concepts. The knowbot is a solicitation of offers. The permissions header is an offer. The matching of the two constitutes an acceptance. Mr. Linn's "envelope" could be the "contract."

There are certain aspects of the data structure design that are not obvious. One is how to link price with specific levels of permission. Another is how to describe particular levels of permission. This representation problem may benefit from the use of some deontic logic, possibly in the form of a grammar developed for intellectual property permissions. Finally, it is not clear what the acceptance should look like. Conceptually, the acceptance occurs when the knowbot matches with a permissions header, but it is unclear how this legally significant event should be represented.

Role of Encryption

The CNRI test bed proposal envisions the use of public key encryption to ensure the integrity of digital signatures and to ensure the authenticity of information objects. Public key encryption permits a person to encrypt a message - like a signature using a secret key, one known only to the sender, while permitting anyone with access to a public key to decrypt it. Use of public key cryptography in this fashion permits any user to authenticate a message, ensuring that it came from the purported sender.13 A related technology called "hashing" permits an encrypted digital signature to be linked to the content of a message. The message can be sent in plain text (unencrypted) form, but if any part of it is changed, it will not match the digital signature. The digital signature and hashing technologies thus permit not only the origin but also the content integrity of a message of arbitrary length to be authenticated without necessitating encryption of the content of the message. This technology has the advantage, among others, that it is usable by someone lacking technological access to public key encryption. An unsophisticated user not wishing to incur the costs of signature verification nevertheless can use the content of the signed information object.

It is well recognized that encryption provides higher levels of security than other approaches. But security through encryption comes at a price. Private key encryption systems require preestablished relationships and exchange of private keys in advance of any encrypted communication. The burdens of this approach have led most proponents of electronic commerce to explore public key encryption instead. But public key systems require the establishment and policing of a new set of institutions. An important infrastructure requirement for practicable public key cryptography is the establishment and maintenance of certifying entities that maintain the public keys and ensure that they are genuine ones rather than bogus ones inserted by forgers. A rough analogy can be drawn between the public key certifying entities and notaries public. Both kinds of institutions verify the authenticity of signature. Both kinds require some level of licensing by governmental entities. Otherwise the word of the "electronic notary" (certifying entity) is no better than an uncertified, unencrypted signature. In a political and legal environment in which the limitations of regulatory programs have been recognized and have led to deregulation of major industries, it is not clear that a major new regulatory arrangement for public key encryption is practicable. Nevertheless, experimentation with the concept in support of digital library demonstration programs can help generate more empirical data as to the cost and benefits of public key encryption to reinforce electronic signatures.

On the other hand, it is not desirable to pursue approaches requiring encryption of content. No need to encrypt the contents is apparent in a network environment. Database access controls are sufficient to prevent access to the content if the permissions header terms are not matched by the knowbot. On the other hand, if the electronic publishing is effected through CDROMs or other physical media possessed by a user, then encryption might be appropriate to prevent the user from avoiding the permissions header and going directly to the content.

While encrypted content affords greater security to the owner of copyrighted material. Someone who has not paid the price to the copyright owner must incur much higher cost to steal the material. But the problem is everyone must pay a higher price to use the material. One of the dramatic lessons of the desktop computer revolution was the clear rejection of copyright protection in personal computer software. The reasons that copy protection did not survive in the market place militate against embracing encryption for content. Encryption interferes with realization of electronic markets, because producer and consumer must have the same encryption and description protocols. Encryption burdens processing of electronic information objects because it adds another layer. Some specific implementations have encryption require additional hardware at appreciable costs.

Digital libraries cannot become a reality until consumers perceive that the benefits of electronic formats outweigh the costs, compared to paper formats. Encryption interferes with electronic formats' traditional advantages of density, reusability, editability, and computer search ability and also, by impairing open architectures may perpetuate some of papers' advantages with respect with browsibility.14

The need for encryption of any kind depends upon whether security is available without it. That depends, in turn, on the kinds of free rides that may be obtainable and the legal status of various kinds of electronics transactions in the digital library system.

Legal Issues

Copyright: What legal effect is intended?

The design of the permissions header and the values in the elements of the header must be unambiguous as to whether an outright transfer of a copyright interest is intended or whether only a license is intended. If an outright transfer[15] is intended, then the present copyright statute requires a writing signed by the owner of the rights conveyed.[16] Recordation of the transfer with the Copyright office is not required, but provides advantages in enforcing transferee rights.[17] On the other hand, non exclusive licenses need not be in writing nor registered. If the electronic transaction transfers the copyright in its entirety, then the rights of the transferor are extinguished, and the rights of the transferee are determined by the copyright statute. The only significant legal question is whether the conveyance was effective.

On the other hand, when the copyright is not transferred outright but only certain permissions are granted or certain rights conveyed, the legal questions become more varied. Then, the rights of the transferor and the obligations of the transferee are matters of contract law. It is important to understand the degree to which the contract is enforceable and how it is to be interpreted in the event of subsequent disputes. The following sections consider briefly the first sale doctrine as a potential public policy obstacle to enforcing contractual restrictions different from those imposed by the copyright statute and then explore in greater depth whether electronic techniques satisfy the formalities traditionally required for making a contract, whether they adequately ensure against repudiation, and whether they provide sufficient information to permit predictable interpretation of contractual obligations and privileges.

First Sale Doctrine

The first sale doctrine may invalidate restrictions on use. It is impermissible for the holder of a patent to impose restrictions on the use of a patented product after the product has been sold. Restrictions may be imposed, however, on persons who merely license the product.[18] The rationale for this limit on the power of the owner of the intellectual property interest is that to allow limitations on use of the product would interfere with competition beyond what the Congress - and arguably the drafters of the Constitution - intended in setting up the patent system.

The first sale doctrine applies to copyright owners.[19] Indeed, because of the First Amendment's protection of informational activity, the argument against restrictions after the first sale may be even stronger in the copyright arena then in the patent arena.

The first sale doctrine is potentially important because it may invalidate restrictions imposed on the use of information beyond what is authorized by the Copyright Act and by common law trade secret. Thus, there may be serious

questions about the legal efficacy of use restrictions suggested in ___, although such restrictions are common in remote database service agreements. The vendors could argue that the limitations pertain to the contractual terms for delivery of a service rather than use of information as such. The characterization avoids the overlap with copyright and thus may also avoid the conflict between federal policy and contract enforcement.20

Contract Formation Issues

The law does not enforce every promise. Instead, it focuses its power only on promises surrounded with certain formalities to make it likely that the person making the promise (the "promisor") and the person receiving the promise (the "promisee") understood that their communication had legal consequences. A threshold question for the digital library system is whether the traditional formalities for making a contract are present when the contract is made through electronic means. The digital library system considered in this paper clearly contemplates that a contract is formed when the knowbot and the permissions header achieve a match. In this respect, the digital library concept converges with EDI where trading parties contemplate that a contract to perform services or deliver goods is formed when a match occurs either upon the receipt of a purchase order or upon the transmission of a purchase order acknowledgment.

It is not altogether clear, however, whether the match between values and computer data structures meets contract formation requirements, particularly those expressed in various statutes of frauds. Statutes of frauds require "writings" and "signatures" for certain kinds of contracts - basically those contemplating performance extending beyond a period of one year.21

In many instances, the digital library contract will be fully performed almost instantaneously upon delivery of the information object after the knowbot and the permissions header match. In such a case, the statute of frauds is not a problem and its requirements need not be satisfied. In other cases, however, as when the intent of the owner of the information object is to grant a license to do things that will extend beyond one year, the statute of frauds writing and signature requirements must be met.

Historical application of Statutes Of Frauds by the courts clearly indicates that there is flexibility in the meaning of "writing" and "signature." A signature is any mark made with the intent that it be a signature.22 Thus an illiterate person signs by making an "X," and the signature is legally effective. Another person may sign a document by using a signature stamp. Someone else may authorize an agent to sign his name or to use the signature stamp. In all three cases the signature is legally effective. There may of course be arguments about who made the X, or whether the person applying the signature stamp was the signer or his authorized agent, but these are evidentiary and agency questions, not arguments about hard and fast contract-law requirements.

Under the generally accepted legal definition of a signature, there is no legal reason why the "mark" may not be made by a computer printer, or for that matter by the write head on a computer disk drive or the data bus in a

computer random access memory. The authorization to the computer agent to make the mark may be given by entering a PIN ("Personal Identification Number") on a keyboard. To extend the logic, there is no conceptual reason to doubt the legal efficacy of authority to make a mark if the signer writes a computer program authorizing the application of a PIN upon the existence of certain conditions that can be tested by the program. The resulting authority is analogous to a signature pen that can be operated only with a mechanical key attached to somebody's key ring, coupled with instructions to the possessor of the key.

Which of these various methods should be selected for particular types of transactions must depend, not on what the law requires, because the law permits any of these methods. Rather, it must depend on the underlying purposes of the legal requirement and which method best serves those purposes.

The real issue is how to prove that a particular party made the mark. In other words, the contingency to be concerned about is repudiation, not absence of formalities. Repudiation should be dealt with through usual evidentiary and fact finding processes rather than artificial distinctions between signed and unsigned documents.

Authority is skimpier on how flexible the "writing" requirement is. The best approach is to borrow the fixation idea from the copyright statute and conclude that a writing is "embodiment in a copy . . . sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for more a period of more than transitory duration."23

The most important thing conceptually is to understand the purpose of the writing and signature requirements. They have two purposes: awareness or formality and reliability of evidence. Signature requirements, like requirements for writings and for original documents have an essentially evidentiary purpose. If there is a dispute later, they specify what kind of evidence is probative of certain disputed issues, like "who made this statement and for what purpose?" The legal requirements set a threshold of probativeness. Surely the values in a knowbot as well as the values in a permissions header constitute and "mark," and someone who knowingly sets up potential transactions in a digital library scheme can have the intent that the mark be a signature.

When a contract is made through a signed writing, it is more likely that the parties to the contract understand what they are doing. They are aware of the legal affect of their conduct because the writing in the signature involve a greater degree of formality than a simple conversation.

The awareness/formality purpose can be served by computerized contracting systems. This is so not so much because the computers are "aware" of the affect of their "conduct." Rather, it is true because the computers are agents of human principals. The programming of the computer to accept certain contract terms is the granting of authority to the computer agent to enter into a contract. The fact that a principal acts through an agent engaging in conduct at a later point and time never has been thought to defeat contract formation in the traditional evolution of

agency and contract law. Nor should it when the agent is a computer.

Fulfillment of the evidentiary purpose depends on the reliability of the information retained by the computer systems making up the digital library. Such systems must be designed to permit the proponent of contract formation to establish the following propositions if the other party to the purported contract attempts to repudiate it.

1. It came from computer X

2. It accurately represents what is in computer X24 now25

3. What is in computer X now is what was in computer X at the time of the transaction

4. What was in computer X at the time of the transaction is what was received from the telecommunications channel26

5. What was received from the telecommunications channel is what was (a) sent, (b) by computer Y.

Two other questions relate to matters other than the authenticity of the message:

6 Computer Y was the agent of B

7 The message content expresses the content of the contract (or more narrowly, the offer or the acceptance).27

Factual propositions 1-4 can be established by testimony as to how information is written to and from telecommunications channel processors, primary storage, and secondary storage. Factual proposition 5 requires testimony as to the accuracy of the telecommunications channel and characteristics of the message that associate it with computer Y. Only the last proposition (number 5) relates to signatures, because signature requirements associate the message with its source.28 The other propositions necessitate testimony as to how the basic message and database management system works. It is instructive to compare these propositions with the kinds of propositions that must be established under the business records exception to the hearsay rule when it is applied to computer information.

Those propositions may be supported with non technical evidence, presented by non programmers. A witness can lay a foundation for admission of computer records simply by testifying that the records are generated automatically and routinely in the ordinary course of business. The more inflexible the routine, and the less human intervention in the details of the computer's management of the database the better the evidence.29

The ultimate question is trustworthiness, and if the computer methods are apparently reliable, the information should be admitted unless the opponent of admissibility can raise some reasonable factual question undercutting trustworthiness.30

Contract Interpretation Issues

Assuming that the permissions header and knowbot

constitute sufficient writings to permit a contract to be formed and that the signature requirement also is met, through digital signature technology or otherwise, there still are difficult contract interpretation questions. Contract interpretation questions arise not only after contractual relationships are formed, but also in connection with deciding whether there has been offer and acceptance, the prerequisites to contract formation.31 Contract interpretation always seeks to draw inferences about what the parties intended. When contract interpretation issues arise at the contract formation stage, the questions are what the offeror intended the content of the offer to be and what the offeree intended the content of the purported acceptance to be. The proposed Digital Library System envisions extremely cryptic expressions of offer and acceptance - by means of codes. The codes have no intrinsic meaning. Rather, extrinsic reference must be made to some kind of table, standard, or convention associating particular codes with the concepts they represent. Extrinsic evidence is available to resolve contract interpretation questions when the language of the contract itself is ambiguous, and perhaps at other times as well.32 The codes in the permissions header and knowbots certainly are ambiguous and become unambiguous only when extrinsic evidence is considered. So there is no problem in getting a standard or cable into evidence. The problem is whether the parties meant to assent to this standard.

In current EDI practice, this question is resolved by having parties who expect to have EDI transactions with each other to sign a paper trading partner agreement, in which the meaning of values or codes in the transaction sets is established.33 But requiring each pair of suppliers and users of information in a digital library to have written contracts with each other in advance would defeat much of the utility of the digital library. Thus the challenge is to establish some ground rules for the meaning of permissions header and knowbot values that all participants are bound by. There are analogous situations. One is a standard credit card agreement that establishes contractual terms among credit card issuer, credit card subscriber, and merchant who accepts the credit card. The intermediary - the credit card company - unilaterally establishes contract terms to which the trading partners assent by using and accepting the credit card.34 Also, it is widely recognized that members of a private association can, through their constitution and bylaws establish contractual relationships that bind all of the members in dealing with each other.35 In the Digital Library System, similar legal arrangements can establish the standards by which electronic transactions between permissions header and knowbots will bind transferor and transferee of information.

Third Party Liability

It is not enough merely to ensure that the licensee is contractually bound. Trading partners also must ensure that the participants in funds transfers have enforceable obligations. For example, if the digital library system envisions that the information object would not be released to the purchaser without simultaneous release of a payment order, the supplier may be interested in enforcing the obligations of financial intermediaries who handle the payment order. This implicates the federal Electronic Funds Transfer Act, and Article 4A of the Uniform Commercial Code, regulating wire transfers.

Solutions

Satisfy the Business Records Exception to the Hearsay Rule

The discussion of contract formalities earlier in this paper concluded that legally enforceable contracts can be formed through electronic means and that the significant legal questions relate to reliability of proof and intent of the parties to be bound by using the electronic techniques. This section considers the reliability of proof further. Traditional evidence law permits computer records to be introduced in evidence when they satisfy the requirements of the business records exception: basically that they are made in the ordinary course of business, that they are relied on for the performance of regular business activities, and that there is no independent reason for questioning their reliability.36

The business records exception shares with the authentication concept statute of frauds and the parol evidence rule a common concern with reliability.37 The same procedural guarantees and established practices that ensure reliability for hearsay purposes also ensure reliability for the other purposes. Under the business records exception, the proponent must identify the source of a record, through testimony by one familiar with a signature on the record, or circumstantially.38 The steps in qualifying a business record under the common law, which since have been relaxed,39 were:

Proving that the record is an original entry made in the routine course of business

Proving that the entries were made upon the personal knowledge of the proponent/witness or someone reporting to him

Proving that the entries were made at or near the time of the transaction

Proving that the recorder and his informant are unavailable.40

These specific requirements are easier to understand and to adapt to electronic permissions and obligations formed in a digital library system by understanding the rationale for the business records exception. The hearsay rule excludes out of court statements because they are inherently unreliable, primarily because the maker of the statement's demeanor cannot be observed by the jury and because the maker of the statement is not subject to cross examine. On the other hand, there are some out of court statements that have other guarantees of reliability. Business records are one example. If a continuing enterprise finds the records sufficiently reliable to use them in the ordinary course of business, they should be reliable enough for a court. The criteria for the business records exception all aim at ensuring that the records really are relied upon the business to conduct its ordinary affairs.

The Manual for Multidistrict Litigation suggests steps for qualifying computer information under the business records exception:

1.The document is a business record

2.The document has probative value

3.The computer equipment used is reliable

4.Reliable data processing techniques were used41

The key in adapting the business records exception to electronic permissions in a digital library system are points 3 and 4. Establishing these propositions and the propositions set forth in section ___ of this paper requires expert testimony. Any designer of a digital library system must consult with counsel and understand what testimony an expert would give to establish these propositions. Going through that exercise will influence system design.

Reinforce the Evidentiary Reliability by Using Trusted Third Parties

The evidentiary purpose of contract formation requirements can be satisfied by using a trusted third party as an intermediary, when the third party maintains archival records of the transactions. The third party lacks any incentive for tampering with the records and when the third parties archiving system is properly designed, it can provide evidence sufficient to establish all of the propositions identified in ___.

This third party intermediary concept is somewhat different from the concept for a certifying agent in digital signature systems. To be sure, the custodian of transaction records envisioned by this section could be the same as the certifying entity for public and key encryption, but the custodian role can be played in the absence of any encryption. Indeed, the digital library itself is a good candidate for the custodian role. The library has no incentive to manipulate its records in favor of either of the producers of information value or the consumers. In order to carry out its affairs, it must use these transactional records in the ordinary course of business, thereby making it likely that digital library records would qualify under the business records exception.

Standardization

Obviously, the digital library concept depends upon the possibility of an automated comparison between the knowbot and the permissions header. This means that potential requesters of information and suppliers of information must know in advance the data structures for representing the elements of the permissions header and the knowbot. This requires compatibility. Compatibility requires standardization. Standardization does not, however, necessarily require "Standard" in the sense that they are developed by some bureaucratic body like ANSI. It may simply imply market acceptance of a particular vendor's approach. Indeed, each digital library might use different data structures. All that is necessary is that the structure of the knowbot and the structure of the permissions header be compatible within any one digital library system. Also, as demands emerge for separate digital libraries to communicate with each other, there can be proprietary translation to assure compatibility between systems much as common word processing programs translate to and from other common formats and much as printers and word processing software communicate with each other through appropriate printer drivers. In neither of these cases has any independent

standards organization developed a standard that is at all relevant in the marketplace.

Standardizing the elements of Knowbot and permissions headers involves content standardization, which generally is more challenging than format standardization.42 A permissions header/Knowbot standard is a system for representing legal concepts and for defining legal relations. As such, the standard is basically a grammar for a rule based substantive system in a very narrow domain.43 The data elements must correspond to legally meaningful relational attributes. The allowable values must correspond to legally allowable rights, obligations, privileges and powers. In other words, the standard setter must meet many of the challenges that a legal expert system designer working with Hohfeldian frameworks must meet.44 This adds a constraint to the standards setting process. Unlike setting format standards, where the participants are free to agree on an arbitrary way of expressing format attributes, participants in setting a content standard must remain within the universe of permissible content. The set of permissible values is determined by the law rather than being determined only by the imagination of format creators.

Enforcement and Bottlenecks

One of the many profound observations by Ithiel de Sola Pool was that copyright always has depended upon technological bottlenecks for its enforceability. The printing press was the original enforcement bottleneck. Now, a combination of the printing press and the practical need to inventory physical artifacts representing the work constitute the enforcement bottlenecks. As technologies change, old bottlenecks disappear and enforceability requires a search for new bottlenecks. When there are single hosts, like Westlaw, Dialog, Lexis, and CompuServe, access to that host is the bottleneck. The problem with distributed publishing on an open architecture internet is that there is no bottleneck in the middle of the distribution chain corresponding to the printer, the warehouse or the single host.

If new bottlenecks are to be found, they almost surely will be found at the origin and at the point of consumption. Encryption and decryption techniques discussed elsewhere in this volume concentrate on those bottlenecks as points of control. It also is possible that rendering software could become the new bottleneck as Mr. Linn suggests.

Even with those approaches, however, a serious problem remains in that the new technologies make it difficult or impossible to distinguish between mere use and copying. Thus the seller cannot distinguish between an end user45 and a potential competitor. On the other hand, the new technologies permit a much better audit trail, potentially producing better evidence for enforcement adjudication.

If network architectures for electronic publishing evolve in the way that Ted Nelson suggests with his Xanadu concept, the real value will be in the network and the pointers, not in the raw content. Thus, the creative and productive effort that the law should reward is the creation and productive effort that the law should reward is the creation and production and delivery of pointers, presentation, distribution, and duplication value. If this

is so, then technological means will be particularly important, foreclosing access by those lacking passwords and other keys and limiting through contract what a consumer may do with the information.

In such an architecture, the law either will be relatively unimportant because technology can be counted on to prevent free riding or, the law will need to focus not on prohibiting copying or use without permission, but on preventing circumvention of the technological protections. Thus, legal approaches like that used to prevent the sale of decryption devices for television broadcasts and legal issues associated with contract enforcement may be more important than traditional intellectual property categories.

Weighing Risks and Costs

The law generally imposes sensible levels of transaction costs. Usually, transaction costs are proportional to the risk. Figure 1 shows a continuum of risk and transaction cost in traditional and new technologies. A real estate closing involves significant risks if there is some dispute later about the transaction. Therefore, the law affords much protection, including a constitutional officer called a registrar of deeds who is the custodian of records associated with the transaction. The risk level analogous to this in electronic publishing might be access to an entire library including access software as well as contents. Next, is a transaction involving a will or power of attorney. There, the risk is substantial because the maker of the instrument is not around to help interpret it. The law requires relatively high levels of assurance here, though not as great as those for real estate transactions. The law requires witnesses and attestation by a commissioned minor official called a notary public. The electronic publishing analogy of this level of risk might be the contents of an entire CDROM.

Next, in level of risk is the purchase of a large consumer durable like an automobile. The law requires somewhat less, but still significant protections for this kind of transaction: providing for the filing and enforcement of financing statements under the Uniform Commercial Code. The electronic publishing analogy might be the transfer of copyright to a complete work. Next, down the risk continuum, is the purchase of a smaller consumer durable like a television set. Here, the law typically is reflected in written agreements of sale, but no special third party custodial mechanisms. The electronic publishing analogy might be use permission for a complete work.

Finally, is the purchase of a relatively small consumer item, say a box of diskettes. Neither the law or commercial practice involves much more than the exchange of the product for payment, with no written agreement or anything else to perform channeling, cautionary, evidentiary, or protective functions [make sure these function and the citation appears earlier]. The electronic publishing analogy might be use permission for part of a work.

Cost effectiveness = risk-proportional security

traditional transaction institutions electronic equivalent

real estate closing library - software and	registrar of deeds	entire contents
will/power of attorney entire CDROM	witnesses, notary public	contents of
auto purchase work - transfer of	UCC financing statement	complete copyright
television set purchase work - use permission	written sale agreement	complete
box of diskettes work - use	-	part of a permission

An encrypted object combined with rendering software is probably inconsistent with an open architecture. Because of the difficulty of setting standards for such technologies, this approach to intellectual property protection probably would be effectuated by proprietary approaches thus frustrating the vision of an open market for electronic publishing.

Conclusion

Realization of the digital library vision requires a method for collecting money and granting permission to use works protected by intellectual property. The concept of a knowbot and a permissions header attached to the work is the right way to think about such a billing and collection system. Standards for the data structures involved must be agreed to, and systems must be designed to satisfy legal formalities aimed at ensuring awareness of the legal significance of transactions and reliable proof of the terms of the transactions.

In the long run, not only must these technological issues be resolved, with appropriate attention to levels of risk and protections available under traditional legal doctrines, but also further conceptual development must be undertaken. Proponents of electronic publishing over wide area networks need to think about the appropriate metaphors: whether it is a library or a bookstore, if a library whether with or without xerox machines, if a bookstore whether it is a retail bookstore, or a mail order operation. Then, thought must be given to how standards will be set. Finally, and most important, much more needs to be understood about the need for third party institutions. There is a good deal of enthusiasm for public key encryption. Yet the vulnerability of public key encryption systems is in the integrity of the key authority. In traditional legal protections, the third party custodians or authenticating agents like notary public and registrars of deeds receive state sanction and approval, and in the case of registrars of deeds, public funding. We must be clearer as to whether a similar infrastructure must be developed to protect against substantial risks and the use of EDI and electronic publishing technologies.

Finally, and perhaps most importantly, we must be thoughtful about what legal obligations, imposed on whom,

are appropriate? The suggested 102(e) and (f) in the High Performance Computing Act looks very much like King James I's licensing of printing presses. It also looks like the FBI's proposal to prohibit the introduction of new technologies until certain conformity with past legal concepts is assured. Such approaches make the law a hurdle to new technology -- an uncomfortable position for both law and technology.

---

1 The use of EDI techniques to meter usage and determine charges for use of intellectual property is an example of billing and collection value in a typology of different types of value that can be produced in electronic marketplaces for information. See Henry H. Perritt, Jr., Market Structures for Electronic Publishing and Electronic Contracting in Brian Kahin, ed., Building Information Infrastructure: Issues in the Development of the National Research and Education Network (Harvard University and McGraw-Hill 1992) (developing typology for different types of value and explaining how market structures differ for the different types); Henry H. Perritt, Jr., Tort Liability, the First Amendment, and Equal Access to Electronic Networks, 5 Harv.J.Law & Tech. 65 (1992) (using typology of ten types of value to analyze access by competing producers of value).

2 See, e.g.U.S.Pat. No. 5,016,009, Data compression apparatus and method (May 14, 1991); U.S. Pat. No. 4,996,690, Write operator with gating capability (Feb. 26, 1991);U.S. Pat. No. 4,701,745, Data compression system (Oct. 20, 1987); Multi Tech Systems, Inc. v. Hayes Microcomputer Products, Inc., 800 F. Supp. 825 (D. Minn. 1992) (denying summary judgment on claim that patent for modem escape sequence is invalid)..

3 Comments on the 8\21 draft of "Knowbots in the Real World" from the intellectual property workshop participants at page 6 (author unknown, source unknown). Professor Samuelson also observed that the workshop, despite its title, actually did not focus much on intellectual property issues.

4 Corporation for National Research Initiatives, Workshop On The Protection Of Intellectual Property Rights In A Digital Library System: Knowbots in the Real World-May 18-19, 1989 (describing digital library system).

5 See generally Clifford A. Lynch, Visions of Electronic Libraries (libraries of future can follow acquisition-on-demand model rather than acquiring an advance of use; Z39.50 protocol will facilitate realization of that possibility, citing Robert E. Kahn & Vinton G. Serf, An Open Architecture for a Digital Library System and a Plan for Its Development. The Digital Library Project, volume 1: The World of Knowbots (draft) (Washington D.C.: Corporation for National Research Initiatives; 1988)).

6 Clifford A. Lynch, The Z39.50 Information Retrieval Protocol: An Overview and Status Report, ACM Sigcomm Computer Communication Review at 58 (describing Z39.50 as an OSI application layer protocol that relieves clients from having to known the structure of data objects to be queried, and specifies a framework for transmitting and managing queries and results and syntax for formulating queries).

7 Brewster Kahle, Wide Area Information Server Concepts (Nov. 3, 1989 working copy; updates available from Brewster @THINK. (describing WAIS as "open protocol for connecting user interfaces on workstations and server computers") (describing information servers as including bulletin board services, shared databases, text searching and automatic indexing and computers containing current newspapers and periodicals, movie and television schedules with reviews, bulletin boards and chat lines, library catalogues, Usenet articles).

8 Robert E. Kahn, Deposit, Registration, Recordation in an Electronic Copyright Management System (August 1992) (Corporation for National Research Initiatives, Reston, Virginia).

9 Kahn 1992 at 4.

10 Kahn 1992 at 6.

11 Kahn 1992 at 10.

12 Kahn 1992 at 12.

13 Kahn 1992 at 15.

14 Browsability through techniques like the collapsible outliner function in Microsoft Word for Windows and competing products require more chunking and tagging value in the form of style and text element codes. Handling this additional formatting information through encryption and description processes is problematic.

15 " A 'transfer of copyright ownership' is an assignment, mortgage, exclusive license, or any other conveyance, alienation, or hypothecation of a copyright or of any of the exclusive rights comprised in a copyright, whether or not it is limited in time or place of effect, but not including a non-exclusive license " 17 U.S.C. 101 (1988).

16 17 U.S.C. 204(a) (1988); Valente-Kritzer Video v. Pinckney, 881 F.2d 772, 774 (9th Cir. 1989) (affirming summary judgment for author; oral agreement unenforceable under Copyright Act); Library Publications, Inc. v. Medical Economics Co., 548 F. Supp. 1231, 1233 (E.D. Pa. 1982) (granting summary judgment against trade book publisher who sought enforcement of oral exclusive distribution agreement; transfer of exclusive rights, no matter how narrow, must be in writing), aff'd mem., 714 F.2d 123 (3d Cir. 1983).

17 17 U.S.C. 205 (1988) provides constructive notice of the contents of the recorded document, determining priority as between conflicting transfers, and determines priority as between recorded transfer and non-exclusive license. The former requirement for transfers to be recorded in order for the transferee to maintain an infringement, 17 U.S.C. 205(d), was repealed by the Berne Act Amendments 5.

18 under Adams v. Burke, 84 U.S. (17 Wall.) 453 (1873), a patentee must not attempt to exert control past the first sale. In general, use restrictions may be placed only on licensees, consistent with General Talking Pictures v. Western Elec., 304 U.S. 175 (1938). See generally Baldwin-Lima-Hamilton Corp. v. Tatnall, 169 F. Supp. 1 (E.D.

Pa.1958) (applying no control after purchase rule).

19 See Red-Baron-Franklin Park, Inc. v. Taito Corp., 883 F.2d 275, 278 (4th Cir. 1989) (purchase of video game circuit boards did not create privilege to perform video game under first sale doctrine); United States v. Moore, 604 F.2d 1228, 1232 (9th Cir. 1979) (pirated sound recording not within first sale doctrine in criminal copyright infringement prosecution). But see Mirage Editions, Inc. v. Albuquerque A.R.T. Co., 856 F.2d 1341, 1344 (9th Cir. 1988) (first sale doctrine did not create privilege to prepare derivative work by transferring art in book to ceramic tiles).

20 The way in which the first sale doctrine would impact the electronically imposed use restrictions is by frustrating a breach-of-contract lawsuit by the licensor against a licensee who exceeds the use restrictions. The licensee exceeding the use restrictions would argue that it violates public policy to enforce the restrictions and therefore that state contract law may not impose liability for their violation. See generally Restatement (second) of Contracts 178 (1981) (stating general rule for determining when contract term in unenforceable on grounds of public policy).

21 In addition, as ___ of this paper notes, the Copyright Act itself requires signed writings for transfers of copyright interests. 17 U.S.C. 204(a). (1988).

22 Michael S. Baum & Henry H. Perritt, Jr., Electronic Contracting, Publishing and EDI Law ch. 6 (1991) (contract, evidence and agency issues) [hereinafter "Baum & Perritt"]. Accord, Signature Requirements Under EDGAR, Memorandum from D. Goelzer, Office of the General Counsel, SEC to Kenneth A. Fogash, Deputy Executive Director, SEC (Jan. 13, 1986) (statutory and non-statutory requirements for "signatures" may be satisfied by means other than manual writing on paper in the hand of the signatory . . . "In fact, the electronic transmission of an individual's name may legally serve as that person's signature, providing it is transmitted with the present intention to authenticate.").

23 17 U.S.C. 101 (1988). For copyright purposes, a work is created, and therefore capable of protection, when it is fixed for the first time. 17 U.S.C. 101 (1988). "[I]t makes no difference what the form, manner, or medium of fixation may be - whether it is in words, numbers, notes, sounds, pictures, or any other graphic or symbolic indicia, whether embodied in a physical object in written, printed, photographic, sculptural, punched, magnetic, or any other stable form, and whether it is capable of perception directly or by means of any machine or device 'now known or later developed.'" 1976 U.S. Code Cong. & Admin. News 5659, 5665. The legislative history further says that, "the definition of `fixation' would exclude from the concepts purely of an evanescent or transitory nature -- reproductions such as those projected briefly on a screen shown electronically on a television or other video display or captured momentarily in the `memory' of a computer." 17 U.S.C. 102 note (excerpting from House Report 94-1476).

24 Or, more likely, what is on computer medium read by computer x, such as a magnetic cartridge used for archival records. Further references in the textual discussion to

"what is in computer x now" should be understood to include such computer readable media.

25 Cf. Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 980 (1986) (proof that a printout accurately reflects what is in the computer is too limited a basis for authentication of computer records).

26 In some cases, the electronic transaction will be accomplished by means of a physical transfer of computer readable media. In such a case, this step in the proof would involve proving what was received physically.

27 See generally Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 979 (1986) (citing as examples of authentication Ford Motor Credit Co. v. Swarens, 447 S.W.2d 53 (Ky. 1969) (authentication by establishing relationship between computer-generated monthly summary of account activity and the customer reported on); Ed Guth Realty, Inc. v. Gingold, 34 N.Y.2d 440, 315 N.E.2d 441, 358 N.Y.S.2d 367 (1974) (authentication of summary of taxpayer liability and the taxpayer)).

28 Of course, a paper document signed at the end also is probative of the fact that no alternations have been made. In this sense, a signature requirement telescopes several steps in the inquiry outlined in the text.

29 United States v. Linn, 880 F.2d 209, 216 (9th Cir. 1989) (computer printout showing time of hotel room telephone call admissible in narcotics prosecution). See also United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) (computer generated toll and billing records in price-fixing prosecution based on testimony by billing supervisor although he had no technical knowledge of system which operated from another office; no need for programmer to testify; sufficient because witness testified that he was familiar with the methods by which the computer system records information).

30 See United States v. Hutson, 821 F.2d 1015, 1020 (5th Cir. 1987) (remanding embezzlement conviction, although computer records were admissible under business records exception, despite trustworthiness challenged based on fact that defendant embezzled by altering computer files; access to files offered in evidence was restricted by special code).

31 Restatement (Second) of Contracts ___ (1981).

32 Cite for when extrinsic evidence is admissible.

33 See Baum & Perritt 2.6; The Electronic Messaging Services Task Force, The Commercial Use of Electronic Data Interchange--A Report and Model Trading Partner Agreement, 45 Bus.Law. 1645 (1990); Jeffrey B. Ritter, Scope of the Uniform Commercial Code: Computer Contracting Cases and Electronic Commercial Practices, 45 Bus.Law. 2533 (1990); Note, Legal Responses to Commercial Transactions Employing Novel Communications Media, 90 Mich.L.Rev. 1145 (1992)

34 Garber v. Harris Trust & Savings Bank, 432 N.E.2d 1309, 1311-1312 (Ill. App. 1982) ("each use of the credit

card constitutes a separate contract between the parties;" citing cases).

It is not quite this simple, because both merchant and credit card customer have separate written contracts with the credit card issuer. But there is no reason that a supplier of information to a Digital Library System and all customers of that system might not have their own contracts with the Digital Library System in the same fashion.

35 Rowland v. Union Hills Country Club, 757 P.2d 105 (Ariz. 1988) (reversing summary judgment for country club officers because of factual question whether club followed bylaws in expelling members); Straub v. American Bowling Congress, 353 N.W.2d 11 (Neb. 1984) (rule of judicial deference to private associations, and compliance with association requirements, counseled affirmance of summary judgment against member of bowling league who complained his achievements were not recognized). But see Wells v. Mobile County Board of Realtors, Inc., 387 So.2d 140 (Ala. 1980) (claim of expulsion of realtor from private association was justiciable and bylaws, rules and regulations requiring arbitration were void as against public policy; reversing declaratory judgment for defendant association).

36 F.R.E. 803(6) (excluding business records from inadmissibility as hearsay); 28 U.S.C. 1732 ("Business Records Act" permitting destruction of paper copies of government information reliably recorded by any means and allowing admission of remaining reliable record).

37 See Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 978-80, 984-85 (1986) (noting body of commentator opinion saying that business records exception and authentication are parallel ways of establishing reliability).

38 See F.R.E. 901(b)(4) (appearance, contents, substance, internal patterns, as examples of allowable authentication techniques).

39 Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 963-64 (1986) (identifying steps and trend resulting in F.R.E.).

40 Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 963 (1986).

41 Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 974 (1986) (reporting four requirements of Manual, and endorsing their use generally).

42 See Henry H. Perritt, Jr., ___, ___ Jurimetrics ___ (1993) (distinguishing between format and content standardization).

43 See Marc Lauritsen, ___ (explaining relationship between substantive legal systems and the field of artificial intelligence).

44 See Thorne, McCarty; Kevin Ashley; and Gardner.

45 It may not be particularly important to limit competition by consumers, because the consumers will never have the pointers and the rest of the network infrastructure.

Requested Patent: WO9748203A1

Title: TAMPER RESISTANT METHODS AND APPARATUS ;

Abstracted Patent: US5892899 ;

Publication Date: 1999-04-06 ;

Inventor(s): AUCSMITH DAVID (US); GRAUNKE GARY (US) ;

Applicant(s): INTEL CORP (US) ;

Application Number: US19960662679 19960613 ;

Priority Number(s): US19960662679 19960613 ;

IPC Classification: H04L9/00 ;

Equivalents: AU3488397, AU723556, CA2258087, EP0900488 (WO9748203) ;

ABSTRACT:

In accordance with a first aspect of the present invention, a security sensitive program that operates with a secret is made tamper resistant by distributing the secret in space as well as in time. In accordance with a second aspect of the present invention, a security sensitive program is made tamper resistant by obfuscating the program. In accordance with a third aspect of the present invention, a security sensitive application is made tamper resistant by isolating its security sensitive functions, and making the isolated security sensitive functions tamper resistant by distributing the secrets of the security sensitive functions in time as well as in space, and/or obfuscating the security sensitive functions. In one embodiment where obfuscation is employed, the pseudo-randomly selected pattern(s) of mutations is (are) unique for each installation. In accordance with a fourth aspect of the present invention, a security sensitive system with security sensitive applications is made further tamper resistant by deploying an interlocking trust mechanism. In accordance with a fifth aspect of the present invention, a content industry association, in conjunction with content manufacturers, content reader manufacturers, and content player manufacturers of the industry jointly implement a coordinated encryption/decryption scheme, with the player apparatus manufactured by the content player manufacturers employing playing software that include tamper resistant decryption functions.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04K 1/00	A1	(11) International Publication Number: WO 97/48203
		(43) International Publication Date: 18 December 1997 (18.12.97)

(21) International Application Number: PCT/US97/10359

(22) International Filing Date: 12 June 1997 (12.06.97)

(30) Priority Data:
08/662,679 13 June 1996 (13.06.96) US

(71) Applicant: INTEL CORPORATION [US/US]; 2200 Mission College Boulevard, Santa Clara, CA 95052 (US).

(72) Inventors: AUCSMITH, David; 6995 S.W. Laber Road, Portland, OR 97225 (US). GRAUNKE, Gary; 12120 S.W. Trail Place, Beaverton, OR 97008 (US).

(74) Agents: TAYLOR, Edwin, H. et al.; Blakely, Sokoloff, Taylor & Zafman LLP, 7th floor, 12400 Wilshire Boulevard, Los Angeles, CA 90025 (US).

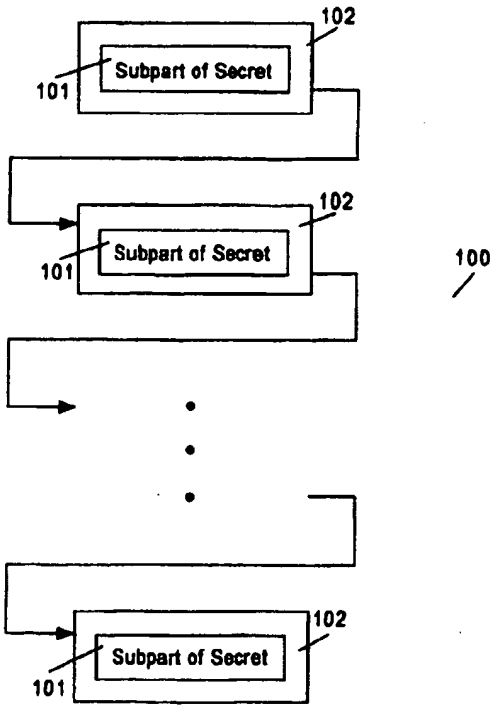
(81) Designated States: AL, AM, AT, AT (Utility model), AU (Petty patent), AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: TAMPER RESISTANT METHODS AND APPARATUS

(57) Abstract

In accordance with a first aspect of the present invention, a security sensitive program (100) that operates with a secret (101) is made tamper resistant by distributing the secret in space as well as in time. In accordance with a second aspect of the present invention, a security sensitive program is made tamper resistant by obfuscating the program. In accordance with a third aspect of the present invention, a security sensitive application is made tamper resistant by isolating its security sensitive functions, and making the isolated security sensitive functions tamper resistant by distributing the secrets of the security sensitive functions in time as well as in space, and/or obfuscating the security sensitive functions. In one embodiment where obfuscation is employed, the pseudo-randomly selected pattern(s) of mutations is (are) unique for each installation. In accordance with a fourth aspect of the present invention, a security sensitive system with security sensitive applications is made further tamper resistant by deploying an interlocking trust mechanism. In accordance with a fifth aspect of the present invention, a content industry association, in conjunction with content manufacturers, content reader manufacturers, and content player manufacturers of the industry jointly implement a coordinated encryption/decryption scheme, with the player apparatus manufactured by the content player manufacturers employing playing software that include tamper resistant decryption functions.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

Tamper Resistant Methods And Apparatus

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to the field of system security. More specifically, the present invention relates to the tamper resistant methods and apparatus.

2. Background Information

Many applications, e.g. financial transactions, unattended authorizations and content management, require the basic integrity of their operations to be assumed, or at least verified. While a number of security approaches such as encryption and decryption techniques are known in the art, unfortunately, the security approaches can be readily compromised, because these applications and the security approaches are implemented on systems with an open and accessible architecture, that renders both hardware and software including the security approaches observable and modifiable by a malevolent user or a malicious program.

Thus, a system based on open and accessible architecture is a fundamentally insecure platform, notwithstanding the employment of security measures. However, openness and accessibility offer a number of advantages, contributing to these systems' successes. Therefore, what is required are techniques that will render software execution virtually unobservable or unmodifiable on these fundamentally insecure platforms, notwithstanding their openness and accessibility. As will be disclosed in more detail below, the present invention of tamper resistant methods and apparatus achieve these and other desirable results.

SUMMARY OF THE INVENTION

In accordance with a first aspect of the present invention, a security sensitive program that operates with a secret is made tamper resistant by distributing the secret in space as well as in time. The secret is partitioned into a number of subparts, and the security sensitive program is unrolled into a number of subprograms

that operate with the subparts, one subpart per subprogram. The subprograms are then executed over a period of time. In one embodiment, the subprograms are further interleaved with unrelated tasks. In one application, the security sensitive program is a decryption program and the secret is a private key.

In accordance with a second aspect of the present invention, a security sensitive program is made tamper resistant by obfuscating the program. The security sensitive program is divided into a number of subprograms, and a plaintext appearance location schedule is selected for the subprograms. An appropriate mutated initial state is determined for each of the subprograms, except for the subprogram where the program's entry point is located. The mutated initial states are determined based on one or more pseudo-randomly selected patterns of mutations that return the program to the initial state at the end of an execution pass. During execution, the subprograms are recovered when they are needed, one or more but not all at a time, following the pseudo-randomly selected pattern(s) of mutations. In one embodiment, each pseudo-randomly selected pattern of mutations is determined using a predetermined partnership function in conjunction with an ordered set of pseudo-random keys. In one application, the security sensitive program is a decryption program that operates with a secret private key. The decryption program may or may not have been made tamper resistant by distributing the secret private key in time as well as in space.

In accordance with a third aspect of the present invention, a security sensitive application is made tamper resistant by isolating its security sensitive functions, and making the isolated security sensitive functions tamper resistant by distributing the secrets of the security sensitive functions in time as well as in space, and/or obfuscating the security sensitive functions. In one embodiment where obfuscation is employed, the pseudo-randomly selected pattern(s) of mutations is (are) unique for each installation. In one application, the application is a content management application having a decryption function.

In accordance with a fourth aspect of the present invention, a security sensitive system with security sensitive applications is made further tamper resistant by providing a system integrity verification program having tamper resistant integrity verification kernels, that jointly deploy an interlocking trust mechanism with the tamper resistant security sensitive functions of the security sensitive applications. In one

application, the system is a content manipulation system, and the application is a content management application.

In accordance with a fifth aspect of the present invention, a content industry association, in conjunction with content manufacturers, content reader manufacturers, and content player manufacturers of the industry jointly implement a coordinated encryption/decryption scheme, with the player apparatus manufactured by the content player manufacturers employing playing software that include tamper resistant decryption functions.

BRIEF DESCRIPTION OF DRAWINGS

The present invention will be described by way of embodiments, but not limitations, illustrated in the accompanying drawings in which like references denote similar elements, and in which:

Figure 1 is a block diagram illustrating a first aspect of the present invention for making a security sensitive program tamper resistant by distributing the program's secret(s) in time and in space;

Figure 2 is a block diagram illustrating one embodiment of the first aspect of the present invention including a subprogram generator for generating the subprograms that operate with corresponding subparts of the distributed secret(s);

Figure 3 is a flow diagram illustrating one embodiment of the operational flow of the subprogram generator of **Figure 2**;

Figure 4 is a block diagram illustrating a second aspect of the present invention for making a security sensitive program tamper resistant by obfuscating the various subparts of the security sensitive program;

Figure 5 is a block diagram illustrating one embodiment of a subpart of the obfuscated program;

Figure 6 is a block diagram illustrating one embodiment of the second aspect of the present invention including an obfuscation processor for generating the obfuscated program;

Figure 7 is a graphical diagram illustrating distribution of key period for the second aspect of the present invention;

Figures 8a - 8b are flow diagrams illustrating one embodiment of the operational flow of the obfuscation processor of **Figure 6**;

Figure 9 is a flow diagram illustrating one embodiment of the operational logic of an obfuscated subprogram of the obfuscated program;

Figures 10 - 14 are diagrams illustrating a sample application of the second aspect of the present invention;

Figure 15 is a block diagram illustrating a third aspect of the present invention for making a security sensitive application tamper resistant;

Figure 16 is a block diagram illustrating a fourth aspect of the present invention for making a security sensitive system tamper resistant;

Figure 17 is a block diagram illustrating a fifth aspect of the present invention for making security sensitive industry tamper resistant; and

Figures 18 - 19 are block diagrams illustrating an example computer system and an embedded controller suitable for programming with the various aspects of the present invention.

DETAILED DESCRIPTION OF THE INVENTION

In the following description, various aspects of the present invention will be described. However, it will be apparent to those skilled in the art that the present invention may be practiced with only some or all aspects of the present invention. For purposes of explanation, specific numbers, materials and configurations are set forth in order to provide a thorough understanding of the present invention. However, it will also be apparent to one skilled in the art that the present invention may be practiced without the specific details. In other instances, well known features are omitted or simplified in order not to obscure the present invention.

Parts of the description will be presented in terms of operations performed by a computer system, using terms such as data, flags, bits, values, characters, strings, numbers and the like, consistent with the manner commonly employed by those skilled in the art to convey the substance of their work to others skilled in the art. As well understood by those skilled in the art, these quantities take the form of electrical, magnetic, or optical signals capable of being stored, transferred, combined, and otherwise manipulated through mechanical and electrical components of the computer system; and the term computer system include general purpose as well as special purpose data processing machines, systems, and the like, that are standalone, adjunct or embedded.

Various operations will be described as multiple discrete steps in turn in a manner that is most helpful in understanding the present invention, however, the order of description should not be construed as to imply that these operations are necessarily order dependent, in particular, the order of presentation.

Referring now to **Figure 1**, a block diagram illustrating a first aspect of the present invention is shown. In accordance with this first aspect of the present invention, security sensitive program **100** is made tamper resistant by distributing its secret in space as well as in time. The secret (not shown in totality) is "partitioned" into subparts **101**, and program **100** is unrolled into a number of subprograms **102** that operate with subparts **101**; for the illustrated embodiment, one subpart **101** per subprogram **102**. Subprograms **102** are then executed over a period of time. As a result, the complete secret cannot be observed or modified in any single point in space nor in any single point in time.

For example, consider the artificially simple "security sensitive" program for computing the result of X multiply by S, where S is the secret. Assuming S equals to 8, S can be divided into 4 subparts, with each subpart equals 2, and the "security sensitive" program can be unrolled into 4 subprograms with each program computing A = A + (X multiply by 2). Thus, the complete secret 8 can never be observed or modified in any point in space nor time.

As a further example, consider the "security sensitive" program for computing the result of (X to the power of S) modulo Y, where S again is the secret. If S equals 16, S can be divided into 8 subparts, with each subpart equals 2, and the "security sensitive" program can be unrolled into 8 subprograms with each program computing A = (A multiply by ((X to the power of 2) modulo Y)) modulo Y. Thus, the complete secret 16 can never be observed or modified in any point in space nor time.

As will be appreciated by those skilled in the art, the function (X to the power of S) modulo Y is the basis function employed in many asymmetric key (private/public key) schemes for encryption and decryption. Thus, by practicing this first aspect of the present invention, an encryption/decryption function can be made tamper resistant.

Petitioner Apple Inc. - Exhibit 1012, p. 1324

In one embodiment, the subprograms are further interleaved with unrelated tasks to further obscure the true nature of the tasks being performed by the unrolled subprograms. The tasks may even have no purpose to them.

Figure 2 illustrates one embodiment of the first aspect of the present invention including a subprogram generator for generating the subprograms. For the illustrated embodiment, subprogram generator **104** is provided with the secret as input. Furthermore, subprogram generator **104** is provided with access to library **105** having entry, basis and prologue subprograms **106**, **108**, and **109** for used in generating subprograms **102** of a particular security sensitive program in view of the secret provided. In other words, entry and basis subprograms **106** and **108** employed are different for different security sensitive programs. For the above illustrated examples, in the first case, entry and basis subprograms **106** and **108** will initialize and compute A = A + (X multiply by a subpart of S), whereas in the second case, entry and basis subprograms **106** and **108** will initialize and compute A = (A multiply by ((X to the power of a subpart of S) modulo Y)) modulo Y. Prologue subprogram **109** is used to perform post processing, e.g. outputting the computed results as decrypted content.

For the illustrated embodiment, entry subprogram **106** is used in particular to initialize an appropriate runtime table **110** for looking up basis values by basis subprogram **108**, and basis subprogram **108** is used to perform the basis computation using runtime table **110**. For the modulo function example discussed above, runtime table **110** is used to retum basis values for (X to the power of a subpart of secret) modulo Y for various subpart values, and basis subprogram **108** is used to perform the basis computation of A = (A multiply by (basis value of a subpart of secret)) modulo Y, where A equals the accumulated intermediate results. A's initial value is 1.

For example, entry subprogram **106** may initialize a runtime table **110** of size three for storing the basis values of bv1, bv2 and bv3, where bv1, bv2 and bv3 equal (X to the power of 1) modulo Y, (X to the power of 2) modulo Y, and (X to the power of 3) modulo Y respectively. For the modulo function (X to the power 5) modulo Y, subprogram generator **104** may partition the secret 5 into two subparts with subpart values 3 and 2, and generate two basis programs **108** computing A = (A * Lkup(3)) modulo Y and A = (A * Lkup(2)) modulo Y respectively.

Figure 3 illustrates one embodiment of the operational flow of subprogram generator **104** of **Figure 2**. For the illustrated embodiment, upon invocation, subprogram generator **104** first generates an instance of entry subprogram **106** for initializing at least an appropriate runtime lookup table **110** (Lkup) for returning the basis values of a modulo function for various subparts of a secret, and an accumulation variable (A) to an appropriate initial state, step **112**. Subprogram generator **104** then partitions the secret into subparts, step **114**. In one embodiment, the partition is performed to require the least number of basis programs, within the constraint of the basis values stored in runtime table **110**.

Next, subprogram generator **104** sets a subpart of the secret as the lookup index (LIDX), steps **116**. Then, subprogram generator **104** generates the current basis subprogram to compute A = [A multiply by Lkup (LIDX)] modulo Y, step **118**. Subprogram generator **104** repeats steps **116 - 118** for all subparts, until a basis program has been generated for each subpart of the secret, step **120**. Finally, subprogram generator **104** generates an instance of prologue subprogram **109** for performing post processing, as described earlier, step **122**.

Figure 4 illustrates a second aspect of the present invention. In accordance with this second aspect of the present invention, security sensitive program **203** is made tamper resistant by obfuscating the program. Security sensitive program **203** is divided and processed into a number of obfuscated subprograms **204**. A plaintext (i.e. unmutated) appearance location schedule (i.e. where in memory) is selected for obfuscated subprograms **204**. For the illustrated embodiment, the plaintext appearance location schedule is formulated in terms of the memory cells **202** of two memory segments, memory segment **201a** and memory segment **201b**. Initially, except for the obfuscated subprogram **204** where the program's entry point is located, all other obfuscated subprograms **204** are stored in mutated states. Obfuscated subprograms **204** are recovered or made to appear in plaintext form at the desired memory cells **202**, one or more at a time, when they are needed for execution, and mutated again, once executions are completed. As will be described in more detail below, the initial mutated states, and the process of recovery are determined or performed, in accordance with one or more pseudo-randomly selected pattern of mutations. The pseudo-randomly selected pattern(s) of mutations is (are) determined using a predetermined mutation partnership function in

conjunction with one or more ordered sets of pseudo-random keys. As a result, obfuscated subprograms **204** cyclically mutate back to their respective initial states after each execution pass. Actually, obfuscated subprograms **204** implementing the same loop also cyclically mutate back to the loop entry states after each pass through the loop.

For the illustrated embodiment, each obfuscated subprogram **204** and each cell **202** are of the same size, and first memory segment **201a** is located in high memory, whereas second memory segment **201b** is located in low memory. Furthermore, there are even number of obfuscated subprograms **204**, employing dummy subprogram if necessary.

Figure 5 illustrated one embodiment of subprogram **204**. In accordance with the present invention, for the illustrated embodiment, in addition to original subprogram **102**, obfuscated subprogram **204** is provided with mutation partner identification function **206**, mutation function **207**, partner key **208** and jump block **209**. Original subprogram **102** performs a portion of the functions performed by program **200**. Original subprogram **102** may be an entry/basis/prologue subprogram **106/108/109** in accordance with the first aspect of the present invention. Mutation partner identification function **206** is used to identify the partner memory cells **202** for all memory cell **202** at each mutation round. In one embodiment, the partner identification function **206** is the function: Partner Cell ID = Cell ID XOR Pseudo-Random Key. For a pseudo-random key, mutation partner identification function **206** will identify a memory cell **202** in the second memory segment **201b** as the partner memory cell for of a memory cell **202** in the first memory segment **201a**, and vice versa. Only ordered sets of pseudo-random keys that will provide the required periods for the program and its loops will be employed. The length of a period is a function of the pseudo-random keys' set size (also referred to as key length). Mutation function **207** is used to mutate the content of the various memory cells **202**. In one embodiment, mutation function **207** XORs the content of each memory cell **202** in first memory segment **201a** into the partner memory cell **202** in second memory segment **201b** in an odd mutation round, and XORS the content of each memory cell **202** in second memory segment **201b** into the partner memory cell **202** in first memory segment **201a** in an even mutation round. Partner key **208** is the pseudo-random key to be used by mutation partner identification function **206** to identify mutation partners of the various memory cells **202** for a

mutation round. Jump block **209** transfers execution control to the next obfuscated subprogram **204**, which at the time of transfer, has been recovered into plaintext through the pseudo-random pattern of mutations.

In one embodiment, an obfuscated subprogram **204** may also include other functions being performed for other purposes or simply unrelated functions being performed to further obscure the subpart functions being performed.

Figure 6 illustrates one embodiment of the second aspect of the present invention including an obfuscation processor for processing and transforming subprograms into obfuscated subprograms. For the illustrated embodiment, obfuscation processor **214** is provided with program **200** as inputs. Furthermore, obfuscation processor **214** is provided with access to pseudo-random keys' key length lookup table **212**, mutation partner identification function **206**, and mutation function **207**. For the illustrated embodiment, obfuscation processor **214** also uses two working matrices **213** during generation of obfuscated program **203**.

Key length lookup table **212** provides obfuscation processor **214** with key lengths that provide the required periods by the program and its loops. Key lengths that will provide the required periods is a function of the mutation technique and the partnership function. **Figure 7** illustrates various key lengths that will provide various periods for the first and second memory segment mutation technique and the partnership function described above.

Referring back to **Figure 6**, mutation partner identification function **206** identifies a mutation partner memory cell **202** for each memory cell **202**. In one embodiment, mutation partner identification function **206** identifies mutation partner memory cells in accordance with the "XOR" mutation partner identification function described earlier. Mutation function **207** mutates all memory cells **202**. In one embodiment, mutation function **207** mutates memory cells **202** in accordance with the two memory segments, odd and even round technique described earlier.

For the illustrated embodiment, working matrices **213** include two matrices M1 and M2. Working matrix M1 stores the Boolean functions of the current state of the various memory cells **202** in terms of the initial values of memory cells **202**. Working matrix M2 stores the Boolean functions for recovering the plaintext of

the various obfuscated subprograms **204** in terms of the initial values of memory cells **202**.

Referring now to **Figures 8a - 8b**, two block diagrams illustrating one embodiment of obfuscation processor **214** are shown. For the illustrated embodiment, as shown in **Fig. 8a** in response to a program input (in object form), obfuscation processor **214** analyzes the program, step **216**. In particular, obfuscation processor **214** analyzes branch flow of the program, identifying loops within the program, using conventional compiler optimization techniques known in the art. For the purpose of this application, any execution control transfer, such as a call and subsequent return, is also considered a "loop".

Next, obfuscation processor **214** may perform an optional step of peephole randomization, step **218**. During this step, a peephole randomization pass over the program and replaces code patterns with random equivalent patterns chosen from an optional dictionary of such patterns. Whether it is performed depends on whether the machine architecture of the instructions provide alternate ways of accomplishing the same task.

Then, obfuscation processor **214** restructures and partitions the program **200** into a number of equal size subprograms **204** organized by their loop levels, padding the subprograms **204** if necessary, based on the analysis results, step **220**. Except for very simple program with a single execution path, virtually all programs **200** will require some amount of restructuring. Restructuring includes e.g. removing as well as adding branches, and replicating instructions in different loop levels. Restructuring is also performed using conventional compiler optimization techniques.

Finally, obfuscation processor **214** determines the subprograms' plaintext appearance location schedule, and the initial state values for the various memory cells **202**, step **221**.

Fig. 8b illustrates step **221** in further detail. As shown, obfuscation processor **214** first initializes first working matrix M1, step **222**. Then, obfuscation processor **214** selects a memory cell for the program's entry subprogram to appear in plaintext, step **223**. In one embodiment, the memory cell **202** is arbitrarily selected

(within the proper memory segment **201a** or **201b**). Once selected, obfuscation processor **214** updates the second working matrix M2, step **224**.

Next, obfuscation processor **214** selects an appropriate key length based on the procedure's period requirement, accessing key length table **212**, step **226**. Obfuscation processor **214** then generates an ordered set of pseudo-random keys based on the selected key length, step **228**. For example, if key length equals 5 is selected among the key lengths that will provide a required period of 30, obfuscation processor **214** may randomly select 17, 18, 20, 24 and 16 as the ordered pseudo-random keys.

Next, obfuscation processor **214** determines the partner memory cells **202** for all memory cells **202** using the predetermined mutation partner identification function **206** and the next key in the selected set of ordered pseudo-random keys, step **230**. Upon making the determination, obfuscation processor **214** simulates a mutation, and updates M1 to reflect the results of the mutation, step **232**.

Once mutated, obfuscation processor **214** selects a memory cell for the next subprogram **204** to appear in plaintext, step **234**. Having done so, obfuscation processor **214** updates M2, and incrementally invert M2 using the Guassian Method, step **235**. In one embodiment, instead of incremental inversion, obfuscation processor **214** may just verify M2 remains invertable instead. If M2 is not invertable, obfuscation processor **214** cancels the memory cell selection, and restores M2 to its prior state, step **237**. Obfuscation processor **214** repeats steps **234 - 236** to select another memory cell **202**. Eventually, obfuscation processor **214** becomes successful.

Once succeeded, obfuscation processor **214** determines if there was a loop level change, step **238**. If there was a loop level change, obfuscation processor **214** further determines if the loop level change is down level or up level change, i.e. the subprogram is an entry subprogram of a new loop level or a return point of a higher loop level, step **239**. If the loop level change is "down", obfuscation processor **214** selects another appropriate key length based on the new loop's period requirement, accessing key length table **212**, step **241**. Obfuscation processor **214** then generates a new ordered set of pseudo-random keys based on the newly selected key length, step **242**. The newly generated ordered set of pseudo-random

keys becomes the "top" set of pseudo-random keys. On the other hand, if the loop level change id "up", obfuscation processor **214** restores an immediately "lower" set of pseudo random keys to be the "top" set of pseudo-random keys, step **240**.

Upon properly organizing the "top" set of pseudo-random keys or upon determining there's no loop level change, obfuscation processor **214** again determines the partner memory cells **202** for all memory cells **202** using the predetermined mutation partner identification function **206** and the next key in the "top" set of ordered pseudo-random keys, step **243**. Upon making the determination, obfuscation processor **214** simulates a mutation, and updates M1 to reflect the results of the mutation, step **244**.

Once mutated, obfuscation processor **214** determines if there are more subprograms **204** to process, step **245**. If there are more subprograms **204** to process, obfuscation processor **214** returns to step **234** and proceeds as described earlier. Otherwise, obfuscation processor **214** inserts the mutation partner identification function **206**, the partner key to be used to identify mutation partner memory cells, the mutation function, the jump block, and the address of the next subprogram **204** into each of the obfuscated subprograms **204**, step **246**. Finally, obfuscation processor **214** computes the initial values of the various obfuscated subprograms **204**, and outputs them, steps **247 - 248**.

Figure 9 illustrates one embodiment of the operational flow of an obfuscated subprogram **204**. For the illustrated embodiment, obfuscated subprogram **204** first executes the functions of the original subprogram, step **250**. For embodiments including additional and/or unrelated functions, they may be executed also. Then obfuscated subprogram **204** executes mutation partner identification function **206** to identify the mutation memory cell partners for all memory cells **202** using the stored partner key, step **252**. Having identified the mutation partners, obfuscated subprogram **204** executes mutation function **207** to mutate the memory cells based on the identified partnership.

Next, depending on whether obfuscated subprogram **204** is the last subprogram in an execution pass, obfuscated subprogram **204** either jumps to the next obfuscated subprogram (which should be in plaintext) or returns to the "caller".

Note that if obfuscated subprogram **204** returns to the "caller", all other obfuscated subprograms **204** are in their respective initial states.

Figures 10 - 14 illustrate a sample application of this second aspect of the present invention. **Figure 10** illustrates a sample security sensitive program **200** having six subprograms SPGM0 - SPGM5 implementing a simple single level logic, for ease of explanation, with contrived plaintext values of "000", "001", "010", "011", "100" and "111". Thus, the required period is 6. For ease of explanation, a keylength of one will be used, and the pseudo-random key selected is 3. Furthermore, the mutation partnership identification function is simply Partner Cell ID = Cell ID + 3, i.e. cell 0 always pairs with cell 3, cell 1 pairs with cell 4, and cell 2 pairs with cell 5.

Figure 10 further illustrates at invocation (mutation 0), memory cells (c0 - c5) contains initial values (iv0 - iv5), as reflected by M1. Assuming, cell c0 is chosen for SPGM0, M2 is updated to reflect that the Boolean function for recovering the plaintext of SPGM0 is simply iv0. **Figure 10** further illustrates the values stored in memory cells (c0 - c5) after the first mutation. Note that for the illustrated mutation technique, only the content of the memory cells (c3 - c5) have changed. M1 is updated to reflect the current state. Assuming, cell c3 is chosen for SPGM1, M2 is updated to reflect that the Boolean function for recovering the plaintext of SPGM1 is simply iv0 XOR iv3. Note that for convenience of manipulation, the columns of M2 have been swapped.

Figure 11 illustrates the values stored in memory cells (c0 - c5) after the second, third and fourth mutations. As shown, the content of half of the memory cells (c0 - c5) changed alternatingly after each mutation. In each case, M1 is updated to reflect the current state. Assuming, cells c1, c4 and c2 are chosen for SPGM2, SPGM3 and SPGM4 respectively after the second, third and fourth mutations respectively, in each case M2 is updated to reflect that the Boolean functions for recovering the plaintexts of SPGM2, SPGM3 and SPGM4, i.e. iv4, iv1, and iv2 XOR iv5.

Figure 12 illustrates the values stored in memory cells (c0 - c5) after the fifth mutation. As shown, the content of memory cells (c3 - c5) changed as in previous odd rounds of mutation. M1 is updated to reflect the current state.

Assuming, cell c5 is chosen for SPGM5, M2 is updated to reflect that the Boolean function for recovering the plaintext of SPGM5 is iv5.

Figure 13 illustrates how the initial values iv0 - iv5 are calculated from the inverse of M2, since M2 x ivs = SPGMs, ivs = M2-1 x SPGMs. Note that a "1" in M2-1 denotes the corresponding SPGM is selected, whereas a "0" in M2-1 denotes the corresponding SPGM is not selected, for computing the initial values (iv0 - iv5).

Figure 14 illustrates the content of the memory cells of the above example during execution. Note that at any point in time, at most only two of the subprograms are observable in their plaintext forms. Note that the pairing of mutation partners is fixed only because of the single pseudo-random key and the simple mutation partner function employed, for ease of explanation. Note also that with another mutation, the content of the memory cells are back to their initial states. In other words, after each execution pass, the subprograms are in their initial states, ready for another invocation.

As will be appreciated by those skilled in the art, the above example is unrealistically simple for the purpose of explanation. The plaintext of a subprogram contains many more "0" and "1" bits, making it virtually impossible to distinguish memory cell storing an obfuscated subprogram in a mutated state from a memory cell storing an obfuscated subprogram in plaintext form. Thus, it is virtually impossible to infer the plaintext appearance location schedule from observing the mutations during execution.

Figure 15 illustrates a third aspect of the present invention. In accordance with this aspect of the present invention, security sensitive application **300** may be made tamper resistant by isolating its security sensitive functions **302** and making them tamper proof by incorporating the first and/or second aspects of the present invention described above.

In employing the above described second aspect of the present invention, different sets of pseudo-random keys will produce a different pattern of mutations, even with the same mutation partner identification function. Thus, copies of the security sensitive application installed on different systems may be made unique by employing a different pattern of mutations through different sets of pseudo-random

keys. Thus, the security sensitive applications installed in different systems are further resistant from class attack, even if the obfuscation scheme is understood from observation on one system.

Figure 16 illustrates a fourth aspect of the present invention. In accordance with this aspect of the present invention, a security sensitive system **400** may be made tamper resistant by making its security sensitive applications **400a** and **400b** tamper resistant in accordance with the first, second and/or third aspects of the present invention described above. Furthermore, security of system **400** may be further strengthened by providing system integrity verification program (SIVP) **404** having a number of integrity verification kernels (IVKs). For the illustrated embodiment, a first and a second level IVK **406a** and **406b**. First level IVK **406a** has a published external interface for other tamper resistant security sensitive functions (SSFs) **402a - 402b** of the security sensitive applications **400a - 400b** to call. Both IVKs are made tamper resistant in accordance with the first and the second aspects of the present invention described earlier. Together, the tamper resistant SSFs **402a - 402b** and IVKs **406a - 406b** implement an interlocking trust mechanism.

In accordance with the interlocking trust mechanism, for the illustrated embodiment, tamper resistant SSF1 and SSF2 **402a - 402b** are responsible for the integrity of security sensitive applications **400a - 400b** respectively. IVK1 and IVK2 **406a - 406b** are responsible for the integrity of SIVP **404**. Upon verifying the integrity of security sensitive application **400a** or **400b** it is responsible for, SSF1/SSF2 **402a - 402b** will call IVK1 **406a**. In response, IVK1 **406a** will verify the integrity of SIVP **404**. Upon successfully doing so, IVK1 **406a** calls IVK2 **406b**, which in response, will also verify the integrity of SIVP **404**.

Thus, in order to tamper with security sensitive application **400a**, SSF1 **402a**, IVK1 **406a** and IVK2 **406b** must be tamper with at the same time. However, because IVK1 and IVK2 **406a - 406b** are also used by SSF2 and any other SSFs on the system, all other SSFs must be tamper with at the same time.

Figure 17 illustrates a fifth aspect of the present invention. In accordance with this aspect of the present invention, content industry association **500**, content manufacturers **502**, content reader manufacturers **510** and content

player manufacturer **506** may jointly implement a coordinated encryption/decryption scheme, with content players **508** manufactured by content player manufacturers **506** employing playing software that include content decryption function made tamper resistant in accordance with the above described various aspects of the present invention.

Content industry association **500** owns and holds secret private encryption key Kciapri. Content industry association **500** encrypts content manufacturer's secret content encryption key Kc and content player manufacturer's public encryption Kppub for the respective manufacturers **502** and **506** using Kciapri, i.e. Kciapri[Kc] and Kciapri[Kppub].

Content manufacturer **502** encrypts its content product Kc[ctnt] and includes with the content product Kciapri[Kc]. Content reader manufacturer **510** includes with its content reader product **512** the public key of content industry association Kciapub, whereas content player manufacturer **506** includes with its content player product **508** content player manufacturer's secret private play key Kppri, content industry association's public key Kciapub, and the encrypted content player public key Kciapri[Kppub].

During operation, content reader product **512** reads encrypted content Kc[ctnt] and the encrypted content encryption key Kciapri[Kc]. Content reader product **512** decrypts Kc using Kciapub. Concurrently, content player product **508** recovers its public key Kppub by decrypting Kciapri[Kppub] using content industry association's public key Kciapub. Content reader product **512** and content player product **508** are also in communication with each other. Upon recovering its own public key, content player product **508** provides it to content reader product **512**. Content reader product **512** uses the provided player public key Kppub to encrypt the recovered content encryption key Kc, generating Kppub[Kc], which is returned to content player product **508**. In response, content player product **508** recovers content encrypt key Kc by decrypting Kppub[Kc] using its own private key Kppri.

Thus, as content reader product **512** reads encrypted content Kc[ctnt], and forwards them to content player product **508**, content player product **508** decrypts them with the recovered Kc, generating the unencrypted content (ctnt). In accordance with the above described aspects of the present invention, the decryption

functions for recovering the content player's manufacturer's public key, and recovering the content encryption key Kc are made tamper resistant.

As will be appreciated by those skilled in the art, in addition to being made tamper resistant, by virtue of the interlocking trust, tampering with the content player product's decryption functions will require tampering of the content industry association, content manufacturer and content reader manufacturer's encryption/decryption functions, thus making it virtually impossible to compromise the various encryption/decryption functions' integrity.

As will be also appreciated by those skilled in the art, a manufacturer may play more than one role in the above described tamper resistant industry security scheme, e.g. manufacturing both the content reader and the content player products, as separate or combined products.

Figure 18 illustrates a sample computer system suitable to be programmed with security sensitive programs/applications with or without SIVP, including industry wise security mechanism, made tamper resistant in accordance with the first, second, third, fourth and/or fifth aspect of the present invention. Sample computer system **600** includes CPU **602** and cache memory **604** coupled to each other through processor bus **605**. Sample computer system **600** also includes high performance I/O bus **608** and standard I/O bus **618**. Processor bus **605** and high performance I/O bus **608** are bridged by host bridge **606**, whereas high performance I/O bus **608** and standard I/O bus **618** are bridged by bus bridge **610**. Coupled to high performance I/O bus **608** are main memory **612**, and video memory **614**. Coupled to video memory **614** is video display **616**. Coupled to standard I/O bus **618** are mass storage **620**, and keyboard and pointing devices **622**.

These elements perform their conventional functions. In particular, mass storage **620** is used to provide permanent storage for the executable instructions of the various tamper resistant programs/applications, whereas main memory **612** is used to temporarily store the executable instructions tamper resistant programs/applications during execution by CPU **602**.

Figure 19 illustrates a sample embedded controller suitable to be programmed with security sensitive programs for a security sensitive apparatus, made

tamper resistant in accordance with the first, second, third, fourth and/or fifth aspect of the present invention. Sample embedded system **700** includes CPU **702**, main memory **704**, ROM **706** and I/O controller **708** coupled to each other through system bus **710**. These elements also perform their conventional functions. In particular, ROM **706** may be used to provide permanent and execute-in-place storage for the executable instructions of the various tamper resistant programs, whereas main memory **704** may used to provide temporary storage for various working data during execution of the executable instructions of the tamper resistant programs by CPU **702**.

Thus, various tamper resistant methods and apparatus have been described. While the methods and apparatus of the present invention have been described in terms of the above illustrated embodiments, those skilled in the art will recognize that the invention is not limited to the embodiments described. The present invention can be practiced with modification and alteration within the spirit and scope of the appended claims. The description is thus to be regarded as illustrative instead of restrictive on the present invention.

CLAIMS

What is claimed is:

1. An apparatus comprising:

an execution unit for executing programming instructions; and

a storage medium coupled to the execution unit, having stored therein a plurality of programming instruction blocks to be executed by the execution unit during operation, the programming instruction blocks operating on corresponding subparts of a secret distributed among them, and the execution being distributed over a period of time.

2. The apparatus as set forth in claim 1, wherein the programming instruction blocks jointly implement a decryption function, and the secret is a private key.

3. The apparatus as set forth in claim 1, wherein one or more of the programming instruction blocks further perform one or more unrelated tasks to further obscure the operations on the subparts of the secret.

4. A machine implemented method for executing a program that operates on a secret in a tamper resistant manner, the method comprises the steps of:

a) executing a first unrolled subprogram of the program at a first point a time, with the first unrolled subprogram operating on a first subpart of the secret; and

b) executing a second unrolled subprogram of the program at a second point a time, with the second unrolled subprogram operating on a second subpart of the secret.

5. The method as set forth in claim 3, wherein the first and second unrolled subprograms are unrolled subprograms of a decryption function; and the secret is a private key.

6. The method as set forth in claim 3, wherein

step (a) further includes the first unrolled subprogram performing at least a first unrelated task; and

step (b) further includes the second unrolled subprogram performing at least a second unrelated task;

said at least a first and a second unrelated task are performed to further obscure the first and second unrolled subprograms' operation on the first and second subparts of the secret.

7. An apparatus comprising:

an execution unit for executing programming instructions; and

a storage medium having stored therein a plurality of programming instructions to be executed by the execution unit during operation, wherein when executed, in response to a secret being provided, the programming instructions partition the secret into a plurality of subparts, and generate a plurality of programming instruction blocks that operate on the subparts.

8. The apparatus as set forth in claim 7, wherein the apparatus further includes a library having an entry programming instruction block, and a basis programming instruction block, to be accessed by the programming instructions in generating the programming instruction blocks.

9. The apparatus as set forth in claim 7, wherein during execution,

the entry programming instruction block initializes a table of values for use by the basis programming blocks to operate on their corresponding subparts of the secret; and

the basis programming blocks' operations on their corresponding subparts of the secret, include looking up values initialized in the table using the basis programming blocks' corresponding subparts of the secret.

10. A machine implemented method for generating a tamper resistant program to operate on a secret, the method comprising the steps of:

a) receiving the secret;

b) partitioning the secret into a plurality of subparts; and

c) generating a plurality of subprograms to correspondingly operate on the subparts of the secret.

11. The method as set forth in claim 10, wherein step (c) includes accessing a library having an entry subprogram, and a basis subprogram to generate the subprograms.

12. The method as set forth in claim 11, wherein during execution,

the entry subprogram initializes a table of values for use by the basis subprograms to operate on their corresponding subparts of the secret; and

the basis subprograms' operations on their corresponding subparts of the secret, include looking up values initialized in the table using the basis subprograms' corresponding subparts of the secret.

13. An apparatus comprising:

an execution unit for executing programming instructions; and

a storage medium having stored thereon a plurality of programming instruction blocks to be executed by the execution unit, the programming instruction blocks being stored in a mutated form, except for at least one, which is stored in a plaintext form, wherein the mutated programming instruction blocks are recovered into the plaintext form during execution on an as needed basis, one or more but not all at a time.

14. The apparatus as set forth in claim 13, wherein each programming instruction block includes a first programming instruction sub-block for performing a task, a second programming instruction sub-block for computing mutation partners for a plurality of memory cells, a key to be employed in said computation of mutation partners, a third programming instruction sub-block for mutating memory cells in accordance with the computed mutation partnering, and a fourth programming instruction sub-block for transferring execution control to another programming instruction block.

15. The apparatus as set forth in claim 14, wherein the first programming instruction sub-block operates on a subpart of a secret.

16. The apparatus as set forth in claim 14, wherein the second programming instruction sub-block computes the mutation partnering by performing a logical XOR operation on a memory cell's identifier and the key.

17. The apparatus as set forth in claim 14, wherein the key is a member of an ordered set of pseudo-randomly selected members, the ordered set having a set size that will provide a required period for a pattern of memory cell mutations, with the memory cells being partnered for mutation in accordance with the computed mutation partnering using the key.

18. The apparatus as set forth in claim 14, wherein the memory cells are divided into two memory cells groups, and pair-wise partnered by the second programming instruction sub-block, with the partnered memory cells being in different group; and the third programming instruction sub-block performs a logical XOR operation on the contents of each pair of partnered memory cells, and alternating between the two memory cell groups for odd and even mutation rounds, in storing the results of the logical XOR operations

19. A machine implemented method for executing a program, the method comprising:

a) executing a first of a plurality of subprograms generated to obfuscate the program;

b) computing mutation partners for a plurality of memory cells storing the plurality of subprograms, using a key, the subprograms being stored initially in the memory cells in a mutated form, except for at least one, which is stored initially in a plaintext form;

c) mutating the memory cells in accordance with the computed mutation partnering to recover a second of the plurality of subprograms for execution.

20. The method as set forth in claim 19, wherein the first and second subprograms operate on a first and a second subpart of a secret.

21. The method as set forth in claim 19, wherein step (b) comprises performing a logical XOR operation on a memory cell's identifier and the key for each memory cell.

22. The method as set forth in claim 19, wherein the key is a member of an ordered set of pseudo-randomly selected members, the ordered set having a set size that will provide a required period for a pattern of memory cell mutations, with the memory cells being partnered for mutation in accordance with the computed mutation partnering using the key.

23. The method as set forth in claim 19, wherein step (c) comprises performing logical XOR operations on the contents of memory cells of a first memory cell group and the contents of memory cells of a second memory cell group, and storing the results of the logical XOR operations into the first memory cell group if step (c) is being

performed for an odd number of times, and the second memory cell group if step (c) is being performed for an even number of times.

24 The method as set forth in claim 19, wherein the method further comprises the steps of:

d) executing the second of the plurality of subprograms;

e) computing mutation partners for the plurality of memory cells; and

f) mutating the memory cells in accordance with the computed mutation partnering to mutate the first of the plurality of subprograms, and recover a third of the plurality of subprograms for execution.

25. An apparatus comprising:

an execution unit for executing programming instructions; and

a storage medium having stored therein a first plurality of programming instructions to be executed by the execution unit, wherein when executed, in response to a program input, the first plurality of programming instructions generate a plurality of subprograms for the program to obfuscate the program, the subprograms being generated in a mutated form, except for at least one, which is generated in a plaintext form, the subprograms being further generated with logic to recover the subprograms in plaintext form on an as needed basis, one or more but not all at a time.

26. The apparatus as set forth in claim 25, wherein the storage medium further having stored therein a table of keylengths to be accessed by the first plurality of programming instructions in generating the subprograms, the keylengths denoting sizes of ordered sets of pseudo-randomly selected members that will provide various required mutation periods.

27. The apparatus as set forth in claim 25, wherein the storage medium further having stored therein a second plurality of programming instructions to be incorporated into each of the generated subprograms by the first plurality of programming instructions for identifying mutation partners for a plurality of memory cells storing the subprograms, for a mutation round, using a key, the key being a member of an ordered set of pseudo-randomly selected members that will provide a mutation period required by the generated subprograms.

28. The apparatus as set forth in claim 25, wherein the storage medium further having stored therein a second plurality of programming instructions to be incorporated into each of the generated subprograms by the first plurality of programming instructions for mutating memory cells storing the generated subprograms in accordance with computed mutation partnerings for a mutation round.

29. The apparatus as set forth in claim 25, wherein the first plurality of programming instructions include logic for analyzing the program for branch flow.

30. The apparatus as set forth in claim 25, wherein the first plurality of programming instructions include logic for performing peephole randomization on the program.

31. The apparatus as set forth in claim 25, wherein the first plurality of programming instructions include restructuring and partitioning the program into the subprograms.

32. The apparatus as set forth in claim 25, wherein the first plurality of programming instructions include logic for scheduling memory cells for the generated subprograms to be recovered in the plaintext form, and determining the appropriate initial values for the memory cells.

33. The apparatus as set forth in claim 32, wherein the first plurality of programming instructions include logic for determining a mutation period requirement for the program, a keylength for the required mutation period, the keylength denoting a set's set size, the set being an ordered set of pseudo-randomly selected members that will provide the required mutation period.

34. The apparatus as set forth in claim 32, wherein the first plurality of programming instructions include logic for selecting a memory cell for a generated subprogram to be recovered in the plaintext form, and determining a Boolean function for recovering the generated subprogram in the plaintext form in terms of initial state values of the memory cells used for storing the generated subprograms.

35. The apparatus as set forth in claim 32, wherein the first plurality of programming instructions include logic for determining mutation partners for a

plurality of memory cells storing the generated subprograms, using a key of an ordered set of pseudo-randomly selected keys, simulating memory cell mutations in accordance with the determined mutation partnering, and determining a plurality of Boolean functions for the memory cells, the Boolean functions expressing the post mutation states of the memory cells in terms of the memory cells' initial values.

36. A machine implemented method for generating a plurality of subprograms for a program to obfuscate the program, the method comprising the steps:

a) analyzing the program for branch flow;

b) restructuring and partitioning the program into a plurality of subprograms; and

c) determining a schedule in terms of a plurality of memory cells for recovering the subprograms in a plaintext form for execution, and initial state values for the memory cells to store the subprograms in the memory cells in a mutated form, except for at least, which is stored in one of the memory cells in the plaintext form.

37. The machine as set forth in claim 36, wherein step (a) further includes performing peephole randomization on the program.

38. The method as set forth in claim 36, wherein step (c) includes determining a mutation period requirement for the program, a keylength for the required mutation period, the keylength denoting a set's set size, the set being an ordered set of pseudo-randomly selected members that will provide the required mutation period.

39. The method as set forth in claim 36, wherein step (c) includes selecting a memory cell for a generated subprogram to be recovered in the plaintext form, and determining a Boolean function for recovering the generated subprogram in the plaintext form in terms of initial state values of the memory cells used for storing the generated subprograms.

40. The method as set forth in claim 36, wherein step (c) includes determining mutation partners for a plurality of memory cells storing the generated subprograms, using a key of an ordered set of pseudo-randomly selected keys, simulating memory cell mutations in accordance with the determined mutation partnering, and determining a plurality of Boolean functions for the memory cells, the Boolean

functions expressing the post mutation states of the memory cells in terms of the memory cells' initial values.

41. The method as set forth in claim 36, wherein the method further includes step (d) inserting a function and a key into each of the generated subprograms, the function being used for identifying mutation partners for a plurality of memory cells storing the subprograms, for a mutation round, using the key, the key being a member of an ordered set of pseudo-randomly selected members that will provide a mutation period required by the generated subprograms.

42. The method as set forth in claim 36, wherein the method further includes step (d) inserting a function into each of the generated subprograms for mutating memory cells storing the generated subprograms in accordance with computed mutation partnerings for a mutation round.

43. An apparatus comprising:
an execution unit for executing programming instructions;
a storage medium having stored therein a first and a second plurality of programming instructions to be executed by the execution unit, the first and second plurality of programming instructions implementing an application with the first plurality of programming instructions implementing a security sensitive function of the application and the second plurality of programming instructions implementing a non-security sensitive function of the application, the first plurality of programming instructions having incorporated a first defensive technique of distributing a secret in space and in time and/or a second defensive technique of obfuscation to render the first plurality of programming instructions virtually unobservable and unmodifiable during execution.

44. The apparatus as set forth in claim 43, wherein the first plurality of programming instructions incorporated the second defensive technique of obfuscation, including one or more unique ordered sets of pseudo-randomly selected members for generating one or more patterns of memory cell mutations, rendering the application unique from other copies of the application installed on other apparatus.

45. An apparatus comprising:
an execution unit for executing programming instructions;

a storage medium having stored therein a first, a second, a third, and a fourth, plurality of programming instructions to be executed by the execution unit, the first and second plurality of programming instructions implementing a first and a second integrity verification function for a first and a second application respectively, whereas the third and fourth programming instructions implementing a third and a fourth integrity verification function for a system integrity verification program, all four pluralities of programming instructions having incorporated defensive techniques rendering them tamper resistant, the four pluralities of programming instructions jointly implementing an interlocking trust mechanism, requiring the first and the second pluralities of programming instructions each to cooperate with both the third and fourth pluralities of programming instructions to complete any integrity verification on the apparatus.

46. A machine implemented method for verifying integrity on an apparatus, the method comprising the steps of:

a) a first and a second tamper resistant integrity verification function of a first and a second application of the apparatus individually calling a third tamper resistant integrity verification function of a system integrity verification program to jointly perform integrity verification with the first and second tamper resistant integrity verification functions respectively;

b) in response, the third tamper resistant integrity verification function calling a fourth tamper resistant integrity verification function of the system integrity verification program to jointly perform the requested integrity verifications;

c) the fourth tamper resistant integrity verification function providing the first and the second tamper resistant integrity verification functions with respective results of the requested integrity verifications.

47. An apparatus comprising:

an execution unit for executing programming instructions;

a storage medium having stored therein a first and a second plurality of programming instructions to be executed by the execution unit, and a first secret private key, the first and second pluralities of programming instructions implementing a first and a second tamper resistant decryption function,

the first tamper resistant decryption function being used for recovering a first public key asymmetric to the first secret private key, using a second public

key, the first public key having been previously encrypted using a second secret private key asymmetric to the second public key,

the second tamper resistant decryption function being used for recovering a content encryption key using the first secret private key, the content encryption key having been previously encrypted using the first public key.

48. The apparatus as set forth in claim 47, wherein the storage medium further having stored therein a third plurality of programming instructions to be executed by the execution unit, the third plurality of programming instructions implementing a third decryption function for recovering content using the recovered content encryption key, the content having been previously encrypted using the content encryption key.

49. A machine implemented method for recovering content, the method comprising the steps of:

a) recovering a first public key using a second public key, the first and second public keys having a first and a second asymmetric private key respectively, the first public key having been previously encrypted by the second private key;

b) providing the recovered first public key to be used for encrypting a content encryption key;

c) receiving the encrypted content encryption key; and

d) recovering the content encryption key using the first private key.

50. The method as set forth in claim 47, wherein the method further comprises the steps of:

e) receiving encrypted content; and

f) recovering content using the recovered content encryption key.

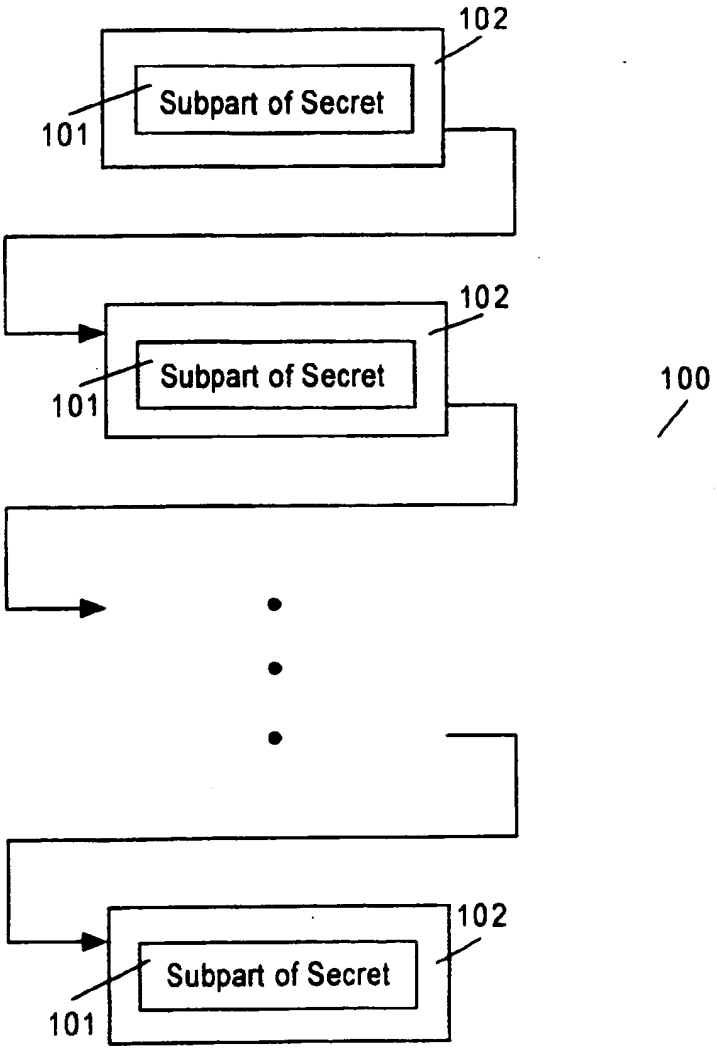

102
Subpart of Secret
101
102
Subpart of Secret
101
100
102
Subpart of Secret
101

Figure 1

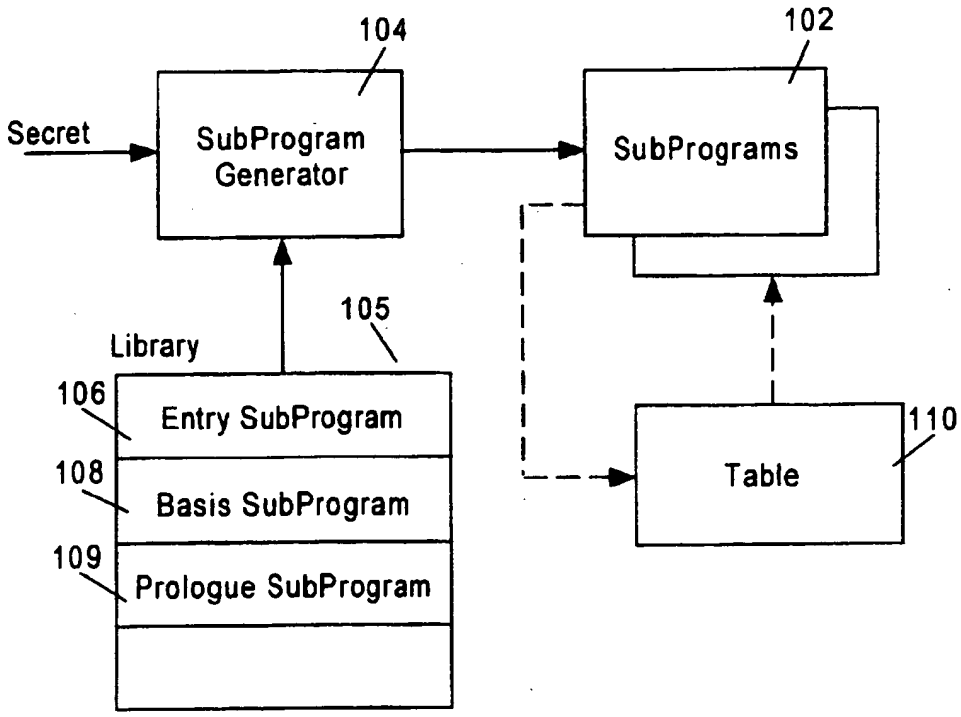

104
102
Secret
SubProgram Generator
SubPrograms
105
Library
106
Entry SubProgram
108
Basis SubProgram
109
Prologue SubProgram
110
Table

Figure 2

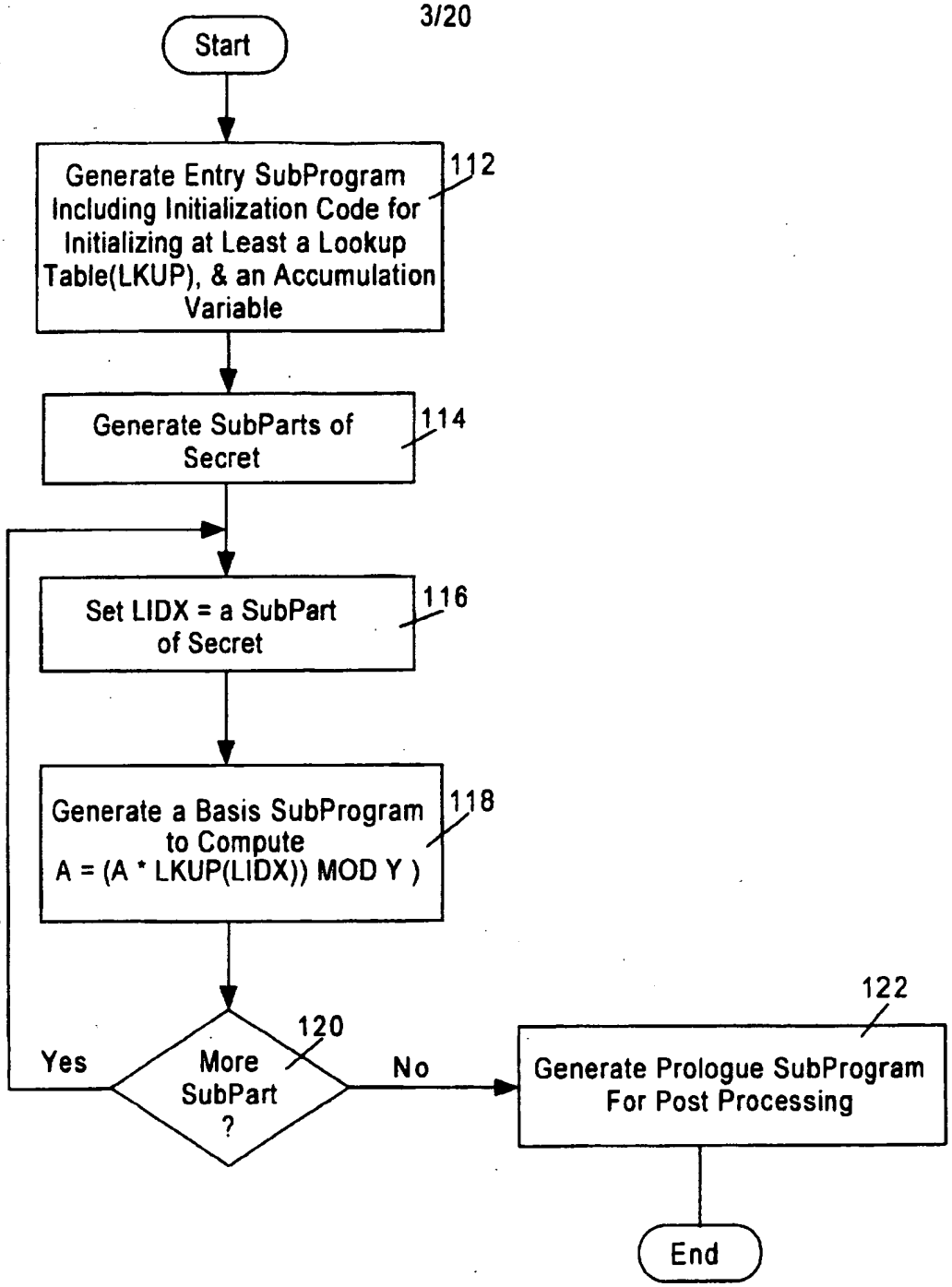

Start
Generate Entry SubProgram Including Initialization Code for Initializing at Least a Lookup Table(LKUP), & an Accumulation Variable
112
Generate SubParts of Secret
114
Set LIDX = a SubPart of Secret
116
Generate a Basis SubProgram to Compute A = (A * LKUP(LIDX)) MOD Y)
118
More SubPart ?
120
Yes
No
Generate Prologue SubProgram For Post Processing
122
End

Figure 3

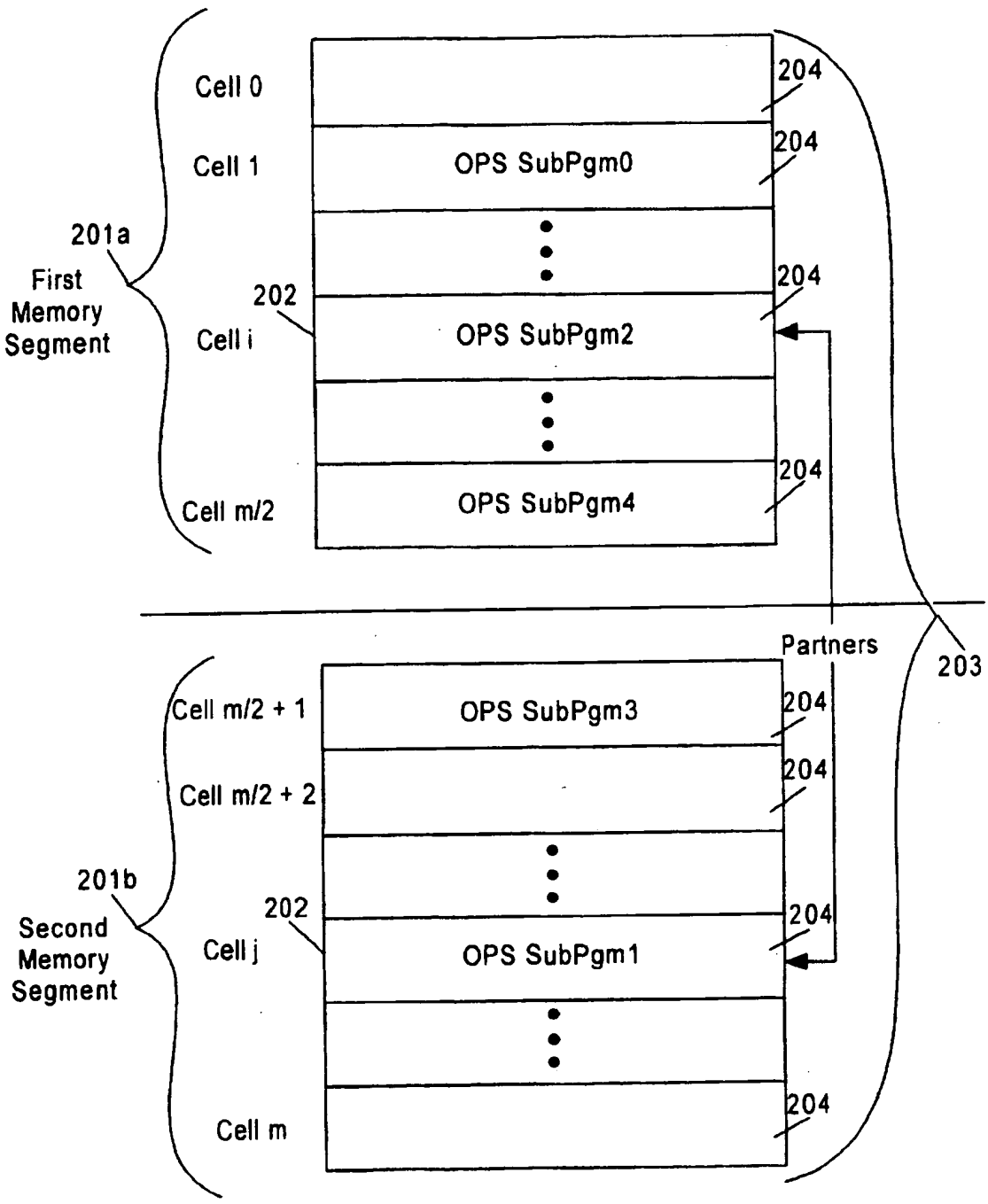

Cell 0
Cell 1
Cell i
Cell m/2
OPS SubPgm0
OPS SubPgm2
OPS SubPgm4
204
201a
First Memory Segment
202
Partners
203
Cell m/2 + 1
Cell m/2 + 2
Cell j
Cell m
OPS SubPgm3
OPS SubPgm1
201b
Second Memory Segment

Figure 4

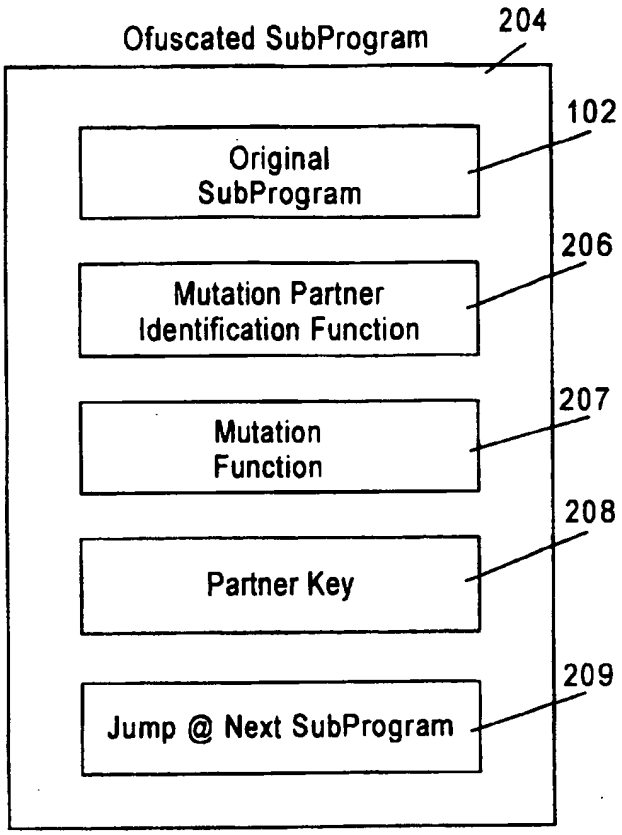

Ofuscated SubProgram
204
Original SubProgram
102
Mutation Partner Identification Function
206
Mutation Function
207
Partner Key
208
Jump @ Next SubProgram
209

Figure 5

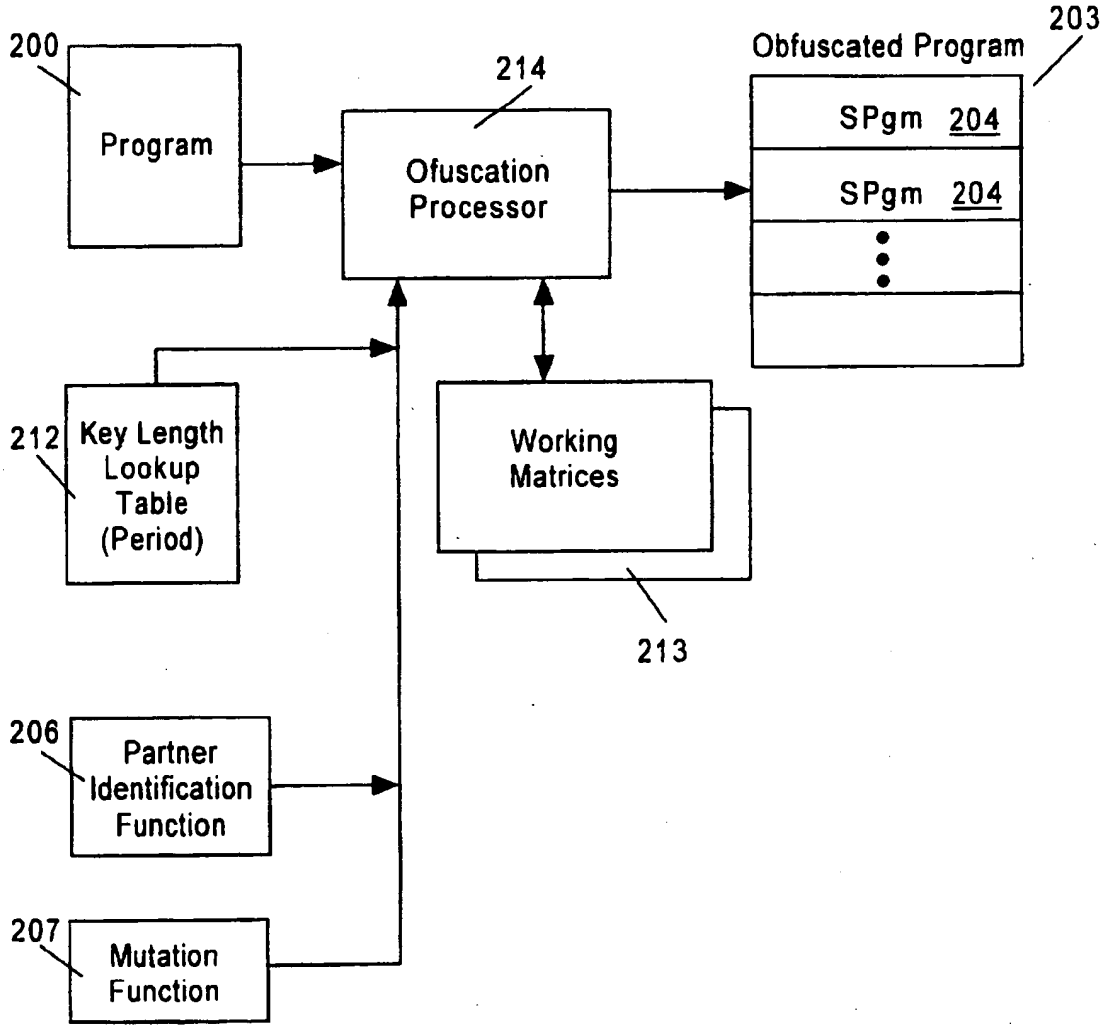

200
Program
214
Ofuscation Processor
Obfuscated Program
203
SPgm 204
SPgm 204
212
Key Length Lookup Table (Period)
Working Matrices
213
206
Partner Identification Function
207
Mutation Function

Figure 6

Distribution of Key Period

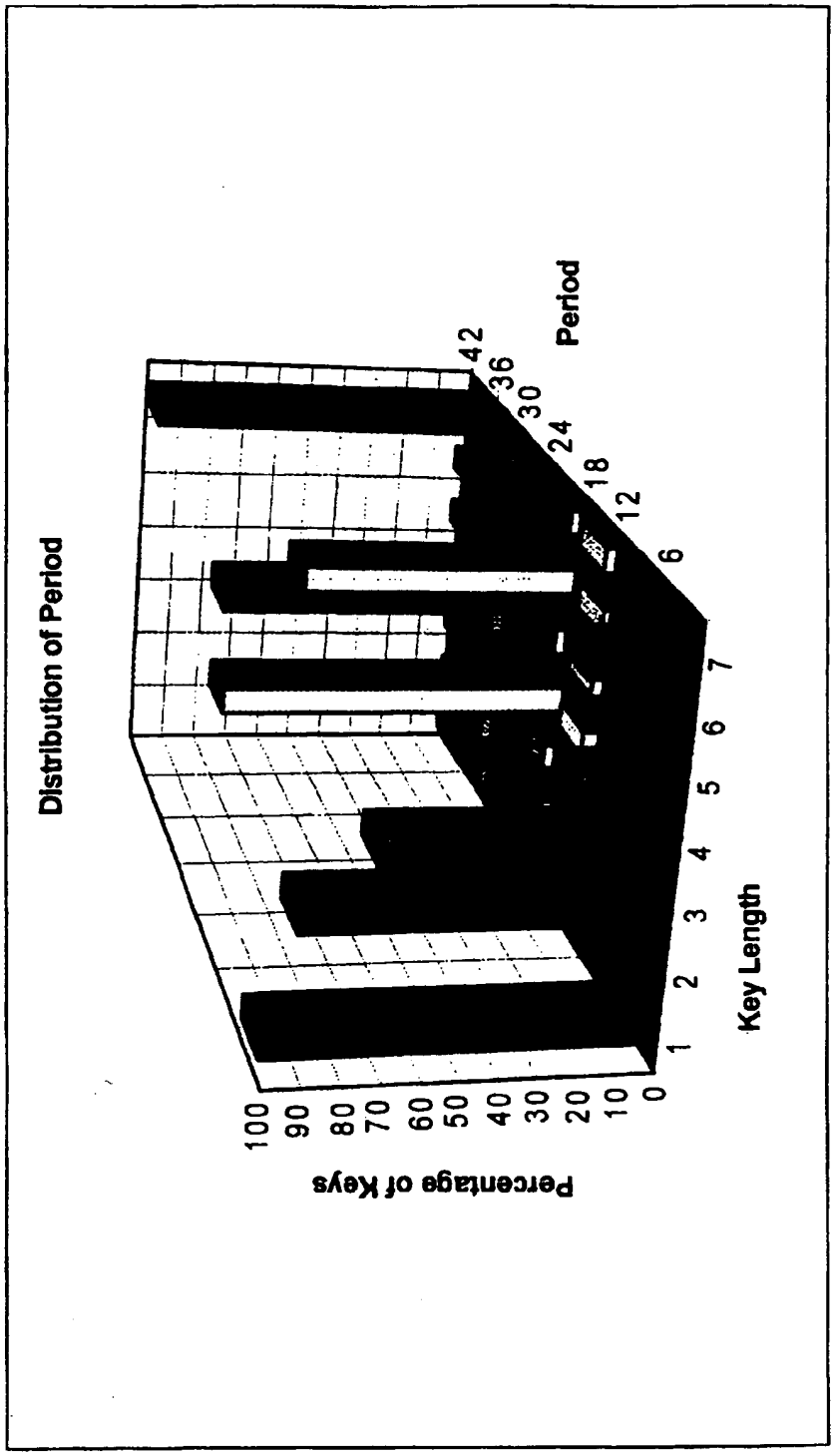


Figure 7

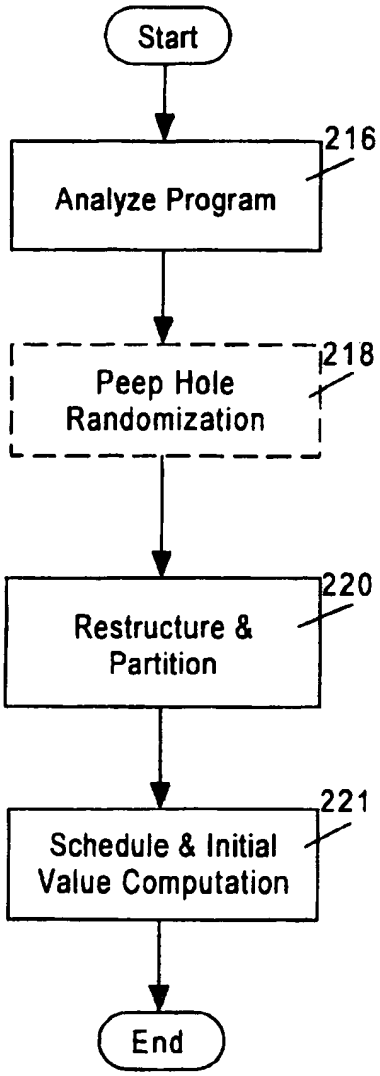

Start
Analyze Program
216
Peep Hole Randomization
218
Restructure & Partition
220
Schedule & Initial Value Computation
221
End

Figure 8a

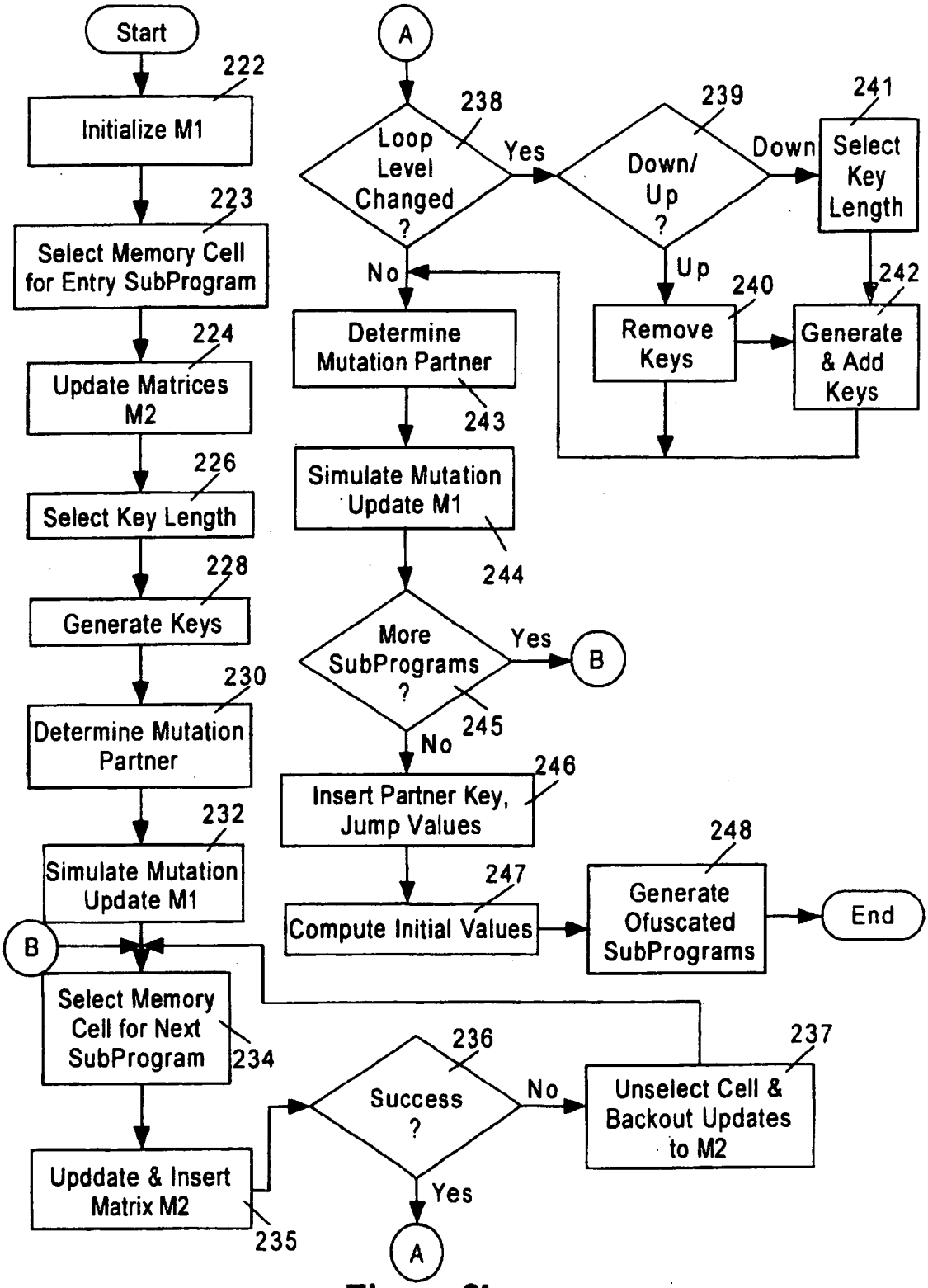

Start
222
Initialize M1
223
Select Memory Cell for Entry SubProgram
224
Update Matrices M2
226
Select Key Length
228
Generate Keys
230
Determine Mutation Partner
232
Simulate Mutation Update M1
B
Select Memory Cell for Next SubProgram
234
Upddate & Insert Matrix M2
235
A
238
Loop Level Changed ?
Yes
239
Down/ Up ?
Down
241
Select Key Length
242
Generate & Add Keys
Up
240
Remove Keys
No
Determine Mutation Partner
243
Simulate Mutation Update M1
244
More SubPrograms ?
Yes
B
245
No
246
Insert Partner Key, Jump Values
247
Compute Initial Values
248
Generate Ofuscated SubPrograms
End
236
Success ?
No
237
Unselect Cell & Backout Updates to M2
Yes
A

Figure 8b

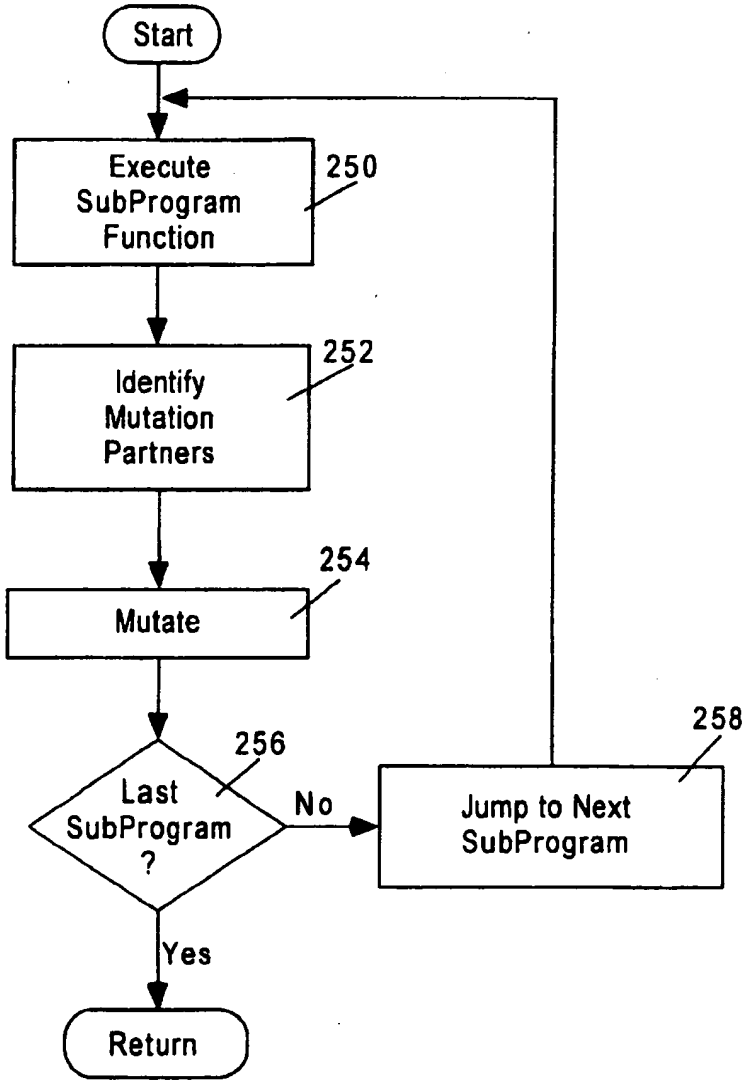

Start
Execute SubProgram Function
250
Identify Mutation Partners
252
Mutate
254
Last SubProgram ?
256
No
Jump to Next SubProgram
258
Yes
Return

Figure 9

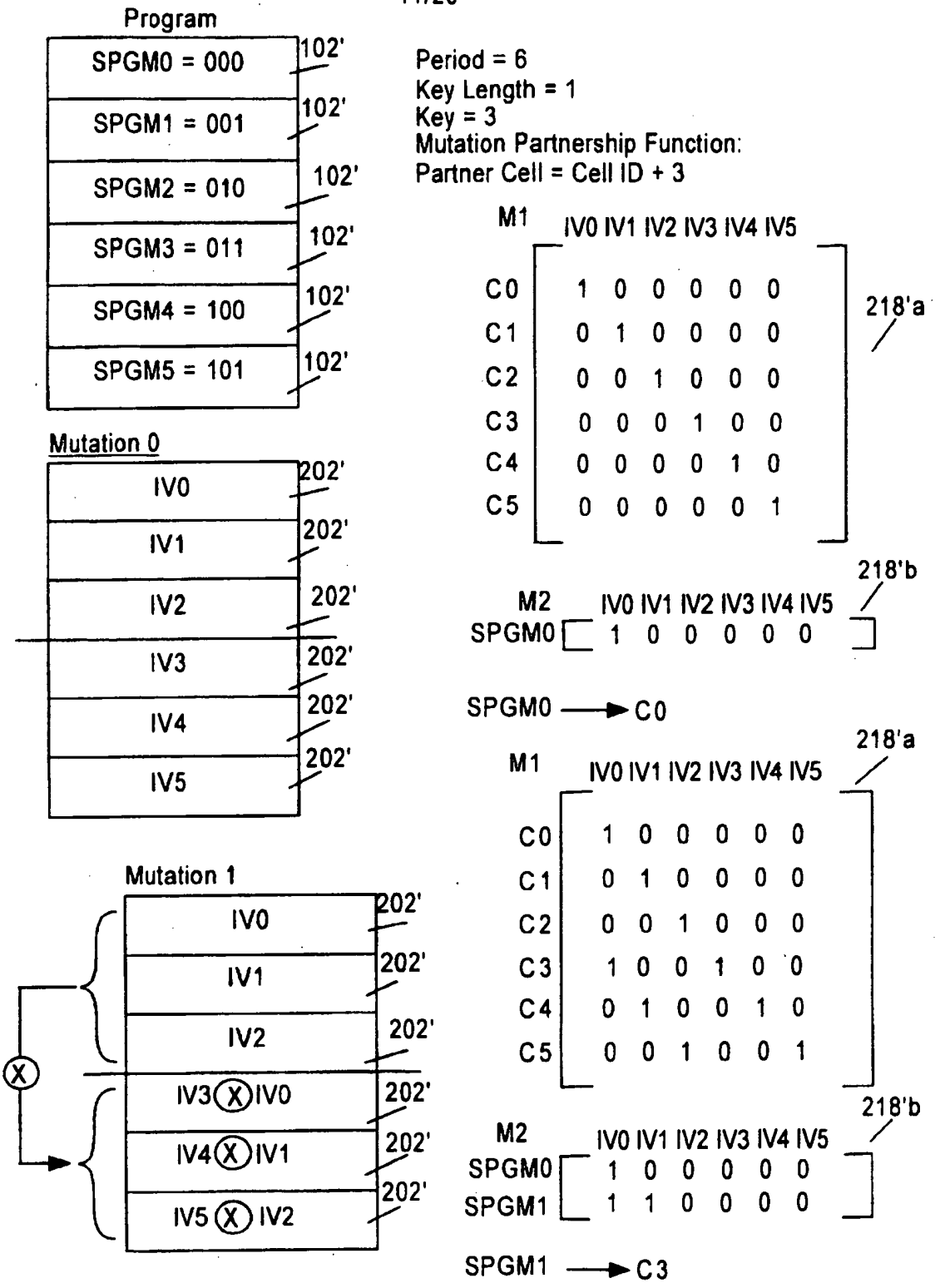

Program
SPGM0 = 000
SPGM1 = 001
SPGM2 = 010
SPGM3 = 011
SPGM4 = 100
SPGM5 = 101
102'
Mutation 0
IV0
IV1
IV2
IV3
IV4
IV5
202'
Mutation 1
IV3 X IV0
IV4 X IV1
IV5 X IV2
Period = 6
Key Length = 1
Key = 3
Mutation Partnership Function:
Partner Cell = Cell ID + 3
M1
IV0 IV1 IV2 IV3 IV4 IV5
C0 1 0 0 0 0 0
C1 0 1 0 0 0 0
C2 0 0 1 0 0 0
C3 0 0 0 1 0 0
C4 0 0 0 0 1 0
C5 0 0 0 0 0 1
218'a
M2
SPGM0 1 0 0 0 0 0
218'b
SPGM0 → C0
M1
C0 1 0 0 0 0 0
C1 0 1 0 0 0 0
C2 0 0 1 0 0 0
C3 1 0 0 1 0 0
C4 0 1 0 0 1 0
C5 0 0 1 0 0 1
M2
SPGM0 1 0 0 0 0 0
SPGM1 1 1 0 0 0 0
SPGM1 → C3

Figure 10

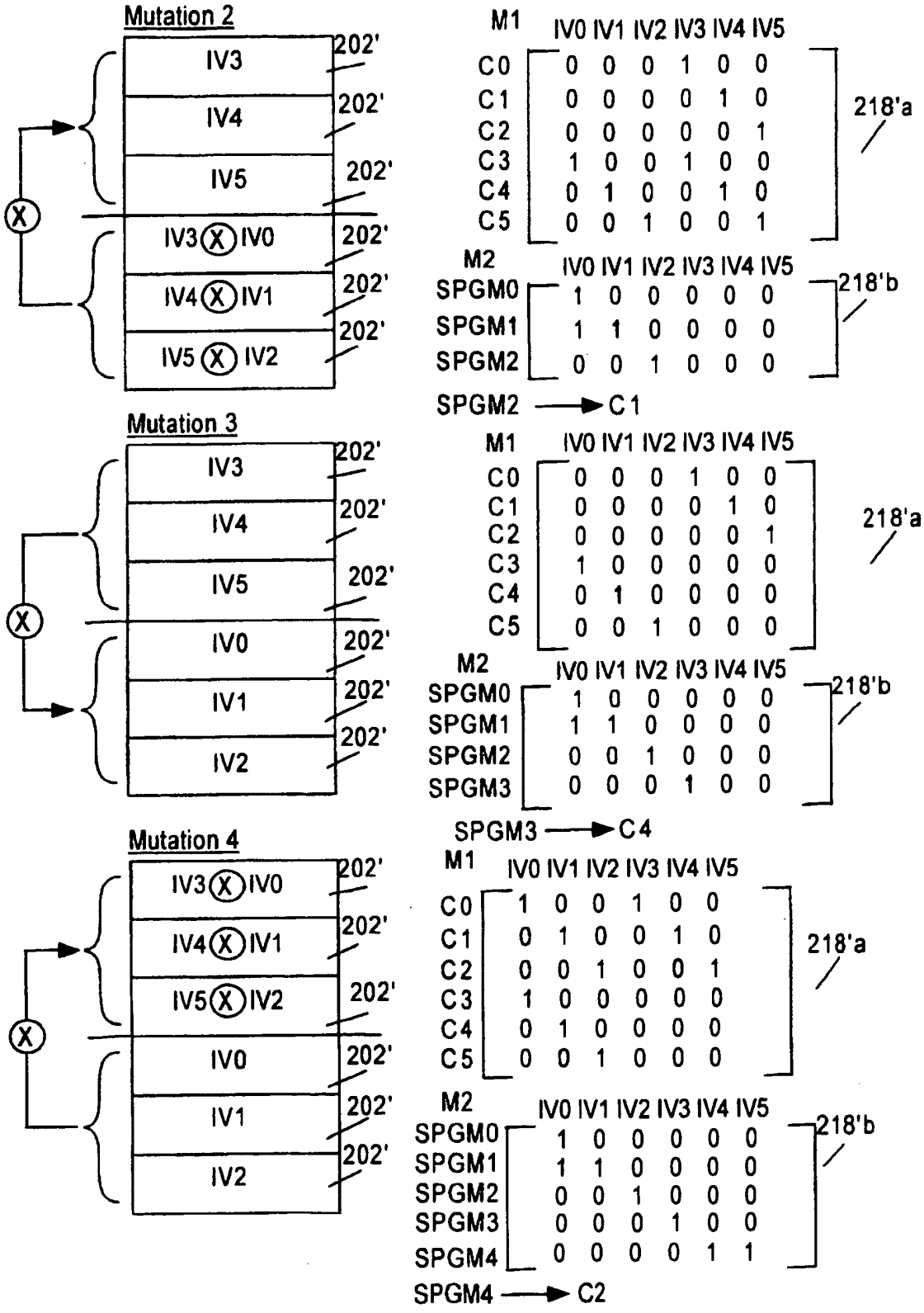

Mutation 2
IV3
IV4
IV5
IV3 X IV0
IV4 X IV1
IV5 X IV2
202'
M1
IV0 IV1 IV2 IV3 IV4 IV5
C0 0 0 0 1 0 0
C1 0 0 0 0 1 0
C2 0 0 0 0 0 1
C3 1 0 0 1 0 0
C4 0 1 0 0 1 0
C5 0 0 1 0 0 1
218'a
M2
IV0 IV1 IV2 IV3 IV4 IV5
SPGM0 1 0 0 0 0 0
SPGM1 1 1 0 0 0 0
SPGM2 0 0 1 0 0 0
218'b
SPGM2 → C1
Mutation 3
IV3
IV4
IV5
IV0
IV1
IV2
M1
IV0 IV1 IV2 IV3 IV4 IV5
C0 0 0 0 1 0 0
C1 0 0 0 0 1 0
C2 0 0 0 0 0 1
C3 1 0 0 0 0 0
C4 0 1 0 0 0 0
C5 0 0 1 0 0 0
218'a
M2
IV0 IV1 IV2 IV3 IV4 IV5
SPGM0 1 0 0 0 0 0
SPGM1 1 1 0 0 0 0
SPGM2 0 0 1 0 0 0
SPGM3 0 0 0 1 0 0
218'b
SPGM3 → C4
Mutation 4
IV3 X IV0
IV4 X IV1
IV5 X IV2
IV0
IV1
IV2
M1
IV0 IV1 IV2 IV3 IV4 IV5
C0 1 0 0 1 0 0
C1 0 1 0 0 1 0
C2 0 0 1 0 0 1
C3 1 0 0 0 0 0
C4 0 1 0 0 0 0
C5 0 0 1 0 0 0
218'a
M2
IV0 IV1 IV2 IV3 IV4 IV5
SPGM0 1 0 0 0 0 0
SPGM1 1 1 0 0 0 0
SPGM2 0 0 1 0 0 0
SPGM3 0 0 0 1 0 0
SPGM4 0 0 0 0 1 1
218'b
SPGM4 → C2

Figure 11

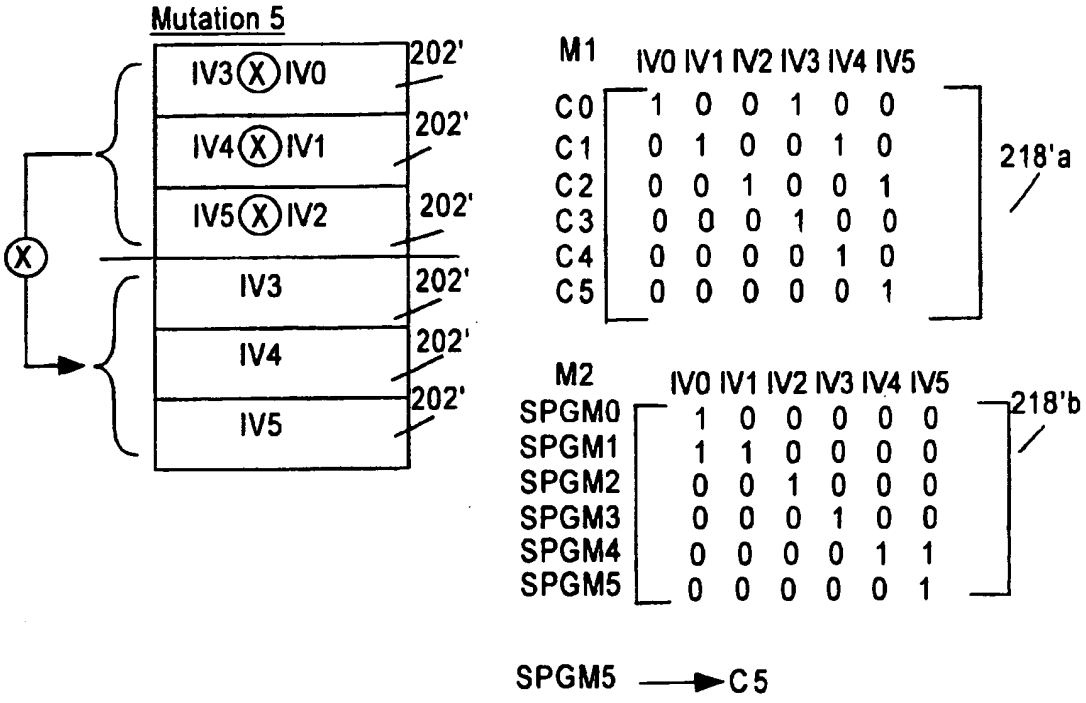

Mutation 5
IV3 X IV0
IV4 X IV1
IV5 X IV2
IV3
IV4
IV5
202'
M1
IV0 IV1 IV2 IV3 IV4 IV5
C0 1 0 0 1 0 0
C1 0 1 0 0 1 0
C2 0 0 1 0 0 1
C3 0 0 0 1 0 0
C4 0 0 0 0 1 0
C5 0 0 0 0 0 1
218'a
M2
IV0 IV1 IV2 IV3 IV4 IV5
SPGM0 1 0 0 0 0 0
SPGM1 1 1 0 0 0 0
SPGM2 0 0 1 0 0 0
SPGM3 0 0 0 1 0 0
SPGM4 0 0 0 0 1 1
SPGM5 0 0 0 0 0 1
218'b
SPGM5 → C5

Figure 12

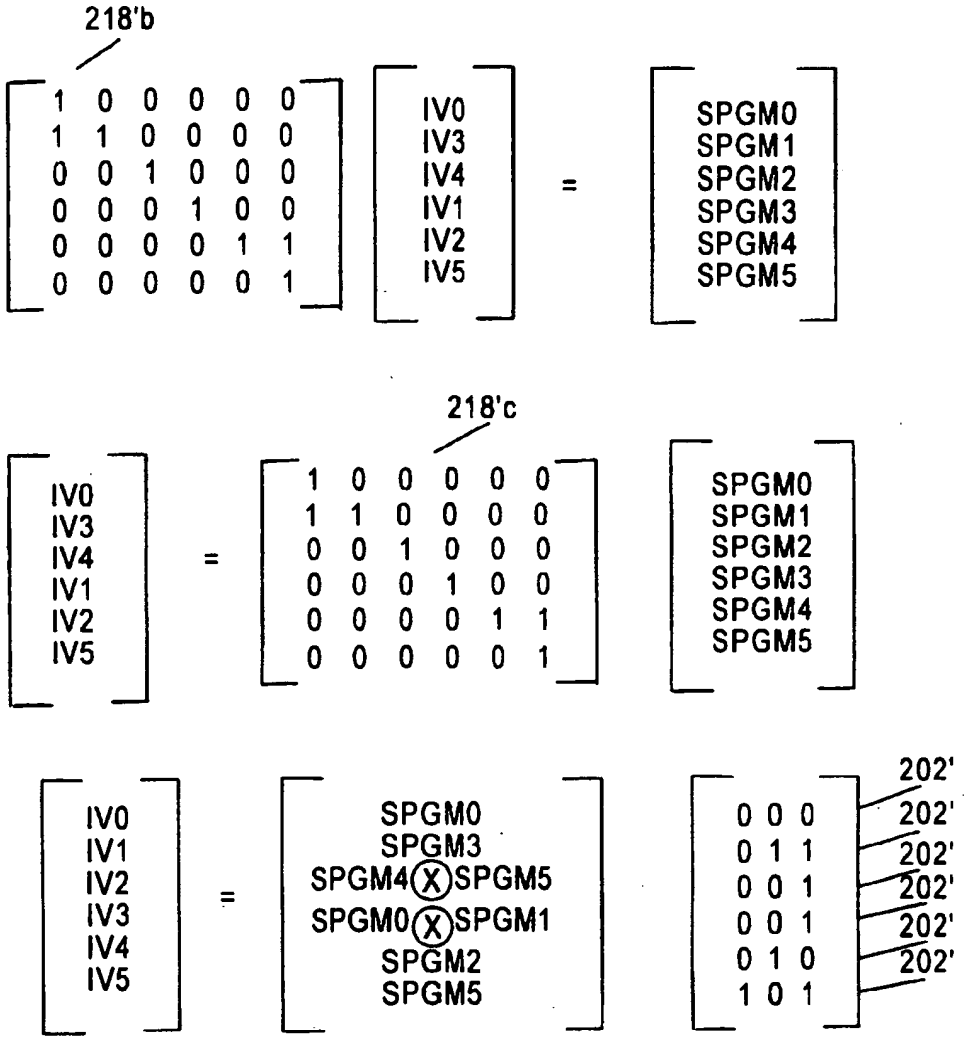

218'b
1 0 0 0 0 0
1 1 0 0 0 0
0 0 1 0 0 0
0 0 0 1 0 0
0 0 0 0 1 1
0 0 0 0 0 1
IV0 IV3 IV4 IV1 IV2 IV5
=
SPGM0 SPGM1 SPGM2 SPGM3 SPGM4 SPGM5
218'c
IV0 IV3 IV4 IV1 IV2 IV5
=
SPGM0 SPGM1 SPGM2 SPGM3 SPGM4 SPGM5
IV0 IV1 IV2 IV3 IV4 IV5
=
SPGM0
SPGM3
SPGM4 X SPGM5
SPGM0 X SPGM1
SPGM2
SPGM5
0 0 0
0 1 1
0 0 1
0 0 1
0 1 0
1 0 1
202'
202'
202'
202'
202'
202'

Figure 13

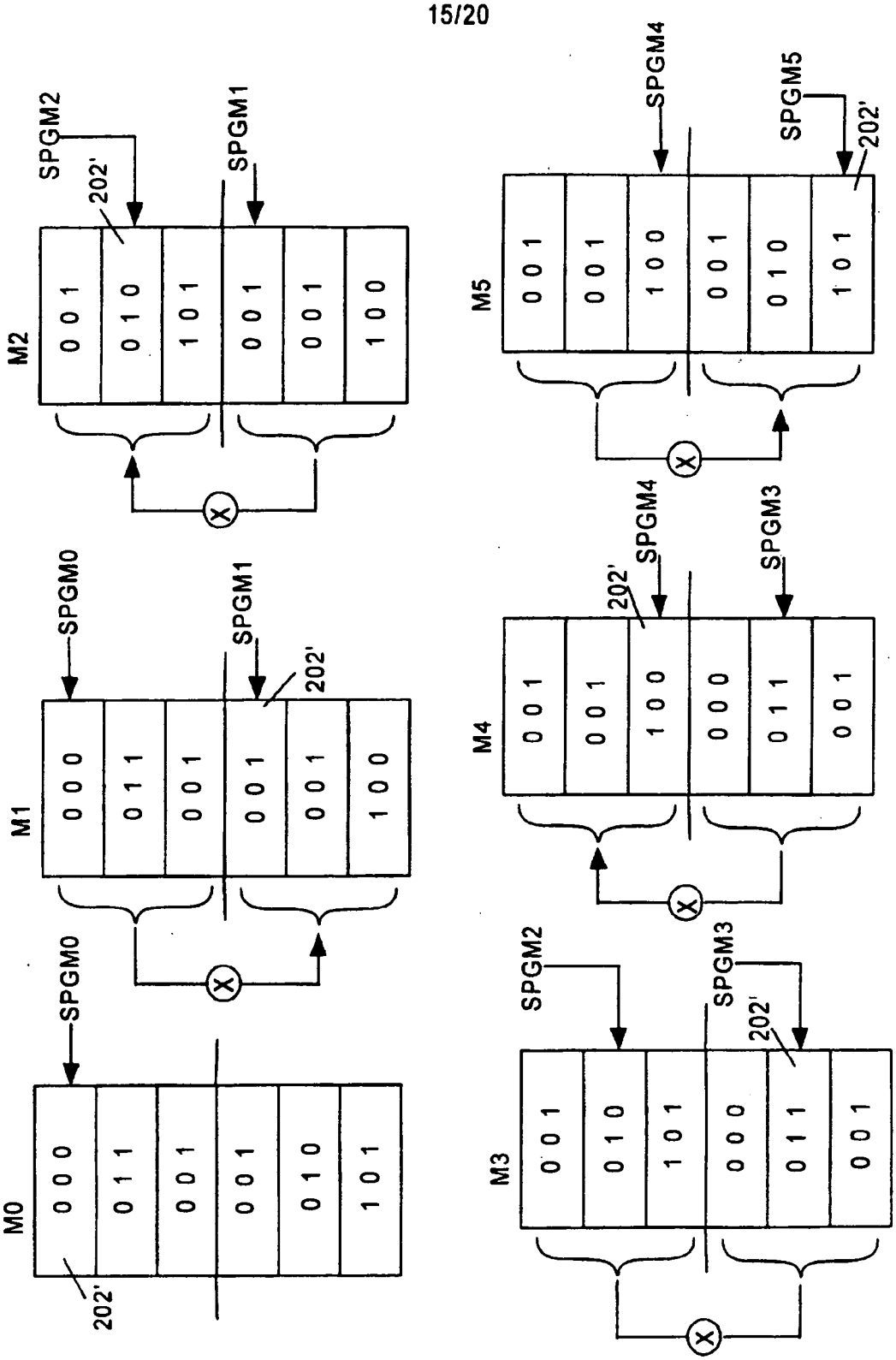

M2
SPGM2
202'
SPGM1
0 0 1
0 1 0
1 0 1
0 0 1
0 0 1
1 0 0
M5
SPGM4
SPGM5
202'
0 0 1
0 0 1
1 0 0
0 0 1
0 1 0
1 0 1
M1
SPGM0
SPGM1
202'
0 0 0
0 1 1
0 0 1
0 0 1
0 0 1
1 0 0
M4
202'
SPGM4
SPGM3
0 0 1
0 0 1
1 0 0
0 0 0
0 1 1
0 0 1
M0
SPGM0
202'
0 0 0
0 1 1
0 0 1
0 0 1
0 1 0
1 0 1
M3
SPGM2
SPGM3
202'
0 0 1
0 1 0
1 0 1
0 0 0
0 1 1
0 0 1

Figure 14

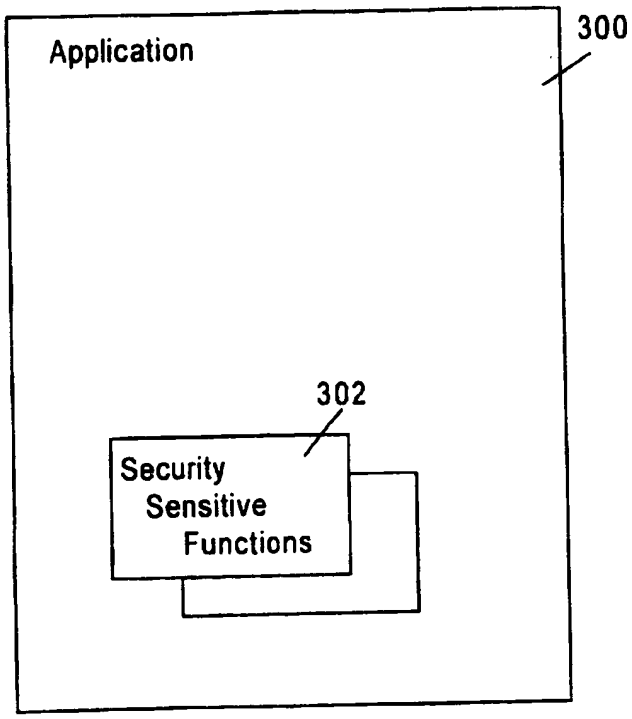


Figure 15

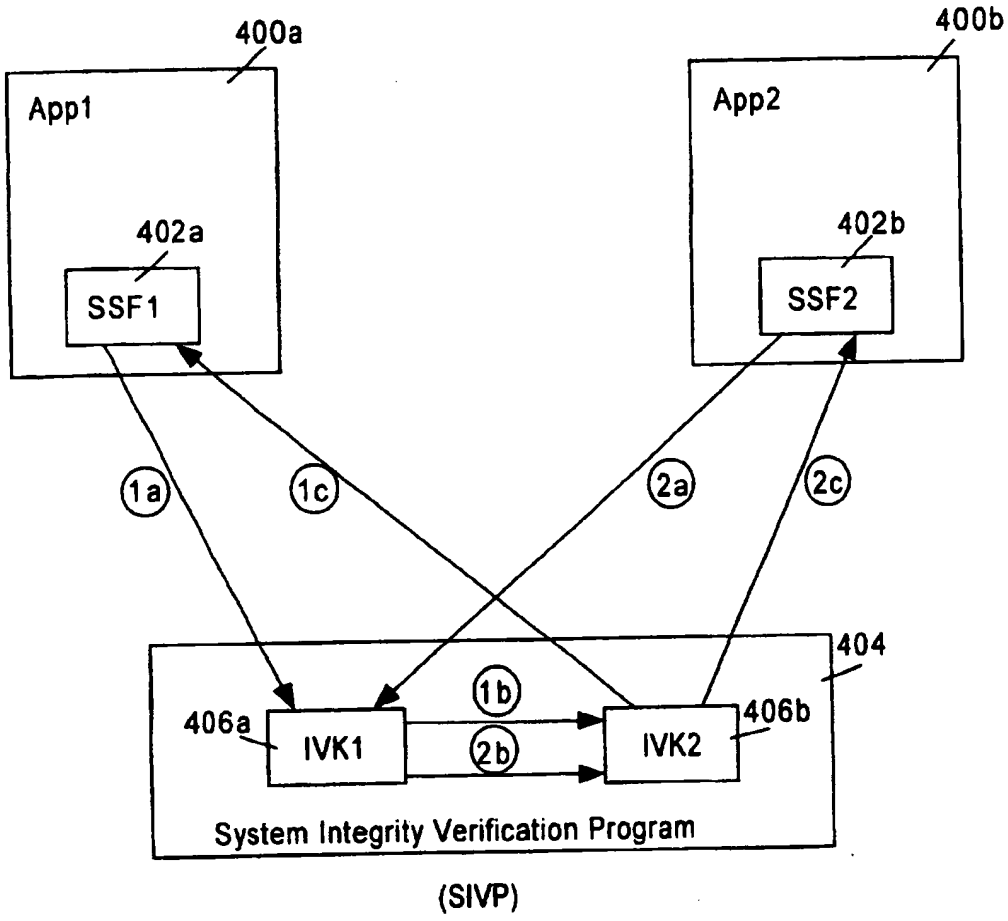

400a
App1
402a
SSF1
400b
App2
402b
SSF2
1a
1c
2a
2c
404
1b
406a
IVK1
2b
IVK2
406b
System Integrity Verification Program
(SIVP)

Figure 16

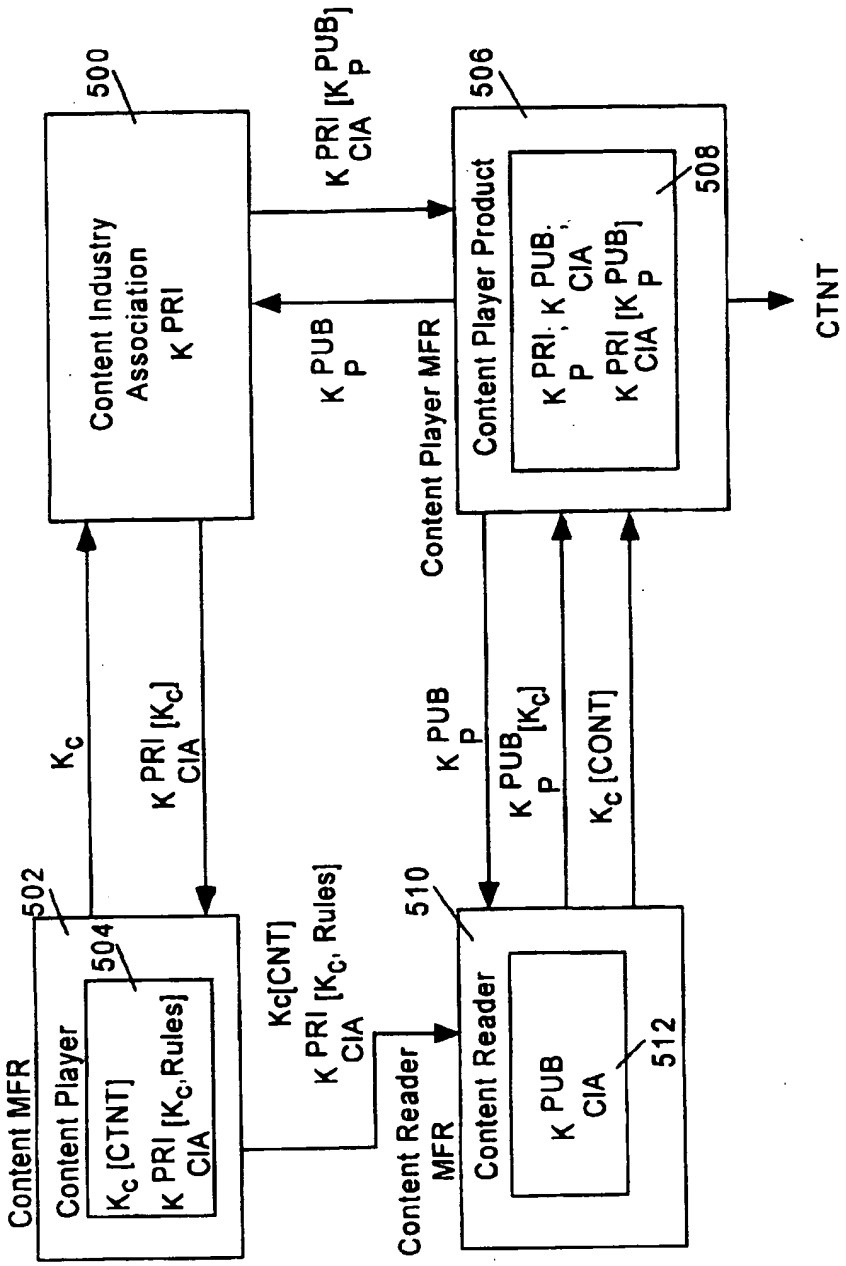

500
Content Industry Association
K PRI
506
Content Player Product
508
K PRI, K PUB, CIA
K PRI CIA [K PUB P]
K PRI CIA [K PUB P]
K PUB P
Content Player MFR
CTNT
Kc
K PRI CIA [Kc]
K PUB P
K PUB P [Kc]
Kc [CONT]
502
Content MFR
Content Player
504
Kc [CTNT]
K PRI CIA [Kc, Rules]
Kc[CNT]
K PRI CIA [Kc, Rules]
510
Content Reader MFR
Content Reader
K PUB CIA
512

Figure 17

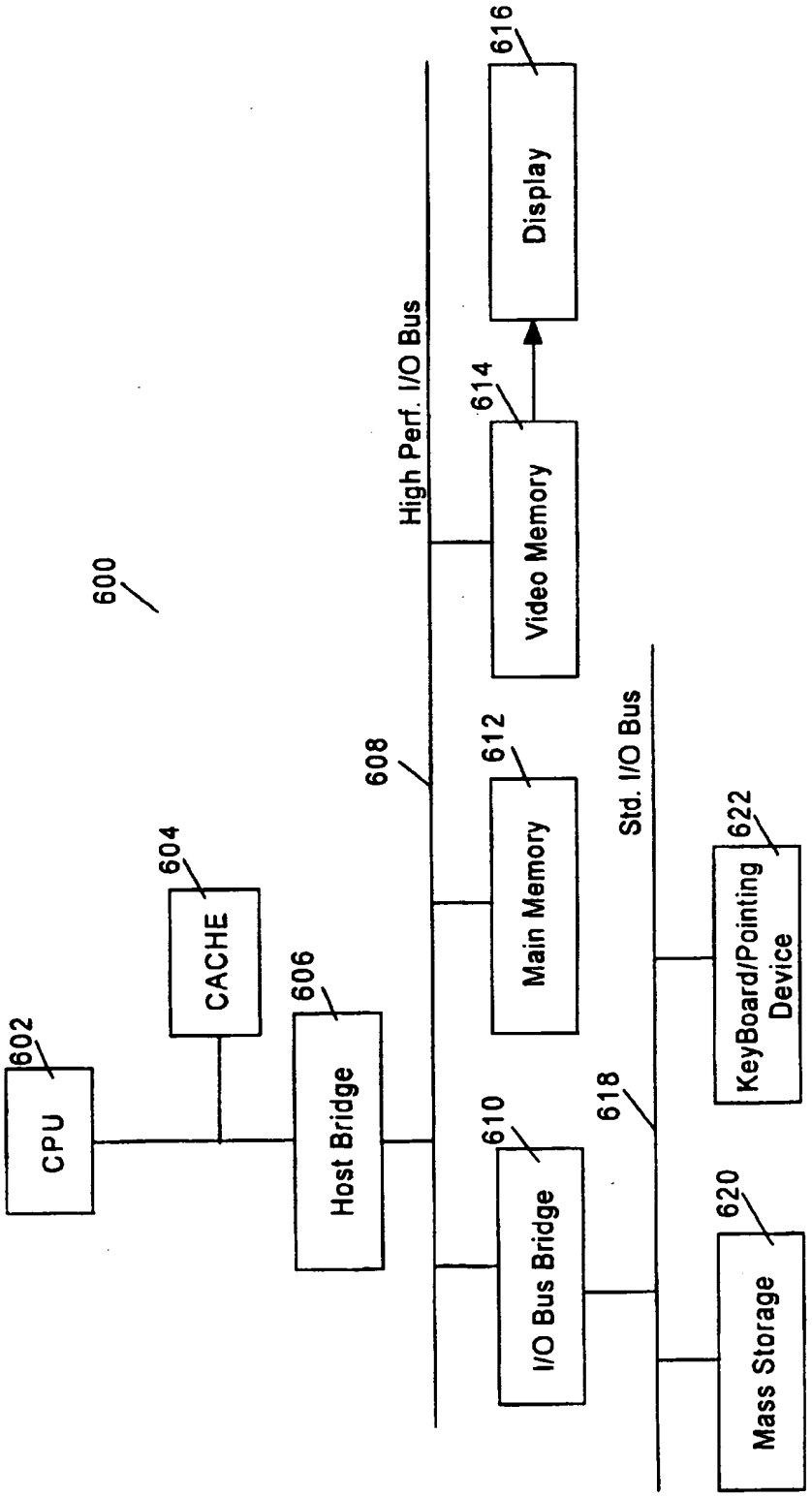

600
602
CPU
604
CACHE
606
Host Bridge
608
High Perf. I/O Bus
610
I/O Bus Bridge
612
Main Memory
614
Video Memory
616
Display
618
Std. I/O Bus
620
Mass Storage
622
KeyBoard/Pointing Device

Figure 18

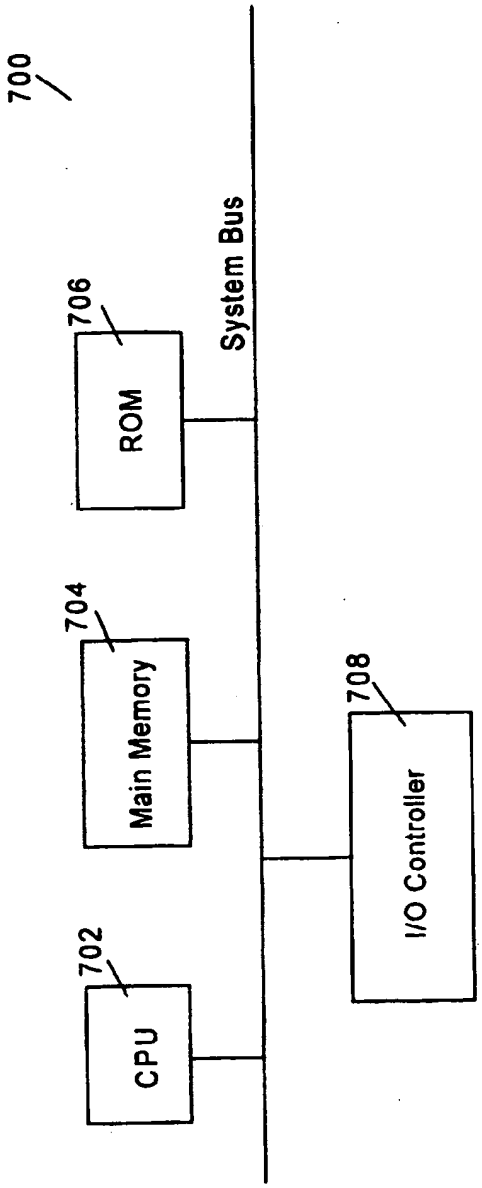

700
System Bus
706
ROM
704
Main Memory
708
I/O Controller
702
CPU

Figure 19

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/10359

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04K 1/00
US CL :395/186

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 395/186, 187.01, 188.01; 380/ 4, 23, 24

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

APS, STN (WPIDS)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 4,786,790 (KRUSE et al.) 22 November 1988, see the abstract, see col. 2, lines 20-56.	10-12, 19-24, 36-42
Y	US 4,926,480 (CHAUM) 15 May 1990, see the abstract	1-50
Y	US 5,224,160 (PAULINI et al.) 29 June 1993, see the abstract and col. 6, lines 28-45.	1-50
Y	US 5,265,164 (MATYAS et al.) 23 November 1993, see fig. 10.	1-50

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"B" earlier document published on or after the international filing date

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
22 AUGUST 1997	05 NOV 1997

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	ALBERT DECADY
Facsimile No. (703) 305-3230	Telephone No. (703) 308-3900

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/10359

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X ---- Y	US 5,347,579 (BLANDFORD) 13 September 1994, col. 5, lines 24-56.	1-9, 25-35, 43-50 ---------- 10-12, 19-24, 36-42
Y	US 5,535,276 (GANESAN) 09 July 1996, see the abstract, col. 2, lines 55-62, col. 10, lines 33 et seq.	1-50

Form PCT/ISA/210 (continuation of second sheet)(July 1992)*

Requested Patent: WO9624092A2

Title:

A METHOD AND SYSTEM FOR MANAGING A DATA OBJECT SO AS TO COMPLY WITH PREDETERMINED CONDITIONS FOR USAGE ;

Abstracted Patent: WO9624092 ;

Publication Date: 1996-08-08 ;

Inventor(s): BENSON GREG (SE); URICH GREGORY H (SE) ;

Applicant(s): BENSON GREG (SE); URICH GREGORY H (SE) ;

Application Number: WO1996SE00115 19960201 ;

Priority Number(s): SE19950000355 19950201 ;

IPC Classification: G06F1/00; G06F12/14 ;

Equivalents:

AU4681496, EP0807283 (WO9624092), A3, JP10513289T, SE504085, SE9500355, US5845281 ;

ABSTRACT:

The present invention relates to a method and a system for managing a data object so as to comply with predetermined conditions for usage of the data object. To control the usage of the data object, a set of control data, defining usages of the data object which comply with the predetermined conditions, is created for the data object. The data object is concatenated with the user set of control data, encrypted and transferred to the user. When the user wants to use the data object, a special user program checks whether the usage complies with the control data. If so, the usage is enabled. Otherwise it is disabled.

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 1/00, 12/14 — A2

(11) International Publication Number: **WO 96/24092**

(43) International Publication Date: 8 August 1996 (08.08.96)

(21) International Application Number: PCT/SE96/00115

(22) International Filing Date: 1 February 1996 (01.02.96)

(30) Priority Data:
9500355-4 1 February 1995 (01.02.95) SE

(71)(72) Applicant and Inventor: BENSON, Greg [US/SE]; Dalbackavägen 3, S-240 10 Dalby (SE).

(72) Inventor; and

(75) Inventor/Applicant *(for US only)*: URICH, Gregory, H. [US/SE]; Warholmsvägen 8 B, S-224 65 Lund (SE).

(74) Agent: AWAPATENT AB; P.O. Box 5117, S-200 71 Malmö (SE).

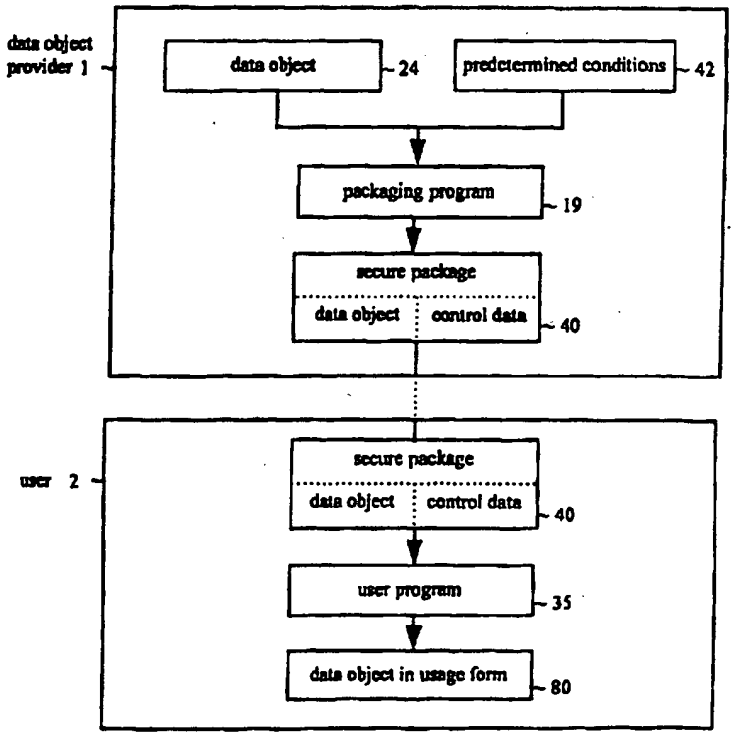
(81) Designated States: AL, AM, AT, AT (Utility model), AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, CZ (Utility model), DE, DE (Utility model), DK, DK (Utility model), EE, EE (Utility model), ES, FI, FI (Utility model), GB, GE, HU, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SK (Utility model), TJ, TM, TR, TT, UA, UG, US, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AZ, BY, KG, KZ, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: A METHOD AND SYSTEM FOR MANAGING A DATA OBJECT SO AS TO COMPLY WITH PREDETERMINED CONDITIONS FOR USAGE

(57) Abstract

The present invention relates to a method and a system for managing a data object so as to comply with predetermined conditions for usage of the data object. To control the usage of the data object, a set of control data, defining usages of the data object which comply with the predetermined conditions, is created for the data object. The data object is concatenated with the user set of control data, encrypted and transferred to the user. When the user wants to use the data object, a special user program checks whether the usage complies with the control data. If so, the usage is enabled. Otherwise it is disabled.



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AM	Armenia	**GB**	United Kingdom	**MW**	Malawi
AT	Austria	**GE**	Georgia	**MX**	Mexico
AU	Australia	**GN**	Guinea	**NE**	Niger
BB	Barbados	**GR**	Greece	**NL**	Netherlands
BE	Belgium	**HU**	Hungary	**NO**	Norway
BF	Burkina Faso	**IE**	Ireland	**NZ**	New Zealand
BG	Bulgaria	**IT**	Italy	**PL**	Poland
BJ	Benin	**JP**	Japan	**PT**	Portugal
BR	Brazil	**KE**	Kenya	**RO**	Romania
BY	Belarus	**KG**	Kyrgystan	**RU**	Russian Federation
CA	Canada	**KP**	Democratic People's Republic of Korea	**SD**	Sudan
CF	Central African Republic			**SE**	Sweden
CG	Congo	**KR**	Republic of Korea	**SG**	Singapore
CH	Switzerland	**KZ**	Kazakhstan	**SI**	Slovenia
CI	Côte d'Ivoire	**LI**	Liechtenstein	**SK**	Slovakia
CM	Cameroon	**LK**	Sri Lanka	**SN**	Senegal
CN	China	**LR**	Liberia	**SZ**	Swaziland
CS	Czechoslovakia	**LT**	Lithuania	**TD**	Chad
CZ	Czech Republic	**LU**	Luxembourg	**TG**	Togo
DE	Germany	**LV**	Latvia	**TJ**	Tajikistan
DK	Denmark	**MC**	Monaco	**TT**	Trinidad and Tobago
EE	Estonia	**MD**	Republic of Moldova	**UA**	Ukraine
ES	Spain	**MG**	Madagascar	**UG**	Uganda
FI	Finland	**ML**	Mali	**US**	United States of America
FR	France	**MN**	Mongolia	**UZ**	Uzbekistan
GA	Gabon	**MR**	Mauritania	**VN**	Viet Nam

A METHOD AND SYSTEM FOR MANAGING A DATA OBJECT SO AS TO COMPLY WITH PREDETERMINED CONDITIONS FOR USAGE

Technical Field

The present invention relates to data processing and more particularly to a method and a system for managing data objects so as to comply with predetermined conditions for usage.

Background

Much has been written recently regarding the puzzle of universal connectivity. A typical vision of the data highway has long distance high speed data carriers interconnecting regional networks which provide telecommunications services and a wide range of interactive on-line services to consumers. Many of the pieces are already in place, others are in development or testing. In fact, even though the data highway is under construction it is currently open to limited traffic. On-line services are springing up daily and video on demand services are currently being tested.

The potential to benefit society is immense. The scope of information available to consumers will become truly global as the traditional barriers to entry for distribution of, and access to, information are lowered dramatically. This means that more diverse and specialized information will be made available just as conveniently as generic sources from major vendors used to be. The end result is that organizations and individuals will be empowered in ways heretofore only imagined.

However, a fully functioning data highway will only be as valuable as the actual services which it provides. Services envisioned for the data highway that involve the delivery of data objects (e.g. books, films, video, news, music, software, games, etc.) will be and are currently limited by the availability of such objects. Library and educational services are similarly affected. Before owners will allow their data objects to be offered they

must be assured of royalty payments and protection from piracy.

Encryption is a key component of any solution to provide copy protection. But encryption alone is not enough. During transmission and storage the data objects will be protected by encryption, but as soon as anyone is given the key to decipher the content he will have unlimited control over it. Since the digital domain permits data objects to be reproduced in unlimited quantities with no loss of quality, each object will need to be protected from unlimited use and unauthorized reproduction and resale.

The protection problem must not be solved by a separate solution for each particular data format, because then the progress will indeed be slow. It is important to consider the effect of standardization on an industry. Consider how the VHS, the CD and the DAT formats, and the IBM PC compatibility standards have encouraged growth in their respective industries. However, if there is to be any type of standardization, the standard must provide universal adaptability to the needs of both data providers and data users.

The data object owner may want to have permanent secure control over how, when, where, and by whom his property is used. Furthermore, he may want to define different rules of engagement for different types of users and different types of security depending on the value of particular objects. The rules defined by him shall govern the automated operations enabled by data services and networking. The owner may also want to sell composite objects with different rules governing each constituent object. Thus, it is necessary to be able to implement variable and extensible control.

The user on his part wants to be able to search for and purchase data objects in a convenient manner. If desired, the user should be able to combine or edit purchased objects (i.e. for creating a presentation).

Furthermore, the user may want to protect his children from inappropriate material. A complete solution must enable these needs as well.

What is needed is a universally adaptable system and method for managing the exchange and usage of data objects while protecting the interests of data object owners and users.

Prior Art

A method for enforcing payment of royalties when copying softcopy books is described in the European patent application EP 0 567 800. This method protects a formatted text stream of a structured document which includes a royalty payment element having a special tag. When the formatted text stream is inputted in the user's data processor, the text stream is searched to identify the royalty payment element and a flag is stored in the memory of the data processor. When the user for instance requests to print the document, the data processor requests authorization for this operation from a second data processor. The second data processor charges the user the amount indicated in the royalty payment element and then transmits the authorization to the first data processor.

One serious limitation of this method is that it can only be applied to structured documents. The description of the above-mentioned European patent application defines a structured document as: a document prepared in accordance with an SGML-compliant type definition. In other words it can not be applied to documents which are not SGML compliant and it cannot be applied to any other types of data objects.

Furthermore, this method does not provide for variable and extensible control. Anyone can purchase a softcopy book on a CD, a floppy disc or the like, and the same royalty amount is indicated in the royalty payment element of all softcopy books of the same title.

Thus, the method described in EP 0 567 800 does not satisfy the above-mentioned requirements for universally adaptable protection of data objects.

Summary of the Invention

Accordingly, it is a first object of the invention to provide a method and a data processing system for managing a data object in a manner that is independent of the format and the structure thereof, so as to comply with predetermined conditions for usage control and royalty payment.

It is a further object of the invention to provide such a method and system which is universally adaptable to the needs of both the owner and the user of the data object.

A further object of the invention is to provide such a method and system which enables a data object provider to distribute his data object while maintaining control of the usage thereof.

Yet another object of the invention is to provide a method and system which allows a data object provider to select the level of security for his data object in a flexible way.

Yet another object of the invention is to provide such a method and system which makes it possible to establish an audit trail for the data object.

Yet another object is to provide such a method and system which makes it possible to sell and buy data objects in a secure way.

The above-mentioned objects are achieved by a method and a system having the features of claims 1, 16, 21, 24 and 27.

Particular embodiments of the inventions are recited in the subclaims.

More particularly, a data object provider, e.g. the owner of a data object or his agent (broker), stores the data object in a memory device, e.g. a bulk storage device, where it is accessible by means of the data

provider's data processor. The data object can consist of digital data, analog data or a combination or hybrid of analog and digital data.

A general set of control data, which is based on the predetermined conditions for usage of the data object, is created and stored in the same memory device as the data object or another memory device where it is accessible by the data provider's data processor. The predetermined conditions for usage may be defined by the data object owner, by the broker or by anyone else. They may differ between different data objects.

The general set of control data comprises at least one or more usage control elements, which define usages of the data object which comply with the predetermined conditions. These usages may encompass for instance the kind of user, a time limit for usage, a geographical area for usage, allowed operations, such as making a hard copy of the data object or viewing it, and/or claim to royalty payment. The general set of control data may comprise other kinds of control elements besides the usage control element. In a preferred embodiment, the general set of control data comprises a security control element which defines a security procedure which has to be carried out before usage of the data object. It also comprises an identifier, which uniquely identifies the general set of control data.

The general set of control data is concatenated with a copy of the data object. Thus, the control data does not reside in the data object, but outside it, which makes the control data independent of the format of and the kind of data object and which allows for usage control independently of the data object format.

At least the usage control element(s) and the data object are encrypted, so that the user is unable to use the data object without a user program which performs the usage control and which decrypts the data object. Alter-

natively, the whole set of control data and the copy of the data object may be encrypted.

A user may request authorization for usage of a data object residing at a data provider's processor via a data network or in any other appropriate way. The authorization may or may not require payment. When a request for authorization for usage is received, a user set of control data is created by the data provider's processor. The user set of control data comprises the general set of control data or a subset thereof including at least one of said usage control elements which is relevant for the actual user. It typically also includes a new identifier which uniquely identifies this set of control data. If relevant, the user set of control data also comprises an indication of the number of usages authorized. If more than one kind of usage is authorized, the number of each kind of usage may be specified. Finally, the user set of control data is concatenated with a copy of the data object, and at least the usage control elements and the copy of the data object are encrypted to create a secure data package ready for transfer to the user.

Before the data package is transferred to the user, it should be confirmed that the request for authorization for usage has been granted. The check is preferably carried out before the user set of control data is created. However, it can also be carried out in parallel with or after the creation of the user control data. In the latter case, the number of usages requested by the user is tentatively authorized and included in the user set, but if the request is refused the user set is cancelled or changed.

The data package may be transferred to the user by electronic means or stored on bulk storage media and transferred to the user by mail or by any suitable transportation means.

Once the data object has been packaged in the above-described manner, it can only be accessed by a user

program which has built-in usage control and means for derypting the data package. The user program will only permit usages defined as acceptable in the control data. Moreover, if the control data comprises a security control element, the security procedure prescribed therein has to be complied with. In one embodiment, the usage control may be performed as follows. If the user decides to use a data object, the user program checks the control data to see if this action is authorized. More particularly, it checks that the number of authorized usages of this kind is one or more. If so, the action is enabled and the number of authorized usages decremented by one. Otherwise, the action is interrupted by the user program and the user may or may not be given the opportunity to purchase the right to complete the action.

After the usage, the user program repackages the data object in the same manner as it was packaged before.

When a data object is redistributed by a user or a broker, new control elements are added in the control data to reflect the relation between the old user/broker and the new user/broker. In this way, an audit trail for the data object may be created.

According to another aspect of the invention at least two data packages are stored on a user's data processor, which examines the usage control elements of the data packages in order to find a match. If a match is found, the user's data processor carries out an action which is specified in the user set of control data. This method can be used for selling and buying data objects.

Brief Description of Drawings

Fig. 1 is a flow diagram showing the general data flow according to the invention.

Fig. 2 is a system block diagram of a data object provider's data processor.

Fig. 3 is a block diagram showing the different modules of a data packaging program according to the invention.

Fig. 4 is a data flow diagram of a data packaging process.

Fig. 5 is an example of a header file.

Fig. 6 is an example of a usage data file.

Fig. 7 is a data flow diagram of loading an object to the data object provider's data processor.

Figs 8a and 8b are examples of control data for a data object on the data object provider's data processor and for an object ready to be transferred to a user, respectively.

Fig. 9 is a data flow diagram of data packaging on the data object provider's data processor.

Fig. 10 is a flow diagram of a data packaging procedure.

Fig. 11 is a memory image of a data object and its control data.

Fig. 12a is a memory image of the concatenated control data and data object.

Fig. 12b is a memory image of the concatenated and encrypted control data and data object.

Fig. 13 is a system block diagram of a user's data processor.

Fig. 14 is a block diagram showing the different modules of a user program according to the invention.

Fig. 15 is a flow diagram of using a data object on the user's data processor.

Fig. 16 is a flow diagram of how the user program operates in a specific application example.

Fig. 17 is an example of various data package structures for composite objects.

Description of the Best Mode for Carrying Out the Invention

General Overview

Fig. 1 is a flow diagram showing the general data flow according to the invention. The flow diagram is divided into a data object provider part 1 and a user part 2.

In the data object provider part 1, a data object 24 is created by an author. The data object can consist of digital data, analog data or a combination or hybrid of analog and digital data. The primary difference between analog data objects and digital data objects is the means for storage, transfer and usage.

The author also determines the conditions 42 for the usage of the data object 24 by a user. The data object 24 and the usage conditions 42 are input to a data packaging program 19, which creates a secure data package 40 of the data object and of control data which are based on the input usage conditions 42. Once packaged in this way, the data object can only be accessed by a user program 35.

The data object may be packaged together with a general set of control data, which is the same for all users of the data object. This may be the case when the data object is sent to a retailer or a bulletin board, wherefrom a user may obtain it. The data object may also be packaged as a consequence of a request from a user for usage of the data object. In that case, the package may include control data which is specifically adapted to that user. This control data is called a user set of control data. It may for example comprise the number of usages purchased by the user. Typically, the user set of control data will be created on the basis of the general set of control data and include at least a subset thereof. A user set of control data need not always be adapted for a specific user. All sets of control data which are created on the basis of a general set of control data will be called a user set of control data. Thus, a set of control data can be a general set in one phase and a user set in another phase.

The above-mentioned data packaging can be carried out by the author himself by means of the data packaging program 19. As an alternative, the author may send his data object to a broker, who inputs the data object and the usage conditions determined by the author to the data

packaging program 19 in order to create a secure package 3. The author may also sell his data object to the broker. In that case, the broker probably wants to apply his own usage conditions to the data packaging program. The author may also provide the data object in a secure package to the broker, who repackages the data object and adds further control data which is relevant to his business activities. Various combinations of the above alternatives are also conceivable.

In the user part 2 of the flow diagram, the secure package 40 is received by a user, who must use the user program 35 in order to unpackage the secure package 40 and obtain the data object in a final form 80 for usage. After usage, the data object is repackaged into the secure package 40.

The different parts of the system and the different steps of the method according to the invention will now be described in more detail.

The data provider's data processor:

Fig. 2 is a system block diagram of a data object provider's data processor. As mentioned above, the data object provider may be an author of a data object, an owner of a data object, a broker of a data object or anyone else who wants to distribute a data object, while retaining the control of its usage. The data processor is a general or special purpose processor, preferably with network capabilities. It comprises a CPU 10, a memory 11 and a network adapter 12, which are interconnected by a bus 13. As shown in Fig. 2, other conventional means, such as a display 14, a keyboard 15, a printer 16, a bulk storage device 17, and a ROM 18, may also be connected to the bus 13. The memory 11 stores network and telecommunications programs 21 and an operating system (OS) 23. All the above-mentioned elements are well-known to the skilled person and commercially available. For the purpose of the present invention, the memory 11 also stores a data packaging program 19 and, preferably, a database

20 intended for control data. Depending upon the current operation, one or more data objects 24 can be stored in the memory 11 as shown or in the bulk storage 17. The data provider's data processor is considered secure.

The Data Packaging Program:

The data packaging program 19 is used for creating control data for controlling the usage of a data object and for packaging the data object and the control data into a secure package.

As shown in Fig. 3, it comprises a program control module 301, a user interface module 302, a packaging module 303, a control data creation module 304, an encryption module 305, one or more format modules 306, and one or more security modules 307.

The control module 301 controls the execution of the other modules. The user interface module 302 handles interaction with the data object provider. The packaging module 303 packages the control data and the data object. It uses the control data creation module 304, the format modules 306, the security modules 307 and the encryption module 305 as will be described more in detail below.

The format modules 306 comprise program code, which is required to handle the data objects in their native format. They can fulfill functions such as data compression and data conversion. They can be implemented by any appropriate, commercially available program, such as by means of a routine from the PKWARE Inc. Data Compression Library for Windows and the Image Alchemy package from Handmade Software Incorporated, respectively. They can also be implemented by custom designed programs.

The security modules 307 comprise program code required to implement security, such as more sophisticated encryption than what is provided by the encryption module 305, authorization algorithms, access control and usage control, above and beyond the basic security inherent in the data package.

The data packaging program 19 can contain many different types of both format and security modules. The program control module 301 applies the format and security modules which are requested by the data provider.

The encryption module 305 may be any appropriate, commercially available module, such as "FileCrypt" Visual Basic subprogram found in Crescent Software's QuickPak Professional for Windows - FILECRPT.BAS, or a custom designed encryption program.

The control data creation module 304 creates the control data for controlling the usage of the data object. An example of a control data structure will be described more in detail below.

The Control Data:

The control data can be stored in a header file and a usage data file. In a preferred embodiment, the header file comprises fields to store an object identifier, which uniquely identifies the control data and/or its associated data object, a title, a format code, and a security code. The format code may represent the format or position of fields in the usage data file. Alternatively, the format code may designate one or more format modules to be used by the data packaging program or the user program. The security code may represent the encryption method used by the encryption module 305 or any security module to be used by the data packaging program and the user program. The header file fields will be referred to as header elements.

The usage data file comprises at least one field for storing data which controls usage of the data object. One or more usage data fields which represent one condition for the usage of the data object will be referred to as a usage element. In a preferred embodiment, each usage element is defined by an identifier field, e.g. a serial number, a size field, which specifies the size of the usage element in bytes or in any other appropriate way, and a data field.

The header elements and the usage elements are control elements which control all operations relating to the usage of the object. The number of control elements is unlimited. The data provider may define any number of control elements to represent his predetermined conditions of usage of the data object. The only restriction is that the data packaging program 19 and the user program 35 must have compatible program code to handle all the control elements. This program code resides in the packaging module and the usage manager module, to be described below.

Control elements can contain data, script or program code which is executed by the user program 35 to control usage of the related data object. Script and program code can contain conditional statements and the like which are processed with the relevant object and system parameters on the user's data processor. It would also be possible to use a control element to specify a specific proprietary user program which can only be obtained from a particular broker.

It is evident that the control data structure described above is but one example. The control data structure may be defined in many different ways with different control elements. For example, the partitioning of the control data in header data and usage data is not mandatory. Furthermore, the control elements mentioned above are but examples. The control data format may be unique, e.g. different for different data providers, or defined according to a standard.

The operation of the data packaging program

The operation of a first embodiment of the data packaging program will now be described with reference to the block diagram of Fig. 3 and the flow diagram of Fig. 4.

First a data provider creates a data object and saves it to a file, step 401. When the data packaging program is started, step 402, the user interface module

302 prompts the data object provider to input, step 403, the header information consisting of e.g. an object identifier, a title of the data object, a format code specifying any format module to be used for converting the format of the data object, and a security code specifying any security module to be used for adding further security to the data object. Furthermore, the user interface module 302 prompts the data object provider to input usage information, e.g. his conditions for the usage of the data object. The usage information may comprise the kind of user who is authorized to use the data object, the price for different usages of the object etc. The header information and the usage information, which may be entered in the form of predetermined codes, is then passed to the control module 301, which calls the packaging module 303 and passes the information to it.

The packaging module 303 calls the control data creation module 304, which first creates a header file, then creates header data on the basis of the header information entered by the data object provider and finally stores the header data, step 404-405. Then a usage data file is created, usage data created on the basis of the usage information entered by the data provider, and finally the usage data is stored in the usage data file, step 406-407.

The packaging module 303 then applies any format and security modules 306, 307 specified in the header file, steps 408-413, to the data object.

Next, the packaging module 303 concatenates the usage data file and the data object and stores the result as a temporary file, step 414. The packaging module 303 calls the encryption module 305, which encrypts the temporary file, step 415. The level of security will depend somewhat on the quality of the encryption and key methods used.

Finally, the packaging module 303 concatenates the header file and the encrypted temporary file and saves

the result as a single file, step 416. This final file is the data package which may now be distributed by file transfer over a network, or on storage media such as CD-ROM or diskette, or by some other means.

Example 1

An example of how the data packaging program 19 can be used will now be described with reference to Figs 5 and 6. In this example the data object provider is a computer graphics artist, who wants to distribute an image that can be used as clip art, but only in a document or file which is packaged according to the method of the invention and which has usage conditions which do not permit further cutting or pasting. The artist wants to provide a free preview of the image, but also wants to be paid on a per use basis unless the user is willing to pay a rather substantial fee for unlimited use. The artist will handle payment and usage authorization on a dial-up line to his data processor.

The artist uses some image creation application, such as Adobe's Photoshop to create his image. The artist then saves the image to file in an appropriate format for distribution, such as the Graphical Interchange Format (GIF). The artist then starts his data packaging program and enters an object identifier, a title, a format code and a security code, which in this example are "123456789", "image","a", and "b", respectively. In this example, the format code "a" indicates that no format code need be applied, and this code is selected since the GIF format is appropriate and already compressed. Furthermore, the security code "b" indicates that no security module need be applied and this code is selected since the security achieved by the encryption performed by means of the encryption module 305 is considered appropriate by the artist.

Then the artist enters his dial-up phone number, his price for a single use of the image and for unlimited use of the data object, a code for usage types approved, and

for number of usages approved. For this purpose, the user interface module 302 may display a data entry form.

The data packaging program 19 creates control data on the basis of the information entered by the artist and stores the data in the header file and in the usage data file as shown in Figs 5 and 6, respectively. This data consitutes a general set of control data which is not specifically adapted to a single user, but which indicates the conditions of usage determined by the artist for all future users.

Then the package program 19 concatenates the data object and the control data in accordance with steps 414-416 of Fig. 4 to achieve the secure package. No format module or security module is applied to the data object, since they are not needed according to the data in the header file.

When the secure package has been obtained, the artist sends it to a bulletin board, from where it can be retrieved by a user.

Example 2

Below, another embodiment of the data packaging program 19 will be described with reference to Figs 7-12b. In this example, the data object consists of a video film, which is created by a film company and sent to a broker together with the predetermined conditions 42 for usage of the video. The broker loads the video 24 to the bulk storage 17 of his data processor. Then, he uses his data packaging program 19 to create a general set of control data 50 based on the predetermined conditions 42 for usage indicated by the film company. Furthermore, the address to the video in the bulk storage 17 is stored in an address table in the control database 20 or somewhere else in the memory 11. It could also be stored in the general set of control data 50. Finally, the general set of control data 50 is stored in the control database 20. It could also be stored somewhere else in the memory 11.

After these operations, which correspond to steps 401-407 of Fig. 4, the data packaging program is exited.

Fig. 8a shows the general set of control data for the video according to this example. Here the control data includes an identifier, a format code, a security code, the number of usage elements, the size of the data object, the size of the usage elements and two usage elements, each comprising an identifier field, a size field and a data field. The identifier may be a unique number in a series registered for the particular broker. In this example, the identifier is "123456789", the format code "0010", which, in this example, indicates the format of a AVI video and the security code is "0010". Furthermore, the first usage element defines the acceptable users for the video and the second usage element data defines the number of viewings of the video purchased by a user. The first usage element data is 1 which, for the purposes of this example will signify that only education oriented users are acceptable to the film company. The data field of the second usage element data is empty, since at this stage no viewings of the video has been purchased.

Managing Object Transfer:

The broker wants to transfer data objects to users and enable controlled usage in return for payment of usage fees or royalties. Managing the broker-user business relationship and negotiating the transaction between the broker and the user can both be automated, and the control data structure can provide unlimited support to these operations. The payment can be handled by transmitting credit card information, or the user can have a debit or credit account with the broker which is password activated. Preferably, payment should be confirmed before the data object is transferred to the user.

Data packaging:

When a user wants to use a data object, he contacts the broker and requests authorization for usage of the data object. When the request for authorization is recei-

ved in the broker's data processor, a data program compares the usage for which authorization is requested with the usage control elements of the control data of the data object to see if it complies with the predetermined conditions for usage indicated therein. The comparison may include comparing the user type, the usage type, the number of usages, the price etc. If the requested usage complies with the predetermined conditions the authorization is granted, otherwise it is rejected.

Fig. 9 is a data flow diagram of the data packaging on the broker's data processor, which occurs in response to a granted request from a user for authorization for usage of the video, e.g. a granted request for the purchase of two viewings.

In response to a granted request, the broker again applies the data packaging program 19. The general set of control data 50 and the data object 24 are input to the program from the control database 20 and the bulk storage 17, respectively. The program creates a user set of control data 60 on the basis of the general set of control data 50 and concatenates the user set 60 and the data object 24 to create a secure data package 40, which may then be transferred to the user by any suitable means. A copy of the user set of control data is preferably stored in the broker's control database. This gives the broker a record with which to compare subsequent use, e.g. when a dial-up is required for usage.

Fig. 10 is a flow diagram of an exemplary procedure used for creating a user set of control data and for packaging the user set of control data and the video into a secure package. Here, the procedure will be described with reference to the general set of control data shown in Fig. 8a.

The user set of control data 60, i.e. a set of control data which is adapted to the specific user of this example, is created in steps 1001-1003 of Fig. 11. First, the general set of control data 50 stored in the control

database is copied to create new control data, step 1001. Second, a new identifier, here "123456790", which uniquely identifies the user set of control data, is stored in the identifier field of the new control data 60, step 1002. Third, the data field of the second usage element is updated with the usage purchased, i.e. in this example with two, since two viewings of the video were purchased, step 1003.

The thus-created user set of control data, which corresponds to the general set of control data of Fig. 8a is shown in Fig. 8b.

The user set of control data is stored in the control database 20, step 1004. Then, the video, which is stored in the bulk storage 17, is copied, step 1005. The copy of the video is concatenated with the user set of control data, step 1006. The security code 0010 specifies that the entire data package 40 is to be encrypted and that the user program 35 must contain a key which can be applied. Accordingly, the whole data package is encrypted, step 1007. Finally, the encrypted data package is stored on a storage media or passed to a network program, step 1008, for further transfer to the user.

Fig. 11 is a memory image of the video 24 and the user control data 60. The user control data and a copy of the video 24 are concatenated as shown in Fig. 12a. The encrypted data package 40 is shown in Fig. 12b.

The procedure of Fig. 10 can be implemented by the data packaging program of Fig. 3. As an alternative to the procedure of Fig. 10, the user set of control data can be created as in steps 1001-1003 and saved in a header file and in a usage data file, whereafter steps 408-416 of the data packaging program of Fig. 4 can be performed to create the secure package.

The above-described process for creating a user-adapted set of control data may also be used by a user who wants to redistribute a data object or by a broker who wants to distribute the data object to other brokers.

Obviously, redistribution of the data object requires that redistribution is a usage approved of in the control data of the data object. If so, the user or the broker creates a user set of control data by adding new control elements and possibly changing the data fields of old control element to reflect the relation between the author and the current user/broker and between the current user/broker and the future user/broker. In this way, an audit trail is created.

The user's data processor:

The user's data processor, which is shown in Fig. 13, is a general or special purpose processor, preferably with network capabilities. It comprises a CPU 25, a memory 26, and a network adapter 27, which are interconnected by a bus 28. As shown in Fig. 13, other conventional means, such as a display 29, a keyboard 30, a printer 31, a sound system 32, a ROM 33, and a bulk storage device 34, may also be connected to the bus 28. The memory 26 stores network and telecommunications programs 37 and an operating system (OS) 39. All the above-mentioned elements are well-known to the skilled person and commercially available. For the purpose of the present invention, the memory 26 also stores a user program 35 and, preferably, a database 36 intended for the control data. Depending upon the current operation, a data package 40 can be stored in the memory 26, as shown, or in the bulk storage 34.

The user program:

The user program 35 controls the usage of a data object in accordance with the control data, which is included in the data package together with the data object.

As shown in Fig. 14, the user program 35 comprises a program control module 1401 a user interface module 1402, a usage manager module 1403, a control data parser module 1404, a decryption module 1405, one or more format modules 1406, one or more security modules 1407, and a file transfer program 1409.

The control module 1401 controls the execution of the other modules. The user interface module 1402 handles interactions with the user. The usage manager module 1403 unpackages the secure package 40. It uses the control data parser module 1404, the decryption module 1405, the format modules 1406, and the security modules 1407.

The format modules 1406 comprise program code, which is necessary to handle the data objects in their native format, such as decompression and data format procedures. The security modules 1407 comprises program code required to implement security above the lowest level, such as access control, usage control and more sophisticated decryption than what is provided by the basic decryption module 1405.

The user program 35 can contain many different types of both format and security modules. However, they should be complementary with the format and security modules used in the corresponding data packaging program. The usage manager module 1401 applies the format and security modules which are necessary to use a data object and which are specified in its control data. If the proper format and security modules are not available for a particular data object, the usage manager module 1401 will not permit any usage.

The decryption module 1405 can be the above-mentioned FileCrypt Visual Basic subprogram or some other commercially available decryption program. It can also be a custom designed decryption module. The only restriction is that the decryption module used in the user program is complementary with the encryption module of the data packaging program.

The control data parser module 1403 performs the reverse process of the control data creation module 304 in Fig. 3.

The user program 35 can have code which controls use of the program by password or by any other suitable method. A password may be added in a password control

element during packaging of the data object. The password is tranferred to the user by registered mail or in any other appropriate way. In response to the presence of the password control element in the control data structure, the user program prompts the user to input the password. The input password is compared with the password in the control data, and if they match, the user program continues, otherwise it is disabled.

The user program 35 can also have procedures which alter the behavior of the program (e.g. provide filters for children) according to the control data of the user object 41. It is important to mention that the user program 35 never stores the object in native format in user accessible storage and that during display of the data object the print screen key is trapped.

The file transfer program 1409 can transfer and receive files via network to and from other data processor.

Since the data object is repackaged into the secure package after the usage, the user program should also include program code for repackaging the data object. The program code could be the same as that used in the corresponding data packaging program 19. It could also be a separate program which is called from the user program.

Operation of the user program:

The operation of an embodiment of the user program 35 will now be described with reference to the block diagram of Fig. 14 and the flow diagram of Fig. 15.

First the user receives a data package 40 via file transfer over a network, or on a storage media such as CD-ROM or diskette, or by any other appropriate means, step 1501. He then stores the data package as a file on his data processor, step 1502.

When the user wants to use the data object, he starts the user program 35, step 1503. Then he requests usage of the data object, step 1504. The request is received by the user interface module 1402, which noti-

fies the control module 1401 of the usage request. The control module 1401 calls the usage manager module 1403 and passes the usage request.

The usage manager module 1403 reads the format code from the data package to determine the control data format. Then it calls the decryption module 1405 to decrypt and extract the control data from the data package. The usage manager module 1403 applies the decryption module 1405 incrementally to decrypt only the control data. Finally, it stores the control data in memory, step 1505.

The usage manager module 1403 then calls the control data parser module 1404 to extract the data fields from the usage elements.

The usage manager module 1403 then compares the user request for usage with the corresponding control data, steps 1506-1507. If the requested usage is not permitted in the control data, the requested usage is disabled, step 1508. However, if the requested usage is approved of in the control data, the usage manager module 1403 applies any format and security modules 1406, 1407 specified in the header data or usage data, steps 1509-1514, to the data package.

Then the usage manager module 1403 calls the decryption module 1405, which decrypts the object data, step 1515, whereafter the requested usage is enabled, step 1516. In connection with the enabling of the usage, the control data may need to be updated, step 1517. The control data may for instance comprise a data field indicating a limited number of usages. If so, this data field is decremented by one in response to the enabling of the usage. When the user has finished usage of the data object, the user program 35 restores the data package in the secure form by repackaging it, step 1518. More particularly, the data object and the usage elements are reconcatenated and reencrypted. Then the header elements are added and the thus-created package is stored in the user's data processor.

Example 1 contd.

A specific example of how the user program operates will now be described with reference to Figs 6 and 15. The example is a continuation of Example 1 above, where an artist created an image and sent it to a bulletin board.

Assume that a user has found the image at an electronic bulletin board (BBS) and is intrested in using it. He then loads the data package 40 containing the image to his data processor and stores it as a file in the bulk storage. The user then executes the user program 35 and requests to preview the image. The user program then performs steps 1505-1507 of the flow diagram in Fig. 15. The request for a preview of the image is compared with the data field of the usage element "code for usage type approved". In this example, the code "9" designates that previews are permitted. Thus, the requested preview is OK. Then, the user program 35 performs step 1509-1515 of Fig. 15. Since the format code "a" and the security code "b" of the header data indicate that neither conversion, nor decompression, nor security treatment is required, the user program only decrypts the object data. The usage manager module 1403 then displays the preview on the user's data processor and passes control back to the user interface 1402.

When the user is finished previewing the image, the user interface module 1402 displays the costs for usage of the image in accordance with the price usage data of the control data ("price for single use" and "price for unlimited use" in Fig. 6) and prompts the user to enter a purchase request. The user decides to buy unlimited use of the image, and the user interface module 1402 inputs purchase information, such as an identification, billing, and address for that request and passes the request to the control module 1401. The control module calls the file transfer program 1409, which dials the artist's dial-up number as indicated in the usage data ("control

element for artist's phone number" in Fig. 6) and transfers the request and purchase information to a broker program on the artist's data processor. Upon approval of the purchase, the broker program returns a file containing an update for "usage type approved" control elements. The update is "10" for the usage type approved, which in this example indicates that unlimited use by that user is permitted. The file transfer program 1409 passes this update to the usage manager module 1403 which updates the control data with the "usage type approved" code. The user interface module 1402 then displays a confirmation message to the user.

Subsequently, the user interface module inputs a request to copy the image to a file packaged according to this invention, on the user's machine. The usage manager module then compares the user request control data. The usage manager module examines the data filed for "usage type approved", which now is "10". The usage manager module copies the image to the file.

When the user is finished with the image, the usage manager module 1403 repackages the image as before except with updated control data. This repackaging process is exactly like that shown in Fig. 4, except that the header and usage data already exist, so the process starts after step 406 where control data is created.

Improved security

If the data object provider wants to improve the security of a data package containing a data object, a security module 307 containing a sophisticated encryption algorithm, such as RSA, could be used. In that case the packaging module 303 calls the security module 307 in step 412 of the flow diagram of Fig. 4. The security module encrypts the image and passes a security algorithm code to the control data creation module 302, which adds a control element for the security module code, which will be detected by the user program 35. Then the data packaging continues with step 414. When the data package

is sent to the user, the public key is mailed to the user by registered mail. When the user program is executed in response to a request for usage of this data object, the usage manager module will detect the security module code in the control data and call the security module. This module passes control to the user interface module 1402, which requests the user to input the public key. If the key is correct, the user security module applies complementary decryption using that key and passes a usage approved message to the usage manager module, which enables the usage.

As another example of improved security, a security module may implement an authorization process, according to which each usage of the data object requires a dial-up to the data processor of the data object provider. When the corresponding security module code is detected by the user program 35, the relevant security module is called. This module passes a request for authorization to the control module 1401, which calls the file transfer program 1409, which dial the data object provider's dial-up number, which is indicated in a usage element and transfers the request for authorization of usage. Upon a granted authorization, the data provider's data processor returns a usage approved message to the user security module, which forwards the approval tl the usage control module, which enables one usage. If the user requests further usages of the data object, the authorization process is repeated. This procedures results in a permanent data object security.

Example 2 contd.

A further specific example of how the user program 35 operates will now be described with reference to Fig. 16. The example is a continuation of Example 2 above, where a user purchased two viewings of a video film from a broker.

The user wants to play the video which was purchased and transferred from the broker. The user applies the

user program 35, step 1601, and requests to play the video, step 1602. The user program 35 first examines the user set of control data 60, step 1603. In this example, the user program 35 contains only those format and security modules for objects with format code of 0010 and with a security code of 0010. Consequently, only those types of data objects may be used. If the program encounters other codes it will not enable the usage action, step 1604-1605.

Next, the user program 35 compares the first control element data which is 1, for educational users only, to user information entered by the user on request of the user program. Since the user type entered by the user is the same as that inicated in the first usage element the process continues, steps 1606-1607. Then the user program checks the second control element data which specifies that the number of plays purchased is 2. Consequently, the usage is enabled, step 1609. The user program applies the decryption module with the universal key and the AVI format video is displayed on the display unit 29. Then, the second control element data is decremented by one, step 1610. Finally, the video is repackaged, step 1611

Implementation of Variable and Extensible Object Control:

Object control is achieved through the interaction of the data packaging program 19 and the usage program 35 with the control data. Variation of object control can be applied to a particular object by creating a control data format with control elements defining the control variation and the circumstances in which the variation is applied. Program procedures should then be added to program modules to process the control elements. For example, suppose a broker wants to allow students to print a particular article for free but require business users to pay for it. He defines control elements to represent the user types student and business and the associated costs for each. He then adds program logic to examine the user type and calculate costs accordingly. Object control is

extensible in the sense that the control data format can have as many elements as there are parameters defining the rules for object control.

Implementation of Variable and Extensible Object Security:

Object security is also achieved through the interaction of the data packaging program 19 and the user program 35 with the control data. Security process and encryption/decryption algorithms can be added as program modules. Variation of object security can be applied to a particular object by creating a control data format with control elements defining the security variation and the circumstances in which the variation is applied. Program procedures should be added to program modules to process the control elements. For example, suppose a broker wants to apply minimal security to his collection of current news articles but to apply tight security to his encyclopedia and text books. He defines a control element for security type. He then adds program logic to apply the security algorithms accordingly. Object security is extensible in the sense that multiple levels of security can be applied. The level of security will of course be dependent on the encryption/key method which is implemented in the security modules. One level of security may be to require online confirmation when loading a data object to the user's data processor. This can be implemented in program code in a security module. This permits the broker to check that the object has not already been loaded as well as double check all other parameters.

It is also important to have version control with time stamping between the usage program and the user's control database. Otherwise the database can be duplicated and reapplied to the user program. The user program can place a time stamp in the control database and in a hidden system file each time the control database is accessed. If the time stamps are not identical, the control database has been tampered with and all usage is

disabled. Program code for handling time stamps can reside in a security module.

Handling Composite Objects:

A composite object can be handled by defining a control data format with control elements defining relationships between constituent objects and by defining a parent/child element and a related object id element. For example, suppose a broker wants to include a video and a text book in an educational package. He creates a parent object with control elements referring to the video and textbook objects. He also includes control elements in the control data for the video object and the textbook object referring to the parent object. Finally, he adds program procedures to program modules to process the control elements.

In other words, when the data object is a composite data object including at least two constituent data objects, a respective general set of control data is created for each of the constituent data object and the composite data object. In response to a request from a user, a respective user set of control data is created for each of the constituent data objects as well as for the composite data object.

Examples of various data package structures for composite objects are given in Fig. 17.

Another side of composite objects is when the user wants to combine data objects for some particular use. Combination is a usage action that must be permitted in each constituent data object. A new data object is created with control data linking the constituent data objects. Each constituent data object retains its original control data which continues to control its subsequent usage.

When a user requests authorization for usage of one constituent data object in a composite data object, a user set of control data is created only for that consti-

tuent data object and concatenated only with a copy of that constituent data object.

Scaleable Implementation:

The flexible control data structure and modular program structure permit almost boundless extensibility with regard to implementation of the owner's requirements for usage control and royalty payment. The control data structure can include control elements for complex user types, usage types, multiple billing schemes, artistic or ownership credit requirements and others. Security modules can be included which interact with any variation of the control data structure and the control data. Security modules could require a dial up to the brokers data processor to approve loading or usage actions and to implement approval authentication mechanisms.

User acting as a broker:

A limited or full implementation of the broker's data packaging program can be implemented on the user's machine to permit further distribution or reselling. However, only those data objects with control data permitting further distribution or reselling are enabled in that way.

Rebrokering

An author of a data object may want to allow his original broker to distribute his data objec to other brokers whom will also distribute his image. He then includes a control element which enables rebrokering in tne control data before distributing the data object with its associated control data to the origingal broker. Upon request for rebrokering, the original broker copies the general set of control data and updates the copy to create a user set of control data which will function as the general set of control data on the subsequent brokers data processor. The original broker packages the data object with the user set of control data and transfers the package to the subsequent broker. The subsequent broker then proceeds as if he were an original broker.

Automated transaction negotiation

This is an example of how the predetermined conditions for usage included in the control data can be used for achieving automated transaction negotiation.

Suppose some company wnats to provide a computer automated stock trading. Buy and sell orders could be implemented in the form of data packages and a user program could process the data packages and execute transactions. Data packages could carry digital cash and manage payment based on conditions defined in the control data.

In this example, the buy order is created using a data packaging program according to the invention on the buyer's data processor. The sell order is created using the data packaging program on the seller's data processor. Both orders are used by the the user program on the stock trader's data processor. The usages would take the form of using a sell order data package to sell stock and a buy order data package to buy stock. The rules or conditions for buying and selling stocks could be indicated in the control data of the packages. The data object consists of digital money. In this context it is important to remember that digital money is merely data which references real money or vitual money that is issued and maintained for the purpose of digital transactions.

In this example the buyer starts with a digital money data file. He uses the data packaging program to create control data, e.g. kind of stock, price, quantity, for the purchase, and he then packages the digital money data file and the control data into a secure package as described above.

The seller starts with an empty data file. This empty file is analogous to the digital money data file except it is empty. The seller creates control data, e.g. kind of stock, price, quantity, and packages the empty file and the control data into a secure package.

Both the sell order package and the buy order package are transferred to the data processor of the stock trading company, where they are received and stored in the memory. The user program of the stock trading company examines the control data of the buy and sell order packages in the same way as has been described above and looks for a match. Upon identifying matched buy and sell orders the user program executes a transaction, whereby the digital money is extracted from the buy order data package and transferred to the sell order package. Then the control data of the data packages is updated to provide an audit trail. Both packages are repackaged in the same manner as they were previously packaged and then transferred back to their authors.

The above described technique could be used for selling and buying any object as well as for automated negotiations. Payment may be carried out in other ways than by digital money.

In the general case, the data processor of the user decrypts the usage control elements of the user sets of control data and examines the usage control elements to find a match. In response to the finding of a match, the user's data processor carries out an action which is specified in the user set of control data.

CLAIMS

1. A method for managing a data object so as to comply with predetermined conditions for usage of the data object, comprising the steps of:

- storing the data object in a memory device, where it is accessible by means of a data object provider's data processor;

- creating, by said data processor, a general set of control data for the data object based on said predetermined conditions for usage, said general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with said predetermined conditions;

- storing said general set of control data in a memory device, where it is accessible by said data processor;

- concatenating the general set of control data with a copy of the data object; and

- encrypting at least the copy of the data object and said one or more usage control elements to create a secure data package which is ready for transfer to a user.

2. A method as set forth in claim 1, wherein the step of encrypting comprises encrypting the data object and the general set of control data.

3. A method as set forth in claims 1 or 2, wherein the step of creating control data comprises creating an identifier which uniquely identifies the general set of control data.

4. A method as set forth in claims 1, 2 or 3, wherein the step of creating a general set of control data comprises creating a security control element which identifies a security process to be applied before usage of the data object is allowed.

5. A method as set forth in any of the preceding claims, wherein the step of creating a general set of

control data comprises creating a format control element which identifies the format of the control data.

6. A method as set forth in any of the preceding claims, comprising the further steps of:

- creating, in response to a request for authorization for usage of the data object by a user, a user set of control data, which comprises at least a subset of the general set of control data, including at least one of said usage control elements;
- using the user set of control data instead of the general set of control data in said concatenating step;
- using the at least one usage control element of the user set of control data instead of the one or more usage control elements of the general set of control data in the encrypting step;
- checking, before allowing transfer of the data package to the user, that said request for authorization for usage of the data object has been granted.

7. A method as set forth in any of the preceding claims, further comprising the steps of receiving in said data processor the request for authorization for usage by a user; comparing the usage for which authorization is requested with said one or more usage control elements of the general set of control data and granting the authorization if the usage for which authorization is requested complies with the usages defined by said one or more usage control elements.

8. A method as set forth in claim 7, further comprising the step of securing payment for the requested authorization for usage before granting the authorization.

9. A method as set forth in any one of claims 6-8, wherein the data object is composed of at least two constituent data objects and wherein the user set of control data, in response to a request for authorization for usage of one of said constituent data objects by a user, is created only for that constituent data object and

concatenated only with a copy of that constituent data object.

10. A method as set forth in any one of claims 6-9, wherein the data provider's data processor is connected to a data network and the request for authorization is received from a data processor of the user, which is also connected to the data network, further comprising the step of transferring the data package through the data network to the user's data processor.

11. A method as set forth in any one of claims 6-8 or 10, wherein the data object is a composite data object including at least two constituent data objects and wherein the step of creating a general set of control data comprises the step of creating a respective general set of control data for each of the constituent data objects and the composite data object and wherein the step of creating a user set of control data comprises the step of creating a respective user set of control data for each of the constituent data objects and the composite data object.

12. A method as set forth in any one of claims 6-11, comprising the further step of storing a copy of the user set of control data in the data object provider's processor.

13. A method as set forth in any of the preceding claims, comprising the further steps of:

- receiving the data package in a user's data processor;

- storing the data package in a memory device where it is accessible by means of the user's data processor;

- decrypting said one or more usage control elements;

- checking, in response to a request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the general set of control data;

- decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the general set of control data, the data object and enabling the requested usage, otherwise disabling it.

14. A method as set forth in any one of claims 6-12, comprising the further steps of:

- receiving the data package in a user's data processor;

- storing the data package in a memory device where it is accessible by means of the user's data processor;

- decrypting the at least one usage control element of the user set of control data;

- checking, in response to a request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the user set of control data;

- decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the user set of control data, the data object and enabling the requested usage, otherwise disabling it.

15. A method as set forth in claims 13 or 14, comprising the further steps of reconcatenating, after the usage of the data object, the data object and the one or more usage control elements, reencrypting at least the data object and the one or more usage control elements, and storing the thus-repackaged data package in the memory of the user's data processor.

16. A method for controlling the usage by a user of a data object so as to comply with predetermined conditions for usage of the data object, comprising the steps of:

- storing a data package in a memory device, where it is accessible by means of a data processor of the user, said data package comprising the data object and control data, which comprises at least one usage control

element defining a usage of the data object which complies with the predetermined conditions, the data object and said at least one usage control element being encrypted;

- receiving a request by the user for usage of the data object;

- decrypting the control data;

- checking, in response to the request by the user for usage of the data object, whether the requested usage complies with the usage defined by the at least one usage control element of the control data;

- decrypting, in response to the requested usage complying with the usage defined by the at least one usage control element of the control data, the data object and enabling the requested usage, otherwise disabling it.

17. A method as set forth in claim 16, wherein the usage control element is updated after the usage of the data object.

18. A method as set forth in claims 16 or 17, wherein said control data comprises an indication of the number of times the user is authorized to use the data object in accordance with said at least one user control element; wherein the requested usage of the data object is only enabled when said number of times is one or more; and wherein said number of times is decremented by one when the requested usage is enabled.

19. A method as set forth in any one of claims 16-18, wherein the control data comprise a security control element, and further comprising the step of carrying out, before each usage of the data object, a security procedure defined in the security control element.

20. A method as set forth in any one of claims 16-19, wherein the step of checking whether the requested usage complies with the usage defined by the at least one usage control element comprises the step of checking that the user's data processor is capable of carrying out the

security procedure specified in the security control element of the user set of control data, and if not, disabling the usage.

21. A method as set forth in any one of claims 16-20, comprising the further steps of reconcatenating, after the usage of the data object, the data object and the one or more usage control elements, reencrypting at least the data object and the one or more usage control elements, and storing the thus-repackaged data package in the memory of the user's data processor.

22. A system for managing a data object so as to comply with predetermined conditions for usage of the data object, comprising

- first means in the data object provider's data processor for creating a general set of control data for the data object based on the predetermined conditions for usage, said general set of control data comprising at least one or more usage control elements defining usages of the data object which comply with the predetermined conditions;

- storing means, which are accessible by means of said data processor, for storing the data object and the general set of control data;

- concatenating means for concatenating the general set of control data with a copy of the data object; and

- encrypting means for encrypting the copy of the data object and at least said one or more usage control elements to create a secure data package, which is ready for transfer to a user.

23. A system as set forth in claim 22, further comprising

- second means in said data processor for creating, in response to a request for authorization for usage of the data object by a user, a user set of control data, which comprises at least a subset of the general set of control data, which subset comprises at least one of said usage control elements; and

- checking means in said data processor for checking that said request for authorization for usage of the data object has been granted before allowing transfer of the data package to the user.

24. A system as set forth in claims 22 or 23, wherein the general set of control data comprises a control data element which defines the right to further distribution of the data object by the user.

25. A system for controlling the usage by a user of a data object so as to comply with predetermined conditions for usage of the data object, comprising

- storing means for storing a data package which comprises a data object and a control data comprising at least one usage control element defining a usage of the data object which complies with the predetermined conditions;

- means for decrypting the at least one usage control element and the data object;

- checking means for checking whether a usage requested by the user complies with the usage defined by said at least one usage control element;

- enabling means for enabling the usage requested by the user when the usage complies with the usage defined by said at least one usage control element; and

- disabling means for disabling the usage requested by the user when the usage does not comply with the usage defined by said at least one usage control element.

26. A system as set forth in claim 25, further comprising means for repackaging the data object after usage thereof.

27. A method for controlling the usage by a user of data objects so as to comply with predetermined conditions for usage of the data objects, comprising the steps of:

- storing at least two data packages in a memory device, where they are accessible by a data processor of the user, each said data package comprising a data object

and a user set of control data, which comprises at least one usage control element defining a usage of the data object which complies with the predetermined conditions, the data object and said at least one usage control elements being encrypted;

- decrypting the usage control elements of the user sets of control data;

- examining the usage control elements of said at least two data packages to find a match;

- using, in response to the finding of a match, the data processor to carry out an action, which is specified in the user sets of control data.

28. A method as set forth in claim 27, comprising the further steps of updating the usage control element of each data package, reconcatenating after the usage of the data objects, each of the data object and its usage control element, reencrypting each of the concatenated data objects and its usage control element and transferring the repackaged data objects to their creators.

Fig 1

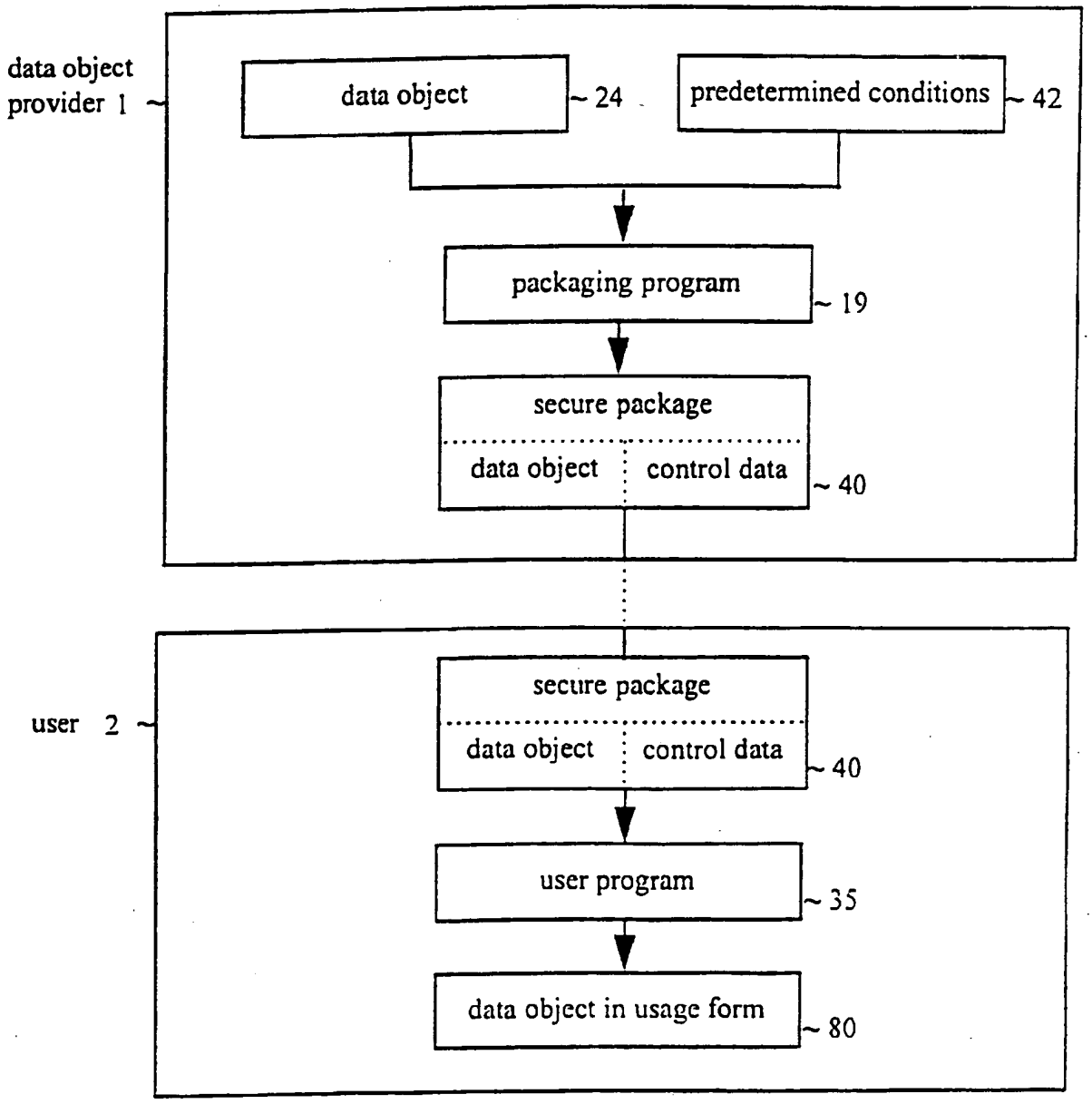
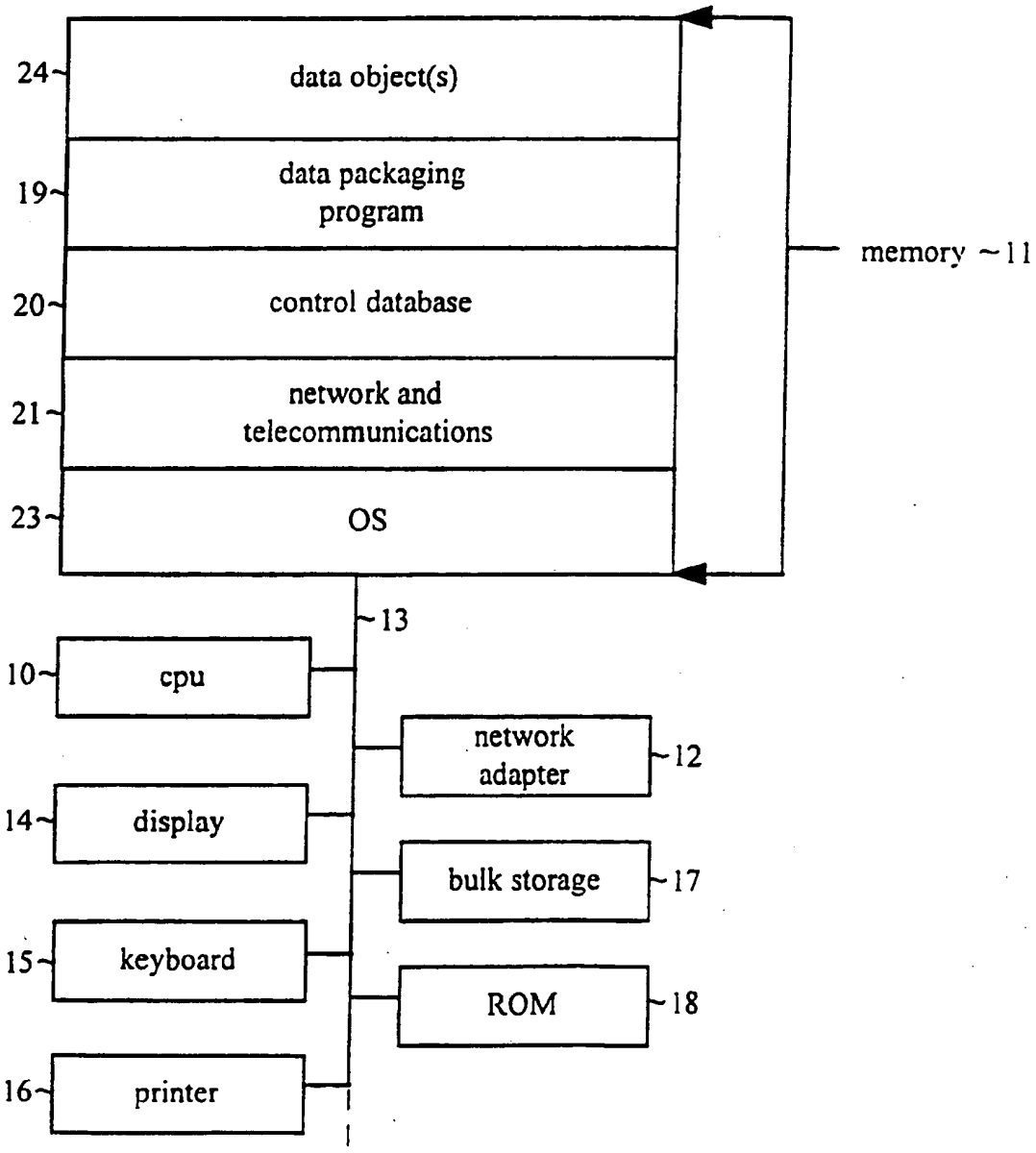
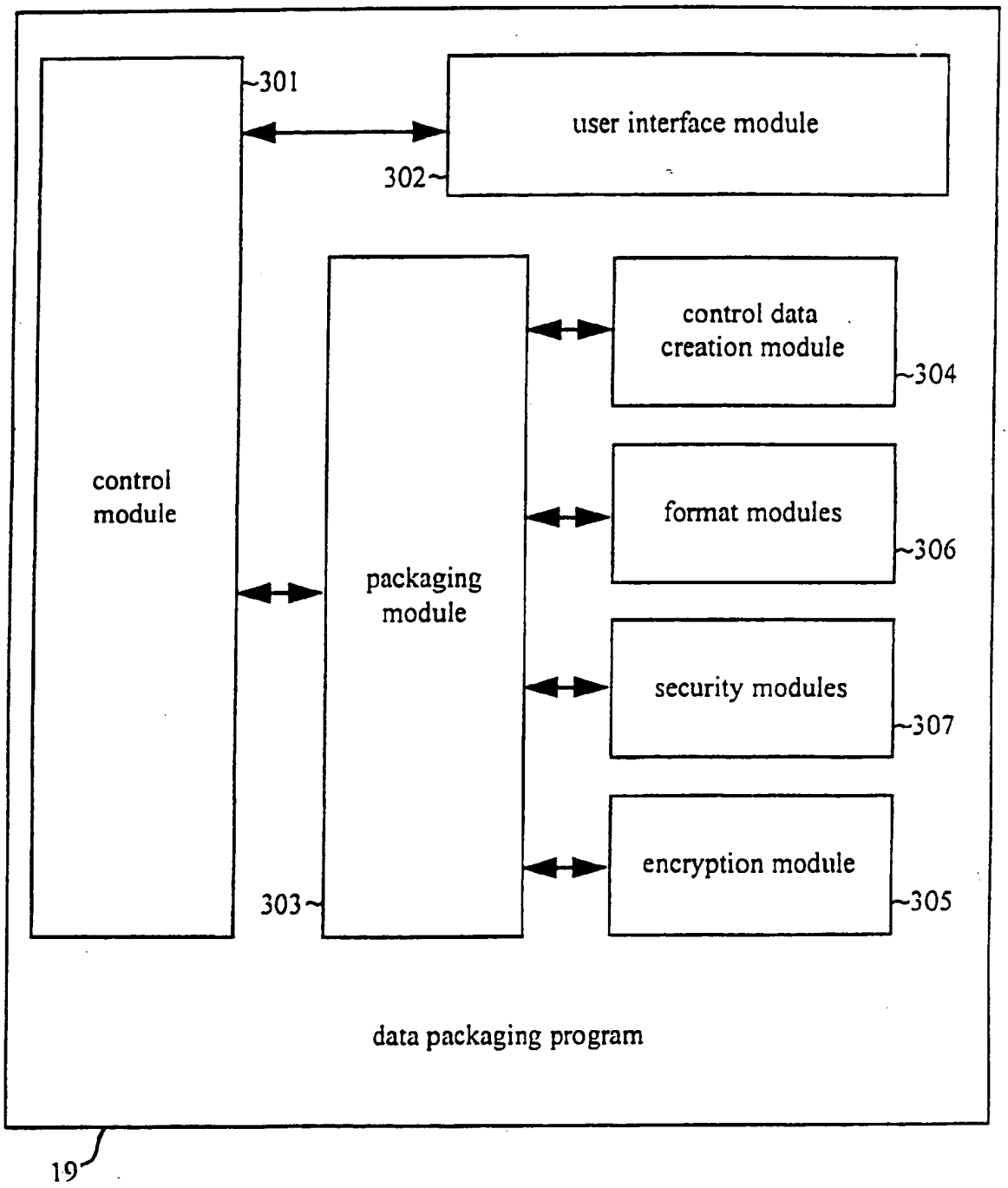

data object provider 1
data object
24
predetermined conditions
42
packaging program
19
secure package
data object
control data
40
user 2
secure package
data object
control data
40
user program
35
data object in usage form
80

Fig 2



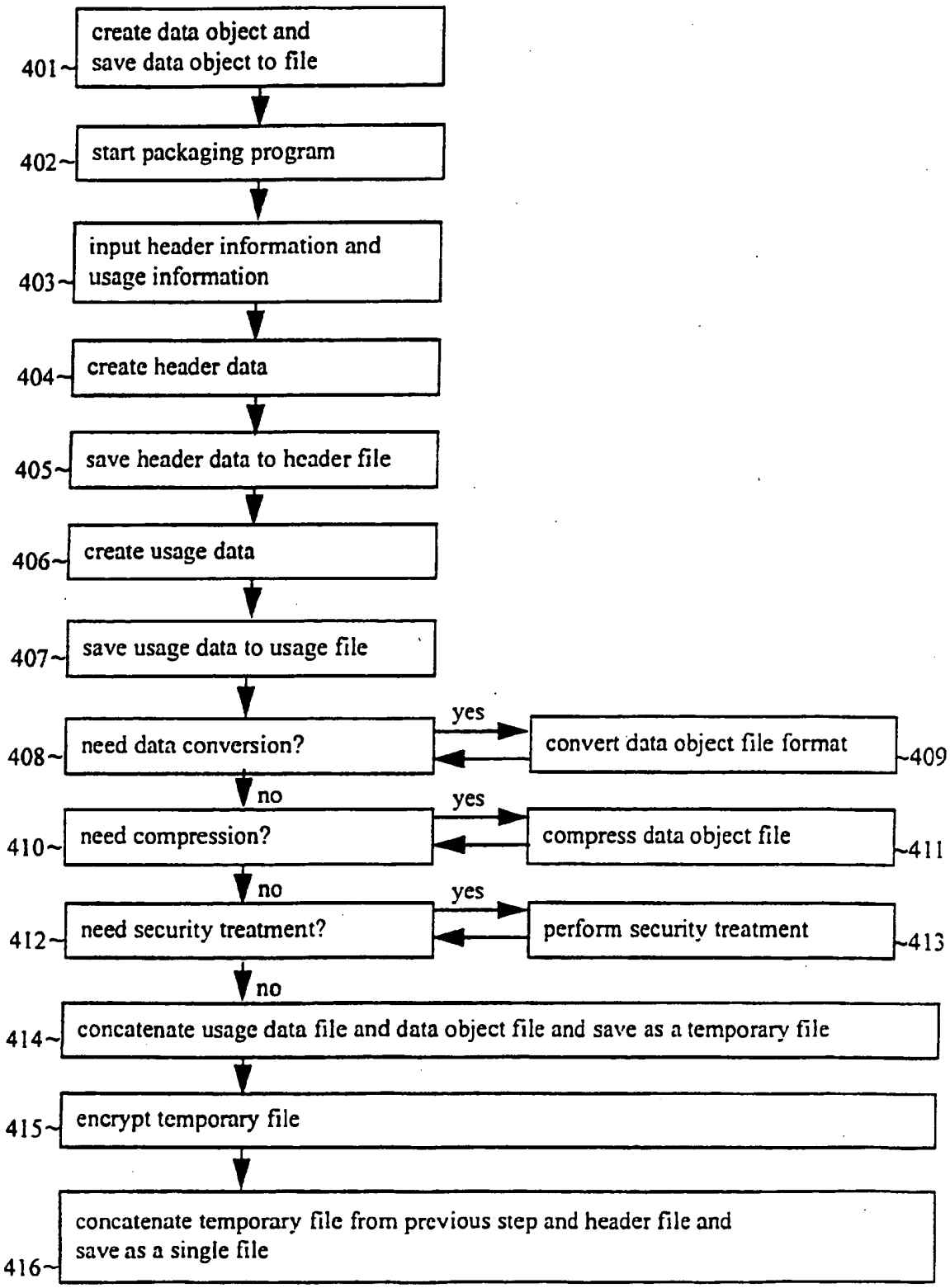
Petitioner Apple Inc. - Exhibit 1012, p. 1414

Fig 3



Petitioner Apple Inc. - Exhibit 1012, p. 1415

Fig 4



Petitioner Apple Inc. - Exhibit 1012, p. 1416

Fig 5

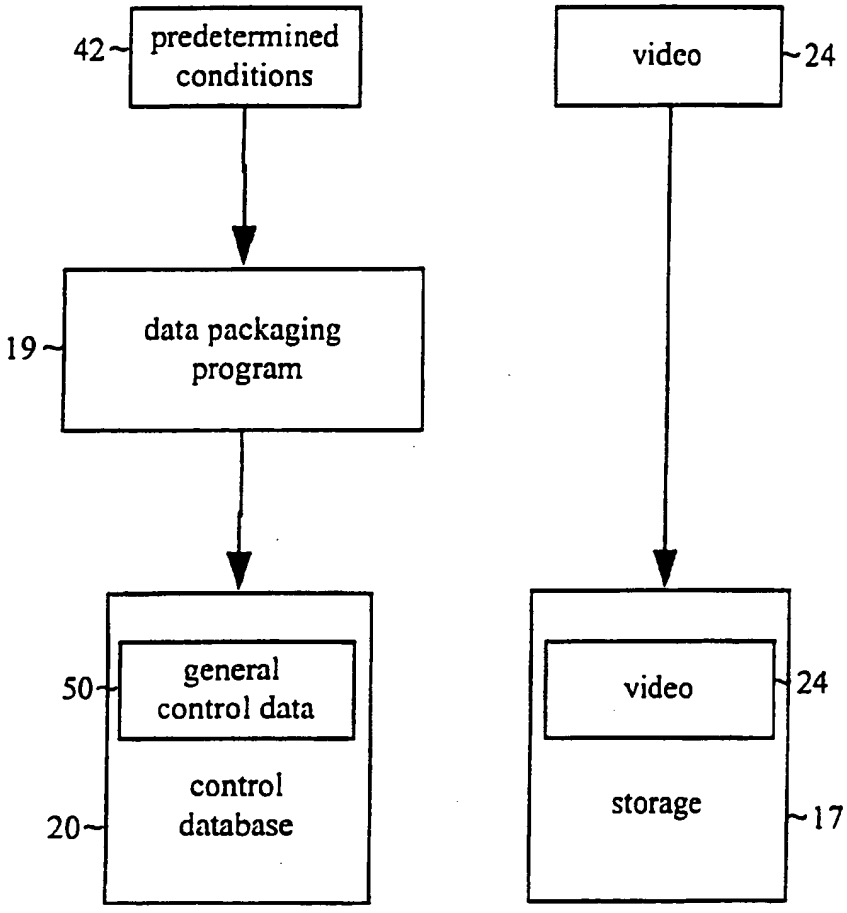
file identifier	123456789
title	image
format code	a
security code	b

Fig 6

usage element for author's phone number	identifer	1
	size	13
	data	716 381 5356
...price for single use	identifer	2
	size	4
	data	.50
...price for unlimited use	identifer	3
	size	4
	data	50.00
...code for usage type approved	identifer	4
	size	2
	data	9
...code for number of usages approved	identifer	5
	size	2
	data	1

Petitioner Apple Inc. - Exhibit 1012, p. 1417

Fig 7



Petitioner Apple Inc. - Exhibit 1012, p. 1418

Fig 8a

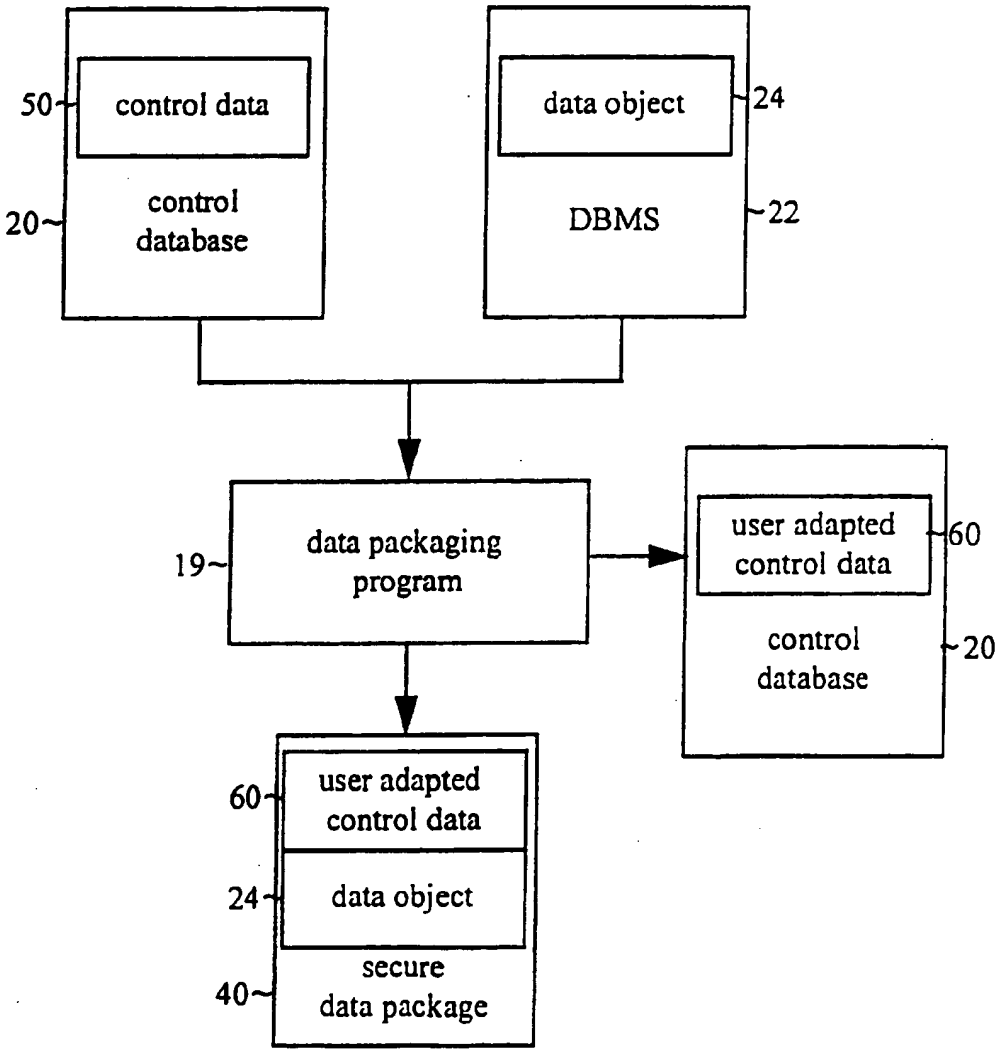
header	object identifier	123456789
	format code	0010
	security code	0010
	number of usage elements	2
	size of usage data	17
	size of data object	273
	1st usage element id	001
	1st usage element size	6
	1st usage element data	1
	2nd usage element id	002
	2nd usage element size	3
	2nd usage element data	

Fig 8b

header	object identifier	123456790
	format code	0010
	security code	0010
	number of usage elements	2
	size of usage data	17
	size of data object	273
	1st usage element id	001
	1st usage element size	6
	1st usage element data	1
	2nd usage element id	002
	2nd usage element size	3
	2nd usage element data	2

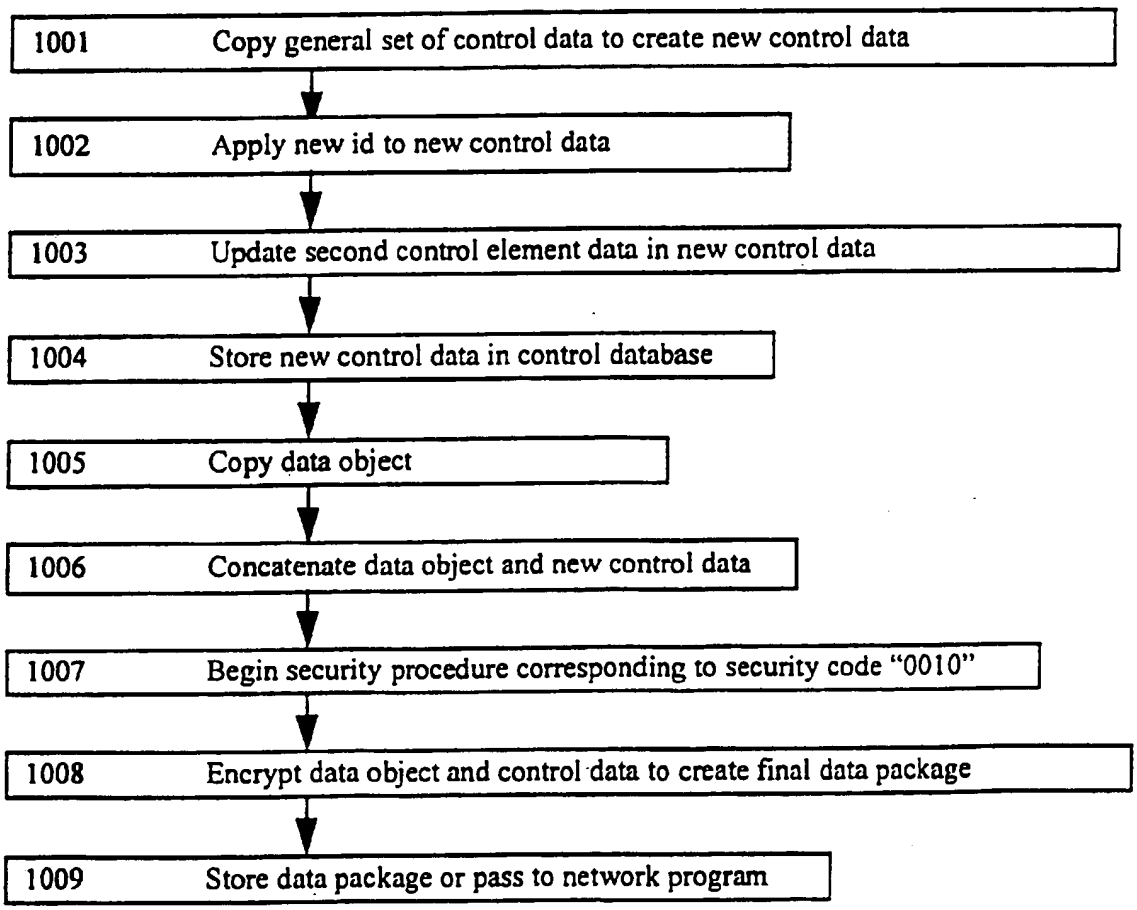
Petitioner Apple Inc. - Exhibit 1012, p. 1419

Fig 9



Petitioner Apple Inc. - Exhibit 1012, p. 1420

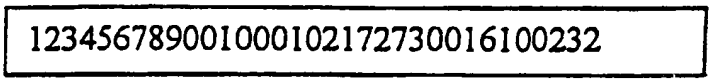
Fig 10



Petitioner Apple Inc. - Exhibit 1012, p. 1421

Fig 11

control data in memory



AVI file in memory

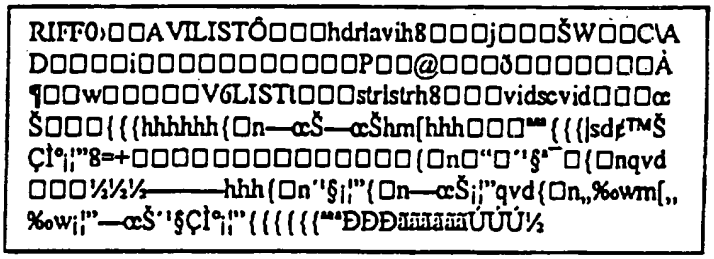


Fig 12a

concatenated control data and AVI file in memory

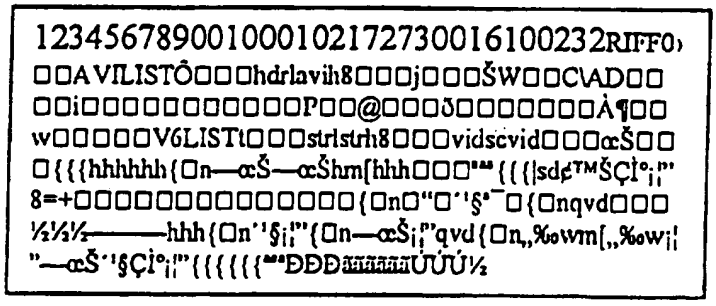
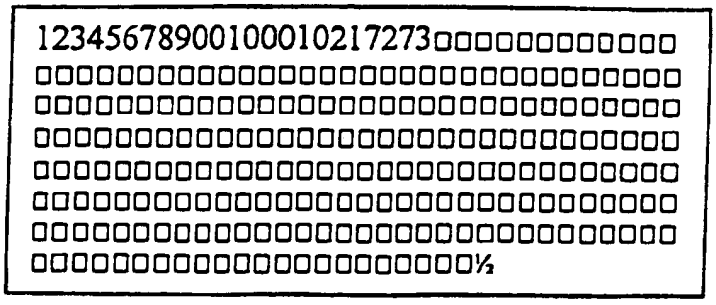


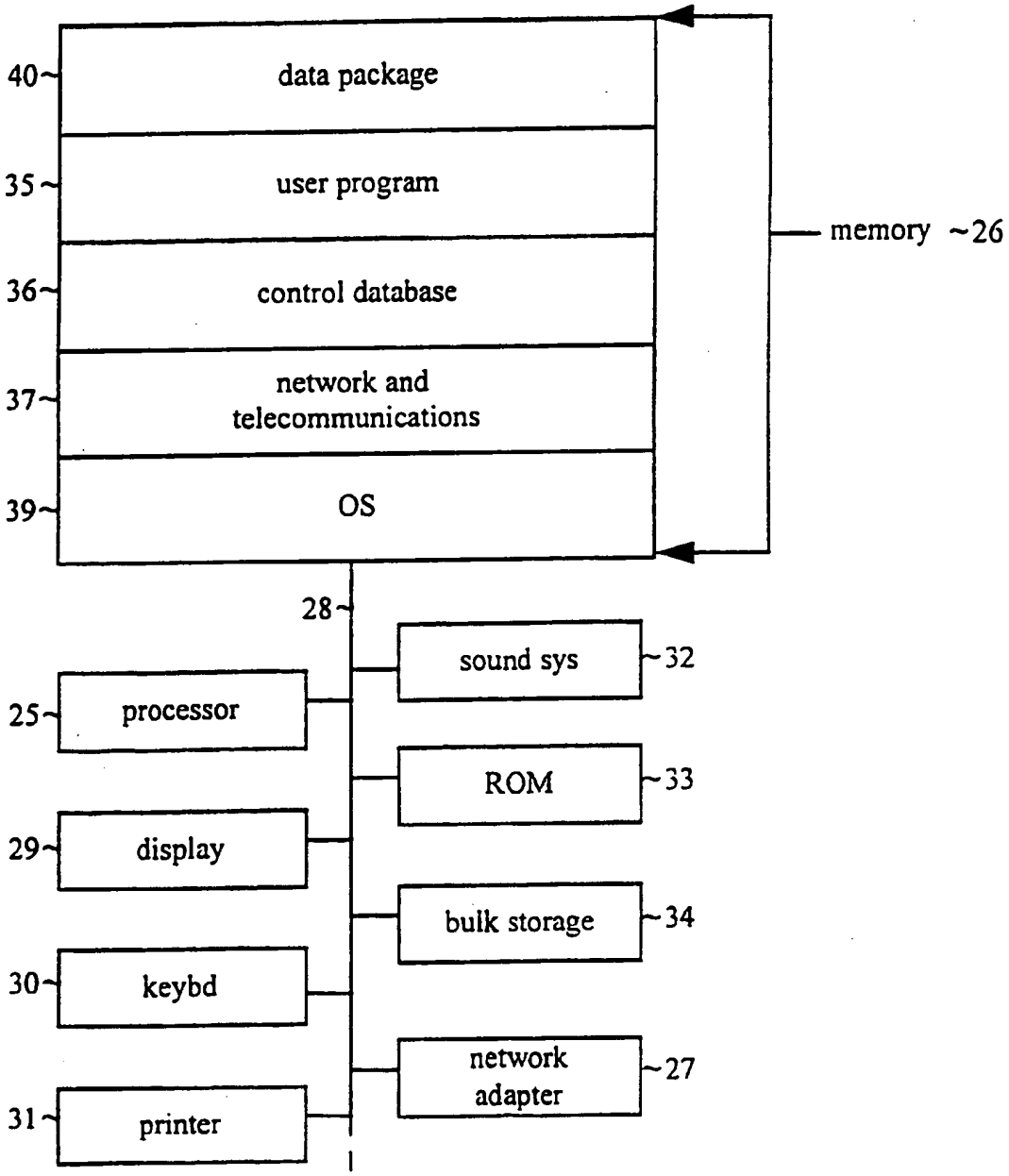
Fig 12b

concatenated and encrypted control data and AVI file in memory



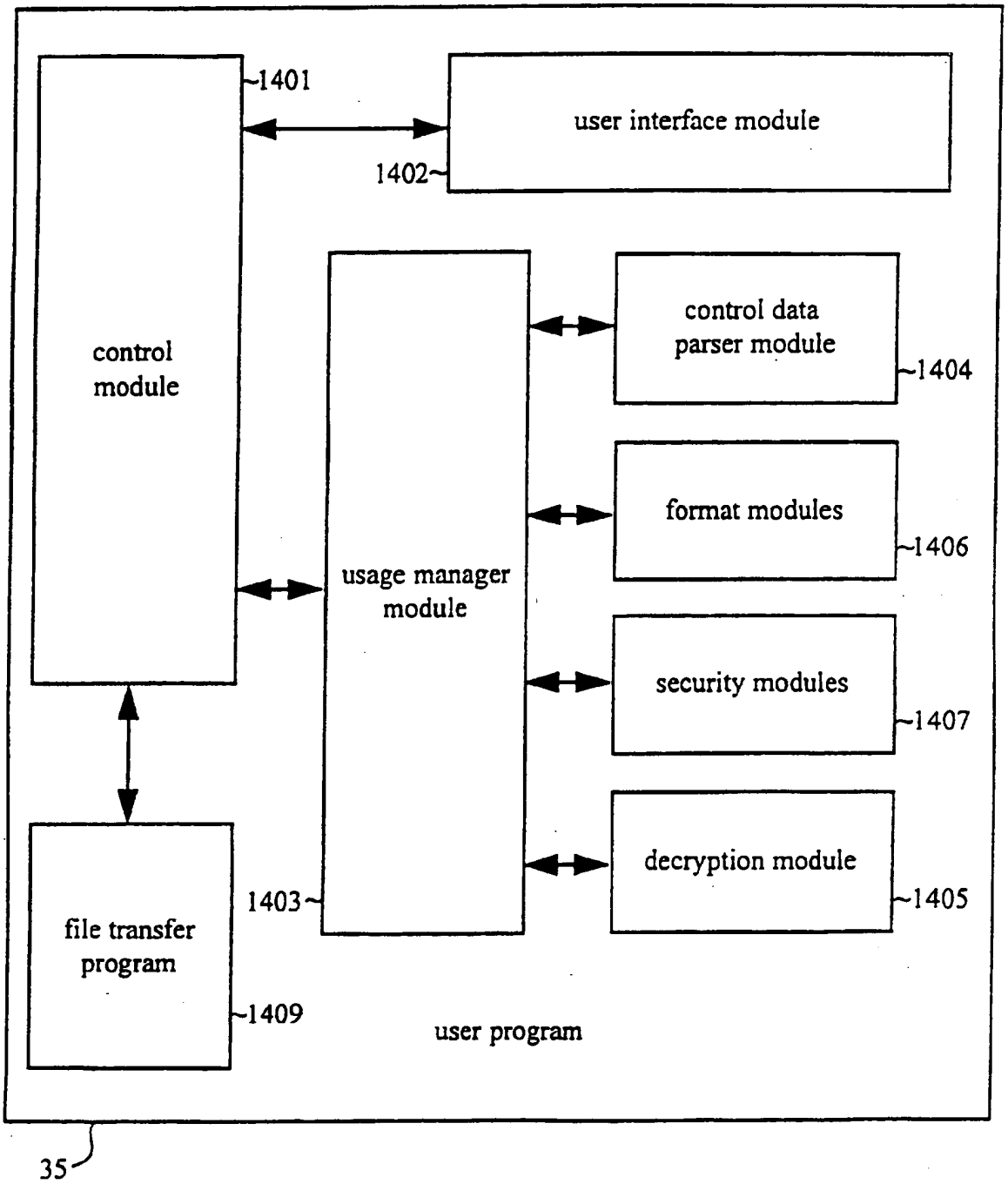
Petitioner Apple Inc. - Exhibit 1012, p. 1422

Fig 13



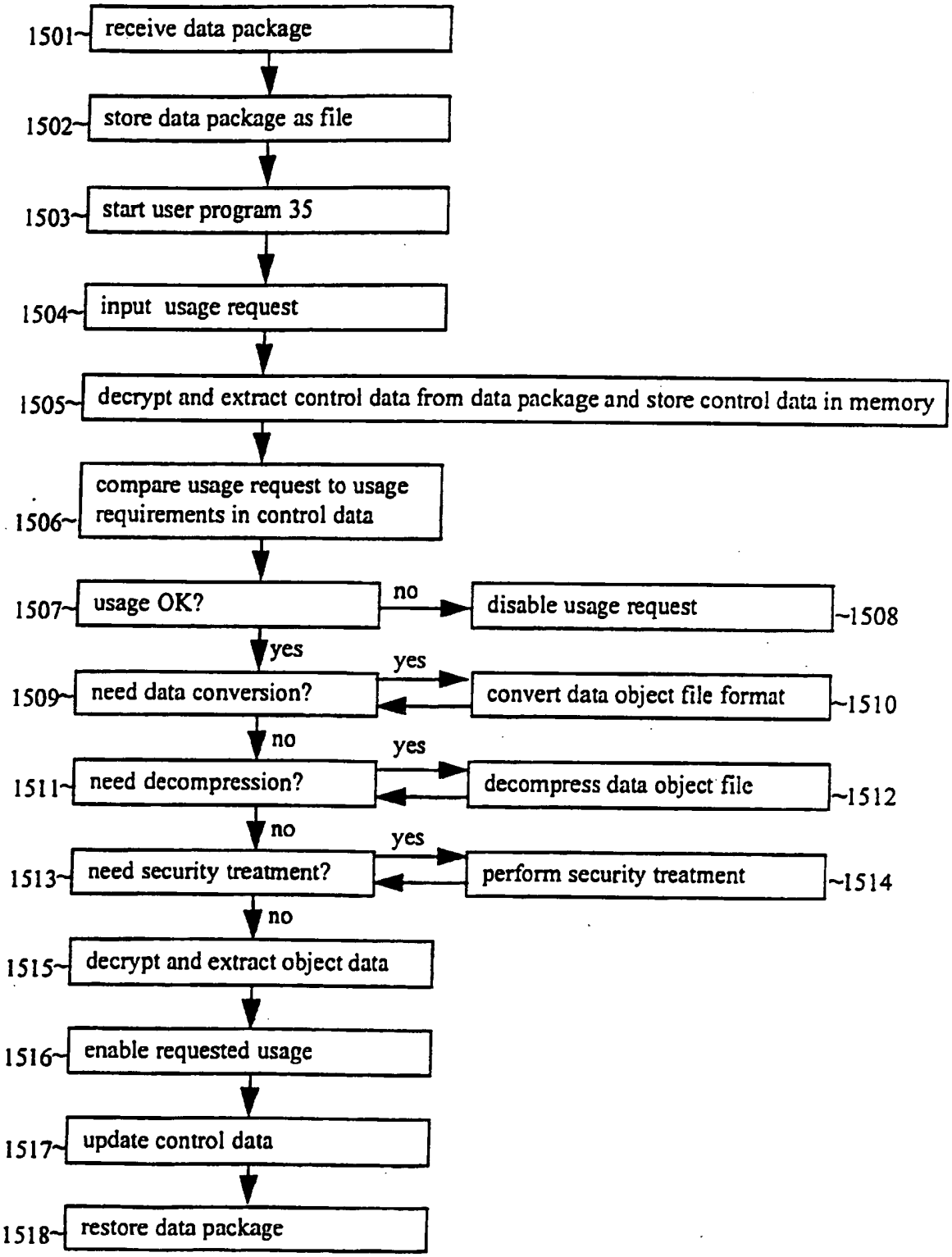
Petitioner Apple Inc. - Exhibit 1012, p. 1423

Fig 14



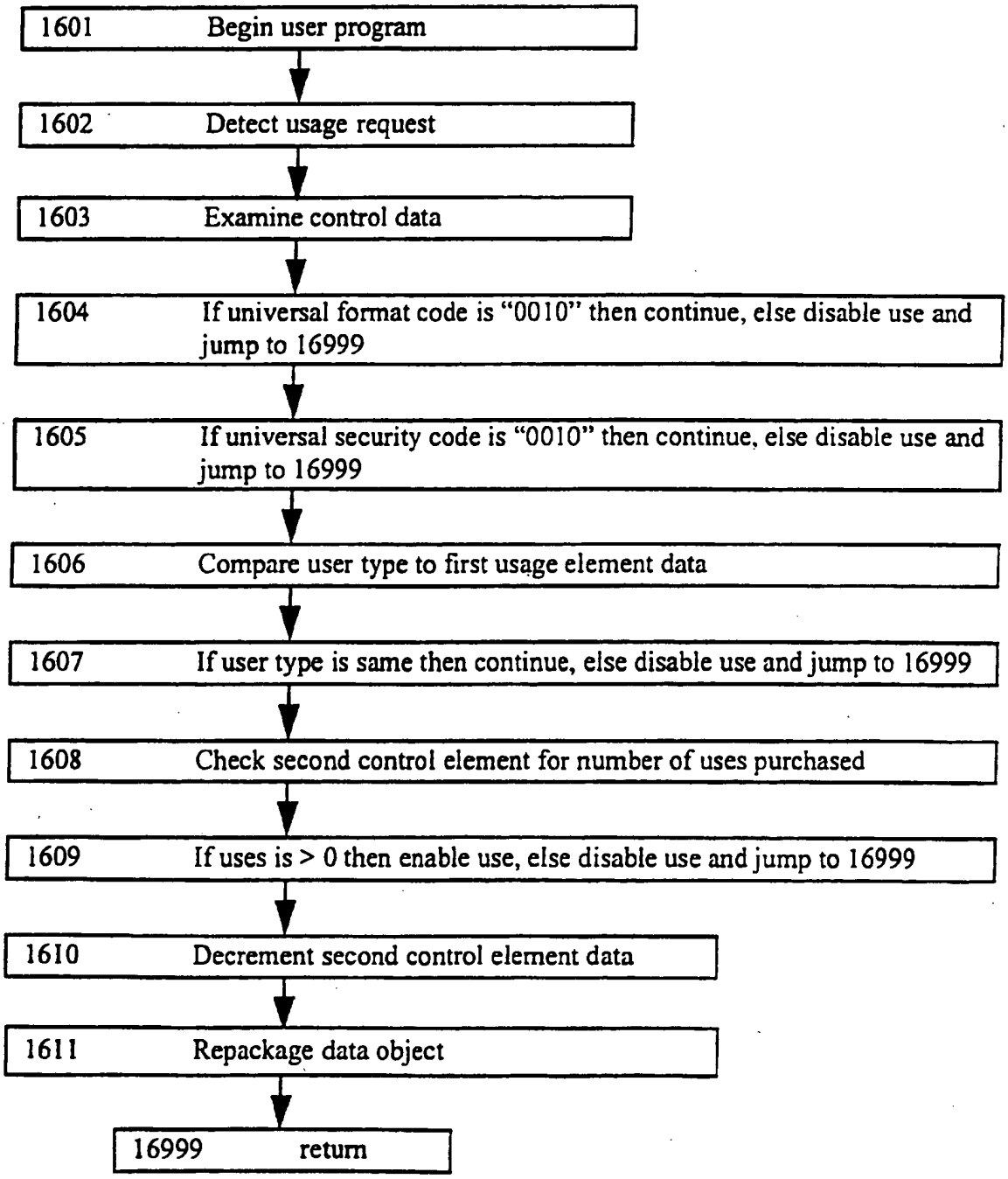
Petitioner Apple Inc. - Exhibit 1012, p. 1424

Fig 15



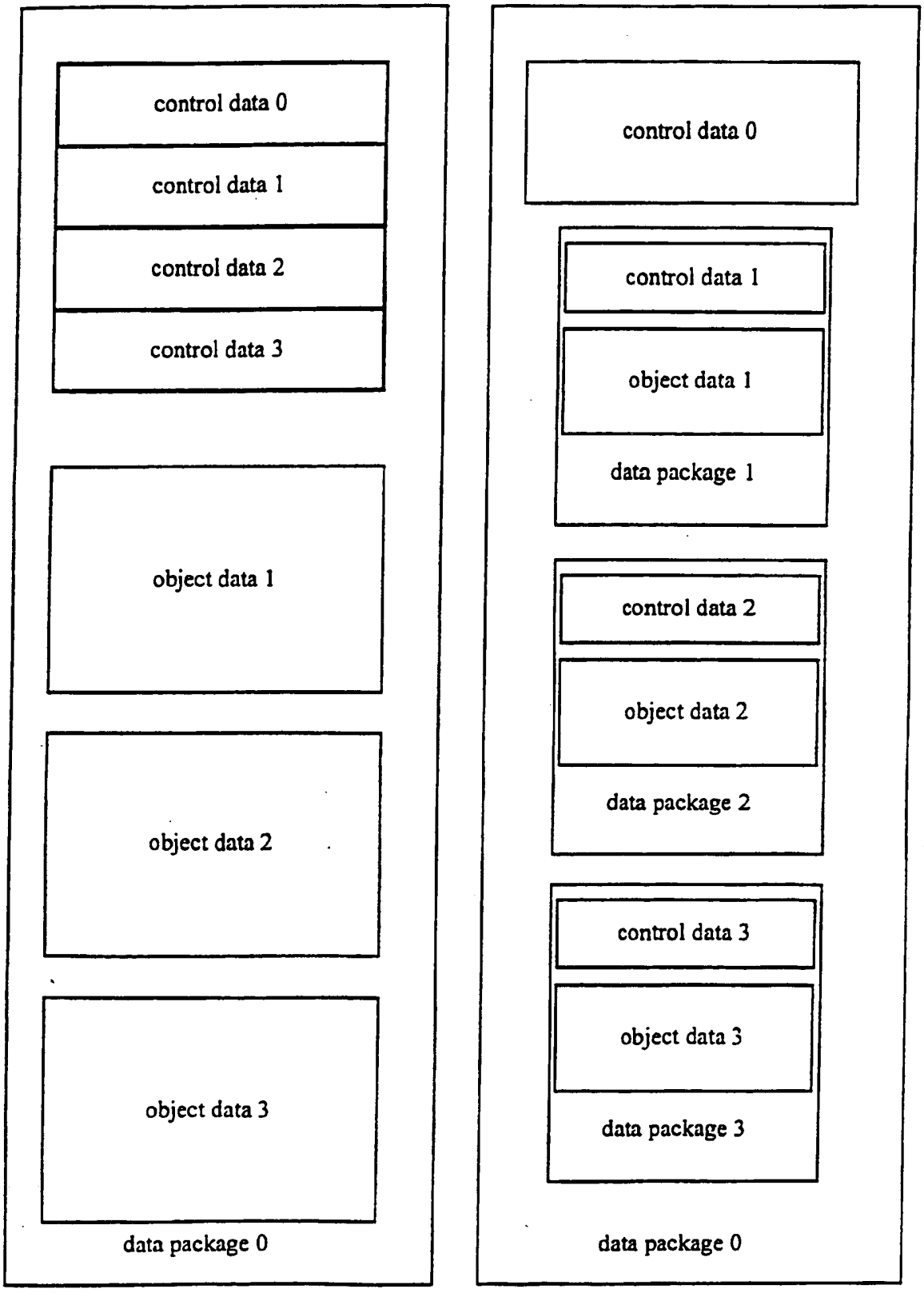
Petitioner Apple Inc. - Exhibit 1012, p. 1425

Fig 16



Petitioner Apple Inc. - Exhibit 1012, p. 1426

Fig 17



Petitioner Apple Inc. - Exhibit 1012, p. 1427

Requested Patent: JP7200317A

Title: OPERATION RIGHT MANAGEMENT EQUIPMENT ;

Abstracted Patent: JP7200317 ;

Publication Date: 1995-08-04 ;

Inventor(s): TAKAHASHI TOSHINARI; others: 04 ;

Applicant(s): TOSHIBA CORP ;

Application Number: JP19930349335 19931228 ;

Priority Number(s): ;

IPC Classification: G06F9/46; G06F1/00; G06F12/14 ;

Equivalents: ;

ABSTRACT:

PURPOSE:To attain flexible operation right management for threads by providing a means storing revision right information and a means referencing the stored revision right information before execution of revision of operation right information and verifying whether or not the revision is permitted to the equipment.

CONSTITUTION:The equipment is provided with a means storing revision right information representing whether or not revision of operation right information is permitted based on a thread or the user being a subject of the revision or a memory area or a program in which the subject of revision is in existence and a means referencing the stored revision right information before execution of the revision of the operation right information and verifying whether or not the revision is permitted. That is, an operation right list storage section 7 stores a table relating to thread protection and storing a fact of the right executing the operation to each thread and used for an operation right discrimination section 12. Thus, not only the management of the operation right to the thread but also the revision right is flexibly expressed and managed by the combination of various conditions.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平7－200317

(43)公開日　平成７年(1995)８月４日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	9/46	３４０　Ｂ	7629－5Ｂ		
	1/00	３７０　Ｅ			
	12/14	３１０　Ｋ			

審査請求　未請求　請求項の数３　ＦＤ　（全 14 頁）

(21)出願番号　特願平5－349335

(22)出願日　平成５年(1993)12月28日

(71)出願人　000003078
株式会社東芝
神奈川県川崎市幸区堀川町72番地

(72)発明者　高橋　俊成
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　岡本　利夫
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　福本　淳
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(74)代理人　弁理士　鈴江　武彦

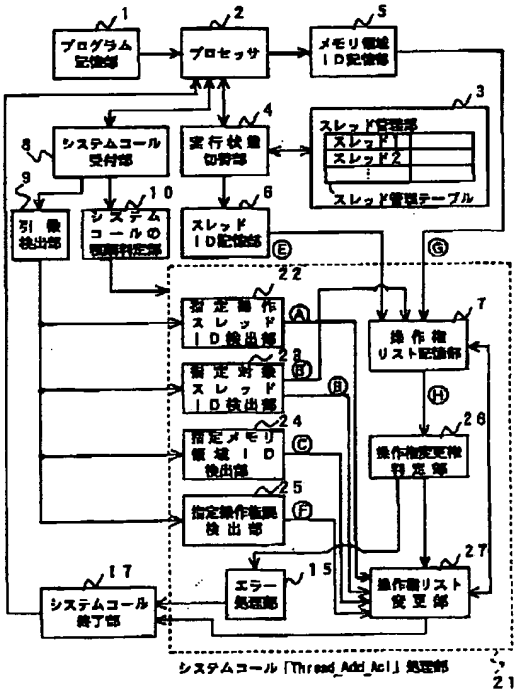
最終頁に続く

(54)【発明の名称】　操作権管理装置

(57)【要約】

【目的】　スレッドの操作権管理の柔軟化を目的とする。

【構成】　本発明は、複数の並行して実行されるスレッドによりプログラムを実行する手段と、各スレッドに対する操作を、この操作を行う主体となるスレッドまたはユーザ、もしくはこの操作を行う主体が存在するメモリ領域またはプログラムの少なくともいずれかに基づいて、許可するか否かを指示する操作権情報を記憶する手段とを備える操作権管理装置において、前記操作権情報の変更を、この変更を行う主体となるスレッドまたは、ユーザもしくはこの変更を行う主体が存在するメモリ領域またはプログラムの少なくともいずれかに基づいて、許可するか否かを示す変更権情報を記憶する手段と、前記操作権情報の変更を実行する前に、記憶された前記変更権情報を参照して、この変更が許可されるか否かを検証する手段とを具備したことを特徴とする。



Petitioner Apple Inc. - Exhibit 1012, p. 1429

1

【特許請求の範囲】

【請求項1】複数の並行して実行されるスレッドによりプログラムを実行する手段と、

各スレッドに対する操作を、この操作を行う主体となるスレッドまたはユーザ、もしくはこの操作を行う主体が存在するメモリ領域またはプログラムの少なくともいずれかに基づいて、許可するか否かを指示する操作権情報を記憶する手段とを備える操作権管理装置において、

前記操作権情報の変更を、この変更を行う主体となるスレッドまたは、ユーザもしくはこの変更を行う主体が存在するメモリ領域またはプログラムの少なくともいずれかに基づいて、許可するか否かを示す変更権情報を記憶する手段と、

前記操作権情報の変更を実行する前に、記憶された前記変更権情報を参照して、この変更が許可されるか否かを検証する手段とを具備したことを特徴とする操作権管理装置。

【請求項2】実メモリまたは仮想メモリを複数のメモリ領域の集合として管理する手段と、

各メモリ領域に対する操作を、この操作を行う主体となるスレッドまたはユーザ、もしくはこの操作を行う主体が存在するメモリ領域またはプログラムの少なくともいずれかに基づいて、許可するか否かを指示する操作権情報を記憶する手段とを備える操作権管理装置において、

前記操作権情報の変更を、この変更を行う主体となるスレッドまたは、ユーザもしくはこの変更を行う主体が存在するメモリ領域またはプログラムの少なくともいずれかに基づいて、許可するか否かを示す変更権情報を記憶する手段と、

前記操作権情報の変更を実行する前に、記憶された前記変更権情報を参照して、この変更が許可されるか否かを検証する手段とを具備したことを特徴とする操作権管理装置。

【請求項3】前記変更権情報を前記操作権情報に付随されて記憶することを特徴とする請求項1または2に記載の操作権管理装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、計算機システム中でのメモリ領域またはスレッドへの操作権を管理する操作権管理装置に関するものである。

【0002】

【従来の技術】近年マイクロプロセッサの性能向上により複数の小型のコンピュータをネットワークでつないで使用することが通常のこととなり、ネットワーク結合された計算機やユーザー同士での協調作業が可能となり、操作権の管理を厳密に行う必要が出てきた。

【0003】またオブジェクト指向技術の進歩やサーバ・クライアント・モデルのような新しいパラダイムの出現により、従来の記憶装置やファイルを単位とした操作

2

権管理では十分な性能が得られなくなってきた。

【0004】こういった問題を解決するために、単一仮想記憶などの技術により、メモリやCD－ROMやハードディスク・ドライブのような記憶装置、さらにはディスプレイやキーボードといったあらゆる計算機資源を同一の概念で管理するオペレーティング・システムの設計が試みられている。中でも、各種の資源を同一の仮想空間上に配置する単一仮想記憶の技術は特徴的なものである。さらに、この単一仮想記憶をいくつかのブロックに分割し、ブロック単位で操作権を管理する方法が提案されている。この管理単位を「メモリ領域」と呼び、あらゆる記憶装置の操作権管理の単位として用いられる。

【0005】一方、オペレーティング・システムはマイクロ・カーネル技術の定着により、プログラムの実行を管理するスレッドという単位を使って管理するのが一般的になりつつある。すなわち、プログラム実行の制御対象としてプロセスまたはスレッドと呼ばれる制御単位が用いられる。個々のスレッドは独立にプロセッサのレジスタ値やスタックなどを持ち、オペーレーティング・システムによりプロセッサを割り当てられた間だけプログラムを実行し、一定時間後またはハードウェア割り込みなどが発生したときにオペレーティング・システムはスレッドに対するプロセッサの割り当てを解除して他のスレッドへプロセッサを割り当てる。個々のスレッドは独立したレジスタ値を持っているため、仮想的に並列に動いているプロセッサであるとみなすことができる。

【0006】このようなオペレーティングシステムでは、メモリ領域とスレッドという二つの概念を単位として計算機資源を構成し、そこへの操作権を管理する情報もACL (Access Control List)という形で各メモリ領域および各スレッドに付随させて管理することが行われる。

【0007】例えば、スレッドの場合を例に説明すると、スレッド自体を操作したいとき、すなわちスレッドの実行を一時停止したり再開したりしたいときやスレッドを強制的に消滅させたいとき、またはスレッドの情報（レジスタ値やスタック等の内部状態）を調べたいときのため、オペレーティングシステムはスレッド操作命令群を備えており、あるスレッドから別のスレッドを操作することが可能である。このようなスレッド操作命令群は、ユーザプログラムからシステムコールとしてオペレーティング・システムに指示し、利用できるようになっている。

【0008】このようなスレッド操作命令があるときに、どのスレッドからでもスレッド操作命令を発行できるようにすると、不当な操作もできることになってしまうので保護の機能が必要になる。たとえばスレッドを強制的に消滅させるようなことは特定の権限を持つスレッドだけから行えるようにすることが必要になる。

【0009】さらに、仮想空間が複数あり、仮想空間ご

Petitioner Apple Inc. - Exhibit 1012, p. 1430

3

とに1つのプログラムやデータが配置されており、スレッドもその空間内しか動きまわれないようなＭａｃｈ（参考文献：「分散オペレーティング・システム」前川守他編、共立出版）をはじめとするオペレーティング・システムの場合、同じ空間内に存在するスレッドの保護を同一とし、スレッドの保護をメモリ空間の保護に依存する方法をとっている。

【００１０】しかし、それらのスレッドを区別して保護することはできない。また、単一仮想空間のシステムのように、1つのアドレス空間内にすべてのプログラムが配置され、複数のスレッドが存在する場合、スレッドの保護はメモリ保護だけではなくオペレーティングシステムによる権限の設定が必要になる。

【００１１】この問題のひとつの解決法は、スレッドの所有者を決めて、同一の所有者のスレッド間ではスレッドの操作を許す方式であり、Unixオペレーティングシステムのsignalはこれに相当する。しかしこれでは同一の所有者のスレッド間の保護の柔軟性に欠け、さらに、操作権限を他の所有者のスレッドに渡すことができない。また、複数の所有者のスレッドからのスレッド操作を可能にしたりできないなど、柔軟にスレッドの操作ができるようなスレッド保護機能が不足していた。

【００１２】また、一方ではデータ・ファイルへの操作権の多彩な設定ができるように、ファイルやディレクトリに対するＡＣＬに、情報の追加権、削除権、ＡＣＬの変更権などのさまざまな情報を付加して柔軟性を高めようとするＤＣＥ（参考文献：ＯＳＦ　ＤＣＥ技術解説、ソフトリサーチセンター）のような試みもあるが、やはり複数の所有者にメモリ領域のＡＣＬの管理を行わせるような柔軟な保護機能は不足している。

【００１３】

【発明が解決しようとする課題】以上述べてきたことに基づいて従来の操作権管理装置の主要な課題をまとめると次のようになる。

【００１４】（1）従来、スレッドに対する操作を、この操作を行う主体や、この操作を行う主体が存在するメモリ領域などに基づいて、許可するか否かを指示する方法は試みられている。しかし、スレッドに対するこの操作権情報を変更する権利については、例えば、そのスレッドの所有者には認める、あるいはルートと呼ばれる特別のユーザにのみ認める、といった単純な管理しか行うことができなかった。

【００１５】（2）また、従来、実メモリ、仮想メモリ、データ・ファイルなどのメモリ領域に対する操作を行う主体や、この操作を行う主体が存在するメモリ領域などに基づいて、許可するか否かを指示する方法は試みられている。しかし、メモリ領域に対するこの操作権情報を変更する権利については、例えば、そのメモリ領域の所有者には認める、あるいはルートと呼ばれる特別のユーザにのみ認める、といった単純な管理しか行うこと

4

ができなかった。

【００１６】（3）さらに、スレッドやメモリに対する操作権を柔軟に記述し、かつ、同様に変更権をも柔軟に記述すると、柔軟な記述ができるようになる反面、スレッドやメモリに対する保護のためのデータ量が多くなり、その管理が複雑になるという欠点を持つという問題がある。

【００１７】このように、従来の操作権管理装置では、メモリ領域単位での操作権限の設定ができなかったり、操作権限の設定の面で柔軟性に欠けたり、または、同一の仮想アドレス空間を共有しているスレッド間では保護が無かったか、または制約が強かった。

【００１８】本発明は、上記課題を考慮してなされたものであり、別々の仮想空間にいるスレッド間はもとより、同一仮想アドレス空間を共有しているスレッド間でのスレッド操作命令あるいは個々のメモリ領域に対して、同一の方法で柔軟性があり、かつ十分な保護を行う操作権管理装置を提供することを目的とする。

【００１９】

【課題を解決するための手段】上記目的を達成するために、本発明（請求項1）では、複数の並行して実行されるスレッドによりプログラムを実行する手段と、各スレッドに対する操作を、この操作を行う主体となるスレッドまたはユーザ、もしくはこの操作を行う主体が存在するメモリ領域またはプログラムの少なくともいずれかに基づいて、許可するか否かを指示する操作権情報を記憶する手段とを備える操作権管理装置において、前記操作権情報の変更を、この変更を行う主体となるスレッドまたは、ユーザもしくはこの変更を行う主体が存在するメモリ領域またはプログラムの少なくともいずれかに基づいて、許可するか否かを示す変更権情報を記憶する手段と、前記操作権情報の変更を実行する前に、記憶された前記変更権情報を参照して、この変更が許可されるか否かを検証する手段とを具備したことを特徴とする。

【００２０】また、本発明（請求項2）では、実メモリまたは仮想メモリを複数のメモリ領域の集合として管理する手段と、各メモリ領域に対する操作を、この操作を行う主体となるスレッドまたはユーザ、もしくはこの操作を行う主体が存在するメモリ領域またはプログラムの少なくともいずれかに基づいて、許可するか否かを指示する操作権情報を記憶する手段とを備える操作権管理装置において、前記操作権情報の変更を、この変更を行う主体となるスレッドまたは、ユーザもしくはこの変更を行う主体が存在するメモリ領域またはプログラムの少なくともいずれかに基づいて、許可するか否かを示す変更権情報を記憶する手段と、前記操作権情報の変更を実行する前に、記憶された前記変更権情報を参照して、この変更が許可されるか否かを検証する手段とを具備したことを特徴とする。

【００２１】また、望ましくは、上記発明（請求項1）

Petitioner Apple Inc. - Exhibit 1012, p. 1431

5

において、スレッド作成時には、あらかじめ定められたデフォルトの変更権情報が設定されることを特徴とする。

【００２２】また、望ましくは、上記発明（請求項２）において、メモリ領域作成時には、あらかじめ定められたデフォルトの変更権情報が設定されることを特徴とする。

【００２３】さらに、上記各操作権管理装置において、前記操作権情報を記憶する手段の情報を変更することが不可能になるような、前記変更権情報を記憶する手段の情報の変更を認めないようにしても良い。

【００２４】また、本発明（請求項３）では、上記発明（請求項１または２）において、前記変更権情報を前記操作権情報に付随されて記憶することを特徴とする。

【００２５】さらに、上記各操作権管理装置において、前記操作権情報を記憶する手段の情報を変更することのできる複数の条件を記憶する操作権管理権限記憶手段と、前記変更権情報を記憶する手段の情報に変更を加えようとする際に該操作権管理権限記憶手段の情報によりこの変更を行う権限があるか否かを検証する手段と、この権限があると検証された場合に前記変更を許可する手段とをさらに設けても良い。また、この場合、前記変更権情報を記憶する手段の情報を変更することが不可能になるような、前記操作権変更権管理権限記憶手段の情報の変更を認めないようにしても良い。

【００２６】

【作用】本発明（請求項１）によれば、スレッドへの操作権の管理のみならず、その操作権の管理の権限である変更権についても、さまざまな条件の組み合わせによって柔軟に表現、管理することができるようになる。

【００２７】この機構を用いれば、スレッドの操作権に関して、特定のスレッドにのみその変更を許可したり、またそれらの複数の条件を組み合わせて表現したりすることができる。

【００２８】特に、近年多く利用されるようになったグループウェアと呼ばれる計算機の協調作業アプリケーションを作成する際には、スレッドの共有や、排他制御、他のプログラムからの保護、などのきめ細かな制御を容易に記述することが必要になるが、本発明を用いればこの記述を柔軟に行うことができる。

【００２９】また、プログラムの誤りや、システム・コールの不正な呼び出しなどによって、スレッドへの操作権が異常に書き換えられてしまうことを未然に防ぐことができるので、スレッドの共有を行いつつもなおスレッドの動作に関する信頼性が飛躍的に向上する。

【００３０】また、本発明（請求項２）によれば、メモリ領域への操作権の管理のみならず、その操作権の管理の権限である変更権についても、さまざまな条件の組み合わせによって柔軟に表現、管理することができるようになる。

6

【００３１】この機構を用いれば、メモリ領域への操作権に関して、特定のスレッドにのみその変更を強化したり、特定のメモリ領域に存在するスレッドにのみその変更を許可したり、またそれら複数の条件を組み合わせて表現したりすることができる。

【００３２】特に、近年利用が試みられている単一仮想記憶と呼ばれる、複数のアプリケーションが同一の仮想空間上で動作するオペレーティング・システムにおいては、メモリ領域の共有や、排他制御、他のプログラムからの保護、などのきめ細かな制御を記述することが必要となるが、本発明を用いればこの記述を柔軟に行うことができる。

【００３３】また、プログラムの誤りや、システム・コールの不正な呼び出しなどによって、メモリ領域への操作権が異常に書き換えられてしまうことを未然に防ぐことができるので、メモリ領域に書かれたデータが不用意に書き換えられてしまうことがおこらず、メモリ領域の共有を行いつつもなおメモリ領域に書かれたデータに対する信頼性が飛躍的に向上する。

【００３４】さらに、本発明（請求項３）によれば、スレッドやメモリに対する操作権情報と、その操作権情報の変更を行う変更権情報とは、一般に共通点が多く、データ構造も似通ったものになることが多い。本発明においては、変更権情報を操作権情報に付随させて記憶することにより、共通のデータをなるべく一つのものとして管理するため、データ量を少なくすることができ、変更権および操作権を検証するための手続きも共通化する。

【００３５】また、スレッドやメモリに対する操作権や変更権などの管理は、一般にメモリ管理ユニットと呼ばれるハードウェアを用いることによって、実行性能を向上させることができる。そのような場合に、操作権および変更権それぞれに別のハードウェアを用意することは、計算機の構成を複雑にする可能性がある。しかし、本発明によって、操作権と変更権を同一に管理することにより、必要なハードウェアを単純化することができる。

【００３６】

【実施例】以下、図面を参照して本発明の実施例について説明する。

【００３７】本発明に係る操作権管理装置は、オペレーティング・システム（ＯＳ）と呼ばれる計算機システム全体の実行制御を行うものの構成要素の一部である。ＯＳは計算機資源であるメモリ、プロセッサ、周辺機器を管理し、また、ユーザプログラムとよばれるユーザが指示した実務上の処理を行うプログラムの実行を制御する。一つの装置上には複数のユーザプログラムがのっており、ＯＳがそれらのプログラム間の制御も行う。

【００３８】ユーザプログラムは、実行上に必要となる物理メモリなどの資源を確保したり、周辺機器にデータを入出力したり、他のユーザプログラムにデータを転送

Petitioner Apple Inc. - Exhibit 1012, p. 1432

7

したり、処理を依頼したり、実行を制御するためにＯＳに対して指示を行うことが必要となる。このＯＳに対する指示をシステムコールを呼ばれる特別な手段で行う。本実施例では、システムコールのうち、操作権を考慮するユーザプログラムの制御に関して説明する。

【００３９】操作権については、スレッドの管理とメモリ領域の管理がある。これらメモリ領域の管理とスレッドの管理については同一の部分が多いので、同様の機構を重複して説明することは避け、主にスレッドに対する操作権管理を例として、同一の部分には同一の用語を用いて説明する。

【００４０】なお、本実施例では、メモリの「操作」とは、アクセス（読み書き実行）のことを表すものとする。

【００４１】最初に、本実施例の特徴を概略的に述べる。本実施例では、個々のメモリ領域またはスレッドに対して、どのような条件で操作を許可するかという情報を登録したリストを設け、このリストにより許可されている場合に限り、操作を許可するとともに、この情報自体を変更することのできる権限を、前記リストと同一の形式、類似の形式あるいは共通の形式で管理する。また、特定の条件の時にのみこの変更を許す機構を付加する。また、この変更をする権限の変更についても同一の形式、類似の形式あるいは共通の形式で管理する。

【００４２】この結果、本実施例は、不当な操作命令やプログラムの誤りからメモリ領域やスレッドを保護し、またこのような誤った操作命令を検出することによってプログラムの誤りの検出を容易とするために、メモリ領域またはスレッドごとに設けた操作の可否を示す情報を変更する権利自体もそのメモリ領域またはスレッドが持つので、操作権の管理のみならず、操作権の管理の権限すらも同一の形式、類似の形式あるいは共通の形式で管理し、削除し、追加し、または変更することを柔軟に行うことができるようになる、という作用効果を奏するものである。

【００４３】また、この操作権の管理の権限は、メモリ領域やスレッドの所有者とは全く別の機構より、通常のアクセス制御リストと同様の形式で複数持つので、操作権管理の権限を複数のスレッドで共有したり、自分の作ったメモリ領域やスレッドの管理権を他のスレッドに譲渡したりするなどの柔軟な操作権管理が可能となる。

【００４４】（第１の実施例）以下、本発明の第１の実施例について説明する。

【００４５】図１は、本実施例の全体構成図である。プログラム記憶部１には、計算機で処理する命令が記述されたユーザプログラムや処理する対象のデータ、計算機で処理途中の結果を一時的に記憶するスタックなどのデータがメモリ空間上に蓄えられている。メモリ空間は、複数の領域（メモリ領域）に区切られて管理され、それぞれの領域には、お互いを区別するための識別子がついており、メモリ領域ごとにプログラムやデータやスタックを配置している。

8

【００４６】さらに、プログラム記憶部１に蓄えられているプログラムを解釈実行し、データを処理する実行主体であるプロセッサ２と、プロセッサ内の状態を管理するスレッド管理部３、プロセッサの実行状態の切り替え処理を行う実行状態切り替え部４がある。

【００４７】プロセッサ２内には、命令の実行途中に一時的に利用するレジスタ類、現在実行している命令のプログラム記憶部での位置を示すためのプログラムカウンタ（ＰＣ）、スタックデータの先頭位置を示すスタックポインタ（ＳＰ）などが存在し、これら一連のデータを入れ替えることで、複数の別々のユーザプログラムの処理を時分割で並行して進めることが可能となる。

【００４８】スレッドとは、上記プロセッサ内で使用する一連のデータのことを呼び、これを複数組用意し、このスレッドを切り替えてプロセッサにセットし実際に実行させることにより、時分割処理が可能となる。

【００４９】メモリ領域ＩＤ記憶部５は、現在実行中のプログラムがプログラム記憶部１のどのメモリ領域に存在しているかを、そのメモリ領域のＩＤとして記憶しているものである。これは、プロセッサ２内のＰＣの値を利用し、現在実行中のメモリ領域ＩＤを求めて、記憶している。このメモリ領域ＩＤは、現在実行中のプログラムＩＤとみなすこともできる。

【００５０】スレッド管理部３の中にはスレッド管理テーブルと呼ぶ表があり、プロセッサ２にセットするレジスタの情報やそのほかの情報がスレッドごとに管理されている。スレッドには、お互いを区別するために識別子（スレッドＩＤ）がついている。

【００５１】実行状態切替部４は、現在プロセッサ２上で実行しているスレッド（例えばスレッドＩＤ＝１）を中断し、スレッド（スレッドＩＤ＝１）の状態をスレッド管理テーブルの所定の位置（スレッドＩＤ＝１の格納領域）に退避し、別のスレッド（例えばスレッドＩＤ＝２）を起動すべく、スレッド管理テーブルのスレッド（スレッドＩＤ＝２）の情報をプロセッサ２に再セットし、スレッド（スレッドＩＤ＝２）の実行を再開させる。また、実行状態切替部４には、さらに、どのスレッドをセットし退避するかを決定するスレッドスケジューリング機構（図示せず）と、いつスケジューリングするか指示するタイマ部（図示せず）が存在する。

【００５２】スレッドＩＤ記憶部６は、スレッドＩＤを記憶するためのものである。

【００５３】操作権リスト記憶部７は、スレッド保護に関するテーブルを保持し、スレッドごとにスレッドに対する操作を実行する権限がどうなっているかを記憶するもので、操作権限判定部１２で使用される。本実施例はスレッドの操作権管理を例として説明しているが、メモリ領域の操作権管理の場合には、この操作権リスト記憶

Petitioner Apple Inc. - Exhibit 1012, p. 1433

9

部７はメモリ領域の保護に関するテーブルを保持し、スレッドごとにメモリ領域に対する操作を実行する権限がどうなっているかを記憶するものである。以下同様にスレッドに関する機構とメモリ領域に関する機構の同一の部分については説明を省略し、スレッドに関するものを代表して記述する。

【００５４】さて、システムコールとしてユーザプログラムを実行しているあるスレッドが他のスレッドに対して制御しようとする例として、Thread_Get _Statusシステムコールを発行する場合について説明する。

【００５５】このシステムコールは、スレッドＩＤで指示されたスレッドの状態、つまりそのスレッドのレジスタ類の情報を、このシステムコールの呼び出し元のユーザ・プログラムに通知するものである。いま、スレッド１（スレッドＩＤ＝１）がプログラムＡ（メモリ領域ＩＤ＝Ａ）を実行中、そこでスレッド２（スレッドＩＤ＝２）の情報をこのシステムコールで得ようとしたとする。Ｃ言語で記載されているプログラムＡでは、次のように記されている。

err = Thread_Get _Status(2, &Thread _Status);ここで、関数Thread_Get _Statusがスレッドの情報を得るシステムコールであって、第１引数の２は、スレッド２（スレッドＩＤ＝２）の情報を得ることを指示しており、第２引数の&Thread _Statusはシステムコールの結果得られたスレッド２の情報を格納するメモリ領域の先頭位置を指示している。また、このシステムコールの実行が成功したかどうかは、この関数の返り値として変数 err に入る。

【００５６】この関数をプログラムＡのスレッド１が実行すると、スレッド１はシステムコールにより実行モードがユーザレベルから特権レベルに遷移し、ＯＳを呼び出す。特権レベルとは、ＯＳが処理を行う専用レベルのことである。

【００５７】呼び出されたＯＳでは、ＯＳ内のシステムコール受付部８に処理が移る。ここでは、このシステムコールを呼びだした元のユーザプログラムの中断処理を行い、要求されたシステムコールの種類と指示された引き数を受取り、それぞれその情報を引数検出部９とシステムコールの種類判別部１０に送る。

【００５８】本例では、指示されたシステムコールは、Thread_Get _Statusなので、システムコールの種類判定部１０で、次には、Thread_Get _Status処理部１１を呼び出す。

【００５９】そこでの処理は、図２に示した操作権リスト記憶部７を使って行われる。この例では操作権リスト記憶部７はスレッドに対する操作権リストを記憶するものである。この記憶部には、図２に示したようなテーブルを保持している。テーブルには、操作スレッドＩＤ、対象スレッドＩＤ，操作スレッドが存在するメモリ領域ＩＤ、スレッド操作権限、スレッド操作権変更権限の各

10

エリアをもっている。

【００６０】同様のエリアとしては、対象スレッドが存在するメモリ領域ＩＤを指定することも考えられるが、本例ではかかるエリアを持たないものを例として説明する。

【００６１】メモリ領域に対する操作権リスト記憶部も同様であるが、テーブルの内容は若干異なる。これについての詳細は第２の実施例で説明する。

【００６２】操作スレッドＩＤとはスレッド操作のシステムコールを実行しようとしているスレッドのスレッドＩＤのことで、対象スレッドＩＤとはこのシステムコールの引数で指定された操作対象のスレッドＩＤを示す。また、操作スレッドが存在するメモリ領域ＩＤとは、この実行されようとしているシステムコールを含むプログラムの存在するメモリ領域ＩＤのことであり、スレッド操作権限とは、どういうスレッド操作が可能かを示すもので、スレッドの内部状態を読み出す権限、スレッドの内部状態を変更する権限、スレッドの実行を停止／再開する権限の３つの権限を独立に指定することができる。スレッド操作権変更権限は、スレッド操作権限の記入されたフィールドの情報を変更する権限のことであり、この権限が指定されている場合、その列に書かれているスレッド操作権限のフィールドの情報が変更できるだけでなく、その列に書かれている対象スレッドＩＤに関する全てのスレッド操作権限フィールドの情報を変更することができる。

【００６３】たとえば図の例では、スレッド１（スレッドＩＤ＝１）が発したシステムコールでは、スレッド２（スレッドＩＤ＝２）の内部状態の参照と変更は可能だが、スレッド２の実行の停止／再開およびスレッド２の操作権限の変更はできないことを示している。また、スレッド１は、スレッド３（スレッドＩＤ＝３）に対しては実行の停止／再開はできるがそれ以外の操作はできない。さらに、スレッド１は、スレッド２とスレッド３以外のスレッドに対しては、何の操作もできないことを示している。また、スレッド１００（スレッドＩＤ＝１００）はスレッド２の内部状態の読み出しおよび操作権限の変更ができることを示している。

【００６４】スレッド１が対象スレッドの場合の例で、テーブル中の操作スレッドが存在するメモリ領域ＩＤの部分にａｌｌという情報が保持されているが、これは、このシステムコールがどのユーザプログラムから行われても同等で、システムコールを実行するスレッドＩＤのみに実行権限が依存することを示している。

【００６５】メモリ領域ＩＤの欄がａｌｌでないときは、そのＩＤのメモリ領域に存在するプログラムからシステムコールが実行された時の操作権限を規定する。たとえば、スレッド３が、プログラムＡ（メモリ領域ＩＤ＝Ａ）の実行中、スレッド１に対しては、すべての操作が可能であるが、それ以外のときは、操作不可である。

Petitioner Apple Inc. - Exhibit 1012, p. 1434

11

つまり、スレッド3がプログラムB（メモリ領域ＩＤ＝B）の実行中、スレッド1に対して同様なシステムコールを実行しても操作できないし、スレッド5（スレッドＩＤ＝5）がプログラムAにおいてスレッド1に対して同じシステムコールを実行しても操作できない。すなわち、このテーブルに記載のないスレッド操作は一切できない。

【００６６】図2の例では、スレッド操作権限変更権限のフィールドは1つだけであるが、前記3つの権限ごとに操作権の変更権限を別々に指定できるようにしても良い。

【００６７】また、スレッド操作権限には、本前の例で挙げた3つの権限の他にもあってよい。例えば、操作をするユーザのユーザＩＤ、該当フィールドを時間制限するための有効期間開始時刻、有効時間終了時刻などが考えられる。その場合にも、それら権限の変更権を設定することができる。

【００６８】また、本実施例では、スレッド操作権限とスレッド操作権の変更権限とを、同一のテーブルの中で操作スレッドＩＤ、対象スレッドＩＤ、操作スレッドが存在するメモリ領域ＩＤを共有して表現しているが、スレッド操作権限と、スレッド操作権の変更権限とを別々のテーブルに記述し、それぞれについて操作スレッドＩＤ、対象スレッドＩＤ、操作スレッドが存在するメモリ領域ＩＤを指定しても良い。

【００６９】次に、Thread_Get _Status処理部１１の処理の流れを図3に示す。

【００７０】まず、ステップＳ１にて、このシステムコールを実行した操作スレッドＩＤ、メモリ領域ＩＤをそれぞれスレッドＩＤ記憶部6とメモリ領域ＩＤ記憶部5から情報を得る。上述したように、現在実行中のスレッドＩＤは、実行状態切替部4でセットされ、現在実行中のメモリ領域ＩＤは、プロセッサの内部にあるＰＣの情報からセットされている。さらに、システムコールの第一引数から対象スレッドＩＤ検出部１３が対象スレッドＩＤを得ている。第二引数からは、スレッド情報格納位置検出部１４が、このシステムコールの実行結果を格納するユーザ・プログラムのメモリ位置を検出する。

【００７１】次にステップＳ２にて、以上の3つの情報をもとに操作権記憶部７１の表を引き、該当エントリをサーチし、スレッド操作権限を調べる。もし、見つかれば、ステップＳ３に進み、なければステップＳ８を行うエラー処理部１５へ進む。

【００７２】サーチは、テーブルの上から順に比較を行い、最初にマッチしたエントリの情報を次のステップ以降で利用する。テーブルのフィールドのａｌｌ部分は、すべてにマッチすることを意味する。もし、テーブルの最後のエントリまで比較し、マッチしなかったらサーチの失敗となる。

【００７３】ステップＳ３では、見つかったエントリの

12

スレッド操作権限を表す部分のうち、スレッド内部状態読出権限に該当する部分の情報を読み出し、許可か否かを判断する。この判定は操作権限判定部１２で行う。もし判定で許可されればステップＳ４へ進み、不許可になればステップＳ８のエラー処理へ移る。

【００７４】次のステップＳ４では、対象スレッドに対して、許可されたスレッドの内部状態を読み出すためのスレッド管理テーブルの参照操作を実行する。この処理はスレッド状態参照実行部１６にて行う。ここでは、該当スレッドの内部状態であるスレッド情報を、スレッド情報格納位置検出部１４で指示されたメモリ中に格納する。

【００７５】ステップＳ５にて、ステップＳ４での処理結果を判定する。処理が成功するとステップＳ６にて、成功を示すコードをシステムコール終了部１７へ伝える。失敗するとステップＳ７にて、失敗を示すコードをシステムコール終了部１７へ伝える。

【００７６】ステップＳ８では、エラーコードをシステムコール終了部１７へ伝える。

【００７７】Thread_Get _Status処理部１１での処理を終えると、最後に、システムコール終了部１７に処理が進む。このシステムコールを実行したユーザプログラムに返す返値をシステムコールの返値として戻るように処理を行い、中断していた呼出元のユーザプログラムの実行ができるように復帰処理を行い、実行レベルを特権レベルからユーザレベルへ戻す処理を行う。

【００７８】次に、操作権記憶部７１に記入されたスレッド操作権限を変更するシステムシステムコールについて説明する。

【００７９】Thread_Add _Acl(指定操作スレッドＩＤ、指定対象スレッドＩＤ、指定メモリ領域ＩＤ、追加する指定操作権限）なるシステムコールは、上記で説明したスレッド操作権限を、新たに追加するものである。

【００８０】いま、スレッド１００（スレッドＩＤ＝１００）がスレッド1（スレッドＩＤ＝1）に対し、スレッド2（スレッドＩＤ＝2）の実行の停止／再開権限を付与しようとしたとする。Ｃ言語で記載されているプログラムＣでは、次のように記されている。

【００８１】err = Thread_Add _Acl(1, 2, all, THREAD _SUSPEND);ここで、関数Thread_Add _Acl は、スレッドに対する操作権を追加するためのシステムコールであって、第1引数の1は、指定した操作スレッド番号（対象スレッドＩＤ）が1であること、すなわちスレッドＩＤ＝1に対して権限を与えることを指示している。第2引数の2は、指定した対象スレッド番号（指定対象スレッドＩＤ）が2であること、すなわちスレッドＩＤ＝2を操作する権限であることを指示している。第3引数のａｌｌは、指定した操作スレッドが存在するメモリ領域ＩＤ（指定メモリ領域ＩＤ）がａｌｌであること、すなわち操作スレッドが存在するメモリ領域ＩＤに

Petitioner Apple Inc. - Exhibit 1012, p. 1435

よって与える権限を制限することはしないということを指示している。第４引数のTHREAD_SUSPEND は、これら３つの指定した組み合わせに対して、付加する操作権限（指定操作権限）を指示している。この例では、スレッドの実行の停止／再開権限を付加することを意味している。第４引数には複数種類の権限を同時に指定することもできる。

【００８２】この関数をプログラムＣのスレッド１００が実行すると、スレッド１００はシステムコールによりプロセッサの実行モードをユーザレベルから特権レベルに遷移させ、ＯＳを呼び出す。特権レベルとは、ＯＳが処理を行う専用レベルのことである。

【００８３】呼び出されたＯＳでは、ＯＳ内のシステムコール受付部８に処理が移る。ここでは、このシステムコールを呼び出した元のユーザプログラムの中断処理を行い、要求されたシステムコールの種類と指示された引数を受け取り、それぞれその情報を引数検出部９とシステムコールの種類判別部１０に送る。

【００８４】本例では、指示されたシステムコールは、Thread_Add _Acl なので、システムコールの種類判別部１０で、Thread_Add _Acl 処理部２１を呼び出す。Thread_Add _Acl 処理部２１は図１におけるThread_Get _Status処理部１１を図４のように置き換えたものである。なお、Thread_Add _Acl 処理部２１とThread_Get _Status処理部１１は本来一体のブロック図として示すべきものであるが、図が煩雑になるため説明の便宜をはかり図１および図４の別々の図としてある。

【００８５】そこでの処理は、図２に示したスレッド操作権リスト記憶部７を使って行われる。その内容および意味は前に説明した通りである。

【００８６】次に、図５にThread_Add _Acl 処理部２１の処理の流れを示す。

【００８７】まず、ステップＳ１１にて、このシステムコールを実行した実行スレッドＩＤ、メモリ領域ＩＤをそれぞれスレッドＩＤ記憶部６とメモリ領域ＩＤ記憶部５から情報を得る。さらに、システムコールの第２引数から指定対象スレッドＩＤ検出部２３が、このシステムコールによってスレッド操作権限の変更を行う対象としたスレッドのＩＤを得る。

【００８８】次にステップＳ１２にて、以上の３つの情報をもとにスレッド操作権リスト記憶部７のテーブルを引き、該当エントリをサーチする。もし、見つかれば、ステップＳ１３に進み、なければステップＳ１９を行うエラー処理部１５へ進む。サーチは、テーブルの上から順に比較を行い、最初にマッチしたエントリの情報を次のステップ以降で利用する。テーブルのフィールドのａ１１部分は、全てにマッチすることを意味する。もし、テーブルの最後のエントリまで比較し、マッチしなかったらサーチの失敗となる。

【００８９】ステップＳ１３では、見つかったエントリ

のスレッド操作権変更権限に該当する部分の情報を読み出し、許可か否かを判断する。この判定は操作権変更権判定部２６で行う。もし判定で許可されればステップＳ１４へ進み、不許可になればステップＳ１９のエラー処理へ移る。

【００９０】ステップＳ１４では、システムコールの第１引数から、指定対象スレッドＩＤ検出部２３が指定した対象スレッドＩＤを得る。また、システムコールの第３引数から、指定メモリ領域ＩＤ検出部２４が指定した操作スレッドが存在するメモリ領域ＩＤを得る。さらに、システム・コールの第４引数から、指定操作権限検出部２５が指定した追加すべき操作権限を得る。

【００９１】ステップＳ１５では、ステップＳ１１およびステップＳ１４で得られた対象スレッドＩＤ、指定対象スレッドＩＤ、指定メモリ領域ＩＤ、指定操作権限をもとに操作権リスト変更部２７が操作権リスト記憶部７を書き換える。つまり、まず操作権リスト記憶部７のテーブルを順にサーチし、対象スレッドＩＤと指定対象スレッドＩＤと指定メモリ領域ＩＤの３つが全て一致する列があれば、その列のスレッド操作権限のフィールドを書き換え、もしなければ、指定した３つのＩＤを示す列を新たに操作権リスト記憶部７のテーブルに追加する。この例では、指定した３つのＩＤと一致する列が最初に見付かるので、その列のスレッド操作権限のフィールドにあるスレッドの実行の停止／再開権限を×から○に変更する。

【００９２】ステップＳ１６にて、ステップＳ１５での処理結果を判定する。処理が成功するとステップＳ１７にて、成功を示すコードをシステムコール終了部１７へ伝える。失敗するとステップＳ１８にて、失敗を示すコードをシステムコール終了部１７へ伝える。ステップＳ１９では、エラーコードをシステムコール終了部１７へ伝える。

【００９３】Thread_Add _Acl 実行部２１での処理を終えると、最後にシステムコール終了部１７に処理が進む。このシステムコールを実行したユーザプログラムに返す返値をシステムコールの返値として戻るように処理を行い、中断していた呼出元のユーザプログラムの実行ができるように復帰処理を行い、実行レベルを特権レベルからユーザレベルへ戻す処理を行う。

【００９４】本例のようなThread_Add _Acl システム・コールの実行が成功した結果、図２で示された操作権リスト記憶部７のデータは図６のように変更される。

【００９５】本例では操作権リスト変更部２７において、書換を必要とする該当フィールドを書き換えるだけで、Thread_Add _Acl システム・コールからの要求を実行することができたが、Thread_Add _Acl システム・コールに与えられた引数の内容によっては、該当フィールドを書き換えるだけでは表現できず、操作権リスト記憶部７のデータを増やさなくてはならない。

Petitioner Apple Inc. - Exhibit 1012, p. 1436

15

【００９６】例えば、操作権リスト記憶部７のデータが先の図２に示したとおりであるとき、 Thread_Add _Acl (3, 2, A, THREAD_SUSPEND*THREAD_GET _STATUS) を実行した場合を考える。

【００９７】ここで、第１引数の３は、指定した操作スレッド番号（対象スレッドＩＤ）が３であること、すなわちスレッドＩＤ＝３に対して権限を与えることを指示しており、第２引数の２は、指定した対象スレッド番号（指定対象スレッドＩＤ）が２であること、すなわちスレッドＩＤ＝２を操作する権限であることを指示しており、第３引数のＡは、指定メモリ領域ＩＤがＡであること、すなわち、このシステムコールの実行により変更される権限は、プログラムＡ（メモリ領域ＩＤ＝Ａ）を実行中にのみ有効であることを指示しており、第４引数のTHREAD_SUSPEND は、これら３つの指定した組み合わせに対して、スレッドの実行の停止／再開権限を付加すること、そしてTHREAD_GET _STATUSはスレッドの内部状態読出権限を付加することを指示している。

【００９８】このシステム・コールが発せられると、操作権リスト変更部２７が、操作権リスト記憶部７のテーブルを順にサーチし、対象スレッドＩＤと指定対象スレッドＩＤと指定メモリ領域ＩＤの３つが全て一致する列をさがすが、この場合そのような列は存在しないので、このシステム・コールは、操作権リスト記憶部７の持つテーブルの一部のフィールドを書き換えるだけでは実行できない。指定した３つのＩＤを示す列を新たに操作権リスト記憶部７のテーブルに追加する。このような手順を踏むことにより、このシステム・コールの実行が終了すると、図２で示された操作権リスト記憶部７のデータは図７のように変更され、操作権リスト記憶部７の列の長さが１つ長くなっている。

【００９９】以上の説明においては、最初に操作権変更権限をどこに指定するかということについては記述されていない。一般にはＯＳの起動時に、一部の特権的なスレッドに対してこの権限を与え、以下階層的に権限を増やしてゆくことにより実現することが可能である。

【０１００】しかし、スレッドの作成時に必ず操作権変更権を指定しなければならないのは、プログラミングの手間を増やすおそれがあるので、メモリ領域またはスレッドの作成時には、あらかじめ定められたデフォルトの操作権変更権が設定されるように構成しても良い。デフォルトを何にするかについては各種考えられるが、最も簡単には、そのメモリ領域またはスレッドを起動したスレッドに対して操作権変更権を与えることが考えられる。この方法は、デフォルトとして従来ＯＳにおけるオーナーの概念を用いたことになり、さらに本実施例で説明した方法により、本発明の操作権管理装置はより柔軟な操作権管理を実現するものである。

【０１０１】また、先の例ではThread_Add _Acl の第４引数に指定することのできる指定操作権限に制約はないものとして記述したので、第４引数にTHREAD_CHANGE _ACL を指定することができる。すなわち、スレッド操作権変更権限を変更させることもできる。また、以上説明したThread_Add _Acl と同様に、Thread_DelAcl なるシステム・コールを用いて、例えば

Thread_Del _Acl(3,1,A,THREAD_CHANGE _ACL)

は、スレッドが、メモリ領域ＩＤ＝Ａのメモリ領域から、スレッドＩＤ＝１のスレッドのスレッド操作権限を取り除くことを意味している。この場合、永遠に誰にも操作権変更権限を変更することのできないようなスレッドを作ってしまうおそれがあるが、そういった変更が行われることが問題となるオペレーティングシステムにおいては、操作権変更権記憶部の情報を変更する際に、操作権記憶部の情報を変更することが不可能になるような変更を禁止するようにしても良い。例えば、先にあげた

Thread_Del _Acl(3,1,A,THREAD_CHANGE _ACL)

を実行すると、もはやスレッドＩＤ＝１のスレッドに対し、スレッド操作権限を変更することのできるスレッドが１つもなくなる。このようなシステム・コールが実行されると、操作権リスト変更部２７はエラーを検出したことになり、失敗を示すコードをシステムコール終了部１７へ伝え、操作権リスト記憶部のデータは変更されない。

【０１０２】また、操作権変更権を変更する権利を別個のものとして扱い、操作権リスト記憶部７に操作権変更権管理権限のフィールド（操作権変更権管理権限記憶部）を用意し、より確実な操作権管理を行っても良い。

【０１０３】さらには、操作権変更権記憶部の情報を変更することが不可能になるような、操作権変更権管理権限記憶部の情報の変更を禁止するようにしても良い。

【０１０４】なお、上記「スレッドＩＤ」を「ユーザＩＤ」に置き換えて構成することも可能である。この場合、図１におけるスレッドＩＤ記憶部６を、ユーザＩＤ記憶部と置き換える修正を施せば良い。

【０１０５】また、前述した「操作スレッドが存在するメモリ領域ＩＤ」を「操作スレッドが実行しているプログラムＩＤ」に置き換えて構成することも可能である。この場合、図１におけるメモリ領域ＩＤ記憶部５は、プログラムＩＤ記憶部と置き換える修正を施せば良い。

【０１０６】（第２の実施例）次に、本発明の第２の実施例について説明する。

【０１０７】本発明の操作権管理装置は、メモリ領域やスレッドに対する操作権管理を、例えばオーナーといった固定的な概念により行うのではなく、操作権変更権を操作権リスト自体に持たせ、自由に削除、追加させることによって柔軟に行うことを目的としている。ここでは、この機構を生かした例として、複数人による共同作業のアプリケーションが動作する場合に、操作権管理が柔軟に行われることを示す実施例について述べる。

【０１０８】ユーザーＡは、計算機を使った電子会議を

Petitioner Apple Inc. - Exhibit 1012, p. 1437

開催すべく、新たにスレッド10（スレッドID＝10）を作成した。より具体的には、ユーザーAの動かしていたログイン・シェルであるスレッド11がスレッド10を作成した。このとき、操作権リスト記憶部7の該当部分のデータは図8のようになっている。以下図には操作権リスト記憶部7のテーブルのうち、本実施例を説明するのに必要な部分のみを記述し、他の部分については記述を省略する。

【0109】スレッド11（スレッドID＝11）はスレッド10（スレッドID＝10）の内部状態読み出しおよびスレッド操作権の変更ができる。しかし、内部状態を変更したり、実行の停止／再開を行うことはできない。つまり、既に動き始めたスレッド10（スレッドID＝10）は、それを作成したスレッド11（スレッドID＝11）によって誤って実行を妨害されることはない。これらの初期状態はスレッドを作成するシステムコールの引数として指定するものとする。

【0110】作成されたスレッド10は電子会議のプログラムを実行し、ユーザーAとのインターフェースを司る。また、スレッド10は電子会議をサポートするためのメモリ領域として、メモリ領域30（メモリ領域ID＝30）を作成する。

【0111】メモリ領域30に関する操作権の管理には、スレッドの操作権の管理と同様に操作権リスト記憶部7を用いる。ただし、スレッドの操作権管理の説明で述べた対象スレッドID、スレッド操作権限、スレッドの内部状態読出権限、スレッドの内部状態変更権限、スレッドの実行の停止／再開権限、スレッド操作権変更権限は、メモリ領域の操作権管理においてはそれぞれ対象メモリ領域ID、メモリ領域操作権限、メモリ領域の内部データ読出権限、メモリ領域の内部データ変更権限、メモリ領域にあるプログラムの実行権限、メモリ領域操作権変更権限、となる。

【0112】図9に示した操作権リスト記憶部は、スレッド10がメモリ領域30の内部データの読み出しおよび変更、操作権変更ができることを意味している。

【0113】次にユーザーBおよびユーザーCが電子会議への参加を表明し、スレッド10は新たにユーザーBおよびユーザーCのためのスレッド12（スレッドID＝12）およびスレッド13（スレッドID＝13）を作成した。その結果、図8の操作権リスト記憶部7のデータは図10のように追加される。また電子会議をサポートするためのメモリ領域であるメモリ領域30は、スレッド12およびスレッド13からも使われるので、図9の操作権リスト記憶部7のデータは図11のように追加される。

【0114】つまり、スレッド12およびスレッド13はスレッド10によりコントロールされており、スレッドに関するあらゆる操作ができるが、スレッド12およびスレッド13は他のスレッドのコントロールをすることはできない。これにより、スレッド10が先導して電子会議の進行をプログラムされた通りに実行することができる。

【0115】共通のメモリ領域として使われるメモリ領域30は、スレッド10、スレッド12、スレッド13のいずれからもデータの読み出し、変更ができるが、その領域が誰から（どのスレッドから）どのような操作ができるかということを変更することができるのはスレッド10だけである。

【0116】このような仕組みで、複雑な依存関係のある電子会議のようなコミュニケーション・プログラムもOSの操作権管理機構を用いて確実に記述することができる。

【0117】次に、会議を先導していたユーザーAのスレッド10が、途中で会議を抜け、会議はそのまま進行している場合を考える。

【0118】単純にスレッド10が自分自身の実行を終了させたのでは、メモリ領域30の操作権を変更することのできるスレッドがいなくなり、会議を正しく進行させることができなくなる。このような場合には、ユーザーAは一旦会議の進行権を他の人（例えばユーザーB）に譲らなければならない。

【0119】まず、メモリ領域30の操作権をスレッド12（ユーザーBのスレッド、スレッドID＝12）に設定する。そして、スレッド13の管理権をスレッド12に譲り、そのあとで実行を終了する。それ以外のもので、操作スレッドIDが10であるものは、スレッド10の終了と同時に自動的に消滅させる。

【0120】これによって、図10および図11の操作権リスト記憶部はそれぞれ図12および図13のようになる。すなわち、メモリ領域30へのアクセスはスレッド12とスレッド13の両方からできるが、スレッドの管理自体の権利はスレッド12が継承する。注意すべき点は、スレッド10の実行が終了したために、ユーザーAのlogin shell であるスレッド11からは、電子会議を実行するいずれのプログラムに対しても何の権利もなくなっていることである。

【0121】ここに示した例は電子会議プログラムを実現する一方法を示したものであり、必ずしもこのような手順で操作権を譲渡してゆかなければプログラムが記述できないということは意味していない。

【0122】このようにして、スレッドおよびメモリ領域への操作権を管理しつつ、管理者の変更を実現することができる。

【0123】本発明の操作権管理装置を使えば、「会議に参加する」あるいは「会議から退室する」という、本実施例で具体的に例をあげて説明したような場合における、曖昧な操作権管理も、アプリケーションで逐一記述することなく、OSのサポートにより柔軟かつ確実に実現することができる。

Petitioner Apple Inc. - Exhibit 1012, p. 1438

【０１２４】また、本発明は上述した実施例に限定されるものではなく、その要旨を逸脱しない範囲で、種々変形して実施することができる。

【０１２５】

【発明の効果】本発明の操作権管理装置によれば、スレッドまたはメモリ領域に対する操作を保護するための操作権管理を柔軟かつ確実に行うことができる。

【図面の簡単な説明】

【図１】Thread_Get _Statusを説明するための構成図

【図２】図１の操作権リスト記憶部７の内部構成例を示す図

【図３】本実施例に係わる操作権管理装置において操作権を変更する動作を示すフローチャート

【図４】Thread_Add _Acl を説明するための構成図

【図５】本実施例に係わる操作権管理装置において操作権変更権を変更する動作を示すフロー図

【図６】図４の操作権リスト記憶部７の内部構成例を示す第１の図

【図７】図４の操作権リスト記憶部７の内部構成例を示す第２の図

【図８】電子会議開催時のスレッド操作権リストを示す図

【図９】電子会議開催直後のメモリ領域操作権リストを示す図

【図１０】電子会議に新たなメンバが参加した際のスレッド操作権リストを示す図

【図１１】電子会議に新たなメンバが参加した際のメモリ領域操作権リストを示す図

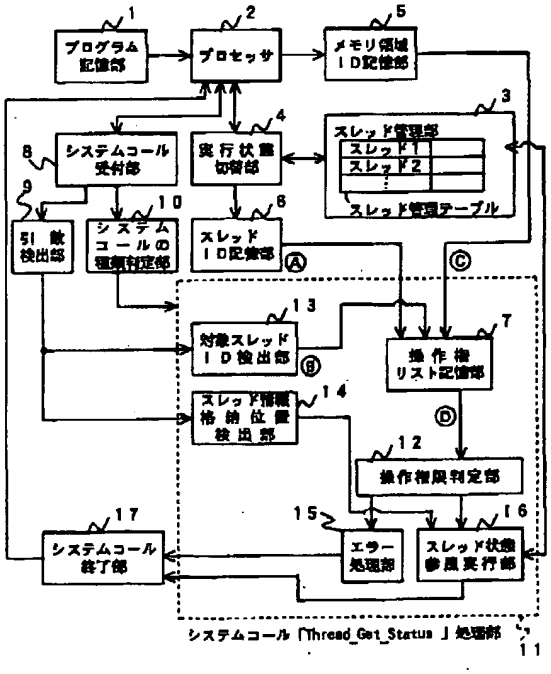
【図１２】ユーザーＡが電子会議の先導権をユーザーＢに委譲した際のスレッド操作権リストを示す図

【図１３】ユーザーＡが電子会議の先導権をユーザーＢに委譲した際のメモリ領域操作権リストを示す図

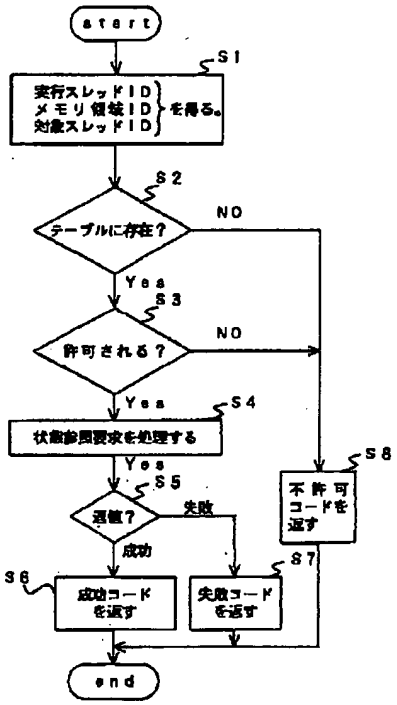
【符号の説明】

１…プログラム記憶部、２…プロセッサ、３…スレッド管理部、４…実行状態切替部、５…メモリ領域ＩＤ記憶部、６…スレッドＩＤ記憶部、７…操作権リスト記憶部、８…システムコール受付部、９…引数検出部、１０…システムコールの種類判定部、１１，２１…システムコール実行部、１２…操作権限判定部、１３…対象スレッドＩＤ検出部、１４…スレッド情報格納位置検出部、１５…エラー処理部、１６…スレッド状態参照実行部、１７…システムコール終了部、２２…指定操作スレッドＩＤ検出部、２３…指定対象スレッドＩＤ検出部、２４…指定メモリ領域ＩＤ検出部、２５…指定操作権限検出部、２６…操作権変更権判定部、２７…操作権リスト変更部

【図１】

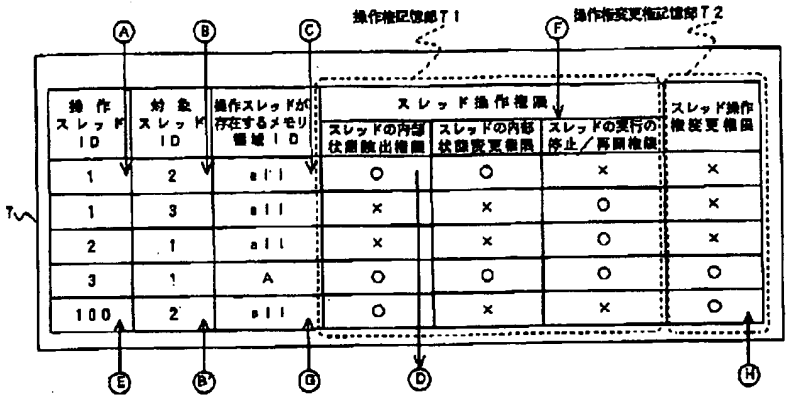


【図３】

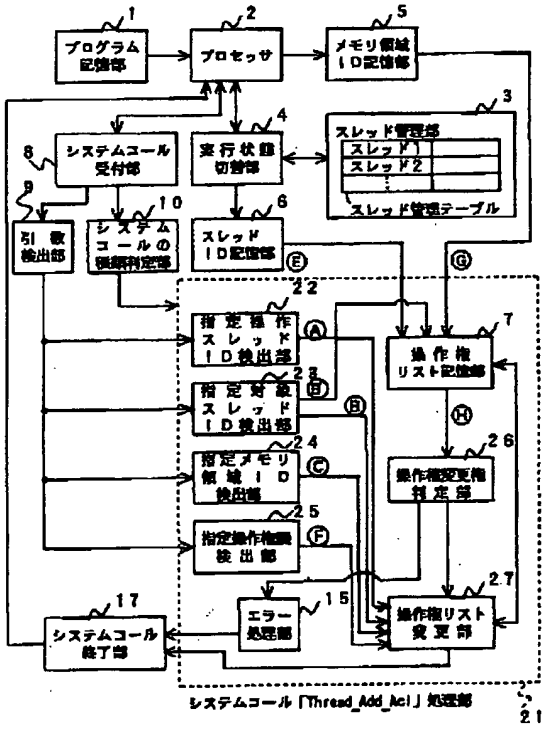


Petitioner Apple Inc. - Exhibit 1012, p. 1439

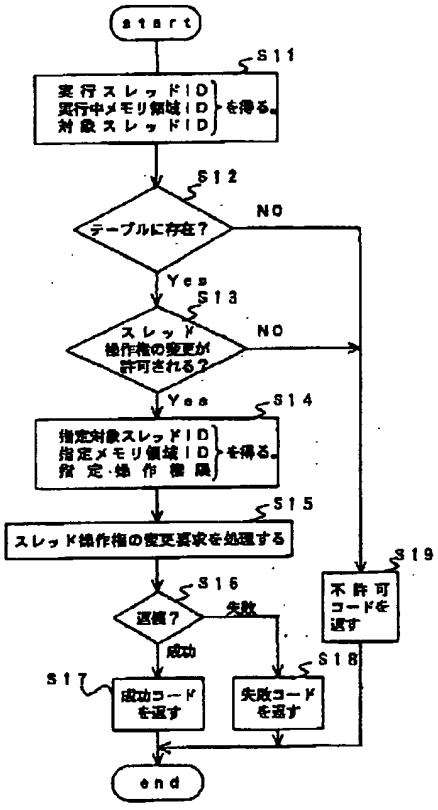
【図2】



【図4】



【図5】



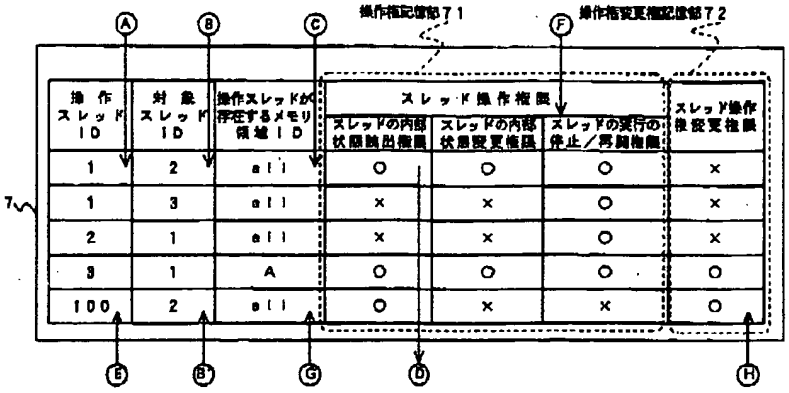
【図9】

操作スレッドID	対象メモリ領域ID	操作スレッドが存在するメモリ領域ID	メモリ領域操作権限			メモリ領域操作権変更権限
			メモリ領域の内部データ読出権限	メモリ領域の内部データ変更権限	メモリ領域のプログラム実行権限	
10	30	all	○	○	×	○

7

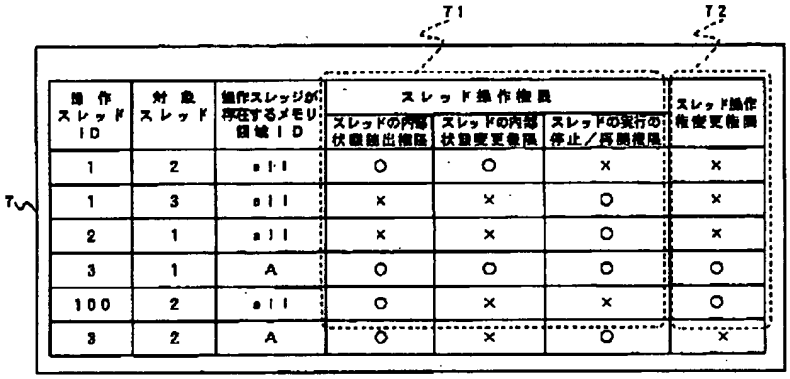
Petitioner Apple Inc. - Exhibit 1012, p. 1440

【図6】



操作スレッドID	対象スレッドID	操作スレッドが存在するメモリ領域ID	スレッド操作権限			スレッド操作権変更権限
			スレッドの内部状態読出権限	スレッドの内部状態変更権限	スレッドの実行の停止／再開権限	
1	2	all	○	○	○	×
1	3	all	×	×	○	×
2	1	all	×	×	○	×
3	1	A	○	○	○	○
100	2	all	○	×	×	○

【図7】



操作スレッドID	対象スレッド	操作スレッジが存在するメモリ領域ID	スレッド操作権限			スレッド操作権変更権限
			スレッドの内部状態読出権限	スレッドの内部状態変更権限	スレッドの実行の停止／再開権限	
1	2	all	○	○	×	×
1	3	all	×	×	○	×
2	1	all	×	×	○	×
3	1	A	○	○	○	○
100	2	all	○	×	×	○
3	2	A	○	×	○	×

【図8】

操作スレッドID	対象スレッドID	操作スレッドが存在するメモリ領域ID	スレッド操作権限			スレッド操作権変更権限
			スレッドの内部状態読出権限	スレッドの内部状態変更権限	スレッドの実行の停止／再開権限	
11	10	all	○	×	×	○

【図10】

操作スレッドID	対象スレッドID	操作スレッドが存在するメモリ領域ID	スレッド操作権限			スレッド操作権変更権限
			スレッドの内部状態読出権限	スレッドの内部状態変更権限	スレッドの実行の停止／再開権限	
11	10	all	○	×	×	○
10	12	all	○	○	○	○
10	13	all	○	○	○	○

Petitioner Apple Inc. - Exhibit 1012, p. 1441

【図11】

操作スレッドID	対象メモリ領域ID	操作スレッドが存在するメモリ領域ID	メモリ領域操作権限			メモリ領域操作権変更権限
			メモリ領域の内部データ読出権限	メモリ領域の内部データ変更権限	メモリ領域のプログラム実行権限	
10	30	all	○	○	×	○
12	30	all	○	○	×	×
13	30	all	○	○	×	×

【図12】

操作スレッドID	対象スレッドID	操作スレッドが存在するメモリ領域ID	スレッド操作権限			スレッド操作権変更権限
			スレッドの内部状態読出権限	スレッドの内部状態変更権限	スレッドの実行の停止／再開権限	
12	13	all	○	○	○	○

【図13】

操作スレッドID	対象メモリ領域ID	操作スレッドが存在するメモリ領域ID	メモリ領域操作権限			メモリ領域操作権変更権限
			メモリ領域の内部データ読出権限	メモリ領域の内部データ変更権限	メモリ領域のプログラム実行権限	
12	30	all	○	○	×	○
13	30	all	○	○	×	×

フロントページの続き

(72)発明者　申　承昊
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

(72)発明者　吉田　英樹
神奈川県川崎市幸区小向東芝町１番地　株式会社東芝研究開発センター内

Petitioner Apple Inc. - Exhibit 1012, p. 1442

Requested Patent: JP4369068A

Title: USER RIGHT MANAGING SYSTEM FOR ON-LINE SYSTEM ;

Abstracted Patent: JP4369068 ;

Publication Date: 1992-12-21 ;

Inventor(s): NISHIWAKI SHINJI ;

Applicant(s): CHIYUUBU NIHON DENKI SOFUTOUEA KK ;

Application Number: JP19910145068 19910618 ;

Priority Number(s): ;

IPC Classification: G06F15/00 ;

Equivalents: ;

ABSTRACT:

PURPOSE:To easily execute the batch grasp of user right and to reduce the maintenance manhour with respect to user right managing information by providing a user right managing table to a host computer.

CONSTITUTION:This user right managing system is constituted of a terminal equipment 1 including a CRT device 11 and a using information input means 12, the host computer 2 and the user right managing table for collectively managing respective user using right. The host computer 2 is provided with a user right registering means 21 for registering a new user in the table 3 from the terminal equipment 1, a user right changing means 22 for changing user right and a user right judging means 23 for judging the validity of a using request inputted from the input means 12 while referring the table 3. The table 3 consists of a user-sorted management table 31 for registering the password and right class (sort code of using right) of each user and a function-sorted management table 32 for registering a usable function code in each right class.

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平4－369068

(43)公開日　平成４年(1992)12月21日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ１	技術表示箇所
Ｇ０６Ｆ　15/00	３３０　Ａ	7323－5L		

審査請求　未請求　請求項の数１(全　5　頁)

(21)出願番号　特願平3－145068

(22)出願日　平成３年(1991)６月18日

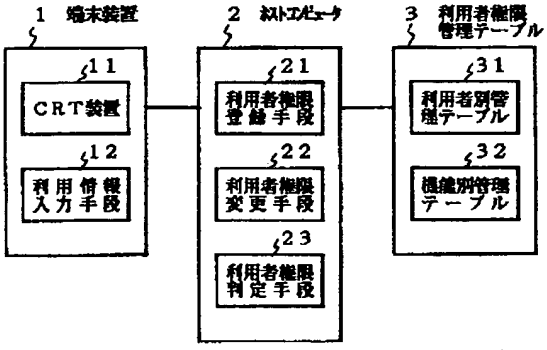
(71)出願人　000213301
中部日本電気ソフトウエア株式会社
愛知県名古屋市中区新栄２丁目28番22号
(72)発明者　西脇　信二
愛知県名古屋市中区新栄二丁目28番22号中部日本電気ソフトウエア株式会社内
(74)代理人　弁理士　内原　晋

(54)【発明の名称】　オンラインシステムの利用者権限管理方式

(57)【要約】

【構成】　ＣＲＴ装置１１，利用情報入力手段１２を含む端末装置１と、ホストコンピュータ２と、各利用者の利用権限を一括管理する利用者権限管理テーブル３で構成される。ホストコンピュータ２は、端末装置１から利用者権限管理テーブル３に新規利用者を登録する利用者権限登録手段２１と、利用者権限を変更する利用者権限変更手段２２と、利用者権限管理テーブル３を参照して利用情報入力手段１２からの利用要求の正当性を判定する利用者権限判定手段２３とを備えている。利用者権限管理テーブル３は、利用者別のパスワードと権限クラス（利用権限の種別コード）を登録した利用者別管理テーブル３１と、各権限クラスの利用可能な機能コードを登録した機能別権限管理テーブル３２とから成る。

【効果】　ホストコンピュータの利用者権限管理テーブルにより、利用者権限の一括把握が容易で、利用者権限管理情報のメンテナンス工数が低減される。



Petitioner Apple Inc. - Exhibit 1012, p. 1444

1

【特許請求の範囲】

【請求項1】　利用者が端末装置からホストコンピュータの各種オンラインサービス機能を利用する際の利用権限を管理するオンラインシステムの利用者権限管理方式において、利用者が入力した利用要求をホストコンピュータに伝達する利用情報入力手段を端末装置に備え、各利用者のオンラインサービス機能の利用権限の管理情報を記録した利用者権限管理テーブルと、端末装置から前記利用者権限管理テーブルに新規利用者を登録する利用者権限登録手段と、端末装置から前記利用者権限管理テーブルの管理情報を変更する利用者権限変更手段と、前記利用者権限管理テーブルを参照して前記利用情報入力手段からの利用要求の正当性を判定する利用者権限判定手段とをホストコンピュータに備えたことを特徴とするオンラインシステムの利用者権限管理方式。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明はオンラインシステムの利用者権限管理方式に関し、特に利用者が端末装置からホストコンピュータの各種オンラインサービス機能を利用する際の利用権限を管理するオンラインシステムの利用者権限管理方式に関する。

【0002】

【従来の技術】従来のオンラインシステムの利用者権限管理方式は、ホストコンピュータを利用して各種サービスを受ける端末装置内に、その端末装置を利用する利用者のパスワードやオンラインサービス機能別の利用権限に関する管理情報を持たせる方式であり、その管理情報の登録や変更を行う際には、各端末装置が配置されている支店や部署などの管理者の申請により、オンラインシステム管理部門が登録や変更を行った新たなフロッピーを作成送付し、端末装置側でこれを利用するなどの処置がとられていた。

【0003】

【発明が解決しようとする課題】上述した従来のオンラインシステムの利用者権限管理方式は、端末装置が設置されている職場ごとに利用権限を管理し、その情報を各端末装置が保持しているため、システム全体を一元的に把握し管理することが難しく、全体の状況が不明確になりやすい欠点がある。更に、多数の支店を有する企業等においては、利用者の新規登録や利用者権限の変更などの度にシステム管理部門で作業が発生し、かなりの工数を必要とするなどの問題がある。

【0004】本発明の目的は、上述の欠点に鑑み、オンラインシステムの利用者権限の管理を一元化し、利用者と利用権限の関係の全体像が把握しやすく、新規登録や変更による余分な工数が発生しないオンラインシステムの利用者権限管理方式を提供することにある。

【0005】

【課題を解決するための手段】本発明のオンラインシステムの利用者権限管理方式は、利用者が端末装置からホストコンピュータの各種オンラインサービス機能を利用する際の利用権限を管理するオンラインシステムの利用者権限管理方式において、利用者が入力した利用要求をホストコンピュータに伝達する利用情報入力手段を端末装置に備え、各利用者のオンラインサービス機能の利用権限の管理情報を記録した利用者権限管理テーブルと、端末装置から前記利用者権限管理テーブルに新規利用者を登録する利用者権限登録手段と、端末装置から前記利用者権限管理テーブルの管理情報を変更する利用者権限変更手段と、前記利用者権限管理テーブルを参照して前記利用情報入力手段からの利用要求の正当性を判定する利用者権限判定手段とをホストコンピュータに備えて構成されている。

2

【0006】

【実施例】次に、本発明の実施例について図面を参照して説明する。

【0007】図1は本発明のオンラインシステムの利用者権限管理方式の一実施例の機能構成を示すブロック図である。

【0008】本実施例のオンラインシステムの利用者権限管理方式は、ＣＲＴ装置１１と利用情報入力手段１２とを含む端末装置１と、ホストコンピュータ２と、ホストコンピュータ２に接続され各利用者の利用権限を一括管理する利用者権限管理テーブル３とから構成されている。ホストコンピュータ２には、端末装置１から利用者権限管理テーブル３に新規利用者を登録する利用者権限登録手段２１と、端末装置１から利用者権限管理テーブル３を更新する利用者権限変更手段２２と、利用者権限管理テーブル３を参照して利用情報入力手段１２からの利用要求の正当性を判定する利用者権限判定手段２３とを備えている。又、利用者権限管理テーブル３は、利用者別のパスワードと権限クラス（利用権限の種別を表すコード）とを登録した利用者別管理テーブル３１と、各権限クラスについて利用可能な機能コードを登録した機能別権限管理テーブル３２とで構成されている。

【0009】図2は利用情報入力手段１２による入力画面の説明図である。利用者はＣＲＴ装置１１の画面上に表示される図2の入力画面により、利用者を識別する利用者コードと、利用者コードと1対1に対応して定められているパスワードと、利用しようとするオンラインサービス機能を識別するために定められている機能コードと、処理に必要な固有処理項目とを入力する。

【0010】図3は利用者権限管理テーブル３の構成を示す説明図である。図3（a）に示すように、利用者別管理テーブル３１は、利用者コード，パスワード，権限クラスと、利用者権限管理テーブル３にエントリを登録できるか否かを識別する登録許可コードと、利用者権限管理テーブル３のエントリを変更できるか否かを識別する変更許可コードとから構成されている。一方、機能別

Petitioner Apple Inc. - Exhibit 1012, p. 1445

3

管理テーブル３２は、図３（ｂ）に示すように、オンラインサービスの機能コードと、これらの各機能を実行可能な権限クラスとの関係を示す機能許可コードテーブル部とから構成されている。

【００１１】次に、このように構成された本実施例の動作について、図２及び図３を参照して具体的なデータ例を用いて説明する（データは〔　〕で囲んで示す）。

【００１２】図２に示すように、入力画面上に利用者コード〔1〕，パスワード〔１１〕，機能コード〔A〕及び固有処理項目から成る利用要求が入力され、利用情報入力手段１２によりホストコンピュータ２に送信される。ホストコンピュータ２は、この利用要求を利用者権限判定手段２３に渡す。利用者権限判定手段２３は、利用者権限管理テーブル３を参照してこの利用要求が正当な利用者からのものであるか否かを判定する。

【００１３】その判定方法は、入力された利用者コード〔1〕で利用者別管理テーブル３１を検索し、テーブル上のパスワードが入力されたパスワード〔１１〕と一致するかを判定し、一致しなければ不当入力として処理を中断する。一致した場合は権限クラスを取得する。図３（ａ）の例では、入力されたパスワード〔１１〕が利用者別管理テーブル３１上のパスワード〔１１〕と一致するので、その権限クラス〔１０〕を取得する。

【００１４】次に、入力された機能コード〔A〕で機能別管理テーブル３２を検索し、機能許可コードテーブル部の権限クラス〔１０〕と等しいテーブル番号の許可コードが“０”ならば、利用者の権限は不当として処理を中断し、“１”ならば利用者の権限を正当と判定してオンライン処理を継続する。図３（ｂ）の例では、機能別管理テーブル３２のテーブル番号〔１０〕の許可コードは“1”であるから、利用要求は正当とみなされオンライン処理が継続される。

【００１５】次に、利用者権限管理テーブル３にエントリを登録する場合につき、その機能コードを〔B〕と仮定し説明する。利用者コード〔2〕，パスワード〔２２〕，機能コード〔B〕及び固有処理項目（テーブルへの登録内容）が入力され、ホストコンピュータ２へ送信される。ホストコンピュータ２は、この利用要求を利用者権限判定手段２３に渡す。利用者権限判定手段２３は、利用者権限管理テーブル３を参照して上述と同様な判定を行い、正当と判断した場合に利用者権限登録手段２１に利用要求を渡す。利用者権限登録手段２１は更に利用者別管理テーブル３１上の登録許可コードを判断し、登録許可コードが“０”ならば利用者に登録機能の利用権限が無いと判定し処理を中断する。登録許可コードが“１”ならば利用者は正当な権限を有すると判定し、利用者権限管理テーブル３へエントリを登録する。図３（ａ）の例では、利用者別管理テーブル３１上の利用者コード〔2〕の登録許可コードは“1”であるから、利用要求は正当とみなされ、固有処理項目の内容に

4

従って利用者権限管理テーブル３にエントリを登録する。

【００１６】次に、利用者権限管理テーブル３のエントリを変更する場合について、その機能コードを〔C〕と仮定して説明する。利用情報入力手段１２から利用者コード〔3〕，パスワード〔３３〕，機能コード〔C〕及び固有処理項目（エントリの変更内容）がホストコンピュータ２に送信されると、ホストコンピュータ２はこの利用要求を利用者権限判定手段２３へ渡す。利用者権限判定手段２１は、利用者権限管理テーブル３を参照して上述と同様な判定を行い、正当と判断した場合に利用者権限変更手段２２に利用要求を渡す。利用者権限変更手段２２は更に利用者別管理テーブル３１上の変更許可コードを判断し、変更許可コードが“０”ならば利用者に変更機能の利用権限は無いと判定し処理を中断し、変更許可コードが“１”ならば利用者は正当な権限を有すると判定し、利用者権限管理テーブル３のエントリを変更する。図３（ａ）の例では、利用者別管理テーブル３１上の利用者コード〔3〕の変更許可コードは“1”であるから、利用要求は正当とみなされ利用者権限管理テーブル３のエントリを変更する。

【００１７】上述したように、利用者権限管理テーブル３の登録および変更は、利用者権限判定手段２３による利用権限の判定に加え、それぞれ利用者権限登録手段２１及び利用者権限変更手段２２により利用権限の再チェックを経た後に実行される。なお、利用者別管理テーブル３１上の登録許可コード及び変更許可コードは、ホストコンピュータにおいてのみ変更可能であり、利用者権限登録手段２１及び利用者権限変更手段２２を用いて端末装置から変更することはできない。

【００１８】

【発明の効果】以上説明したように、本発明のオンラインシステムの利用者権限管理方式は、利用者権限の管理情報を利用者権限管理テーブルとしてホストコンピュータで一括して持つことにより、利用者とオンラインサービス機能との関連を一括して把握することが容易となり、加えて利用者権限管理情報のメンテナンス工数を省くことができる効果がある。

【図面の簡単な説明】

【図１】本発明の一実施例の構成を示すブロック図である。

【図２】本実施例の入力画面の説明図である。

【図３】本実施例の利用者権限管理テーブルの構成を示す説明図である。

【符号の説明】

１　端末装置
２　ホストコンピュータ
３　利用者権限管理テーブル
１１　ＣＲＴ装置
１２　利用情報入力手段

Petitioner Apple Inc. - Exhibit 1012, p. 1446

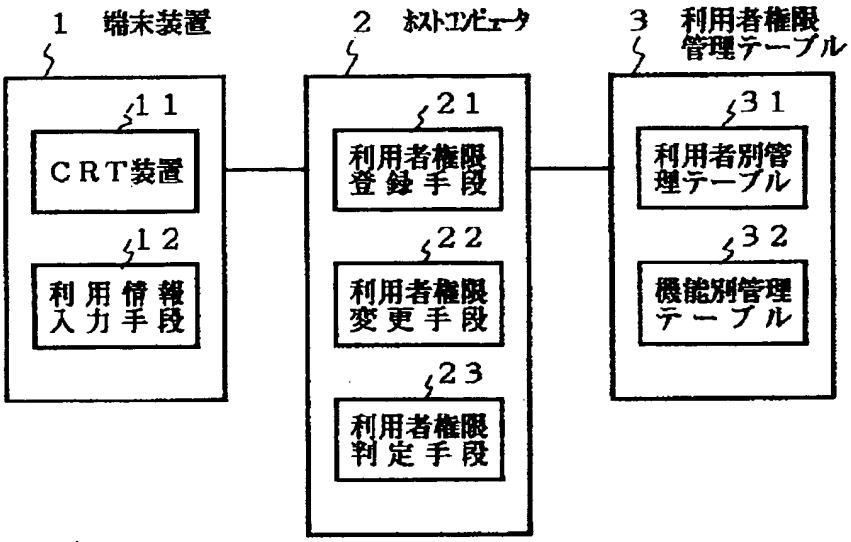
5

２１　利用者権限登録手段
２２　利用者権限変更手段
２３　利用者権限判定手段

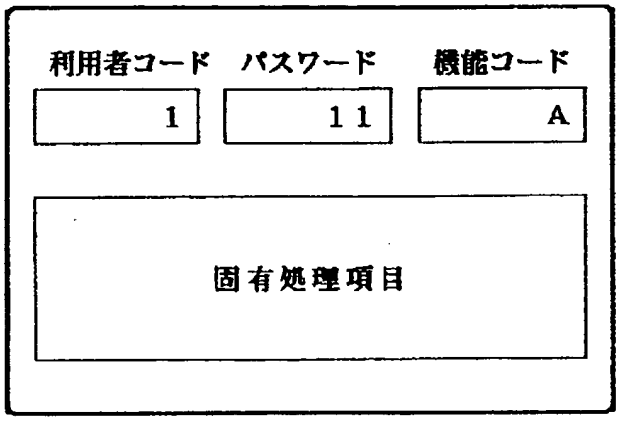
6

３１　利用者別管理テーブル
３２　機能別管理テーブル

【図１】



【図２】



Petitioner Apple Inc. - Exhibit 1012, p. 1447

【図3】

31　利用者別管理テーブル

利用者コード	パスワード	登録許可コード	変更許可コード	権限クラス
1	11	0	0	10
2	22	1	0	20
3	33	0	1	24

(a)

32　機能別管理テーブル

機能コード	機能許可コードテーブル部																							
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
A	0	0	0	0	0	1	0	0	0	1	0	0	0	0	0	1	0	0	0	0	0	0	0	0
B	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1	0	0	0	0
C	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

(b)

Petitioner Apple Inc. - Exhibit 1012, p. 1448

Requested Patent: JP5268415A

Title: PICTURE READER ;

Abstracted Patent: JP5268415 ;

Publication Date: 1993-10-15 ;

Inventor(s): TAGUCHI KAZUE; others: 04 ;

Applicant(s): RICOH CO LTD ;

Application Number: JP19920006527 19920117 ;

Priority Number(s): ;

IPC Classification:

H04N1/04; B41J29/40; B42D9/04; G03B27/50; G03B27/62; G03G15/00; G03G15/04; G06F15/64; H04N1/00; H04N1/10 ;

Equivalents: ;

ABSTRACT:

PURPOSE:To cope with the problem of copy right by detecting an identification code for copy right management with a detecting means and automatically blocking the read of an original added with a code.

CONSTITUTION:A page turnover read unit 1 is provided so as to applies exposure scanning to a book original 92 placed opening on an original platen 18 to read a book original picture. Moreover, a bar code scanner 341a reading a bar code pattern 341c of a back cover of the book original 92 is provided to read an identification code for copy right management and the code is inputted to a one-chip microcomputer 330. The one-chip microcomputer 330 discriminates whether or not the copy of the bar code pattern is permitted and the copying is attained only when the copy of the pattern is permitted.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（Ａ）**　(11)特許出願公開番号

特開平5－268415

(43)公開日　平成5年(1993)10月15日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ１	技術表示箇所
Ｈ０４Ｎ　1/04		Ｚ　7251－5Ｃ		
Ｂ４１Ｊ　29/40		Ｚ　8804－2Ｃ		
Ｂ４２Ｄ　9/04		Ｃ　8604－2Ｃ		
		Ｚ　8604－2Ｃ		
Ｇ０３Ｂ　27/50		Ａ　9017－2Ｋ		

審査請求　未請求　請求項の数８(全 62 頁)　最終頁に続く

(21)出願番号　特願平4－6527

(22)出願日　平成４年(1992)１月17日

(71)出願人　000006747
株式会社リコー
東京都大田区中馬込１丁目３番６号

(72)発明者　田口　和重
東京都大田区中馬込１丁目３番６号・株式会社リコー内

(72)発明者　藤岡　哲弥
東京都大田区中馬込１丁目３番６号・株式会社リコー内

(72)発明者　髙橋　浩
東京都大田区中馬込１丁目３番６号・株式会社リコー内

(74)代理人　弁理士　樺山　亨　(外１名)

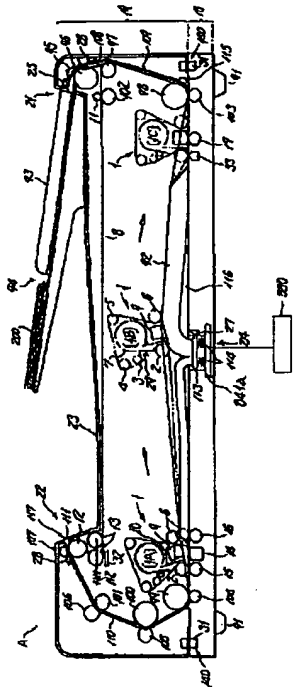
最終頁に続く

(54)【発明の名称】　画像読み取り装置

(57)【要約】

【目的】コピーされるブック原稿が著作権利用となるか否かを複写システム側でのブック原稿の認識およびカウント動作によって管理することのできる原稿読み取り装置を提供する。

【構成】原稿台（１８）上に見開かれて載置されたブック原稿（９２）を露光走査して該ブック原稿画像の読み取りを行なう読み取り手段（ページめくり読取ユニット１）と、原稿台に載置されたブック原稿に付された識別符号（バーコードパターン３４１Ｃ）を検知する検知手段（バーコードスキャナ３４１ａ）と、前記検知手段によって、前記識別符号が検知された場合にのみ前記読み取り手段による読み取り動作を可能とするように前記読み取り手段を制御する制御手段（ワンチップマイコン３３０）と、を有する。



Petitioner Apple Inc. - Exhibit 1012, p. 1450

1

【特許請求の範囲】

【請求項1】原稿台と、

前記原稿台上に見開かれて載置されたブック原稿の原稿面上を露光走査することによって前記ブック原稿画像の読み取りを行なう読み取り手段と、

原稿台に載置されたブック原稿の表紙又は背表紙の所定位置に付された識別符号を検知する検知手段と、

前記検知手段によって、前記識別符号が検知された場合にのみ前記読み取り手段による読み取り動作を可能とするように前記読み取り手段を制御する制御手段と、

を有することを特徴とする画像読み取り装置。

【請求項2】原稿台上に載置されたブック原稿のめくり・読み取りを行なうブック原稿読み取りモードと、

シート原稿トレイ上に載置されたシート原稿を1枚毎に原稿台上に給送して、前記シート原稿画像の読み取りを行なうＡＤＦモードと、が選択可能な画像読み取り装置であって、

原稿台に載置されたブック原稿の表紙又は背表紙の所定位置に付された識別符号を検知する検知手段と、

ブック原稿読み取りモードが選択されている場合には、前記検知手段によって前記識別符号が検知されたときにのみ前記読み取り手段による読み取り動作を可能とするように前記読み取り手段を制御する制御手段と、

を有することを特徴とする画像読み取り装置。

【請求項3】原稿台と、

前記原稿台上に載置されたブック原稿のめくり・読み取りを行なうブック原稿めくり・読み取りモードと、

前記原稿台上に載置された任意の原稿上の原稿画像の読み取りを行なう圧板モードと、が選択可能な画像読み取り装置であって、

原稿台に載置されたブック原稿の表紙又は背表紙の所定位置に付された識別符号を検知する検知手段と、

ブック原稿読み取りモードが選択されている場合には、前記検知手段によって前記識別符号が検知されたときにのみ前記読み取り手段による読み取り動作を可能とするように前記読み取り手段を制御する制御手段と、

を有することを特徴とする画像読み取り装置。

【請求項4】原稿台と、

前記原稿台上に見開かれて載置されたブック原稿の原稿面を露光走査することによって前記ブック原稿画像の読み取りを行なう読み取り手段と、

装置外部から読み取り手段による読み取り動作を可能にするための識別信号を入力する入力手段と、

前記識別信号の入力を検知する検知手段と、

前記検知手段によって前記識別信号の入力が検知された場合にのみ前記読み取り手段による読み取り動作を可能とするように前記読み取り手段を制御する制御手段と、

を有することを特徴とする画像読み取り装置。

【請求項5】原稿台上に載置されたブック原稿のめくり・読み取りを行なうブック原稿読み取りモードと、

2

シート原稿トレイ上に載置されたシート原稿を1枚毎に原稿台上に給送して、前記原稿画像の読み取りを行なうＡＤＦモードと、が選択可能な画像読み取り装置であって、

装置外部から読み取り手段による読み取り動作を可能とするための識別信号を入力する入力手段と、

前記識別信号の入力を検知する検知手段と、

ブック原稿読み取りモードが選択されている場合には前記検知手段によって前記識別信号の入力が検知されたときにのみ前記読み取り手段による読み取り動作を可能とするように前記読み取り手段を制御する制御手段と、

を有することを特徴とする画像読み取り装置。

【請求項6】原稿台と、

前記原稿台上に載置されたブック原稿のめくり・読み取りを行なうブック原稿読み取りモードと、

前記原稿台上に載置された任意の原稿上の原稿画像の読み取りを行なう圧板モードと、が選択可能であって、

装置外部から読み取り手段による読み取り動作を可能とするための識別信号を入力する入力手段と、

前記識別信号の入力を検知する検知手段と、

ブック原稿読み取りモードが選択されている場合には、前記検知手段によって前記識別信号の入力が検知されたとにきのみ前記読み取り手段による読み取り動作を可能とするように前記読み取り手段を制御する制御手段と、

を有することを特徴とする画像読み取り装置。

【請求項7】原稿台と、

前記原稿台上に載置された原稿の原稿面上を露光走査することによって原稿画像の読み取りを行なう読み取り手段と、

前記読み取り手段によって読み取られた画像情報を出力する出力手段と、を有する画像読み取り装置であって、

前記読み取り手段による原稿面上の露光走査によって原稿面上の所定位置に付された識別符号の検出動作を行なうと共に、前記検出動作によって前記識別符号が検知された場合にのみ前記出力手段による出力動作を可能とするように前記出力手段を制御する、

ことを特徴とする画像読み取り装置。

【請求項8】請求項7において、読み取り手段によって読み取られた画像情報を出力する際、所定位置に識別符号が付されたブック原稿から読み取った情報である場合は、その旨を識別するための付加情報を出力手段による出力情報に付加する、

ことを特徴とする画像読み取り装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、複写機及びファクシミリ等のブック原稿の画像読み取り装置に関する。

【0002】

【従来の技術】ブック原稿の読み取り装置および方法としては、（1）原稿支持台上に上向きに見開いて載置し

Petitioner Apple Inc. - Exhibit 1012, p. 1451

たブック原稿の原稿面を情報のコンタクトガラスに当接させ、このコンタクトガラスを挟んで対向配置された走査光学系の走査によって原稿画像を露光走査する装置、（2）原稿載置面上に上向きに見開いて載置されたブック原稿の原稿面上を密着型読み取りセンサにより露光走査して原稿画像を読み取る装置、等が知られている。

【０００３】一方、複写機及びファクシミリ等における原稿読み取り装置として、シート原稿を原稿読み取り位置に自動的に搬送して原稿情報を読み取り、読み取りの終了した原稿を上記原稿読み取り位置から自動的に排出する自動原稿給送装置（ＡＤＦ）が知られている。

【０００４】このように、原稿がシート原稿の場合には、ＡＤＦを搭載することにより、その原稿情報の読み取りを自動的に行うことができるが、原稿がブック原稿の場合には、自動ページめくり機構の実現が事実状困難なため、現段階では、ブック原稿のページめくりを手動的にしか行うことができない状況にある。

【０００５】従来、こうした現状に鑑み、手間の掛るブック原稿の読み取りを自動化するための方法や手段の提案が種々なされている。

【０００６】このブック原稿の自動読み取りを実現させるために不可欠となるブック原稿の自動ページめくり装置および方法としては、（3）下向きに見開いて載置したブック原稿を移動させながら、その原稿ページを吸引して分離する装置、（4）上向きに見開いて載置したブック原稿の原稿ページを吸引して分離する装置、（5）上向きに見開いて載置したブック原稿の原稿ページをローラ，アーム等でめくる装置、等が知られている。

【０００７】しかしながら、上記の従来技術は、アイデアのみの提案が多く、およそ実現し得るレベルには到達しておらず、以下のような問題点がある。

【０００８】すなわち、（1）原稿支持台上に上向きに見開いて載置したブック原稿の原稿面を情報のコンタクトガラスに当接させ、このコンタクトガラスを挟んで対向配置された走査光学系の走査によって原稿画像を露光走査する装置では、ブック原稿の原稿ページをめくる位置から露光走査を行なう位置までブック原稿を移動させる必要があり、原稿露光走査効率が低下するとともに、装置の大型化が避けがたくなる不具合があった。

【０００９】また、（2）原稿載置面上に上向きに見開いて載置されたブック原稿の原稿面上を密着型読み取りセンサにより露光走査して原稿画像を読み取る装置では、装置の大型化という点は解消し得るものの、ブック原稿の原稿面を押圧する手段を備えていないため、載置された原稿面が浮き上がり易く、原稿面の読み取り走査が不安定になる不具合を有していた。

【００１０】一方、（3）下向きに見開いて載置したブック原稿を移動させながら、その原稿ページを吸引して分離する装置では、ブック原稿の自重の影響によりページめくりの信頼性が損なわれるばかりでなく、そのページめくり時に原稿面が擦れて原稿が破損する虞れがあり、さらに、その構成上装置の大型化を余儀なくされる不具合があった。

【００１１】また、（4）上向きに見開いて載置したブック原稿の原稿ページを吸引して分離する装置、並びに、（5）上向きに見開いて載置したブック原稿の原稿ページをローラ，アーム等でめくる装置等では、ブック原稿の上側空間を移動する従来のページ分離機構が複雑且つ大型なため、装置の大型化が避けがたくなる不具合があった。

【００１２】こうした現状に鑑み、本出願人は、例えば、特願平２－１９３５８９号明細書等に開示したように、原稿台の原稿載置面に沿って張架されたページ押えベルトの一部に上記原稿載置面から離間する迂回部を形成させながら、上記原稿載置面とページ押えベルトとの間に見開かれて載置されたブック原稿の原稿面に対して、ページ収納手段，ページ吸着手段，ページ分離手段および読み取り手段等が配設されたページめくり読み取りユニットを相対移動させることによって、上記ブック原稿のページめくりおよび原稿読み取り走査を行なうブック原稿のページめくり読み取り装置（以下、ＭＦＤＳという）を提案した。

【００１３】この提案によるＭＦＤＳによれば、上記明細書等に記述したように、複写作業等に多大な労力を要していたブック原稿のページめくり操作および原稿読み取り走査を完全に自動化させることができ、複写等の生産性を著しく向上させる多機能原稿読み取りシステムを実現することができる。

【００１４】

【発明が解決しようとする課題】前記ＭＦＤＳは、ブック原稿の原稿情報の読み取り走査および原稿ページめくり動作を自動で行なう機能を持っているので、このＭＦＤＳをプリンタと接続することによって、書籍や雑誌等のコピーを人手を掛けずに高速で行なうことができる。

【００１５】しかしながら、周知のように、一般の書籍などを著作者の許可を得ないで複写することは、純粋な私的利用を除いて原則として著作権法違反となる。

【００１６】そこで、本発明は、前記ＭＦＤＳを含むブック原稿画像の読み取り手段を有する画像読み取り装置において、許可された特定のブック原稿から、或いは、特定ユーザーによる画像読み取り（複写）のみを可能とすることにより、著作権問題への対処を図り得る画像読み取り装置を提供することを目的とする。

【００１７】

【課題を解決するための手段】本発明は、上述の課題を解決するために、次の（1）乃至（8）の構成とした。

【００１８】（1）．原稿台と、前記原稿台上に見開かれて載置されたブック原稿の原稿面上を露光走査することによって前記ブック原稿画像の読み取りを行なう読み取り手段と、原稿台に載置されたブック原稿の表紙又は

Petitioner Apple Inc. - Exhibit 1012, p. 1452

5

背表紙の所定位置に付された識別符号を検知する検知手段と、前記検知手段によって、前記識別符号が検知された場合にのみ前記読み取り手段による読み取り動作を可能とするように前記読み取り手段を制御する制御手段と、を有することとした。

【００１９】（２）．原稿台上に載置されたブック原稿のめくり・読み取りを行なうブック原稿めくり・読み取りモードと、シート原稿トレイ上に載置されたシート原稿を１枚毎に原稿台上に給送して、前記シート原稿画像の読み取りを行なうＡＤＦモードと、が選択可能な画像読み取り装置であって、原稿台に載置されたブック原稿の表紙又は背表紙の所定位置に付された識別符号を検知する検知手段と、ブック原稿めくり・読み取りモードが選択されている場合には、前記検知手段によって前記識別符号が検知されたときにのみ前記読み取り手段による読み取り動作を可能とするように前記読み取り手段を制御する制御手段と、を有することとした。

【００２０】（３）．原稿台と、前記原稿台上に載置されたブック原稿のめくり・読み取りを行なうブック原稿めくり・読み取りモードと、前記原稿台上に載置された任意の原稿上の原稿画像の読み取りを行なう圧板モードと、が選択可能な画像読み取り装置であって、原稿台に載置されたブック原稿の表紙又は背表紙の所定位置に付された識別符号を検知する検知手段と、ブック原稿めくり・読み取りモードが選択されている場合には、前記検知手段によって前記識別符号が検知されたときにのみ前記読み取り手段による読み取り動作を可能とするように前記読み取り手段を制御する制御手段と、を有することとした。

【００２１】（４）．原稿台と前記原稿台上に見開かれて載置されたブック原稿の原稿面を露光走査することによって前記ブック原稿画像の読み取りを行なう読み取り手段と、装置外部から読み取り手段による読み取り動作を可能にするための識別信号を入力する入力手段と、前記識別信号の入力を検知する検知手段と、前記検知手段によって前記識別信号の入力が検知された場合にのみ前記読み取り手段による読み取り動作を可能とするように前記読み取り手段を制御する制御手段と、を有することとした。

【００２２】（５）．原稿台上に載置されたブック原稿のめくり・読み取りを行なうブック原稿めくり・読み取りモードと、シート原稿トレイ上に載置されたシート原稿を１枚毎に原稿台上に給送して、前記原稿画像の読み取りを行なうＡＤＦモードと、が選択可能な画像読み取り装置であって、装置外部から読み取り手段による読み取り動作を可能とするための識別信号を入力する入力手段と、前記識別信号の入力を検知する検知手段と、ブック原稿めくり・読み取りモードが選択されている場合には前記検知手段によって前記識別信号の入力が検知されたときにのみ前記読み取り手段による読み取り動作を可能とするように前記読み取り手段を制御する制御手段と、を有することとした。

6

【００２３】（６）．原稿台と、前記原稿台上に載置されたブック原稿のめくり・読み取りを行なうブック原稿めくり・読み取りモードと、前記原稿台上に載置された任意の原稿上の原稿画像の読み取りを行なう圧板モードと、が選択可能であって、装置外部から読み取り手段による読み取り動作を可能とするための識別信号を入力する入力手段と、前記識別信号の入力を検知する検知手段と、ブック原稿めくり・読み取りモードが選択されている場合には、前記検知手段によって前記識別信号の入力が検知されたときにのみ前記読み取り手段による読み取り動作を可能とするように前記読み取り手段を制御する制御手段と、を有することとした。

【００２４】（７）．原稿台と、前記原稿台上に載置された原稿の原稿面上を露光走査することによって原稿画像の読み取りを行なう読み取り手段と、前記読み取り手段によって読み取られた画像情報を出力する出力手段と、を有する画像読み取り装置であって、前記読み取り手段による原稿面上の露光走査によって原稿面上の所定位置に付された識別符号の検出動作を行なうと共に、前記検出動作によって前記識別符号が検知された場合にのみ前記出力手段による出力動作を可能とするように前記出力手段を制御することとした。

【００２５】（８）．（７）において、読み取り手段によって読み取られた画像情報を出力する際、所定位置に識別符号が付されたブック原稿から読み取った情報である場合は、その旨を識別するための付加情報を出力手段による出力情報に付加することとした。

【００２６】

【作用】著作権管理用としての識別符号の付された原稿の読み取りは自動的に阻止され

【００２７】る。

【実施例】以下、本発明の実施例を図に基づいて詳細に説明する。本発明の実施例の説明に先立って、この発明が実施される前記のＭＦＤＳ（ブック原稿のページめくり読み取り装置）について、その構成および動作を説明する。

【００２８】先ず、図１を参照しながら、本発明による原稿読み取り装置におけるめくり搬送ベルトの周辺の構成について説明する。図１は、本発明を実施した、マルチ・ファンクション・ドキュメント・スキャナＡ（以下、”ＭＦＤＳ”とする）の概略断面図である。図１において、めくり搬送ベルト８は、駆動ローラ１２、テンションローラ１３、第１ベルト支持ローラ９７、第２ベルト支持ローラ９８、第３ベルト支持ローラ９９、第４ベルト支持ローラ１００、及び、第５ベルト支持ローラ１０１により支持されている。

【００２９】このとき、めくり搬送ベルト８は、ページめくり読取ユニット１のめくりローラ２、第１パイアス

Petitioner Apple Inc. - Exhibit 1012, p. 1453

7

ローラ3、第1ローラ4、第2ローラ5、及び、押えローラ6を介して、このページめくり読取ユニット1を取り巻くように支持されている。

【0030】テンションローラ13は、ベルトテンションスプリング112によって、図1において左方向に引っ張られ、めくり搬送ベルト8に適度なテンションを与え、ブック原稿92の原稿面を押圧している。ベルトテンションセンサ32は、テンションローラ13の移動量からめくり搬送ベルト8のテンションを検出している。

【0031】一方、MFDSの搬送部19の上部には、シート原稿200をセットするためのシート原稿トレイ94と、シート原稿200のサイド方向のセット位置を調整するシート原稿サイドガイド93と、排紙されたシート原稿200が載置される排紙トレイ23とが、それぞれ配設されている。

【0032】また、MFDSの給紙部21（図1の右上方）には、シート原稿200のセットの有無を検知するシート原稿センサ25と、シート原稿200を一枚ずつ分離給紙する給紙ローラ96及び給紙分離パッド95と、シート原稿200の給紙タイミングをはかる給紙センサ26とが配設されており、さらに、シート原稿200の搬送路を構成する第1搬送ガイド108及び第2搬送ガイド109が配設されている。

【0033】さらに、ベルト支持ローラ97の僅かに左側のめくり搬送ベルト8の外側には、シート原稿200の搬送時の帯電用としての第2バイアスローラ11があり、その内側には、支持用のバイアス対向ローラ102がある。

【0034】また、第2搬送ガイド109の下端には、搬送ガイド爪115があり、シート原稿200の搬送を補助している。さらに、第4ベルト支持ローラ100には第6対向ローラ105、第5ベルト支持ローラ101には第7対向ローラ106、駆動ローラ12には排紙ローラ107が、めくり搬送ベルト8を挟んでめくり搬送ベルト8の外側にそれぞれ配設されている。

【0035】また、第3ベルト支持ローラ99から駆動ローラ12までのめくり搬送ベルト8の外側には、シート原稿200の搬送路を構成する第3搬送ガイド110が配設されている。ここで、第2ベルト支持ローラ98から第3ベルト支持ローラ99までの間は、原稿台18の上面の原稿載置面116がシート原稿200の搬送路として使用される。

【0036】この原稿載置面116は、プレスキャンしてブック原稿92のサイズを検出する際に、このブック原稿92の先端の検知をし易くするために、黒色に形成されている。一方、図1において左上方のMFDSの排紙部22には、排紙ローラ107の手前に排紙センサ28があって、シート原稿200の排紙時におけるジャムの有無を検知している。

【0037】また、この排紙部22の排紙口117の下

8

側には、排紙分離爪111が形成されており、シート原稿200のスムーズな排紙を補助している。MFDSの原稿台18には、第2ベルト支持ローラ98の下側に第4対向ローラ103が、第3ベルト支持ローラ99の下側に第5対向ローラ104がそれぞれ配設され、ページめくり読取ユニット1がホームポジション位置〔1A〕にあるときのめくりローラ2の下側に第1対向ローラ15が、押えローラ6の下側に第2対向ローラ16が、第1読み取りセンサユニット9の下側に第2読み取りセンサユニット14が、それぞれ配設されている。

【0038】また、ページめくり読取ユニット1がエンドポジション位置（シート原稿200の読み込みモード時におけるページめくり読取ユニット1の停止位置）〔1C〕にある時の、第1読み取りセンサユニット9の下側には第3対向ローラ17が、めくりローラ2の下側にはブックサイズ上限センサ33が、それぞれ配設されている。

【0039】さらに、原稿載置面116の中央には、ブック原稿92の載置位置を決めるための中央基準位置決め部24が形成されている。この中央基準位置決め部24には、ブック原稿92が載置された状態でブック原稿92の背に当接する中央位置決め板113と、この中央位置決め板113に対して上昇する習性を与えるための中央位置決めスプリング114と、ブック原稿92の載置状態における中央位置決め板113の下方への変位量を検出するブック原稿センサ27とが、それぞれ配設されている。ここで、中央位置決め板113の一部は切り欠かれていて、この切欠部の下方には、図67にも示すように識別符号検知手段としてのバーコードスキャナ341aが配置され制御手段としてのワンチップマイコン330に接続されている。

【0040】このように構成された原稿台18の下部には、MFDSを略水平に支持するためのスタンド91が設けられている。一方、搬送部19の原稿台18と接する部位の両脇には、搬送部ロックセンサ31を内蔵した搬送部ロック装置140が配設されており、搬送部19と原稿台18との開閉状態を検知している。

【0041】以上述べたように、このMFDSは、シート原稿200の自動原稿給送・読取機能と、ブック原稿の読み取り及び自動ページめくり機能との両機能を合わせ持った原稿読み取り装置として構成される。次に、図2乃至図4を参照しながら、この原稿読み取り装置における駆動系の構成について説明する。

【0042】図2は、MFDSの駆動系の概略横断面図である。図3は、MFDSの駆動系の概略平面図である。図4は、ページめくり読取ユニット1の端部の斜視図である。図2乃至図4において、ページめくり読取ユニット1は、めくりユニット駆動板49のスキャニングパイプ51が、MFDSの手前側と奥側とに平行に横架された一対のスキャニングロッド50に嵌挿されること

Petitioner Apple Inc. - Exhibit 1012, p. 1454

9

によって、ＭＦＤＳの左右方向に沿って摺動自在に支持されている。

【００４３】各スキャニングロッド５０は、ＭＦＤＳの搬送部右側板５８と、搬送部左側板５９とに、それぞれの端部が固定されている。また、図３に示すように、搬送部前側板５６と搬送部後側板５７との間には、第１シャフト６４と第２シャフト６５とが、それぞれ回転自在に軸支されている。これらの第１シャフト６４と第２シャフト６５には、駆動プーリ６２と従動プーリ６３とが、その手前側と奥側とに、それぞれ１つずつ固定されていて、これらの駆動プーリ６２と従動プーリ６３を一対として、２本のめくりユニット駆動ベルト５２が、それぞれ懸架がされている。

【００４４】このページめくり読取ユニット１は、図３及び図４に示すように、めくりユニット駆動板４９の駆動ベルト固定部５３で、駆動ベルト固定板５４と駆動ベルト固定ビス５５によって、めくりユニット駆動ベルト５２と固定されており、このめくりユニット駆動ベルト５２の回動により駆動される。

【００４５】また、第１シャフト６４には、搬送部後側板５７を挟んで、その奥側に第１ギア６６が固定されており、この第１ギア６６がめくりユニット駆動モータ６０の出力軸に固定された第２ギア６７と噛み合って、めくりユニット駆動モータ６０の回転が伝達され、駆動プーリ６２、めくりユニット駆動ベルト５２、従動プーリ６３、及び、ページめくり読取ユニット１が、それぞれ駆動される。

【００４６】一方、図３に示すように、第４ベルト支持ローラ１００と同軸固定された第３シャフト１２１、駆動ローラ１２と同軸固定された第４シャフト１２２、給紙ローラ９６と同軸固定された第７シャフト１２５、第１ベルト支持ローラ９７と同軸固定された第８シャフト１２６は、搬送部前側板５６と搬送部後側板５７との間にそれぞれ回転自在に軸支されている。第４シャフト１２２には、搬送部後側板５７を挟んで、その奥側に第３ギア６８が固定されている。また、第４ギア６９と第５ギア７３とは、同軸固定され回転自在に軸支されている。

【００４７】さらに、めくり搬送ベルト駆動モータ６１の出力軸に固定された第６ギア７４は第５ギア７３と、また、第４ギア６９は第３ギア６８と、それぞれ噛み合っていて、めくり搬送ベルト駆動モータ６１の回転を順次伝達し、駆動ローラ１２を駆動してめくり搬送ベルト８を回動させる。

【００４８】また、図２及び図３に示すように、第８シャフト１２６には、搬送部後側板５７の奥側に第２給紙プーリ１３０が、第７シャフト１２５には、搬送部後側板５７の奥側に給紙クラッチ１２８を介して第１給紙プーリ１２９が、それぞれ固定されており、第２給紙プーリ１３０と第１給紙プーリ１２９とには、給紙駆動ベルト１２７が懸架されている。

10

【００４９】これにより、めくり搬送ベルト８の回動によって回転された第１ベルト支持ローラ９７の回転は、第８シャフト１２６、第２給紙プーリ１３０、給紙駆動ベルト１２７、第１給紙プーリ１２９に順次伝達され、給紙クラッチ１２８の入力側に伝達される。

【００５０】また、メイン制御ボード３１０（図３４参照）から送られる制御信号によって、給紙クラッチ１２８が作動し、第７シャフト１２５及び給紙ローラ９６が駆動される。一方、図１に示した、第１対向ローラ１５、第２対向ローラ１６、及び、第３対向ローラ１７は、図示しない駆動伝達機構によって、めくり搬送ベルト８と同期し、且つ、同じ周速でそれぞれ駆動される。

【００５１】次に、図１乃至図４を参照しながら、ページめくり読取ユニット１の構成について説明する。図１乃至図４において、第１めくりユニット側板４０と、第２めくりユニット側板４１は、めくり搬送ベルト８を挟む位置に互いに対向して配置されており、これらの第１めくりユニット側板４０と、第２めくりユニット側板４１との間には、めくりローラ２、第１バイアスローラ３、第１ローラ４、第２ローラ５、及び、押えローラ６がそれぞれ回転自在に支持されている。これらの各ローラの支持構造は、何れも同じに構成されている。

【００５２】そこで、第１ローラ４を例に取って説明すると、この第１ローラ４は、図５に示すように、第１めくりユニット側板４０と第２めくりユニット側板４１に両端部が固定された第５シャフト１２３が、中空軸からなるこの第１ローラ４の中空部に挿通され、この第５シャフト１２３に配設された一対の軸受１３１によって、この第１ローラ４の両端部が支持されることにより、第５シャフト１２３に対して回転自在に支持されている。

【００５３】ここで、これらのめくりローラ２、第１バイアスローラ３、第１ローラ４、第２ローラ５、及び、押えローラ６は、自らは回転せず、めくり搬送ベルト８の回動によってのみ回転される。また、第１めくりユニット側板４０と第２めくりユニット側板４１の外側には、図１に示す第１読み取りセンサユニット９の長手方向の延長位置に、回動支持ロッド４２（両側とも同じに構成されている）がそれぞれ回転自在に支持されている。

【００５４】そこで、この回動支持ロッド４２の片側のみの支持構造を説明すると、この回動支持ロッド４２は、図４に示すように、摺動パイプ４３、第２スプリング止め爪４８、上限検知部７６と一体に構成されている。図４において、傾き修正スプリング４４は、ねじりコイルスプリングで形成されており、その一端が回動支持ロッド４２に、他端が第１めくりユニット側板４０に、それぞれ固定されている。

【００５５】この傾き修正スプリング４４は、その自然状態、すなわち、傾き修正スプリング４４に外力が加わ

Petitioner Apple Inc. - Exhibit 1012, p. 1455

っていない状態において、摺動パイプ４３の軸心方向（図４の上下方向）と、第１読み取りセンサユニット９の読取光学系の光軸方向（第１読み取りセンサユニット９の第１めくりユニット側板４０及び第２めくりユニット側板４１に対する移動方向（詳しくは後述））とを一致させるように構成されている。

【００５６】これにより、第１めくりユニット側板４０及び第２めくりユニット側板４１が、各回動支持ロッド４２を中心としてそれぞれ一体的に回転した際、この傾き修正スプリング４４によって、これらの第１めくりユニット側板４０及び第２めくりユニット側板４１に対して常に初期状態の姿勢に戻そうとする回転力が作用し、これらの第１めくりユニット側板４０及び第２めくりユニット側板４１の傾きが適時修正される。

【００５７】また、摺動パイプ４３は、図４に示すように、摺動支持ロッド４６に対して滑らかに摺動するように構成されている。この摺動支持ロッド４６の上端は上部ロッド支持板７０に、また、この摺動支持ロッド４６の下端は下部ロッド支持板７１に、それぞれ固定されている。

【００５８】また、上部ロッド支持板７０には第１スプリング止め爪４７が、摺動パイプ４３の上部には第２スプリング止め爪４８が、それぞれ形成されており、これらの第１スプリング止め爪４７及び第２スプリング止め爪４８によって、摺動パイプ４３と上部ロッド支持板７０との間に軸装された、めくりユニット上下スプリング４５の両端がそれぞれ係止されている。

【００５９】ここで、摺動パイプ４３は、通常の状態では、下部ロッド支持板７１に当接しているが、ページめくり読取ユニット１が外力を受けることによって、めくりユニット上下スプリング４５の弾力に抗し、摺動支持ロッド４６に沿って、図４において上方に摺動する。このとき、摺動パイプ４３には、第２スプリング止め爪４８を常に下方に押圧する、めくりユニット上下スプリング４５の弾力によって、上述の通常の状態に戻ろうとする摺動力が作用している。

【００６０】また、この摺動パイプ４３の上方への摺動範囲は、めくりユニット駆動板４９に配置されたスキャンカットオフセンサ３４が、摺動パイプ４３に設けられた上限検知部７６を検知した状態で、摺動パイプ４３の上方への摺動位置が限界位置となるように設定されている。

【００６１】一方、めくりユニット駆動板４９は、図４に示すように、上部ロッド支持板７０、下部ロッド支持板７１、第１スプリング止め爪４７、スキャニングパイプ５１、駆動ベルト固定部５３、及び、ホーム検知フィラ７５と一体的に形成されている。

【００６２】また、このめくりユニット駆動板４９の駆動ベルト固定部５３は、前述したように、駆動ベルト固定板５４と駆動ベルト固定ビス５５によって、めくりユニット駆動ベルト５２に固定されている。さらに、このめくりユニット駆動板４９のスキャニングパイプ５１は、スキャニングロッド５０に対して滑らかに摺動するように嵌合されている。

【００６３】これにより、前述したように、めくりユニット駆動ベルト５２が駆動されて、ページめくり読取ユニット１が、そのホームポジション位置〔１Ａ〕に到達した時点で、図３に示すホームセンサ３０により、スキャニングパイプ５１のホーム検知フィラ７５が検知されるように構成されている。

【００６４】次に、図６乃至図８を参照しながら、この原稿読み取り装置における搬送部ロック装置の構成について説明する。図６乃至図８は、ＭＦＤＳの両側部に配設された搬送部ロック装置１４０（両側とも同じ構成）の一方の構成を示す概略図である。

【００６５】この搬送部ロック装置１４０は、ロック解除ソレノイド１３２、及び、ロック杆１３４等で構成されている。図６乃至図８において、ロック解除ソレノイド１３２は、ロック解除ソレノイドアーム１３３の一端と連結されている。

【００６６】ロック解除ソレノイドアーム１３３の他端は、ロック杆１３４の一端と回転自在に軸支されている。このロック杆１３４のロック解除ソレノイドアーム１３３に対向するがわの側部には、電磁ロック１４１が配置されている。また、ロック杆１３４の他端には、ロック解除ソレノイドアーム１３３が配置されているがわに向けて鍵爪状に折曲されたロック爪１３４ａが形成されている。

【００６７】ロック杆１３４は、回転部１３６で回転自在に支持されており、その回転部１３６の上部がわが、ロックスプリング１３５の一端に繋がれている。このロックスプリング１３５の他端は、搬送部１９の一部に繋がれていて、これにより、ロック杆１３４に対して、第６図において、時計回転方向への回動習性を与えている。

【００６８】このロック杆１３４の回動習性による回動は、その回転部１３６の左下側に配置されたロック爪ストッパ１３７によって、所定の角度に阻止されている。一方、原稿台１８側には、ロックピン１３９、及び、搬送部ロックセンサ３１が配置されたロック部１３８が形成されている。

【００６９】図６において、搬送部１９を押し下げながら閉じていくと、図７に示すように、ロックピン１３９にロック杆１３４のロック爪１３４ａの下端が当接して、ロック杆１３４がその回転部１３６を回転軸として、反時計回りに回動される。この状態から、搬送部１９をさらに閉じていくと、図８に示すように、ロック杆１３４のロック爪１３４ａがロックピン１３９に引っかかって、搬送部１９が原稿台１８に固定される。

【００７０】また、この搬送部１９のロック動作時に、

Petitioner Apple Inc. - Exhibit 1012, p. 1456

13

ロック杆１３４のロック爪１３４ａによって、搬送部ロックセンサ３１が作動される。この搬送部１９のロックの解除は、図１６に示す操作表示ボード３１３のオープンキー６２０を押すことによって実行される。

【００７１】すなわち、操作表示ボード３１３のオープンキー６２０を押下すると、ロック解除ソレノイド１３２が作動して、ロック杆１３４が回転部１３６を回転軸として反時計回りに回動し、ロックピン１３９からロック杆１３４のロック爪１３４ａが外れ、図示せぬ搬送部開閉スプリングによって、搬送部１９が上方へ開放される（図１０参照）。

【００７２】但し、このオープンキー６２０は、ブック原稿９２の一連のページめくり走査時、読み取り走査途中、及び、シート原稿２００の搬送中の場合には、作動しない（入力を受け付けない）ようにプログラムされている。

【００７３】また、このようにオープンキー６２０が入力を受け付けない状態では、電磁ロック１４１が作動され、この電磁ロック１４１によって、ロック爪１３４ａがロックピン１３９に係合されたままの状態で、ロック杆１３４の回動が拘束されるように構成されている。

【００７４】上述のように構成されたＭＦＤＳは、図９及び図１０に示すように、例えば、プリンタ３００の上部に搭載されて使用される。図１０は、上述したように、このＭＦＤＳの搬送部１９を開放した状態を示している。

【００７５】次に、図１１乃至図１３を参照しながら、この原稿読み取り装置におけるページめくり読取ユニット１の内部の第１読み取りセンサユニット９の構成について説明する。図１１は第１読み取りセンサユニット９の端部付近の斜視図、図１２は第１読み取りセンサユニット９の端部付近の側面図、図１３は第１読み取りセンサユニット９の端部の詳細断面図である。

【００７６】この第１読み取りセンサユニット９の両端部は、両方共同じに構成されているので、ここではその片方のみの構成を説明する。第１読み取りセンサユニット９は、図１１に示すように、コの字状に形成された読み取りセンサブラケット１４６によって、その上部が覆われており、かつ、この読み取りセンサブラケット１４６に対して、上下動自在に配設されている。　読み取りセンサブラケット１４６は、その両端が第１めくりユニット側板４０及び第２めくりユニット側板４１に固定されることによって、ページめくり読取ユニット１と一体に構成されている。

【００７７】この読み取りセンサブラケット１４６の端部の少し内側には、読み取りセンサスタッド１４８が下向きに固定されている。この読み取りセンサスタッド１４８の下端部は、図１３に示すように、第１読み取りセンサユニット９の端部に形成されているボス１４９に嵌合されている。これにより、第１読み取りセンサユニット９が、読み取りセンサスタッド１４８を介して、読み取りセンサブラケット１４６に対して上下動自在に支持される。

14

【００７８】ここで、読み取りセンサスタッド１４８とボス１４９とは、読み取りセンサスタッド１４８の下端に形成されたフランジ状の掛り部によって、それらの嵌合が外れないように構成されている。また、読み取りセンサブラケット１４６の読み取りセンサスタッド１４８の基部と、第１読み取りセンサユニット９のボス１４９の基部との間には、読み取りセンサスプリング１４７が軸装されており、この読み取りセンサスプリング１４７の伸長力によって、第１読み取りセンサユニット９に対して、下方への変位習性が付勢されている。

【００７９】これにより、この第１読み取りセンサユニット９は、常に、ページめくり読取ユニット１の最下部位に位置し、例えば、ブック原稿９２の表面の凹凸等によって外力を受けた際に、この外力に逆らうことなく、ブック原稿９２の表面の凹凸等に沿って滑らかに上下動される。また、第１読み取りセンサユニット９の端部には、図１１に示すように、読み取りセンサ解除ソレノイドアーム１５１を介して、読み取りセンサ解除ソレノイド１５０が取付けられている。

【００８０】この読み取りセンサ解除ソレノイド１５０は、図１２に示すように、第１めくりユニット側板４０に固定されており、第１読み取りセンサユニット９で原稿読み取り動作を行なわずにページめくり読取ユニット１が移動されるとき、例えば、ページめくり動作時、非読み取りページの空走査時、及び、シート原稿スキャンモードのリターン時等に、この読み取りセンサ解除ソレノイド１５０が作動される。

【００８１】この読み取りセンサ解除ソレノイド１５０が作動されると、読み取りセンサスプリング１４７の弾力に抗して、第１読み取りセンサユニット９が上方へ移動され、その原稿走査面が原稿の表面から退避（離隔）される。この第１読み取りセンサユニット９は、めくりローラ２の回転によって発せられるエンコーダ１５２の信号をその画像読み取りの基準信号としている。このめくりローラ２とエンコーダ１５２は、第１４図に示すように構成されている。

【００８２】第１４図は、めくりローラ２の奥側の側面図を示している。第１４図において、めくりローラ２の奥側の端部には、王冠状に形成されたフィラ１５３が配設されている。フィラ１５３は、等間隔の同じ幅のスリットを円周上に形成して構成されている。

【００８３】エンコーダ１５２は、このフィラ１５３を上下に挟むようにして、第２めくりユニット側板４１に固定されている。これにより、このエンコーダ１５２は、めくりローラ２の回転に応じ、フィラ１５３がエンコーダ１５２の検知光路を周期的に遮ることによって、第１読み取りセンサユニット９の画像読み取りの基準信

Petitioner Apple Inc. - Exhibit 1012, p. 1457

15

号を発生する。

【００８４】一方、原稿台１８に対するブック原稿９２の位置決めは、中央基準位置決め部２４によって行われる。この中央基準位置決め部２４の詳細断面図を第１５図に示す。この中央基準位置決め部２４は、ブック原稿９２の読み取り走査時、及び、ページめくり走査時の基準位置となっている。

【００８５】中央基準位置決め部２４は、原稿載置面１１６の中央部に形成された溝内に構成されている。この溝内には、中央位置決め板１１３が、原稿載置面１１６に対して昇降自在に嵌合されている。中央位置決め板１１３は、その下部に配設された中央位置決めスプリング１１４によって、常に、上昇する習性が与えられている。

【００８６】この習性による中央位置決め板１１３の上方への移動は、原稿載置面１１６の溝の縁部に形成されたストッパ１１８に、中央位置決め板１１３のストッパ爪１１９が当接することによって阻止され、平生、第１５図の破線で示す位置で停止されている。原稿載置面１１６へのブック原稿９２のセットは、溝内の中央位置決め板１１３の上にブック原稿９２の背（綴じ部）を載せることによって行われる。

【００８７】すなわち、溝内の中央位置決め板１１３の上にブック原稿９２の背（綴じ部）が載せられると、このブック原稿９２の自重によって、中央位置決め板１１３が下方に押し下げられる。これにより、原稿載置面１１６の溝内の側部に配置されたブック原稿センサ２７が、中央位置決め板１１３の移動を検知して、ブック原稿９２のセットが認知される。

【００８８】ところで、この原稿台１８の全面部位には、ＭＦＤＳの操作表示ボード３１３が配置されている（図９及び図１０参照）。この操作表示ボード３１３は、図１６に示すような、多数の入力キーが配置されている。以下、これらの入力キーの機能を順に説明する。

【００８９】スタートキー６００は、原稿の読み取り開始を指示するときに押される。エンターキー６０１は、テンキー入力や液晶表示パネル上での選択入力のときに、その入力を確定する際に押される。テンキー６０２は、原稿のプリント枚数、及び、ページめくり枚数等を設定するときに使用される。

【００９０】読み取り開始ページ選択キー６０３は、ブック原稿読み取りモード時おいて、ブック原稿９２の向かって「左」・「右」どちらのページから読み取りを開始するかを選択するキーであって、このキーを１回押下する毎に、ブック原稿９２の読み取り開始ページの左右が切り替わる。

【００９１】このキーの初期設定時における読み取り開始ページは、「左」ページに設定されており、このキーにより選択されたの読み取り開始ページがブック原稿９２の左右の何れであるかは、２つの読み取り開始ページ

16

表示ＬＥＤ６３１のどちらが点灯されているかによって表示される。

【００９２】読み取り総ページ設定キー６０６は、ブック原稿読み取りモードにおいて、そのページめくり枚数を入力する際の、読み取りたい総ページ枚数を設定するときに押下される。

【００９３】ブック原稿９２の読み取り総ページ枚数は、この読み取り総ページ設定キー６０６を押下して、テンキー６０２でそのページ数を入力した後、エンターキー６０１を押下することにより確定され、この確定された値が液晶表示パネル６３０に表示される。

【００９４】ブックサイズ選択キー６０７は、ブック原稿読み取りモードのときに、「自動ブックサイズ認識モード」、もしくは、「ブックサイズキー入力モード」の何れかを選択する際に押下される。また、このキーが１回押される毎に、ブックサイズ表示ＬＥＤ６３２の表示が、「自動」・「定形」・「不定形（mm入力）」の順に切り替えられ、このブックサイズ表示ＬＥＤ６３２により表示されたモードが選択される。

【００９５】このブックサイズ選択キー６０７の初期設定時の、ブックサイズ表示ＬＥＤ６３２の表示は、「自動」になっており、「自動ブックサイズ認識モード」が選択されている。ここで、ブックサイズキー入力モードには、「定形」と、「不定形（mm入力）」とがあり、ブックサイズが、Ａ５・Ｂ５・Ａ４の場合に限り、「定形」を選択することにより、定形ブックサイズ選択キー６１９によるブックサイズの入力が可能となる。

【００９６】この定形ブックサイズ選択キー６１９が１回押される毎に、定形ブックサイズ表示ＬＥＤ６３３の表示が、「Ａ５」・「Ｂ５」・「Ａ４」の順に切り替えられ、選択されたブックサイズが表示されて認識される。この定形ブックサイズ選択キー６１９の初期設定時の、定形ブックサイズ表示ＬＥＤ６３３の表示は、「Ａ４」となっている。但し、ここでいうブックサイズとは、ブック原稿９２の表紙の大きさを指している。

【００９７】ここで、ブック原稿９２が、上述した定形ブックサイズ以外の場合には、ブックサイズ選択キー６０７により、「不定形（mm入力）」を選択し、テンキー６０２で、セットされたブック原稿９２の縦サイズ、及び、横サイズ（mm単位）をそれぞれ入力した後、エンターキー６０１を押下して、そのブックサイズを確定する。

【００９８】このようにしてブック原稿９２のサイズが確定されると、その入力されたサイズ値が液晶表示パネル６３０に表示される。ブック綴じ部マスク領域設定キー６０８は、ブック原稿読み取りモードのときに、中央基準位置決め部２４のセンターからの非読み取り領域（マスク領域）を、「左（－）」・「右（＋）」の何れとするかを設定するときに押下される。

【００９９】すなわち、ブック原稿９２のブック綴じ部

Petitioner Apple Inc. - Exhibit 1012, p. 1458

にマスク領域を形成するときには、先ず、このブック綴じ部マスク領域設定キー６０８で、ブック原稿９２の左右何れのページにマスク領域を形成するかを設定し、次いで、この設定された「左マスク領域（－）」、もしくは、「右マスク領域（＋）」の長さ（mm単位）を、テンキー６０２により入力した後、エンターキー６０１でこの入力値を確定する。　このようにしてブック原稿９２のマスク領域が確定されると、その入力された値が液晶表示パネル６３０に表示される。このブック綴じ部マスク領域設定キー６０８の初期設定時におけるマスク領域の値は、「±１０mm」となっている。

【０１００】読み取り領域選択キー６０９は、ブック原稿読み取りモードのときに、ブック原稿９２の読み取り領域を、「片頁（左）」・「片頁（右）」・「両頁」のうちの何れとするかを選択する際に押下される。

【０１０１】この読み取り領域選択キー６０９が１回押される毎に、読み取り領域表示ＬＥＤ６３６の表示が、「片頁（左）」・「片頁（右）」・「両頁」の順に切り替えられ、選択された読み取り領域が表示されて認識される。

【０１０２】この読み取り領域選択キー６０９の初期設定時の、読み取り領域表示ＬＥＤ６３６の表示は、「両頁」となっている。ここで、「片頁（左）」が選択された場合には、ブック原稿９２の向かって左ページのみの読み取り走査が実行され、右ページの読み取り走査は行われない。また、ここで、「片頁（右）」が選択された場合には、ブック原稿９２の向かって右ページのみの読み取り走査が実行され、左ページの読み取り走査は行われない。

【０１０３】見開き連写キー６１０は、ブック原稿読み取りモードの「見開き２ページ連続読み取りモード」、及び、その「両面モード」のときに、読み取った原稿情報を等倍率でプリントアウトすることを指示する際に押下される。

【０１０４】見開き連写縮小キー６１１は、ブック原稿読み取りモードの「見開き２ページ連続読み取りモード」、及び、その「両面モード」のときに、読み取った原稿情報を縮小倍率でプリントアウトすることを指示する際に押下される。

【０１０５】この時の、原稿情報の縮小倍率の設定は、プリント変倍キー６１４を操作することによって行われる。また、この見開き連写縮小キー６１１の初期設定時における基準縮小倍率は、「原稿のサイズ×０．７１（Ａ３⇒Ａ４／Ｂ４⇒Ｂ５）」に設定されている。

【０１０６】両面モード選択キー６１２は、ブック原稿読み取りモードが、「見開き１ページ区切り読み取りモード」の「両面モード」のときに、何れの面を表にし、また、何れの面を裏にしてプリントするかを、「見開き両面モード」・「オリジナル両面モード」・「順次両面モード」の３つの両面モードの中から選択する際に押下される。

【０１０７】この両面モード選択キー６１２が１回押される毎に、両面モード表示ＬＥＤ６３４の表示が、「見開き両面モード」・「オリジナル両面モード」・「順次両面モード」の順に切り替えられ、選択された読み取り領域が表示されて認識される。

【０１０８】この両面モード選択キー６１２の初期設定時の、両面モード表示ＬＥＤ６３４の表示は、「オリジナル両面モード」となっている。ここで、「見開き両面モード」が選択された場合には、見開かれたブック原稿９２の左右両ページのうち、左ページを表にし、右ページを裏にして、両面プリントが実行される。

【０１０９】このとき、読み取り開始ページ選択キー６０３により、ブック原稿９２の読み取り開始ページが「右」に設定されている場合には、始めの１枚目のプリントは片面プリントとなる。

【０１１０】また、ここで、「オリジナル両面モード」が選択された場合には、見開かれたブック原稿９２の左右両ページのうち、右ページを表にし、ページめくり動作によりめくられた次のページの左ページを裏にして、両面プリントが実行される。すなわち、この「オリジナル両面モード」では、読み取られるブック原稿９２の装丁と全く同様にプリントされる。

【０１１１】このとき、読み取り開始ページ選択キー６０３により、ブック原稿９２の読み取り開始ページが「右」に設定されている場合には、「見開き両面モード」の場合と同様、始めの１枚目のプリントは片面プリントとなる。さらに、ここで、「順次両面モード」が選択された場合には、見開かれたブック原稿９２の左右両ページのうち、読み取り開始ページ選択キー６０３で設定されたページを表にし、ページめくり動作によりめくられた次のページを裏にして、以後、順次読み取った順番に両面プリントが実行される。

【０１１２】見開き連写高速プリント設定キー６１３は、ブック原稿読み取りモードの「見開き２ページ連続読み取りモード」の「片面モード」のときに、ブック原稿９２の綴じ部付近において、ページめくり読取ユニット１の操作を減速または停止させること無く、連続して読み取り走査を実行し、ブック原稿９２の左右両ページの連続プリントを指示する際に押下される。

【０１１３】プリント変倍キー６１４は、読み取った画像を変倍してプリントするときに、その変倍率を設定するためのキーである。このプリント変倍キー６１４を押下すると、液晶表示パネル６３０に、予め設定された変倍率が表示される。ここで、変倍率は、カーソル移動キー６１７で希望する変倍率にカーソルを合わせてから、エンターキー６０１を押下することにより確定される。

【０１１４】画像処理設定キー６１５は、読み取った画像を画像処理してプリントするときに、その画像処理モードを設定するためのキーである。この画像処理設定キ

Petitioner Apple Inc. - Exhibit 1012, p. 1459

19

ー６１５を押下すると、液晶表示パネル６３０に、予め設定された画像処理モードが表示される。

【０１１５】ここで、画像処理モードは、カーソル移動キー６１７で希望する画像処理モードにカーソルを合わせてから、エンターキー６０１を押下することにより確定される。モード設定選択キー６１６は、ＭＦＤＳの動作モードを設定するためのキーである。

【０１１６】このモード設定選択キー６１６を押下すると、液晶表示パネル６３０に、予め設定されたＭＦＤＳの動作モードが表示される。ここで、ＭＦＤＳの動作モードは、希望するＭＦＤＳの動作モードカーソルを合わせてから、エンターキー６０１を押下することにより確定される。

【０１１７】カーソル移動キー６１７は、液晶表示パネル６３０に表示された各選択エリアにカーソルを移動させるためのキーである。読み取りスキップページ設定キー６１８は、ブック原稿読み取りモードにおいて、読み取り走査を実行せずに読み飛ばすページを設定するためのキーである。　すなわち、ブック原稿９２の各ページのうち、原稿読み取り走査を実行せずに読み飛ばしたいページがある場合には、先ず、この読み取りスキップページ設定キー６１８を押下し、次いで、ブック原稿９２の読み飛ばしたいページ（スキップページ）が、その読み取り開始ページから何ページ目であるかをテンキー６０２で入力した後、エンターキー６０１を押下して、このスキップページを確定する。

【０１１８】このようにして入力されたスキップページは、液晶表示パネル６３０に表示される。定形ブックサイズ選択キー６１９は、ブック原稿９２のブックサイズを選択するためのキーである。

【０１１９】前述したように、ブックサイズキー入力モードには、「定形」と、「不定形（mm入力）」とがあり、ブックサイズが、Ａ５・Ｂ５・Ａ４の場合に限り、「定形」を選択することにより、この定形ブックサイズ選択キー６１９によるブックサイズの入力が可能となる。

【０１２０】この定形ブックサイズ選択キー６１９が１回押される毎に、定形ブックサイズ表示ＬＥＤ６３３の表示が、「Ａ５」・「Ｂ５」・「Ａ４」の順に切り替えられ、選択されたブックサイズが表示されて認識される。

【０１２１】この定形ブックサイズ選択キー６１９の初期設定時の、定形ブックサイズ表示ＬＥＤ６３３の表示は、「Ａ４」となっている。但し、ここでいうブックサイズとは、ブック原稿９２の表紙の大きさを指している。

【０１２２】オープンキー６２０は、ＭＦＤＳの搬送部１９を開放するときに押下される。シート原稿セット選択キー６２５は、シート原稿読み取りモードにおいて、「シート原稿スルーモード」の「片面原稿読み取りモード」のときに、原稿載置面１１６にセットされるシート原稿２００の原稿面を「上向き」・「下向き」の何れかに選択するためのキーである。

20

【０１２３】このシート原稿セット選択キー６２５が１回押される毎に、シート原稿セット表示ＬＥＤ６３５の表示が、「上向き」・「下向き」の順に切り替えられ、選択されたシート原稿セット面が表示されて認識される。このシート原稿セット選択キー６２５の初期設定時の、シート原稿セット表示ＬＥＤ６３５の表示は、「上向き」となっている。

【０１２４】次に、図９及び図１０に示したプリンタ３００について説明する。このプリンタ３００の概略断面図を図１７に示す。画像処理後の画像情報は、プリンタ３００の書き込み部において、レーザ光のラスター走査によって、光の点の集合の形で感光体ドラム１７０上に書き込まれる。

【０１２５】このときのレーザ光源には、半導体レーザが使用されている。このプリンタ３００の書き込み部の平面図を図１８に示す。図１８において、半導体レーザ１７１で発せられたレーザ光は、コリメートレンズ１７２で平行な光束に変えられ、アパーチャ１７３により、一定形状の光束に整形される。

【０１２６】この整形されたビームは、第１シリンダーレンズ１７４により、その副走査方向を圧縮された形でポリゴンミラー１７５に入射される。このポリゴンミラー１７５は、正確な多角形状をしており、ポリゴンモータ１７６により、一定方向に一定の速度で回転されている。

【０１２７】このポリゴンミラー１７５の回転速度は、感光体ドラム１７０の速度と、書き込み密度と、面数とによって決定される。ポリゴンミラー１７５に入射されたレーザ光は、その反射光がミラーの回転により偏向される。この偏向されたレーザ光は、各ｆθレンズ１７７ａ，１７７ｂ，１７７ｃに入射される。

【０１２８】これらのｆθレンズ１７７ａ，１７７ｂ，１７７ｃは、角速度が一定の走査光を感光体ドラム１７０上で等速走査するように変換する機能、感光体ドラム１７０上で最小光点となるようにこの走査光を結像させる機能、及び、その面倒れを補正する機能を有している。

【０１２９】各ｆθレンズ１７７ａ，１７７ｂ，１７７ｃを通過した光は、その画像領域外で、同期検知ミラー１７８により同期検知センサ１７９に導かれ、主走査方向の頭出し信号を出す同期信号が出力されてから、一定時間後に画像データが１ライン分だけ出力され、以下、これを繰り返すことにより、１つの画像を形成する。一方、感光体ドラム１７０の表面には、感光層が塗布されている。

【０１３０】ここで、半導体レーザ１７１の７８０ｎｍという波長に感度を有する感光体としては、有機感光体

Petitioner Apple Inc. - Exhibit 1012, p. 1460

21

（ＯＰＣ）、α－Ｓｉ、Ｓｅ－Ｔｅ等が知られているが、本実施例では、有機感光体を使用している。

【０１３１】また、一般に、レーザ書き込みの場合、画像部に光をあてるＮ／Ｐプロセスと、地肌部に光をあてるＰ／Ｐプロセスがあるが、本実施例では、そのレーザ書き込みプロセスとして、画像部に光をあてるＮ／Ｐプロセスを採用している。

【０１３２】図１７において、感光体ドラム１７０の表面は、感光体ドラム１７０がわにグリッドを持つスコロトロン方式の帯電チャージャ１８０により、均一に負帯電させる。

【０１３３】次いで、この負帯電された感光体ドラム１７０の画像部に、レーザ光が照射されて、この画像部電位が落されると、この感光体ドラム１７０の表面に、地肌部電位が－７５０～－８００Ｖ、画像部電位が－５０Ｖ程度の静電潜像が形成される。

【０１３４】この静電潜像は、現像器１８１の現像ローラに、－５００～－６００Ｖのバイアス電圧を与えて、負帯電されたトナーによって、顕像化される。この現像器１８１によって顕像化された画像は、感光体ドラム１７０の回転にシンクロして給送された転写紙の紙面上に、この転写紙の裏面側から正電位のチャージをかける転写チャージャ１８２の転写作用によって転写される。

【０１３５】この画像の転写された転写紙は、転写チャージャ１８２と一体に保持された分離チャージャ１８３により交流除電されることによって、感光体ドラム１７０の表面から分離される。

【０１３６】このとき、転写紙に転写されずに、感光体ドラム１７０上に残留されたトナーは、クリーニングブレード１８４により感光体ドラム１７０の表面から掻き落され、このクリーニングブレード１８４の周囲に配設されたタンク１８５内に回収される。また、感光体ドラム１７０の表面に残留された電位のパターンは、除電ランプ１８６により光が照射されることによって消去される。

【０１３７】現像器１８１のすぐ下流側には、フォトセンサ１８７が設けられている。このフォトセンサ１８７は、受光素子と発光素子とで構成されており、感光体ドラム１７０の表面の反射濃度を計測し、この反射濃度（現像後のトナー濃度）が予め設定された基準値以下になったときに、現像器１８１内に新たなトナーを補給するためのトナー補給信号を出力する。

【０１３８】すなわち、このフォトセンサ１８７は、例えば、このフォトセンサ１８７の読み取り位置に対応した位置に、その光書き込み部で一定パターン（純黒または網点のパターン）を書き込み、このパターンを現像した後のパターン部の光反射率と、このパターン部位外の感光体ドラム１７０の光反射率との比から現像された画像の濃淡を判断し、この画像の濃度がその基準値よりも低いときにトナー補給信号を出力するように構成される。

22

【０１３９】ここで、新たな補給トナーが不足している場合には、トナー補給信号を出力しても、その現像濃度が高くならない点を利用して、このフォトセンサ１８７をトナーの残量不足を検知するセンサとして兼用させるように構成してもよい。

【０１４０】一方、本実施例のプリンタ３００は、複数のカセット１８８ａ，１８８ｂを備えており、且つ、画像が一度転写された転写紙を再給紙ループ１８９を通して両面給紙し得るように構成されている。

【０１４１】すなわち、図１７において、所定のカセットが選択された後、プリンタ３００のスタートボタンが押されると、各カセット１８８ａ，１８８ｂの各給紙コロ１９０ａ，１９０ｂのうちの選択されたがわの給紙コロが回転されて、そのカセット内の転写紙がレジストローラ１９１のニップに突き当たるまで給送される。

【０１４２】このレジストローラ１９１は、感光体ドラム１７０に形成された画像の位置と転写紙の位置とがシンクロするタイミングをとって、回転が開始され、感光体ドラム１７０の表面に向けて、転写紙を給送する。

【０１４３】これにより、この転写紙は、前述したように、画像が転写され、さらに、感光体ドラム１７０の表面から分離された後、分離搬送部１９２に吸引搬送され、ヒートローラ１９３、及び、加圧ローラ１９４からなる定着ローラによって、その紙面上に転写されたトナーが定着される。

【０１４４】このトナーの定着された転写紙は、通常のプリント時には、切換爪１９５が図１９（ａ）に示すような位置に臨み、この切換爪１９５により、プリンタ３００の排紙口を通して排紙トレイ１６９上に排出される。

【０１４５】ここで、プリンタ３００のプリントモードが「両面モード」の場合には、切換爪１９５が図１９（ｂ）に示す位置に切り換えられ、プリンタ３００の左側部に形成された両面搬送路に向けて転写紙が搬送される。

【０１４６】この転写紙は、反転ガイド爪１９６を通過して、一旦、反転ガイドトレー１９７上へ導かれた後、反転ガイド爪１９６が切り換えられ、且つ、反転ガイドローラ１９８が逆回転（反転）されることによって、再給紙ループ１８９を通して、再び、レジストローラ１９１のニップに当接されるまで給送される。

【０１４７】このようにして、再給送された転写紙は、前述の通常のプリント時と同様にして、感光体ドラム１７０上に形成されたトナー画像が転写・定着された後、図１９（ａ）で示す初期状態に切り換えられた、切換爪１９５を経て排紙トレイ１６９上に排出される。

【０１４８】ここで、片面プリントモード時の排出時における転写紙の画像定着面を排紙トレイ１６９の積載面に対向させて転写紙の排出を行う、「裏面排紙モード」

Petitioner Apple Inc. - Exhibit 1012, p. 1461

が設定されている場合には、上述の「両面モード」時と同様に、切換爪１９５が図１９（ｂ）に示す位置に切り換えられ、転写紙がそのまま排紙されること無く、一旦、両面搬送路に向けて搬送される。

【０１４９】そして、この転写紙の後端が、切換爪１９５を通過すると、その直後に、切換爪１９５が図１９（ｃ）に示す位置に切り換えられるとともに、スイッチバックローラ１９９の回転方向が反転されて、この両面搬送路に導かれた転写紙が、スイッチバック搬送され、プリンタ３００の排紙口を通して排紙トレイ１６９上に排出される。

【０１５０】この「裏面排紙モード」では、片面プリントされた転写紙が、その画像定着面を排紙トレイ１６９の積載面に対向させて排紙トレイ１６９上に排出されるので、原稿の読み取りページ順どおりに、転写紙のプリントページ順序の揃った転写紙の排出が行われる。

【０１５１】ところで、ページめくり読取ユニット１は、図４を参照して説明したように、第１めくりユニット側板４０と第２めくりユニット側板４１との間に、めくりローラ２、第１ローラ４、第２ローラ５、押えローラ６、及び、第１バイアスローラ３が、それぞれ回転自在に配設されている。

【０１５２】これらの、めくりローラ２、第１ローラ４、第２ローラ５、押えローラ６、及び、第１バイアスローラ３には、図２０に示すように、めくり搬送ベルト８が掛け渡されている。

【０１５３】第１バイアスローラ３には、第１高圧電源３２０が接続されていて、２本のボートより、吸着用，除電用の各周波数の交流電圧が、それぞれ与えられるように構成されている。　また、このページめくり読取ユニット１の内部の、めくりローラ２と第１読み取りセンサユニット９との間には、めくりガイド１０が、さらに、このめくりガイド１０の上方には、めくり搬送ベルト８の内周面に沿うようにしてページ収納部７が、それぞれ配設されている。

【０１５４】このページ収納部７には、ページめくり時のエラーを検知するための、フォトセンサなどからなるページめくりセンサ２９が配置されている。このページめくりセンサ２９は、めくりガイド１０に配置してもよい。

【０１５５】また、めくりローラ２と押えローラ６との間には、図１１を参照して説明したように、第１読み取りセンサユニット９が配置されている。この第１読み取りセンサユニット９は、ページめくり読取ユニット１に対して、約３mm程度上下移動可能に取付けられており、原稿読み取り時には、読み取りセンサスプリング１４７により下方に押下されて、ブック原稿９２、またはシート原稿２００の原稿面に密着されるように構成されている。

【０１５６】また、この第１読み取りセンサユニット９は、図２１に示すように、原稿の照明系としてのＬＥＤ３１６、原稿像の結像系としてのＲＭＬＡ８１（ルーフミラーレンズアレイ）、及び、結像された原稿の光像を電気信号に変換する光電変換系としてのＳｉ等倍センサ３１５を備えている。

【０１５７】この第１読み取りセンサユニット９による原稿読み取りは、次のようにように行われる。図２１において、先ず、ＬＥＤ３１６から発せられた光が、バーレンズ８３により、原稿面上に集光されて、原稿が照明される。

【０１５８】次に、この原稿面からの反射光が、光路分離ミラー８４で反射されて、ＬＡ８５（レンズアレイ）、及び、ＲＭＡ８６（ルーフミラーアレイ）を通り、再び、光路分離ミラー８４により反射される。　この光路分離ミラー８４により反射された原稿の画像光は、Ｓｉ等倍センサ３１５の受光面上に結像され、このＳｉ等倍センサ３１５によって、これに結像された画像情報が、電気信号に変換されて読み取られる。

【０１５９】次に、上述のように構成された本願実施例における基本的なページめくり動作について説明する。先ず、本実施例における原稿の読み取りは、次のような手順で行われる。

【０１６０】原稿がブック原稿９２の場合には、操作表示ボード３１３のオープンキー６２０を押して、図１０に示すように搬送部１９を上方に開き、原稿台１８の中央基準位置決め部２４に、ブック原稿９２の綴じ部（背）をセットし、このブック原稿９２の読み取り開始ページを上向きに開いた状態で、図９に示すように搬送部１９を閉じる。

【０１６１】この状態で、操作表示ボード３１３の各キーを操作して、このブック原稿９２の読み取り条件を設定した後、スタートキー６００を押してＭＦＤＳをスタートさせる。これにより、図１に示すように、めくりユニット駆動ベルト５２が、めくりユニット駆動モータ６０（図３４参照）により駆動されて、ページめくり読取ユニット１が、左端のホームポジション位置〔１Ａ〕から、右方向に移動を開始し、このページめくり読取ユニット１の移動により、第１読み取りセンサユニット９が、ブック原稿９２の原稿情報を読み込んでいく。

【０１６２】このとき、めくり搬送ベルト８は、その回転が停止されており、見開かれたブック原稿９２の原稿面をその上から押え付けている。また、ページめくり読取ユニット１は、前述したように、その回動支持ロッド４２を支点として回動され、且つ、これと一体化された摺動パイプ４３が摺動支持ロッド４６に沿って上下動されることによって、ブック原稿９２の原稿面に沿って、この原稿面に第１読み取りセンサユニット９を密着させながら移動される。

【０１６３】さらに、このページめくり読取ユニット１が、ブック原稿９２の略中央のブック原稿読み取り途中

Petitioner Apple Inc. - Exhibit 1012, p. 1462

位置〔1B〕に到達すると、第1バイアスローラ3に、図20に示した第1高圧電源320から、吸着用の交流電圧が印加されて、めくり搬送ベルト8上にストライプ形状の電荷パターンが形成される。

【0164】このように、ページめくり読取ユニット1は、めくり搬送ベルト8上にストライプ形状の電荷パターンを形成しながら、図1の右端のエンドポジション位置〔1C〕まで移動し、その第1読み取りセンサユニット9によって、ブック原稿92の原稿情報を読み取る。

【0165】上述のようにして、ブック原稿92の原稿情報の読み取りが完了すると、ページめくり読取ユニット1は、図22に示すように、そのエンドポジション位置〔1C〕から、ホームポジション位置〔1A〕に向けて、復帰移動される。

【0166】このとき、図23に示すように、めくり搬送ベルト8上には、その読み取り動作時に形成された電荷パターンによって、不平等な電界が発生しており、この静電界により、ブック原稿92の右ページが、めくり搬送ベルト8に、静電的に吸着されるようになっている。

【0167】従って、この状態で、ページめくり読取ユニット1が、そのエンドポジション位置〔1C〕に向けて移動され、このページめくり読取ユニット1が、図22に示す、めくり開始位置〔1D〕に到達すると、図24に示すように、このめくり搬送ベルト8と一緒に、ブック原稿92の右ページ1枚分の原稿の端部が、ページめくり読取ユニット1の中に巻き込まれる。

【0168】このように、ページめくり読取ユニット1内に巻き込まれた原稿は、このページめくり読取ユニット1の移動に伴って、そのめくりローラ2の曲率と原稿の腰の強さとによる曲率分離により、その先端が、めくり搬送ベルト8から徐々に分離される。

【0169】このようにして、めくり搬送ベルト8から徐々に分離された原稿は、図20に示しためくりガイド10に沿って移動され、この原稿の移動方向の下流側に配置されているページ収納部7内に導かれる。

【0170】このページ収納部7は、図20に示すように、円筒状に形成されており、その内周面に沿うように、ページめくり読取ユニット1内に巻き込まれた原稿を巻き取ることによって、極めて僅かなスペースに、読み取りを終えた1ページ分の原稿を収納することができる。

【0171】従って、このページめくり読取ユニット1によれば、図22に示すように、このページめくり読取ユニット1が、そのめくり開始位置〔1D〕から巻き取り完了位置〔1E〕に向けて復帰移動されることにより、その読み取りを終えた1ページ分の原稿と、次の読み取り動作により読み取りが行われる次頁の原稿とを、極めてスムーズに分離させることができる。

【0172】このようにしてページ収納部7に収納された原稿は、ページめくり読取ユニット1が、その巻き取り完了位置〔1E〕から、ブック原稿92の中央を越えて、ブック原稿92の左ページがわのページ排出位置〔1F〕に向けて、さらに復帰移動されることによって、このページめくり読取ユニット1と、これに収納された原稿との相対的な移動により、この原稿がページめくり読取ユニット1のページ収納部7から排出され始める。

【0173】そして、このページめくり読取ユニット1が、そのホームポジション位置〔1A〕に復帰移動されて、その移動が完了することにより、このページめくり読取ユニット1のページ収納部7に収納されていた原稿の排出が完了して、読み取りを終えた原稿の1ページ分のめくり動作が完了される。

【0174】一方、この原稿のめくり動作中においては、ページめくり読取ユニット1のページ収納部7への原稿の巻き取りが開始された直後から、この原稿の巻き取りが完了する間にかけて、第1バイアスローラ3に、図20に示した第1高圧電源320から除電用の交流電圧が印加されることによって、めくり搬送ベルト8上に形成されていた電荷パターンが除電されるようにプログラムされている。

【0175】従って、このページめくり読取ユニット1の復帰移動時においては、読み取りを終えた原稿と、この原稿をめくるめくり搬送ベルト8との間に、静電的な吸着力が発生しないので、この原稿の巻き取り動作、及び、排出動作を極めてスムーズに行うことができる。

【0176】本願実施例では、図20、図23及び図24に示したように、無端ベルトからなる、めくり搬送ベルト8に、高圧電源320から吸着用の交流電圧を印加して、めくり搬送ベルト8の表面に、交番的なストライプ形状、もしくは、市松模様などの電荷パターンを形成することによって、このめくり搬送ベルト8に不平等電界を発生させて、原稿の保持搬送、及び、ページめくりを行っている。

【0177】このページめくり方式によれば、原稿の保持搬送、及び、ページめくり動作を極めてスムーズに行うことがでる。

【0178】以下、このページめくり方式における基本的な構成、及び、静電吸着原理について説明する。このページめくり方式に使用されるめくり搬送ベルト8としては、無端ベルト状に形成された誘電体の裏面に、導電処理を施してなる2層構造のベルトを使用した。

【0179】このめくり搬送ベルト8に対して不平等電界を発生させる手段としては、例えば、このめくり搬送ベルト8の表面に周面を接触させて回転自在に支持された第1バイアスローラ3に、第1高圧電源320により吸着用の交流電圧を印加すればよい。

【0180】図20及び図23に示すように、めくり搬送ベルト8の導電層8bをアース面として、第1バイア

Petitioner Apple Inc. - Exhibit 1012, p. 1463

27

スローラ3に交番的な電界を印加させながら、このめくり搬送ベルト8と第1バイアスローラ3とを相対移動させることによって、めくり搬送ベルト8の誘電体8aの表面に、ストライプ形状の電荷パターンが形成される。

【0181】これによって、めくり搬送ベルト8の誘電体8aの表面近傍に、不平等電界が発生する。この不平等な電界中に、読み取り原稿となる用紙等の誘電体を近づけると、その内部が分極をおこし、この電界が不平等なために、この用紙にめくり搬送ベルト8がわへの吸引力が働く。

【0182】本実施例の具体的な構成としては、めくり搬送ベルト8として、厚さ75μmのPETフィルム（誘電体8a）に、厚さ10μmのアルミ蒸着層（導電層8b）が形成された無端ベルトを使用し、これに形成される電荷パターンのピッチを2．4mmとした。すなわち、ブック原稿92の読み取り速度を120mm／s、交流周波数を50Hz、印加電圧を±2kVp－pとした。また、図25に印加電圧を±2kVp－pに一定としたときの搬送力のピッチ特性の実験値を、図26に印加電圧を±2kVp－pに一定としたときの吸着力のピッチ特性の実験値を、図27に電荷パターンのピッチを2．4mmに一定としたときの搬送力の印加電圧特性の実験値を、第28図に電荷パターンのピッチを2．4mmに一定としたときの吸着力の印加電圧特性の実験値を示す。

【0183】これらの実験値から明らかなように、本実施例に使用される電荷パターンのピッチ、及び、印加電圧は、上述した値に限定されるものではなく、例えば、電荷パターンのピッチとしては、0．5mm～10mmの範囲であれば良く、また、印加電圧としては、±1kVp－p以上であれば良い。

【0184】また、本実施例では、除電用の高周波交流電圧として、2kHzの周波数と、±2kVp－pの印加電圧を使用しているが、これらの各値についても、その除電効果が得られる値であれば、どのような値であっても良い。

【0185】ところで、上記実施例では、第1バイアスローラ3に、第1高圧電源320により、交流電圧を印加することによって、搬送ベルト8上を正・負に帯電させ、この搬送ベルト8の表面近傍に不平等な電界を発生させて、原稿の保持搬送およびページめくりを行なうように構成されている。

【0186】ここで、搬送ベルト8に印加される電圧は、交番電圧であれば、原稿を吸引することが可能であり、交流電圧のみに限定する必然性は無い。すなわち、交流電圧は、周期的にその方向を変える電流であって、1周期にわたって平均値が“0”であることを言い、本発明では、このような電圧に限定されない。

【0187】但し、搬送ベルト8に印加される電圧を交流電圧にすることによって、搬送ベルト8の原稿吸着力

28

が均一化されるという一応の効果は得られる。従って、搬送ベルト8の表面近傍に不平等電界を発生させるための手段としては、上記実施例以外の構成としてもよい。

【0188】例えば、搬送ベルト8の表面近傍に不平等電界を発生させるための手段として、図29および図30に示すように、金属等の導電性電極ローラからなるバイアスローラ3－Aの外周面に、市松模様の凹凸を形成し、このバイアスローラ3－Aに、第1高圧電源320により、直流電圧を印加するように構成してもよい。

【0189】この手段によれば、搬送ベルトの表面に対して、バイアスローラ3－Aの外周面をなす凸部3aのみが接触し、凹部3bが非接触となるので、搬送ベルト8の表面に、バイアスローラ3－Aの周面の凹凸に対応した市松模様の高密度な電荷パターンが形成される。

【0190】これにより、誘電体である搬送ベルト8上の帯電領域（図29の＋部分）と非帯電領域との境界部には、他の部分よりも強い電場が存在し、不平等電界が形成され、上記の市松模様の電荷パターンのそれぞれの端縁部に発生した強い電場によって、ブック原稿のページが搬送ベルト8に静電的に強く吸着される。

【0191】この第2の実施例のように、電荷パターンを市松模様とした場合には、その模様の単位を略正方形にすることによって、図24に示した第1の実施例のようなストライプ模様の電荷パターンに比べ、その単位面積中に存在する端縁部の長さが略2倍になるので、原稿ページの保持吸着力が倍増され、ページめくり動作の信頼性が向上される。

【0192】一方、上記第2の実施例では、バイアスローラ3－Aの周面に凹凸を形成して市松模様を構成したが、例えば、樹脂やセラミック等からなる絶縁ローラの表面に、プリントや蒸着等により市松模様の導電層パターンを形成したり、市松模様のシート状の電極を接着し、この導電層パターンや電極を電気的に結合されるように構成してもよい。

【0193】また、搬送ベルト8の表面近傍に不平等電界を発生させるための第3の実施例としては、図31に示すように、全体が金属等の導電性材料によって形成された電荷付与部材としてのローラ状電極3－Bの外周面に、フランジ状に突出する多数の電極部3cと、周溝状の非電極部3dとを、ローラ状電極3－Bの軸方向に沿って交互に配列し、このローラ状電極3－Bに、第1高圧電源320により、直流電圧を印加するように構成してもよい。

【0194】この第3の実施例によれば、前記第1の実施例と同様に、搬送ベルト8の表面に、帯電領域と帯電領域とが直線状に交互に配列されたストライプ状の電荷パターンが形成される。

【0195】一方、図32に示す第4の実施例は、電極部3cと非電極部3dとを交互に配列してなる電荷印加手段を、前記のローラ状電極3－Bに替えて、櫛歯状の

Petitioner Apple Inc. - Exhibit 1012, p. 1464

29

電極板３－Ｃで構成したもので、前記第３の実施例のものと同様な作用が得られる。

【０１９６】これらの第３，第４の各実施例では、ローラ状電極３－Ｂ、および、電極板３－Ｃが、何れも導電性の材料で構成されるため、母材の一部を切り欠くことによって、その非電極部３ｄを形成したが、例えば、樹脂やセラミック等からなる絶縁ローラの表面に、電極部３ｃとしての多数の導電部を電気的に接続して配列することにより、電荷印加手段を形成してもよい。

【０１９７】上述のように、これらの第３，第４の各実施例では、搬送ベルト８に対して、ローラ状電極３－Ｂ、および、電極板３－Ｃを対向させて配置するだけの構造であるので、回転駆動するための機構が不要になり、そのコストを低減、および、小型化を図ることができる。

【０１９８】ところで、このようにして形成されるストライプ状の電荷パターンは、電極部３ｃの縁端から電荷が回り込むため、その帯電領域の幅が非帯電領域の幅よりも広くなる傾向があり、その境界の電場が弱められる虞れが高い。

【０１９９】そこで、これらの実施例では、搬送ベルト８上に形成される電荷パターンの帯電領域の幅と非帯電領域の幅とが略均等となるように、ローラ状電極３－Ｂ、および、電極板３－Ｃの電極部３ｃの幅が、非電極部３ｄの幅よりも予め大きく形成されている。

【０２００】従って、これらの第３，第４の実施例によれば、その電荷パターンの帯電領域と非帯電領域との境界が明確となり、この境界部の電場の強度を大きくできるので、その電極部３ｃと非電極部３ｄとの配列ピッチを密にしてその端縁効果を増大させることにより、ブック原稿のページの搬送ベルト８に対する吸着力を高めることができる。

【０２０１】また、さらに他の、搬送ベルト８の表面近傍に不平等電界を発生させるための手段としては、図３３に示すように、直流電源からなる高圧電源３２０の印加電圧をスイッチ３２０ａでオン／オフを繰り返しながら、バイアスローラ３－Ｄに直流電圧を印加するように構成してもよい。

【０２０２】上述のように、不平等電界を発生させるための手段は、交流電圧に限定されるものでなく、矩形状、三角状、鋸形状等の交番電圧、あるいは、交流交番電圧に直流成分を重畳し、正・負のどちらかに偏った電圧でもよい。

【０２０３】このように、本実施例におけるページめくり方式によれば、めくり搬送ベルト８に吸着させる用紙（ブック原稿９２）には、何等細工を施す必要が無いので、この用紙どうしが静電気により互いに引き合うことが無く、用紙端部の乱れ（不揃い）の発生による、ブック原稿９２のページめくりミスの発生を無くすことができる。

30

【０２０４】また、このページめくり方式によれば、その吸着力の発生している個所が、めくり搬送ベルト８の表面の近傍であるので、このめくり搬送ベルト８の表面に接触している用紙、すなわち、ブック原稿９２のページめくりが実行されるがわの最上位の原稿に対しては、充分に大きな搬送力、及び、吸着力が作用するが、この原稿の下位に位置する、２枚目以下の原稿に対しては、これらの搬送力、及び、吸着力が、ほとんど作用することが無い。

【０２０５】従って、このページめくり方式によれば、１枚だけのページめくりを確実に実行することができるので、この方式は、ブック原稿９２のページめくり方式として最適な方式となる。

【０２０６】次に、上述のように構成されたＭＦＤＳの動作について説明する。図３４はＭＦＤＳの電装ブロック図、図３５、図３６、図３７はブック原稿読み取り時の動作モード遷移図、図３５、図３８はシート原稿読み取り時の遷移図、及び、図３９はＭＦＤＳの動作モードを示すフローチャートである。

【０２０７】先ず、図３４に基づいて、ＭＦＤＳの制御手段について説明する。図３４において、メイン制御ボード３１０は、各ボード間のコマンド、及び、データを制御し、各負荷のＯＮ／ＯＦＦタイミングや、各センサ入力による異常処理、及び、モード切り換え等を行 いＭＦＤＳ全体のコントロールをしている。

【０２０８】また、このメイン制御ボード３１０は、接続機器との通信を行うことにより、通信プロトコルを設定し、各接続機器に対して個別に対応できるように構成されている。

【０２０９】例えば、プリンタ３００がその出力装置として接続されている場合には、その画素密度、処理速度、両面プリントの可否、及び、裏面排紙の可否等をチェックし、その対応モード選択域を決定できるように構成されている。

【０２１０】さらに、このメイン制御ボード３１０は、各モードに対応して、外部機器へのインターフェースを２系統備えている。本実施例のメイン制御ボード３１０では、各ボード間のコマンドをシリアル通信で行い、そのデータ・制御線から分離して、そのデータ出力中にもコマンド送受信を可能としている。

【０２１１】ここで、その汎用性を高める場合には、そのインターフェースとして、ＧＰＩＢ、セントロニクス、ＳＣＳＩ等の、どちらか一方、もしくは、両方を設定することにより、汎用プリンタや、パーソナルコンピュータを介して、そのディスプレイ表示や、光ディスク装置、ＨＤＤ、及び、ＦＤＤ等の記憶装置に対して、特別なインターフェースを使用すること無く、ストアすることができる。

【０２１２】一方、図３４において、めくり搬送ベルト駆動制御ボード３１１は、めくり搬送ベルト駆動モータ

Petitioner Apple Inc. - Exhibit 1012, p. 1465

31

６１の制御を行っている。また、めくりユニット駆動制御ボード３１２は、めくりユニット駆動モータ６０の制御を行っている。

【０２１３】ここで、めくり搬送ベルト駆動モータ６１は、このめくり搬送ベルト駆動モータ６１に一体的に取付けられたエンコーダの発するエンコーダパルスのフィードバックによって、めくり搬送ベルト８の速度を検出し、その速度位置制御及び正逆転動作を行っている。

【０２１４】これに対し、めくりユニット駆動モータ６０は、めくりローラ２に取付けられているエンコーダ１５２の発するエンコーダパルスのフィードバックによって、めくりローラ２の位置を検出し、その速度位置制御及び正逆転動作を行っている。

【０２１５】また、これらのめくり搬送ベルト駆動制御ボード３１１、及び、めくりユニット駆動制御ボード３１２は、メイン制御ボード３１０とそれぞれ接続されており、このメイン制御ボード３１０との間で、それぞれシリアル通信によりコマンドの送受信を行っている。

【０２１６】操作表示ボード３１３は、プリント置数、変倍率、ページめくり枚数、及び、各モード等を設定する各キー入力と、これらのキー入力に対する表示や、エラー表示、めくり状態表示、及び、各モードの原稿セット方法等の表示を行う。

【０２１７】ここで、モード表示においては、接続機器（プリンタ３００）の能力により可能なモードしか表示しないか、あるいは、不可能なモードが選択された場合にエラー表示を行う。

【０２１８】例えば、両面プリントのできないプリンタが接続されているにも拘らず、両面モード選択キー６１２のキー入力がなされた場合に、”接続のプリンタは両面不可です”等のエラー表示が行われる。

【０２１９】また、原稿の読み取りは、この操作表示ボード３１３上のスタートキー６００のキー入力により開始される。さらに、この操作表示ボード３１３と、メイン制御ボード３１０とは、シリアル通信によりコマンド、あるいは、データの送受信を行っている。

【０２２０】第１画像処理ボード３１４は、第１読み取りセンサユニット９に内蔵されているＳ１等倍センサ３１５（以下これを第１ＣＣＤ３１５とする）のドライブクロックを発生する機能と、同じく第１読み取りセンサユニット９に内蔵されている第１ＬＥＤ３１６のＯＮ／ＯＦＦタイミングをとる機能と、第１ＣＣＤ３１５の出力を増幅し、この出力をＡ／Ｄ変換して画像処理を行う機能を有している。

【０２２１】また、この第１画像処理ボード３１４では、シェーディング補正、ＭＴＦ補正、主走査変倍、文字処理、写真処理、及び、ネガ・ポジ反転等の画像処理が行われる。この第１画像処理ボード３１４は、メイン制御ボード３１０に接続されており、このメイン制御ボード３１０との間で、データやコマンドを送受信している。

32

【０２２２】第２画像処理ボード３１７は、上述の第１画像処理ボード３１４と同様に、第２読み取りセンサユニット１４（第１読み取りセンサユニット９と同様に構成されている）に内蔵されている第２ＣＣＤ３１８のドライブクロックを発生する機能と、同じく第２読み取りセンサユニット１４に内蔵されている第２ＬＥＤ３１９のＯＮ／ＯＦＦタイミングをとる機能と、第２ＣＣＤ３１８の出力を増幅し、この出力をＡ／Ｄ変換して画像処理を行う機能を有している。

【０２２３】また、この第２画像処理ボード３１７では、第１画像処理ボード３１４と同様に、シェーディング補正、ＭＴＦ補正、主走査変倍、文字処理、写真処理、及び、ネガ・ポジ反転等の画像処理が行われる。

【０２２４】さらに、この第２画像処理ボード３１７は、メイン制御ボード３１０に接続されており、このメイン制御ボード３１０との間で、データやコマンドを送受信している。

【０２２５】第１高圧電源３２０は、前述したように、第１パイアスローラ３に高圧交流電圧を印加する電源であって、原稿吸着用と、ベルト除電用の２通りの周波数を発生できるように構成されており、各周波数の切り換えは、メイン制御ボード３１０の２本の出力ポートからの切り換え信号により行われる。

【０２２６】また、第２高圧電源３２１は、第１高圧電源３２０と同様に、第２パイアスローラ１１に高圧交流電圧を印加する電源であって、原稿吸着用と、ベルト除電用の２通りの周波数を発生できるように構成されており、各周波数の切り換えは、メイン制御ボード３１０の２本の出力ポートからの切り換え信号により行われる。

【０２２７】給紙クラッチ１２８は、メイン制御ボード３１０からの制御信号に基づいて、シート原稿２００の給紙開始タイミングを制御している。また、メイン制御ボード３１０の各入力ポートに接続されている各種センサ２５，２６，２７，２８，２９，３０，３１，３２，３３，３４は、前記の機構説明において述べた通り、モード切り換え、タイミング検知、及び、異常検知等を行っており、それぞれ、その検知信号をメイン制御ボード３１０に与えている。

【０２２８】次に、ＭＦＤＳの動作モードについて説明する。ＭＦＤＳの動作モードは、大きく２つのモードに分けられている。このＭＦＤＳの第１の動作モードは、図３５に示すような、ブック原稿の自動ページめくり読み取り動作を行うブック原稿読み取りモードであり、第２の動作モードは、同図３５に示すような、シート原稿の自動給紙読み取り動作を行うシート原稿読み取りモードである。

【０２２９】これらのブック原稿読み取りモード、及び、シート原稿読み取りモードは、それぞれさらに細分化されたモードを持っている。すなわち、ブック原稿読

Petitioner Apple Inc. - Exhibit 1012, p. 1466

み取りモードには、図３７に示すように、ブック原稿９２のブックサイズを自動的に認識する自動ブックサイズ認識モードと、操作表示ボード３１３のキー入力でブックサイズを指定するブックサイズキー入力モードとがある。

【０２３０】これらの、自動ブックサイズ認識モード、及び、ブックサイズキー入力モードでは、何れも、原稿面を上向きに見開いた状態でブック原稿９２をセットする見開き読み取りモードにより、ブック原稿９２に対する自動ページめくり読み取り動作が行われる。

【０２３１】さらに、このブック原稿読み取りモードは、その読み取り方式として、出力装置（特にプリンタ）と関連して、見開かれたブック原稿９２の左右２ページ分の原稿画像を連続して読み取り、この２ページ分の画像を１枚の転写紙上にプリントする見開き２ページ連続読み取りモードと、両面画像形成機能を有するプリンターを使用して、上述の見開き２ページ連続読み取りモードにより左右２ページ分の原稿画像がプリントされた１枚の転写紙の裏面に、見開かれたブック原稿９２の次の左右２ページ分の読み取り画像を連続して形成する、この見開き２ページ連続読み取りモードの両面モードと、見開かれたブック原稿９２の左右両ページの原稿画像を１頁ずつ区切って読み取り動作を行う見開き１ページ区ぎり読み取りモードと、この見開き１ページ区ぎり読み取りモードによりプリントされた転写紙の裏面に、上記両面画像形成機能を有するプリンタにより、見開かれたブック原稿９２の次の左右両ページの原稿画像を１頁ずつ区切って形成する、この見開き１ページ区切り読み取りモードの両面モードとを有している。

【０２３２】一方、シート原稿読み取りモードには、図３８に示すように、第１読み取りセンサユニット９、もしくは、第２読み取りセンサユニット１４の位置を固定した状態で、シート原稿２００を自動で給送・排出移動させながら、シートスルー方式により原稿画像の読み取りを行うシート原稿スルーモードと、原稿載置面１１６上にシート原稿２００をセット（定置）した状態で、ページめくり読取ユニット１の第１読み取りセンサユニット９を繰返し往復移動（スキャン）させて、シート原稿２００の読み取り動作を行うシート原稿スキャンモードと、自動原稿給送機能（ＡＤＦ）で原稿をセットできない（あるいはセットしない）場合に、手動で原稿をセットするシート原稿手動開閉モードとがある。

【０２３３】また、シート原稿スルーモードには、シート原稿２００の片面のみの画像を読み取る片面読み取りモードと、第１読み取りセンサユニット９及び第２読み取りセンサユニット１４で、シート原稿２００の両面の画像を同時に読み取る両面読み取りモードとがある。

【０２３４】さらに、この両面読み取りモードは、第１読み取りセンサユニット９及び第２読み取りセンサユニット１４を、互いに向き合った同一位置に配置して、原稿画像の読み取りを行う同一位置読み取りモードと、第１読み取りセンサユニット９及び第２読み取りセンサユニット１４を、互いにずらした別位置に配置して、原稿画像の読み取りを行う別位置読み取りモードとを有している。　以上、ＭＦＤＳの動作モードについて説明してきたが、次に、図３９を参照しながら、上述した個々のモードの切り換えについて説明する。図３９において、ＭＦＤＳのメイン電源をＯＮすると、図３４で示したメイン制御ボード３１０、めくり搬送ベルト駆動制御ボード３１１、めくりユニット駆動制御ボード３１２、操作表示ボード３１３、第１画像処理ボード３１４、第２画像処理ボード３１７が、それぞれリセットされて初期設定が行われる。

【０２３５】その後、プリンタ３００等の接続機器の接続をチェックし、この接続機器に対応可能なモードを表示する一方、プリント置数、変倍率、ページめくり枚数、及び、各モード等を設定する各キーの入力を受け付ける。また、この間に、ブック原稿９２またはシート原稿２００のセットが行われる。ここで、シート原稿２００が、シート原稿トレイ９４にセットされた場合には、シート原稿センサ２５がＯＮされる。また、ここで、操作表示ボード３１３のオープンキー６２０によりＭＦＤＳの搬送部１９が開放され、その原稿載置面１１６の中央基準位置決め部２４に、ブック原稿９２が、見開かれた状態でセットされた場合には、ブック原稿センサ２７がＯＮされる。

【０２３６】これらのシート原稿センサ２５とブック原稿センサ２７のＯＮ／ＯＦＦの状態、及び、操作表示ボード３１３のテンキー６０２により入力されたシート原稿２００のプリント枚数を示すプリント置数に応じて、原稿画像の読み取りモードが、図３９に示すように切り替わる。

【０２３７】すなわち、ここで、ブック原稿センサ２７がＯＦＦ、シート原稿センサ２５がＯＮで、且つ、プリント置数が「１」の場合には、シート原稿スルーモードへ遷移する。また、ここで、ブック原稿センサ２７がＯＦＦ、シート原稿センサ２５がＯＮで、且つ、プリント置数が「２」以上の場合には、シート原稿スキャンモードへ遷移する。

【０２３８】さらに、ブック原稿センサ２７、及び、シート原稿センサ２５が、両方共ＯＦＦの場合には、シート原稿手動開閉モードへ遷移する。また、ブック原稿センサ２７がＯＮで、シート原稿センサ２５がＯＦＦの場合には、ブック原稿読み取りモードに遷移する。

【０２３９】さらに、ここで、ブック原稿センサ２７、及び、シート原稿センサ２５が、両方共ＯＮの場合には、異常処理１（警告ブザーＯＮ、及び、エラー表示）を行って、ユーザーに注意を促した後、ブック原稿読み取りモードに遷移する。

【０２４０】このようにして、それぞれ選択されたモー

Petitioner Apple Inc. - Exhibit 1012, p. 1467

ドサブルーチンへ入った後、操作表示ボード３１３のスタートキー６００が押されていなければ、画像読み取り動作を実行せずに、キー入力を受け付けるステップにリターンされる。

【０２４１】次に、上述した、各モードの動作について、説明する。先ず、図４０を参照して、ブック原稿読み取りモードについて説明する。ＭＦＤＳのモードが、ブック原稿読み取りモードに入ると、スキャンカットオフセンサ３４のＯＮ／ＯＦＦのチェックが行われる。

【０２４２】このスキャンカットオフセンサ３４は、図４に示したように、ページめくり読取ユニット１が、その上限位置まで上昇したときに、その上限検知部７６を検知してＯＮされる。ページめくり読取ユニット１は、前述したように、原稿載置面１１６上に載置されたブック原稿９２の厚さに応じて上下動される。このページめくり読取ユニット１の上昇、すなわち、ブック原稿９２の厚さが厚くなるに従って、これを駆動するめくり搬送ベルト８のテンションが高くなる。

【０２４３】従って、このめくり搬送ベルト８のテンションが高くなりすぎると、つまり、ブック原稿９２が厚すぎてページめくり読取ユニット１が上昇しすぎると、このテンションがブレーキとなって、ページめくり読取ユニット１のスキャンができなくなる。

【０２４４】スキャンカットオフセンサ３４は、このような、ブック原稿９２が厚すぎて、ページめくり読取ユニット１がスキャンできないレベルを検知している。このスキャンカットオフセンサ３４がＯＮの場合には、異常処理２（警告ブザーのＯＮと、”ブック原稿が厚すぎます”のエラー表示）を行って、ユーザーが無理に搬送部１９を閉じて、この搬送部１９を破損することがないようにしている。

【０２４５】ここで、ブック原稿９２の厚さが適応レベル以下の場合には、ユーザーにより搬送部１９が閉じられることによって、搬送部ロックセンサ３１がＯＮされる。このとき、搬送部１９が開いたまま、すなわち、搬送部ロックセンサ３１がＯＦＦのままであれば、異常処理３（警告ブザーのＯＮと、”搬送部を閉じて下さい”の表示）が行われる。

【０２４６】そして、この搬送部１９が閉じられると、ブックサイズ上限センサ３３のＯＮ／ＯＦＦのチェックが行われる。ここで、ブックサイズ上限センサ３３が、ブック原稿９２のブックサイズを検知してＯＮされている場合、すなわち、原稿載置面１１６にセットされているブック原稿９２のブックサイズが、ページめくり読取ユニット１の読み取り領域を越えた読み取り不可能なブックサイズの場合には、異常処理４（警告ブザーのＯＮと、”ブック原稿のサイズが大きすぎます”の表示）が行われる。

【０２４７】その後、プリンド置数、変倍率、めくり枚数のキー入力の有無のチェックが行われた後、自動ブックサイズ認識モードの場合には、プレスキャンフラグがセットされ、自動ブックサイズ認識モードでない場合には、ブックサイズ入力モードとなり、操作表示ボード３１３により所定のキー入力を行ってブックサイズを設定することにより、ブック原稿９２の読み取り領域が決定される。

【０２４８】そして、スタートキー６００が押されることにより、搬送部ロック装置１４０が作動して、搬送部１９が原稿台１８にロックされる。これにより、ページめくり読取ユニット１によるページめくり動作中に、ユーザーが間違って搬送部１９を開放して、ブック原稿９２を破損するような事態が回避される。

【０２４９】次いで、この搬送部ロック装置１４０の作動後、前述したプレスキャンフラグがセットされている場合には、ページめくり読取ユニット１のプレスキャン動作が実行される。ここで、プレスキャンフラグがセットされていない場合には、このプレスキャン動作がスキップされる。

【０２５０】このプレスキャン動作後は、接続機器（プリンタ３００）の準備が整うまで待機される。そして、この接続機器（プリンタ３００）の準備が整った段階で、接続機器（プリンタ３００）から出力される読み取り開始信号を受けると、ページめくり読取ユニット１が駆動されて、前述したように、ブック原稿９２の原稿画像の読み取り動作が開始される。

【０２５１】このページめくり読取ユニット１による読み取り動作は、前に設定されているプリント置数に応じた回数だけ、繰り返して行われる。そして、この所定回数の読み取り動作が完了すると、次ページの原稿画像の読み取り動作を行うべく、前述したように、ページめくり読取ユニット１によって、ページめくり動作が実行される。

【０２５２】このようにして、ブック原稿９２の原稿画像の読み取り動作、及び、ページめくり動作は、それぞれ、予め設定された置数に応じて、その最終ページがめくられるまで、繰り返し実行される。そして、予め設定された最終めくりページのページめくり動作が完了し、且つ、最終読み取りページに対する所定回数の読み取り動作が完了すると、この最終読み取りページのページめくり動作を行わずに、ページめくり読取ユニット１が、そのホームポジション位置〔１Ａ〕に復帰されて、このブック原稿読み取りモードルーチンがリターンされる。

【０２５３】ブック原稿読み取りモードの基本動作は、以上の図４０に示すフローチャートの通りであるが、このモード中の前述した、見開き２ページ連続読み取りモードと、その両面モード、及び、見開き１頁区切り読み取りモードと、その両面モードは、図４１のキー入力セット時に受け付けた入力モードとなる。

【０２５４】これらの各入力モードについては、スタートキー６００が押されてからの経過を示すタイミングチ

Petitioner Apple Inc. - Exhibit 1012, p. 1468

ャートを参照して説明する。先ず、図４１に示すタイミングチャートを使用して、見開き２ページ連続読み取りモードについて説明する。

【０２５５】図４１において、操作表示ボード３１３のスタートキー６００が押されて、読み取りスタートスイッチＳＷがＯＮされると、第１読み取りセンサユニット９内のシャッタ（図示せず）が閉じる。このシャッタの内面は、白色基準板になっていて、これにより、第１読み取りセンサユニット９のシェーディング補正が行われる。

【０２５６】このシェーディング補正は、ページめくり読取ユニット１の立上り時に毎回行われ、ページめくり読取ユニット１の移動速度が一定速度になる前に完了される（この部分のタイミングチャートは図示せず）。このページめくり読取ユニット１のスタートは、メイン制御ボード３１０から、めくりユニット駆動制御ボード３１２へ送られる正転スタート信号によって行われる。

【０２５７】この正転スタート信号により、ページめくり読取ユニット１が、プレスキャンを開始する。ここで、ページめくり読取ユニット１の移動速度が一定速度Ｖｆに立ち上がった後は、前述のシャッタが既に開かれており、第１ＣＣＤ３１５により、ブック原稿９２の原稿画像の読み取りが開始されている。

【０２５８】このページめくり読取ユニット１のプレスキャン時の読み取りにより、見開かれたブック原稿９２の端部を画像処理でエッジ検出し、このときのめくりローラ２に取付けられたエンコーダ１５２の出力をカウントすることによって、原稿載置面１１６にセットされたブック原稿９２のブックサイズを認識して、ページめくり読取ユニット１の原稿画像の読み取り領域、及び、ページめくり領域を決定する。

【０２５９】このように、このＭＦＤＳは、ブック原稿９２が原稿載置面１１６のセンターを基準としてセットされるように構成されているので、このセットされたブック原稿９２の左端部のみを検出することによって、そのページめくり読取ユニット１の原稿画像の読み取り領域、及び、ページめくり領域を算出することができる。

【０２６０】従って、このＭＦＤＳでは、ブック原稿９２のブックサイズ検知に際して、ページめくり読取ユニット１を全面プレスキャンさせる必要がなく、ページめくり読取ユニット１をショートプレスキャンさせるだけで、原稿載置面１１６上に載置されたブック原稿９２のブックサイズを検知することができる。

【０２６１】これにより、このページめくり読取ユニット１のプレスキャン時に、ブック原稿９２の読み取り開始ページを誤ってページめくりすることがなくなる。

【０２６２】このブック原稿９２のブックサイズデータは、メイン制御ボード３１０から、外部接続機器としてのプリンタ３００に送信される。

【０２６３】一方、このブックサイズ検知が完了し、そのブックサイズデータがプリンタ３００に送信されている間に、メイン制御ボード３１０から、めくりユニット駆動制御ボード３１２に対して、めくりユニット駆動モータ６０を逆転させる逆転信号が与えられ、ページめくり読取ユニット１が速度Ｖｒの速さで、そのホームポジション位置〔１Ａ〕に向けて復帰移動される。

【０２６４】なお、このＭＦＤＳの原稿台１８の原稿載置面１１６を、有彩色、例えば、黄色などのような、ブック原稿としてあまり使用されていないような有彩色で着色しておくことにより、この原稿載置面１１６と、ブック原稿９２の原稿画像の読み取り領域との、領域識別精度を高めることができるので、上述のプレスキャン時におけるブックサイズ検知をより正確に行うことができ、そのブックサイズデータの信頼性が向上される。

【０２６５】また、ここで、原稿載置面１１６を、例えば、灰色などの中間色で着色しておけば、第１読み取りセンサユニット９の第１ＣＣＤ３１５として、カラーセンサを使用せずに、プレスキャン時の領域識別が可能となる。上述のプレスキャンが終了して、ページめくり読取ユニット１がホームポジション位置〔１Ａ〕に退避した後、プリンタ３００の準備ができて、プリンタ３００からメイン制御ボード３１０に対し、データの転送を要求する転送要求信号が与えられると、これにより、メイン制御ボード３１０から、めくりユニット駆動制御ボード３１２に対して、めくりユニット駆動モータ６０を正転させる正転信号が与えられ、ページめくり読取ユニット１の正転動作が開始される。

【０２６６】このページめくり読取ユニット１は、前述したように、めくりローラ２のエンコーダ１５２の出力がフィードバックされることによって、ブック原稿９２の原稿面に沿って、速度Ｖｆの速さに定速度制御されて、そのエンドポジション位置〔１Ｃ〕に向けて移動される。

【０２６７】このとき、第１読み取りセンサユニット９のＬＥＤ３１６は、既に点灯されており、この第１読み取りセンサユニット９の第１ＣＣＤ３１５により、ブック原稿９２の原稿情報の読み取りが開始されている。

【０２６８】ここで、図１に示すように、原稿載置面１１６上に見開かれてセットされたブック原稿９２の綴じ部（センター部）付近は、原稿面の反りがきついため、この綴じ部付近の原稿情報を正確に読み取ることが困難となる。また、このブック原稿９２の綴じ部付近には、通常、文字や画像等の原稿情報が形成されることがない。

【０２６９】そこで、このＭＦＤＳでは、図４１に示すように、このブック原稿９２の綴じ部付近において、第１ＣＣＤ３１５の読み取りＳＦＧＡＴＥがＯＦＦされ、この綴じ部付近の原稿情報の読み取りがマスクされるようになっている。

【０２７０】この原稿情報の初期設定時におけるマスク

Petitioner Apple Inc. - Exhibit 1012, p. 1469

39

領域は、前述したように、中央基準位置決め部２４のセンターより＋１０mm、－１０mmとなるように設定されているが、このマスク領域は、操作表示ボード３１３のブック綴じ部マスク領域設定キー６０８のキー入力によって、その設定値を変更し得るようになっており、特殊な装丁のブック原稿にも対応できるようになっている。

【０２７１】ところで、第１読み取りセンサユニット９によるブック原稿９２の原稿情報の読み取りは、ページめくり読取ユニット１がそのエンドポジション位置〔１Ｃ〕に至るまで行われるが、このページめくり読取ユニット１が、ブック原稿９２のセンター付近に到達した時点で、第１高圧電源３２０が周波数ｆ１でＯＮされる。これにより、めくり搬送ベルト８のブック原稿９２の右側のページに当接する部分に、前述した電荷パターンが形成される。

【０２７２】このめくり搬送ベルト８は、上述のように、ページめくり読取ユニット１が駆動されているときには駆動されず、ブック原稿９２を押える働きをしている。このようにして、ページめくり読取ユニット１が、そのエンドポジション位置〔１Ｃ〕まで駆動されて、ブック原稿９２の右端部の読み取り領域までの原稿情報の読み取りが終了すると、第１高圧電源３２０の出力がＯＦＦされるとともに、メイン制御ボード３１０からめくりユニット駆動制御ボード３１２に対して、めくり信号が与えられ、ページめくり読取ユニット１によるブック原稿９２のページめくり動作が開始される。

【０２７３】このとき、この第１読み取りセンサユニット９の読み取った原稿面が、予め設定されたブック原稿９２の最終読み取りページに相当している場合には、メイン制御ボード３１０からめくり信号が出力されず、このページめくり読取ユニット１は、このブック原稿９２の最終読み取りページの読み取りを終えた後、上述のページめくり動作を行わずに復帰移動されて、そのホームポジション位置〔１Ａ〕に退避される。

【０２７４】ブック原稿９２のページめくり動作時において、ページめくりセンサ２９がＯＮされるまでの間は、ページめくり読取ユニット１の逆転動作がスロースタートされ、めくり搬送ベルト８上に静電的に吸着されたブック原稿９２の読み取り終了ページ（図１における右ページ）が、そのページ収納部７内に導かれる。

【０２７５】そして、ページめくり読取ユニット１が、そのホームポジション位置１－Ａに向けて、さらに復帰移動され、このブック原稿９２の読み取り終了ページのセンター部分までが、ページ収納部７内にめくり込まれる。

【０２７６】また、このページめくり読取ユニット１のページめくり動作時においては、めくり搬送ベルト８の原稿吸着領域の電荷パターンを除電するために、第１高圧電源３２０が周波数ｆ２でＯＮされる。

40

【０２７７】このようにして、ページめくり読取ユニット１のページ収納部７内にめくり込まれたブック原稿９２の読み取り終了ページは、ページめくり読取ユニット１が、ブック原稿９２のセンター部を越してから、そのエンドポジション位置〔１Ｃ〕に至る間に、ページ収納部７内から排出されて、そのページめくり動作が完了する。

【０２７８】このページ排出時におけるページめくり読取ユニット１のリターン速度Ｖｒｍは、その原稿読み取り時における速度Ｖｆよりも大きくなるように、すなわち、Ｖｒｍ＞Ｖｆとなるように設定されており、このページめくり動作の高速化が図られている。

【０２７９】この１連のページめくり動作の状態は、ページめくりセンサ２９により検知されている。すなわち、このＭＦＤＳは、ページめくり読取ユニット１の各位置におけるページめくりセンサ２９のＯＮ／ＯＦＦがチェックされることにより異常の有無が検出され、異常がある場合に、異常処理動作が実行される。

【０２８０】この異常処理動作としては、警告ブザーが作動されるとともに、例えば、ページ収納部７へ原稿ページをめくり込めない場合には、”ページめくり不能”、ページ収納部７にめくり込まれた原稿ページを排出できない場合には、”ページ重ね不能”等の表示が、操作表示ボード３１３に表示され、さらに、このページめくり動作が停止される。

【０２８１】また、この異常が発生したページめくり状態をユーザーが確認できるようにするために、このページめくり状態の異常発生箇所が、操作表示ボード３１３に表示される。

【０２８２】以下、ブック原稿９２の２ページ目以降の原稿画像の読み取り、及び、ページめくり動作は、プリンタ３００からの転送要求信号によって、順次スタートされ、上述と同様の読み取り動作、及び、ページめくり動作が、予め設定された最終読み取りページに至るまで、繰り返し実行される。

【０２８３】ここで、図４１のタイミングチャートでは、原稿のプリント置数を「１」とした場合、すなわち、ブック原稿９２の各読み取りページを、それぞれ１回読み取る毎に、この読み取りを終えたページのめくり動作を実行する場合について示したが、この原稿のプリント置数が「２」以上に設定されている場合には、第１読み取りセンサユニット９による第１回目の原稿読み取り動作が完了した時点で、メイン制御ボード３１０からめくりユニット駆動制御ボード３１２に対して、めくり信号の代わりに逆転信号が送信され、ページめくり読取ユニット１が速度Ｖｒの速さで、そのホームポジション位置〔１Ａ〕に向けてリターンされ、このリターン動作が終えると同時に、このページめくり読取ユニット１の第２回目の原稿読み取り動作がスタートされる。

【０２８４】そして、このようなページめくり読取ユニ

Petitioner Apple Inc. - Exhibit 1012, p. 1470

41

ット1の原稿読み取り動作が、予め設定された原稿のプリント置数の回数分だけ、繰り返し実行され、この動作の回数とプリント置数とが一致した時点で、初めて、メイン制御ボード310からめくりユニット駆動制御ボード312に対して、めくり信号が送信され、上述したページめくり動作が実行される。

【0285】以下、ブック原稿92の2ページ目以降の原稿画像の読み取り、及び、ページめくり動作は、プリンタ300からの転送要求信号によって、順次スタートされ、上述と同様のプリント置数に応じた回数の読み取り動作、及び、ページめくり動作が、予め設定された最終読み取りページに至るまで、繰り返し実行される。

【0286】また、ここで、プリント変倍キー614により、読み取った原稿画像が変倍されるように設定されている場合には、第1読み取りセンサユニット9のスキャン速度Vfが、その変倍率に応じた速度に可変されることによって、この原稿画像の副走査方向の変倍がなされるとともに、第1画像処理ボード314によって、この原稿画像の主走査方向の変倍処理がなされる。

【0287】一方、上述のような、見開き2ページ連続読み取りモードの両面モードにおいては、プリンタ300が原稿画像の両面プリントを行なうために、このプリンタ300からのメイン制御ボード310への転送要求信号の送信タイミングが多少遅れる点は異なるが、それ以外の動作に関しては、前述した見開き2ページ連続読み取りモードと同様の動作が実行される。

【0288】次に、図42を参照して、見開き1ページ区切り読み取りモードについて説明する。この見開き1ページ区切り読み取りモードは、見開かれたブック原稿92の左ページと、右ページとを別々に読み取って、画像形成を行なうモードで、これらの各画像を別々の転写紙にプリントするモードと、1枚の転写紙の表裏にプリントするモード（この見開き1ページ区切り読み取りモードの両面モード）とがある。

【0289】また、このモードにおいては、ブック原稿92の左ページから読み取る動作と、右ページから読み取る動作との、何れか一方の動作を、操作表示ボード313の読み取り開始ページ選択キー603のキー入力により選択設定することができる。　図42は、ブック原稿92の向かって左ページから読み取りを開始する場合のタイミングチャートを示している。

【0290】この見開き1ページ区切り読み取りモードの動作は、前述した見開き2ページ連続読み取りモードの両面モードの動作と略同じであり、この見開き2ページ連続読み取りモードの両面モードの動作と異なる点としては、プリンタ300からメイン制御ボード310への転送要求信号が、1ページ毎に送信される点であって、これにより、ページめくり読取ユニット1が、ブック原稿92の左ページから右ページに向けて等速で移動（スキャン）される。

42

【0291】図43は、この見開き1ページ区切り読み取りモードにおいて、ブック原稿92の右ページから読み取りを開始するように、セットされている場合のタイミングチャートを示している。

【0292】このタイミングチャートから明らかなように、ブック原稿92の右ページから読み取りが開始される場合には、このブック原稿92の読み取りが行なわれない左ページに対するページめくり読取ユニット1の移動速度が、右ページに対する第1読み取りセンサユニット9のスキャン速度Vfよりも速い速度となるようにプログラムされていて、原稿読み取り時間の短縮化、すなわち、読み取り機能の性能アップが図られている。

【0293】また、この見開き1ページ区切り読み取りモードにおいて、読み取りスキップページ設定キー618により、スキャンをせずに読み飛ばす（スキップする）ページが設定されている場合には、この読み取りスキップページに対するページめくり読取ユニット1が、読み取りを行なう時の第1読み取りセンサユニット9のスキャン速度Vfよりも速い速度で移動されて、直ちに、この読み取りスキップページのめくり動作が実行されるようにプログラムされている（タイミングチャートは図示せず）。

【0294】ところで、一般的には、図42及び図43に示したように、プリンタ300からメイン制御ボード310に対して、通常状態で連続して転送要求信号を要求できるプリンタは少ない。

【0295】そこで、このような一般的なプリンタを使用して、この見開き1ページ区切り読み取りモードを実施する場合には、このプリンタ側において、2枚の転写紙を重連するように給紙させることによって実現させることができる。

【0296】また、ここで、転写紙と感光体ドラムとのレジストの関係上、これらの2枚の転写紙間に、どうしても、ある程度の距離を設けなければならないような場合には、ブック原稿92の左ページ側の画像データはそのままプリンタに流し、ブック原稿92の右ページ側の画像データは、ディレーメモリを通して、これら転写紙間の距離に相当する時間だけ、プリンタへの転送タイミングを遅延させることにより実現させることができる。

【0297】この後者の場合の一例のブロック図を図44に、また、そのタイミングチャートを図45に示す。この例では、メイン制御ボード310上の内部の各ゲートA，Bにより、切り換え器を通してプリンタへそのまま出力される画像データに対して、ディレーメモリを通してプリンタへ出力される画像データが、時間Tdだけ遅延されるように構成されている。

【0298】次に、この見開き1ページ区切り読み取りモードにおける両面モードについて説明する。先ず、見開かれたブック原稿92の左右2ページの画像データを1枚の転写紙の表裏にプリントする場合について説明す

Petitioner Apple Inc. - Exhibit 1012, p. 1471

る。

【0299】この場合には、プリンタ300側において、転写紙を反転搬送する必要があるため、その左ページの画像データのプリントを終えてから、右ページの画像データのプリントを開始するまでに、多少の時間がかかる。

【0300】このため、このモードでは、ページめくり読取ユニット1がブック原稿92の左ページの読み取りを終えて、その綴じ部付近に到達した時点で、このページめくり読取ユニット1の駆動が一旦停止される。

【0301】そして、プリンタ300側での左ページ画像のプリント、及び、この転写紙の反転搬送が完了し、プリンタ300からメイン制御ボード310に転送要求信号が出されると、停止されていたページめくり読取ユニット1が再び所定のスキャン速度Vfで駆動されて、ブック原稿92の右ページの読み取りが行なわれ、この右ページの画像データがプリンタ300に転送されて、表面に左ページ画像のプリントされた転写紙の裏面に、この右ページ画像がプリントされて、両面プリントが行なわれる。この時の、タイミングチャートを図46に示す。

【0302】次に、この見開き1ページ区切り読み取りモードにおいて、プリントされた転写紙の表裏と、ブック原稿92の原稿面の表裏との関係を、一致させて画像形成する場合の両面モードについて説明する。このモードにおいて、ブック原稿92の左ページから読み取りを開始する場合には、前述したように、プリンタ300に対して、2枚連続給紙を行なうように指示し、左ページ画像のプリントされた転写紙はそのまま排紙させる一方、右ページ画像のプリントされた転写紙は反転搬送させて、その裏面にブック原稿92の次ページの左ページ画像をプリントするための準備を行なっておく。

【0303】この間に、MFDS側においては、読み取りを終えた原稿ページのページめくり動作が行なわれる。このMFDS側でのページめくり動作が完了されると、次ページに対する読み取り動作が実行され、前に、右ページ画像がプリントされて反転搬送された転写紙の裏面に、読み取られた左ページ画像がプリントされて排出される。

【0304】また、この時読み取られた右ページ画像は、新たに給紙された転写紙にプリントされる。この転写紙は、先の転写紙と同様に、反転搬送されて、その裏面にブック原稿92の次ページの左ページ画像をプリントするための準備が行なわれる。このような1連の動作が繰り返し実行されることにより、ブック原稿92と全く同様なページ構成の原稿画像がプリントされた転写紙が得られる。以上が、ブック原稿読み取りモードにおける動作の一例である。

【0305】ここで、見開き読み取りモードにおけるブック原稿のセットについて説明する。　図34の接続機器チェックにおいて、プリンタ300が裏面排紙可能な場合には、次のような表示が行なわれる。

【0306】すなわち、”ブック原稿が横書き（左開き）ならば、読み取りたい先頭ページを見開いて正面上向きにセットして下さい。”　”ブック原稿が縦書き（右開き）ならば、読み取りたい先頭ページを見開いて天地逆上向きにセットして下さい。”のように、ブック原稿の横書き、縦書きに対する、それぞれのセット方法が指示される。

【0307】これに対し、図34の接続機器チェックにおいて、プリンタ300が表面排紙のみ可能な場合には、次のような表示が行なわれる。

【0308】すなわち、”ブック原稿が横書き（左開き）ならば、読み取りたい最終ページを見開いて天地逆上向きにセットして下さい。”　”ブック原稿が縦書き（右開き）ならば、読み取りたい最終ページを見開いて正面上向きにセットして下さい。”のように、ブック原稿の横書き、縦書きに対する、それぞれのセット方法が指示される。

【0309】このMFDSでは、上述のような指示に従って、ブック原稿92をセットすることにより、これに接続されるプリンタ300の機能に関わらず、排出される転写紙のページ揃えを行なうことができる。また、このMFDSにおけるページめくり枚数の入力方法には、操作表示ボード313のキー入力による2通りの入力方法があり、これらの入力方法の内の何れか1つを、ユーザーが好みによって選択できるようになっている。　この入力方法の一つは、読み取り総ページ設定キー606等を使用して、読み取りたい総ページ数を設定する方法であり、他の入力方法は、読み取り開始ページ設定キー604、読み取り最終ページ設定キー605等を使用して、読み取りたい先頭ページと、最終ページを入力する方法である。

【0310】このMFDSにおけるページめくり枚数の入力は、上記の何れの方法で行なうにせよ、ページめくり読取ユニット1のページめくり回数を正確に算出できればよい。以下、上述の各方法におけるページめくり回数の算出方法について説明する。　先ず、読み取りたい総ページ数を入力した場合について説明する。

【0311】ここで、読み取りたい総ページ数をXとし、めくり回数をMとすれば、左ページから読み取る場合には、

（X－2）／2＝M＋余り・・・①

右ページから読み取る場合には、

（X－1）／2＝M＋余り・・・②

となり、これらの式よりMの値を算出する事により、そのめくり回数が求められる。

【0312】次に、読み取りたい先頭ページと、最終ページを入力した場合について説明する。ここで、読み取りたい先頭ページをY、最終ページをZととし、読み取

Petitioner Apple Inc. - Exhibit 1012, p. 1472

45

りたい総ページ数をXとすれば、

X＝Z－Y＋1・・・③

となり、この③式を、前記の②式、③式に代入することにより、めくり回数Mを算出する事ができる。

【0313】ところで、このMFDSは、前述したように、1台の装置で、ブック原稿と、シート原稿とを選択的に読み取って、その画像形成を行うことができるように構成されている。ブック原稿に関する画像読み取りモードは、上述した通りであり、以下、このMFDSにおけるシート原稿の画像読み取りモードについて説明する。

【0314】このシート原稿の読み取りモードには、図38に示したように、シート原稿スルーモードと、シート原稿スキャンモードと、シート原稿手動開閉モードとがある。

【0315】先ず、シート原稿スルーモードについて説明する。このシート原稿スルーモードには、片面原稿読み取りモードと、両面原稿読み取りモードとがあり、この両面原稿読み取りモードに、同一位置読み取りモードと、別位置読み取りモードとがある。

【0316】これらのモードの選択は、図47に示すように行われる。先ず、片面原稿読み取りモードでは、図48、及び、図49に示すように、シート原稿トレイ94に、シート原稿200が下向きにセットされ、この状態で、スタートキー600が押されると、先ず、めくり搬送ベルト駆動モータ61の電源がONされ、駆動ローラ12が回転されて、めくり搬送ベルト8が回動される。

【0317】このとき、各センサと、各入力データに異常がなければ、給紙クラッチ128がONされ、第1ベルト支持ローラ97に取付けられた第2給紙プーリ130から給紙駆動ベルト127を介して、給紙ローラ96が回転され、シート原稿200が給紙分離パッド95に向けて搬送される。

【0318】この給紙分離パッド95によって、最下位の1枚だけのシート原稿200が他のシート原稿から分離され、第1搬送ガイド108及び第2搬送ガイド109に案内されながら、めくり搬送ベルト8に接する位置まで搬送される。

【0319】ここで、この第2搬送ガイド109には、給紙センサ26が取付けられており、この給紙センサ26によって、シート原稿200の後端が検知されされた後、給紙クラッチ128がOFFされるように、シート原稿200の搬送タイミングが設定されている。

【0320】一方この間に、このめくり搬送ベルト8の回転とともに、第2バイアスローラ11に交流電源から交流の高電圧が印加されて、めくり搬送ベルト8にストライプ状の電荷パターンが形成される。これにより、このめくり搬送ベルト8によって、給紙されたシート原稿200が吸着されて搬送される。このときのめくり搬送

46

ベルト8の線速は、等倍時では360mm／sに、変倍時ではその設定倍率に応じて変化されるようになっている。

【0321】一方、このモードでは、ページめくり読取ユニット1が、そのエンドポジション位置〔1C〕に位置しており、その第1読み取りセンサユニット9によって、めくり搬送ベルト8により搬送されたシート原稿200の原稿情報が順次読み取られる（画素密度は400dpi）。

【0322】そして、この読み取りを終えたシート原稿200は、第3搬送ガイド110及び第4対向ローラ103，第5対向ローラ104，第6対向ローラ105，第7対向ローラ106により、挟持搬送されて、排紙口117から排紙トレイ23上に排紙される。

【0323】この排紙口117の近傍の第3搬送ガイド110には、排紙センサ28が取付けられていて、この排紙されるシート原稿200の排紙ジャムが検知されている。　そして、1枚目のシート原稿200の読み取り動作が完了されると、次に、所定の給紙タイミングで、給紙クラッチ128が再びONされ、2枚目のシート原稿200が給紙されて、上述と同様な読み取り動作が実行される。

【0324】このようにして、シート原稿トレイ94にセットされたシート原稿200が順次給送されて読み取られ、最後の（最上位の）シート原稿200が給紙されて、シート原稿センサ25がOFFすると、第2バイアスローラ11の電源が高周波交流電圧に切り替えられ、めくり搬送ベルト8の電荷パターンが除電されて、この最終のシート原稿200が排紙された後、MFDSの全ての動作が停止される。以上の読み取り動作は、このMFDSに裏面排紙機能を有するプリンタが接続されている場合の動作であり、これにより、シート原稿200及びプリントされた転写紙のページ揃え排紙が実現される。

【0325】ここで、このMFDSに接続されているプリンタが表面排紙機能しか有していない場合には、シート原稿トレイ94上に、シート原稿200を上向きにセットして、第2読み取りセンサユニット14によって、このシート原稿200の読み取りを行うことにより、上述した裏面排紙機能を有するプリンタの場合と同様に、シート原稿200及びプリントされた転写紙のページ揃え排紙が実現される。また、この表面排紙機能を持ったプリンタが接続されている場合におけるその他の動作は、裏面排紙機能を有するプリンタが接続されている場合と同様である。

【0326】次に、このシート原稿スルーモードにおける両面原稿読み取りモードについて説明する。この両面原稿読み取りモードでは、横書きのシート原稿が、その原稿先端から下向きにして、シート原稿トレイ94上にセットされる。

Petitioner Apple Inc. - Exhibit 1012, p. 1473

47

【0327】これは、第1読み取りセンサユニット9及び第2読み取りセンサユニット14がメモリーを持っていないため、その主走査方向でのミラー反転しか用いることができないことによる。

【0328】先ず、この両面原稿読み取りモードにおける同一位置読み取りモードの基本動作は、図50、及び、図51に示すように、片面原稿読み取りモードの場合と同様であるが、このモードでは、ページめくり読取ユニット1が、そのホームポジション位置〔1A〕に位置されて、原稿台18がわの第2読み取りセンサユニット14の位置と同一位置で、シート原稿200の表裏両面の原稿情報の読み取りが、これらの第1読み取りセンサユニット9、及び、第2読み取りセンサユニット14によって、同時に平行して実行される。

【0329】一方、この両面原稿読み取りモードにおける別位置読み取りモードの基本動作は、図52、及び、図53に示すように、片面原稿読み取りモードの場合と同様であるが、このモードでは、ページめくり読取ユニット1が、そのエンドポジション位置〔1C〕に位置されている。

【0330】ここで明らかなように、この別位置読み取りモードでは、第1読み取りセンサユニット9と、第2読み取りセンサユニット14との読み取り位置の間隔が、最大サイズの原稿の長さよりも大きくなるため、これらの第1読み取りセンサユニット9及び第2読み取りセンサユニット14によ読み取られたシート原稿200の表裏両面の原稿情報が、時系列的に出力される。

【0331】次に、シート原稿読み取りモードにおけるシートスキャンモードについて説明する。このシートスキャンモードでは、図54、及び、図55に示すように、シート原稿トレイ94に、シート原稿200が上向きにセットされ、この状態で、スタートキー600が押されると、先ず、めくり搬送ベルト駆動モータ61の電源がONされ、駆動ローラ12が回転されて、めくり搬送ベルト8が回動される。

【0332】このとき、各センサと、各入力データに異常がなければ、給紙クラッチ128がONされ、第1ベルト支持ローラ97に取付けられた第2給紙プーリ130から給紙駆動ベルト127を介して、給紙ローラ96が回転され、シート原稿200が給紙分離パッド95に向けて搬送される。

【0333】この給紙分離パッド95によって、最下位の1枚だけのシート原稿200が他のシート原稿から分離され、第1搬送ガイド108及び第2搬送ガイド109に案内されながら、めくり搬送ベルト8に接する位置まで搬送される。

【0334】ここで、この第2搬送ガイド109には、給紙センサ26が取付けられており、この給紙センサ26によって、シート原稿200の後端が検知されされた後、給紙クラッチ128がOFFされるように、シート

48

原稿200の搬送タイミングが設定されている。

【0335】一方この間に、このめくり搬送ベルト8の回転とともに、第2バイアスローラ11に交流電源から交流の高電圧が印加されて、めくり搬送ベルト8にストライプ状の電荷パターンが形成される。

【0336】これにより、このめくり搬送ベルト8によって、給紙されたシート原稿200が吸着されて搬送される。このときのめくり搬送ベルト8の線速は、360mm／sに設定されており、シート原稿200の先端がホームポジション位置〔1A〕に到達したときに、めくり搬送ベルト8の回動が停止されるようになっている。

【0337】一方、このモードでは、ページめくり読取ユニット1が、そのホームポジション位置〔1A〕に位置しており、めくり搬送ベルト8の回動が停止された後に、ページめくり読取ユニット1がめくりユニット駆動モータ60によって、そのエンドポジション位置〔1C〕に向けて移動されながら、その第1読み取りセンサユニット9によって、めくり搬送ベルト8により搬送されたシート原稿200の原稿情報が順次読み取られる（画素密度は400dpi）。

【0338】この原稿情報の読み取り時には、第1バイアスローラ3に、第1高圧電源320により高周波交流電圧が印加され、めくり搬送ベルト8に形成されていた電荷パターンが除電される。これにより、ページめくり読取ユニット1の復帰移動時におけるシート原稿200のページめくり読取ユニット1内への進入が防止されている。このようにしてシート原稿200の読み取りを終えたページめくり読取ユニット1は、そのホームポジション位置〔1A〕に向けてリターンされる。

【0339】また、このページめくり読取ユニット1のリターン時には、第1読み取りセンサユニット9がシート原稿200の原稿面から上方に退避されるとともに、第1バイアスローラ3に第1高圧電源320から高圧交流電圧が印加されて、めくり搬送ベルト8にストライプ状の電荷パターンが形成されて、このシート原稿200がめくり搬送ベルト8に吸着されて固定される。

【0340】そして、上述のような動作がその設定回数だけ繰り返された後、めくり搬送ベルト駆動モータ61がONされて、めくり搬送ベルト8が回動され、この読み取りを終えたシート原稿200が、排紙口117から排紙トレイ23上に排紙される。

【0341】この排紙口117の近傍の第3搬送ガイド110には、排紙センサ28が取付けられていて、この排紙されるシート原稿200の排紙ジャムが検知されている。そして、1枚目のシート原稿200の読み取り動作が完了されると、次に、所定の給紙タイミングで、給紙クラッチ128が再びONされ、2枚目のシート原稿200が給紙されて、上述と同様な読み取り動作が実行される。

【0342】このようにして、シート原稿トレイ94に

Petitioner Apple Inc. - Exhibit 1012, p. 1474

49

セットされたシート原稿２００が順次給送されて読み取られ、最後の（最上位の）シート原稿２００が給紙されて、シート原稿センサ２５がＯＦＦすると、第２パイアスローラ１１の電源が第２高圧電源３２１の高周波交流電圧に切り替えられ、めくり搬送ベルト８の電荷パターンが除電されて、この最終のシート原稿２００が排紙された後、ＭＦＤＳの全ての動作が停止される。

【０３４３】次に、このシート原稿スルーモードにおけるシート原稿手動開閉モードについて説明する。このシート原稿手動開閉モードの動作は、図５６、及び、図５７に示すように、上述したシート原稿スキャンモードの動作における、シート搬送手段、及び、シート吸着用の各電源をそれぞれＯＦＦの状態にし、オペレータが手操作により、シート原稿の入れ替えが行われる。

【０３４４】以下、このＭＦＤＳにおけるページめくり読取ユニット１の操作制御について説明する。図５８に、このＭＦＤＳにおけるページめくり読取ユニット１の操作制御回路を示す。

【０３４５】この操作制御回路は、ページめくり読取ユニット１の往復駆動制御、及び、その速度制御を行っており、めくりユニット駆動制御ボード３１２に組み込まれている。図５８において、マイクロコンピュータ５２０（以下、単にマイコンという）は、このＭＦＤＳのモード制御、及び、シーケンス制御も行っている（詳細は図示せず）。

【０３４６】このようなマイコン５２０としては、例えば、μＰＤ７１０５４Ｇによるプログラマブルインターバルタイマ５２１（以下、単にタイマという）が接続されている。このタイマ５２１は、マイコン５２０の制御により、めくりユニット駆動モータ６０（直流モータ）の速度制御を行うためのパルス幅変調ＰＷＭ出力を送出するためのものである。

【０３４７】このＰＷＭ制御の周期は、５０（μsec）であり、これを４００ビットの分解能で制御する。このタイマ５２１には、８ＭＨｚの発振器５２２が接続され、クロック信号が与えられるように構成されている。また、めくりユニット駆動モータ６０は、マイコン５２０に対し、駆動用トランジスタＱ１～Ｑ４を介して接続されている。

【０３４８】すなわち、トランジスタＱ１，Ｑ４がＯＮで、トランジスタＱ２，Ｑ３がＯＦＦの状態で、めくりユニット駆動モータ６０には、時計方向（ＣＷ）に回転する電流が供給され、トランジスタＱ２，Ｑ３がＯＮで、トランジスタＱ１，Ｑ４がＯＦＦの状態で、めくりユニット駆動モータ６０には、反時計方向（ＣＣＷ）に回転する電流が供給される。

【０３４９】ここで、めくりユニット駆動モータ６０が、時計方向（ＣＷ）に回転すると、ページめくり読取ユニット１は往動され、めくりユニット駆動モータ６０が、反時計方向（ＣＣＷ）に回転すると、ページめくり

50

読取ユニット１は復動されるように設定されている。

【０３５０】このめくりユニット駆動モータ６０の回転方向は、マイコン５２０のポートＰＦ６，ＰＦ７からそれぞれ出力されるＣＷ信号、及び、ＣＣＷ信号により制御される。また、めくりローラ２には、その回転に従ってパルスを発生させるエンコーダ１５２が直結されている。

【０３５１】ここで、このエンコーダ１５２は、めくりユニット駆動モータ６０の回転量、及び、回転方向に応じて、位相の異なる２つのパルス信号を発生する。１つは、Ａ相エンコーダパルスＥＮＣＡであり、他の１つは、Ｂ相エンコーダパルスＥＮＣＢである。Ａ相エンコーダパルスＥＮＣＡは、分周マルチプレクサ５２４を介して、マイコン５２０のカウンタインプット端子Ｃ１に入力されている。

【０３５２】これにより、マイコン５２０は、Ａ相エンコーダパルスＥＮＣＡのパルス間隔が、マイコン５２０の内部のカウンタ（マイコン５２０の発振器５２５の発振周波数１０ＭＨｚにより規制される）によって計測される。

【０３５３】また、このカウンタインプット端子Ｃ１への入力信号は、割込み入力となっており、割込みプログラムの処理中に、Ａ相エンコーダパルスＥＮＣＡのパルス間隔の測定データの値を読み、このデータに基づいて、めくりユニット駆動モータ６０の回転数の算出、比例・積分制御演算によるモータ制御量の算出、並びに、出力（タイマ５２１へのデータロード）等が行われる。

【０３５４】具体的には、Ａ相エンコーダパルスＥＮＣＡの出力を目標速度に応じて分周マルチプレクサ５２４により、１，２，４，８分周することにより、カウンタインプット端子Ｃ１に割込み入力信号が与えられている。

【０３５５】ここで、１分周時には、第１読み取りセンサユニット９が、エンコーダ１５２の１パルスによって、０．１１６ｍｍ移動することにより、その速度が割込み間隔によりマイコン５２０の内部で演算される。そして、この算出された速度データに基づいて比例・積分演算処理により、出力タイマ値が決定される。

【０３５６】また、Ａ相エンコーダパルスＥＮＣＡ、及び、Ｂ相エンコーダパルスＥＮＣＢは、フリップフロップ５２６を介して、マイコン５２０の入力端子ＰＣ３に入力され、両者間の位相差検知に供されて、その位相差によりめくりユニット駆動モータ６０の回転方向が決定される。

【０３５７】つまり、Ａ相エンコーダパルスＥＮＣＡの立上り時における、Ｂ相エンコーダパルスＥＮＣＢの状態がマイコン５２０のポートに入力されることによって、めくりユニット駆動モータ６０の回転方向が判断される。

【０３５８】次に、めくりユニット駆動モータ６０の速

Petitioner Apple Inc. - Exhibit 1012, p. 1475

51

度制御について説明する。このめくりユニット駆動モータ６０の速度制御はＰＷＭ制御によって行われる。先ず、ページめくり読取ユニット１のスキャナ走査時、すなわち、めくりユニット駆動モータ６０の時計方向への回転時には、トランジスタＱ１をＯＮさせる一方、タイマ５２１からのＰＷＭ出力により、ゲート５２７を介して、トランジスタＱ４をＯＮ／ＯＦＦさせ、めくりユニット駆動モータ６０の両端子間に電位差を生じさせて、ＰＷＭ信号のデューティ比に応じた速度でこのめくりユニット駆動モータ６０を回転させる。

【０３５９】一方、ページめくり読取ユニット１のリターン時には、上述の場合と逆に、トランジスタＱ３をＯＮさせるとともに、タイマ５２１からのＰＷＭ出力により、ゲート回路５２８を介して、トランジスタＱ２をＯＮ／ＯＦＦさせ、めくりユニット駆動モータ６０の両端子間に逆向きの電位差を生じさせて、ＰＷＭ信号のデューティ比に応じた速度でこのめくりユニット駆動モータ６０を回転させる。

【０３６０】以下、上述のように構成されたＭＦＤＳでの著作権管理支援システムについて説明する。先ず、図５９により、ＭＦＤＳのメイン制御ボード３１０の内部の構成、および機能について説明する。

【０３６１】図５９において、ワンチップマイクロコンピュータ３３０（以下、単にマイコンという）は、内部ＲＡＭ、内部ＲＯＭ、Ｉ／Ｏ、タイマ、外部・内部割込み、シリアルインターフェース等を含んだ構成となっている。また、アドレスバス、データバスにより、外部ＲＯＭ３３１、外部ＲＡＭ３３２をはじめとする外部デバイスをアクセスすることができるようになっている。

【０３６２】外部ＲＯＭ３３１は、マイコン内部ＲＯＭと同様に動作プログラムが組み込まれている。外部ＲＡＭ３３２は、外部デバイスへの設定データ等をストアすることができ、バッテリーバックアップ用電池３３４により、装置の電源オフ時でもメモリできるようにバックアップされている。

【０３６３】シリアルインターフェース３３７，３３８，３３９は、外部ユニット、外部機器等とシリアル通信で接続されていて、ワンチップマイコンとコマンドおよびデータの送受信が可能となっている。ＩＤカード読み取り装置３４０は、個人や団体に発行されたカードに組み込まれている磁気データ等を読み取り、コード化してシリアルインターフェース３３８を介してマイコンに入力される。このデータにより、誰がブック原稿をコピーしたかを判断することができる。

【０３６４】バーコード読み取り装置３４１は、書籍や雑誌等のブック原稿に貼付または印刷されたバーコードパターンによって、ブック原稿の種類を識別するためのブック原稿識別装置である。

【０３６５】本実施例では、このブック原稿識別装置としてバーコード読み取り装置３４１を示したが、ブック

52

原稿に貼付した磁気パターンを識別する装置であってもよい。

【０３６６】このバーコード読み取り装置３４１は、バーコードスキャナとバーコードデータとからなっている。本例では、バーコードスキャナにＣＣＤを使用したタイプで説明するが、このバーコードスキャナとしては、反射光センサを使用したペンタイプや、レーザスキャンタイプのスキャナであってもよい。

【０３６７】このＣＣＤスキャナにより読み取られたバーコードデータは、そのバーコード信号がＡＳＣＩＩにコードに変換され、シリアル通信でメイン制御ボード３１０へ送信されるようになっている。操作表示ボード３１３は、モードの設定や表示、操作手順表示、エラー表示等を行なう。

【０３６８】メモリコントローラ３４２は、ワンチップマイコン３３０からのコマンドより画像処理ボード３１４からの画像データをプリンタへ直接出力するか、画像メモリボード３４３へ出力するかを切り換えたり、画像処理ボード３１４またはプリンタ３００からの主走査、副走査の同期信号およびゲート信号、クロック信号の切り換えを行なう。

【０３６９】また、メモリコントローラ３４２は、画像メモリボード３４３からの出力をコントロールできるように、主走査、副走査の同期信号（ＬＳＹＮＣ）およびゲート信号（ＦＧＡＴＥ）、クロック信号を発生することができる。さらに、メモリコントローラ３４２は、キャラクタージェネレータ３４４をコントロールする。

【０３７０】キャラクタージェネレータ３４４は、文字フォントや図形パターンのデータを内部ＲＯＭに持っていて出力可能になっている。このキャラクタージェネレータ３４４の出力タイミングは、メモリーコントローラ３４２によって指示され、その出力は、ＯＲ回路３４５を経てプリンタ３００に出力される。

【０３７１】ＯＲ回路３４５は、メモリコントローラ３４２から出力される画像データとキャラクタジェネレータ３４４から出力されるパターンデータとを合成することができる。画像メモリボード３４３は、原稿最大読み取りサイズ分のメモリを標準で２ページ分持っている。

【０３７２】また、この画像メモリボード３４３は、１ドット多値化出力の１ドット当りのビット数増分用およびプリンタジャム時のリカバリー用にメモリを増設できるように構成されている。

【０３７３】次に、本発明に関する動作モードについて説明する。前述したように、ＭＦＤＳの動作モードは、大きく２つのモードにわかれており、一方は、ブック原稿のページめくり読み取り動作を行なうブック原稿読み取りモードであり、他方は、シート原稿に対する読み取りを行なうシート原稿読み取りモード（ＡＤＦモードと圧板モード）である（図３８）。

【０３７４】本発明は、ブック原稿読み取りモードのう

Petitioner Apple Inc. - Exhibit 1012, p. 1476

53

ちで、著作権利用料の管理ができるようにＩＤカード認識モードとバーコード認識モードとを設定できるようになっている（図３６）。

【０３７５】ここで、各モードの設定のオン／オフは、使用者が簡単に変更できないようにするために、操作表示ボード３１３からの暗号キー入力によって設定するか、はじめから各モードが組み込まれたプログラムＲＯＭを使用して行なうようにしてもよい。その他の細分化されたモードは、前記の図３７を参照して述べた通りである。

【０３７６】次に、操作部からのキー入力による個々のモードの切り換えと、センサ入力による自動モード切り換えについて説明する。図６０において、ＭＦＤＳのメイン電源をオンすると、図３４で示したメイン制御ボード３１０、操作表示ボード３１３、めくりユニット駆動制御ボード３１２、めくり搬送ベルト駆動制御ボード３１１、各画像処理ボード３１４，３１７がリセットされ、初期設定が行なわれる。

【０３７７】この初期設定では、図３５に示す自動選択モードが設定される。この自動選択モードでは、各センサ入力によってモードを自動的に選択する。その後、プリンタ３００等の出力装置の接続をチェックし、プリンタ等の接続器機に対応可能なモードを表示する一方、置数枚、変倍、ページめくり枚数、モードのキー入力を受け付ける。

【０３７８】ここで、自動選択モードをオフすると、操作表示ボード３１３からキー入力でモード選択を設定できる。すなわち、操作表示ボード３１３のモード選択キーによりモードが指定されると、この操作表示ボード３１３からのシリアル通信により、モード選択コードが送信され、これによりモード選択フラグがセットされる。

【０３７９】そして、このモード選択フラグチェックにより各モードへの分岐（サブルーチンコール）が行なわれる。一方、自動選択モードのオン時には、ブック原稿またはシート原稿のセットにより、各センサ入力および設定条件によって、次に示すようにモードが分岐される。

【０３８０】シート原稿がシート原稿トレイ９４に置かれると、シート原稿センサ２５がオンされる。また、搬送部１９を開いて原稿台１８の中央位置基準決め部２４に、ブック原稿が見開いた状態でセットされると、ブック原稿センサ２７がオンされる。この２つのセンサ２５，２７により、図６０に示すようにモードが切り替わる。

【０３８１】すなわち、ブック原稿センサ２７がオフ、シート原稿センサ２５がオンで、置数枚が１枚の場合はシート原稿スルーモード（ＡＤＦモード）へ、置数枚が２枚以上の場合はシート原稿スキャンモード（ＡＤＦモード）へ、各センサ２５，２７が共にオフの場合はシート原稿手動開閉モード（圧板モード）へ、それぞれ切り

54

替わる。

【０３８２】また、ブック原稿センサ２７がオンで、シート原稿センサ２５がオフの場合はブック原稿読み取りモードへ、各センサ２５，２７が共にオンの場合は以上処理１を実行して、警告ブザーとエラー表示を行なってユーザに注意を促した後、ブック原稿読み取りモードへ遷移する。

【０３８３】ここで、ブック原稿読み取りモードは、著作権利用管理ができるモードであるのに対し、シート原稿読み取りモード（ＡＤＦモードと圧板モード）は、通常複写動作ができるようになっている。

【０３８４】すなわち、ブック原稿モードと圧板モードのみ（ＡＤＦモード無）の場合には、中央位置決め部２４のブック原稿センサ２７の状態を見てモードの判断がなされ、（１）ブック原稿センサ２７がオンでブック原稿モードの場合には、ブック原稿の画像の読み取りを行なう画像読み取りセンサユニット９の画像読み取り走査回数、または、この読み取りセンサユニット９によって読み取られた画像情報を出力するメモリコントローラ３４２の上記画像情報出力回数が、カウント手段によりカウントが実行され、（２）ブック原稿センサ２７がオフで圧板モードの場合には、上記のカウント手段による画像読み取りセンサユニット９の画像読み取り走査回数、または、メモリコントローラ３４２の上記画像情報出力回数のカウントが不実行となる。

【０３８５】また、それぞれモードサブルーチンへ入った後は、読み取りスタートキーが押されていなければ、処理を実行せずにリターンするようになっている。

【０３８６】それぞれのモード動作は、前述した通りである。

【０３８７】次に、本発明に関する、ブック原稿読み取りモードについて、図６１乃至図６３のフローチャートを用いて説明する。図６１乃至図６３において、ブック原稿読み取りモードに入ると、ベルトテンションセンサ３４のオン／オフのチェックを行なう。

【０３８８】これは、載置されるブック原稿が厚すぎて、めくり読み取りユニット１が原稿面をスキャンできないレベルを検知している。このベルトテンションセンサ３４がオンすると、異常処理２が実行され、ユーザが無理に搬送部１９を閉じて装置を破損することのないように、警告ブザーがオンするとともに、”本が厚すぎます”のエラー表示が行なわれる。

【０３８９】ここで、ブック原稿の厚さが適応レベル以下なら、ユーザにより搬送部１９が閉じられて、搬送部ロックセンサ３１がオンする。このとき、搬送部１９が開いたままであれば、異常処理３が実行され、警告ブザーがオンするとともに、”搬送部を閉じてください”のエラー表示が行なわれる。

【０３９０】このようにして搬送部１９が閉じられると、ブックサイズ上限検知センサ３３のオン／オフのチ

Petitioner Apple Inc. - Exhibit 1012, p. 1477

55

ェックを行ない、このセンサがオンの場合には、本のサイズが読み取り領域以上となるため、異常処理4が実行され、警告ブザーがオンするとともに、”本のサイズが多きすぎます”のエラー表示が行なわれる。

【0391】そして、ここで、ブックサイズ上限検知センサ33がオフの場合は、置数枚、変倍、めくり枚数がセット済みであることを判断し、さらに、IDカード認識モードであることを判断して、サブルーチンがコールされる。

【0392】IDカード認識モードは、図64に示すフローチャートに示すように動作される。このIDカード認識モードが実行されると、図64に示すように、先ず、IDカード読み取り装置340が接続されているか否かが、シリアルインターフェース338（図59）を介して、ブレーク信号通のやり取りでチェックされる。

【0393】ここで、IDカード読み取り装置340が接続されていない場合には、シリアルインターフェース337を介して、操作表示ボード313へ接続方法の指示表示を行なうようにコマンドを送信し、NGフラグをセットして、ブック原稿読み取りモードへリターンする。

【0394】一方、IDカード読み取り装置340が接続されている場合には、操作表示ボード313へIDカード読み取り装置340の操作方法の表示を行なうようにコマンドを送信する。

【0395】次に、IDカードより個別コードが読み取られたかどうかのシリアル通信上でのコマンドのやり取りを行なう。その結果、個別コードの読み取りがまだ行なわれていない場合には、NGフラグをセットしてリターンする。ここで、個別コードの読み取りが行なわれていると判定された場合には、そのIDコードがブック原稿の複写を許可しているか否かの判断を行なう。そして、IDコードがブック原稿の複写を許可していない場合には、”ブック原稿の複写が許可されていません”等のエラー表示を行なうように、操作表示ボード313へコマンドを送信する。

【0396】一方、IDコードがブック原稿複写を許可済の場合には、このIDコード別に設定されている外部RAM332上のカウンタのアドレスをセレクトして、分岐もとルーチンへリターンする。この外部RAM332上のカウンタは、IDコード別にブック原稿の複写枚数をカウントする機能を有している。

【0397】上述したIDカード認識モードのリターン終了後は、NGフラグのセット・リセットを判断する。ここで、NGフラグがセットされている場合には、NGフラグをリセット後、ブック原稿読み取りモードをリターンして終了する。

【0398】一方、NGフラグがセットされていなければ、バーコード認識モードかを判断して、そのサブルーチンをコールする。このとき、バーコード認識モードで

56

なければ、次のモードへ進む。

【0399】〔請求項1に対応する説明〕図65に、上記のバーコード認識モードのフローチャートを示す。

【0400】このサブルーチンでは、先ず、バーコード読み取り装置341の接続チェックを行なう。

【0401】ここで、バーコード読み取り装置341が接続されていない場合には、操作表示ボード313へエラー表示をするコマンドを送信し、NGフラグをセットしてリターンする。

【0402】一方、ここで、異常がなければ、バーコードスキャナ内部のLEDを点灯させ、同じくバーコードスキャナ内部のCCDにより、ブック原稿に貼付または印刷されたバーコードの読み取りを行なう。

【0403】このバーコードスキャナの読み取り位置は、ブック原稿セット基準位置近辺に設定することにより、ブック原稿のサイズに左右されずに、図66に示すようなブック原稿の背表紙部のバーコードパターン341cを読み取ることができる。そこで、本発明の実施例では、図67および図68に示すように、ブック原稿92の中央綴じ部（背表紙部）を支持する原稿台18の中央基準位置決め部24のブック原稿セット基準位置側に、バーコード読み取り装置341のバーコードスキャナ341aが取付けられている。

【0404】この実施例以外のバーコードスキャナ341aの取り付け位置としては、読み取りめくり可能な最小ブック原稿サイズ以内の、ブック原稿の表紙または裏表紙の原稿セット基準位置の近傍でもよい。なお、図68に示すページめくり読み取りユニット1は、めくりローラ2によってめくられた原稿ページを収納するためのページ収納部7と、原稿ページを世に取るための読み取りセンサユニット9とをブック原稿92の載置面に沿うように、原稿読み取り走査方向に並列に配置した例を示している。

【0405】バーコードスキャナ341aによって読み取られたバーコードパターン341cのデータは、バーコード読み取り装置341内のバーコードデコーダ341bに送られ、ASCIIコードに変換されて、メイン制御ボード310のシリアルインターフェース339を介してワンチップマイコン330に送られる。

【0406】ここで、バーコードパターン341cが読み取れない場合には、”バーコードパターンが読み取れません”のエラー表示をし、NGフラグをセットしてリターンする。また、バーコードパターン341cが読み取れた場合には、このバーコードパターンが複写許可されているかどうかを判断する。そして、複写許可されていない場合は、操作表示ボード313へ”このブック原稿（バーコードパターンは複写（コピー）許可されていません”のエラー表示を行なう。

【0407】一方、複写許可されている場合には、読み取りコード別に設定されている外部RAM332上のカ

Petitioner Apple Inc. - Exhibit 1012, p. 1478

57

ウンタのアドレス値をセレクトしてリターンする。この外部ＲＡＭ３３２上のカウンタは、バーコードパターン別に定められた、すなわち、例えば、出版社別、著作社別、あるいは、価格等によってウエイト付けされたカウンタである。

【０４０８】ブック原稿読み取りモードへリターン後は、ＮＧフラグを判断し、ＮＧフラグがセットされていれば、このＮＧフラグをリセットしてリターンする。また、ＮＧフラグがリセットならば、次の自動ブックサイズ認識モードに移行する。

【０４０９】自動ブックサイズ認識モードの場合には、プレスキャンフラグをセットし、そうでなければ、ブック原稿サイズ入力モードとなり、操作表示ボード３１３よりキー入力を行なって、ブック原稿のサイズを設定し、その読み取り領域を決定する。

【０４１０】ここで、読み取りスタートキーが押されている場合には、前述した搬送部ロック機構が作動する。これは、ブック原稿のページめくり動作中に、ユーザが間違って搬送部１９を開いて原稿ページを破損しないようにするためである。そして、この搬送部ロック機構の作動後に、プレスキャンフラグがセットされていれば、プレスキャン動作を行ない、プレスキャンフラグがセットされていなければ、スキップする。

【０４１１】このプレスキャン動作後、またはスキップ後は、接続機器（プリンタ３００）の準備ができるまで、待機される。そして、準備ができると、ブック原稿の読み取り動作が開始される。この読み取り動作の終了後、ＩＤコード・バーコード別カウント動作処理サブルーチンがコールされる。

【０４１２】このＩＤコード・バーコード別カウント動作処理サブルーチンでは、図６９に示すように、先ず、中央綴じユニットセンサ３４６の状態を判断する。図７０に示すように、中央綴じユニット３４７は、著作権の無いステープルされた原稿等を複写する場合に使用される。

【０４１３】すなわち、この中央綴じユニット３４７は、ステープルされた原稿をクリップ（挟持）した状態で、原稿台１８の中央基準位置決め部２４内にセットできるように、装置本体に対して着脱自在に構成されている。そして、この中央綴じユニット３４７が原稿台１８の中央基準位置決め部２４内にセットされると、その端部に形成された検知片３４７ａによって、中央綴じユニットセンサ３４６がオンされ、原稿台１８上にセットされた原稿がブック原稿でないことが判断される。

【０４１４】この中央綴じユニットセンサ３４６がオンの状態では、前記のカウント動作を必要としないので、直ちにリターンされる。ここで、中央綴じユニットセンサ３４６がオフの時には、先程サブルーチンコールされたＩＤカード認識処理（図６４）、バーコード認識処理（図６５）でコード別にセレクトしたカウンタ値をロー

58

ドしてカウントアップし、さらに、もとのアドレス値にストアする。このときに使用される外部ＲＡＭ３３２は、バッテリーバックアップ用電池３３４によって、電源オフ時にもバックアップされるようになっている。

【０４１５】また、このときのカウントアップは、ブック原稿の読み取りページ数と対応するようにカウントする。すなわち、ブック原稿を２ページずつ読み取れば、２カウントアップずつカウントされる。

【０４１６】なお、上記の中央綴じユニットセンサ３４６には、光透過型センサを使用しているが、例えば、中央綴じユニット３４７の裏側に独自のバーコードパターンを貼付もしくは印刷し、この不正防止とコストダウンを兼ねたバーコードパターンをバーコードスキャナ３４１ａで読み取るようにして、ブック原稿と区別してもよい。

【０４１７】このようにして、上記のカウント値により、ブック原稿別に何ページの複写が実行されたかを判断することができる。そして、上記の読み取り動作を予め設定された置数枚分繰り返して、ページめくり動作を実行し、最終ページのめくり読み取り動作が完了するまでこの動作を繰り返す。これにより、ブック原稿の最終ページのページめくり読み取り動作が実行された後、ブック原稿読み取りモードをリターンして動作を終了する。

【０４１８】一方、前述したＩＤコード別、および、バーコード別にカウントしたデータは、操作部よりキー入力することで、随時、表示部へ出力することが可能となっている。また、このＭＦＤＳにプリンタ３００が接続してある場合には、操作表示ボード３１３からのキー入力により、メイン制御ボード３１０のワンチップマイコン３３０が、外部ＲＡＭ３３２にストアしているカウンタ値をコード別に呼び出して、メモリコントローラ３４２により発生される同期信号で制御されたキャラクタジェネレータ３４４によって、一覧表やグラフ等の画像出力とともに、カウントデータを出力させることが可能となる。

【０４１９】これにより、例えば、ＩＤコードカウンタ値に基づいて、個人、あるいは、団体別に著作権料を正確に徴収することができる。また、操作表示ボード３１３よりキー入力で、予め、１ページ複写時の代金を設定しておくことにより、上記のカウンタ値によって、複写終了時の合計金額を計算することも可能である。

【０４２０】さらに、バーコードパターン３４１ｃにより、ブック原稿別にカウントした値により、原稿１ページ当りの代金を予め入力しておけば、原稿の著作者や出版社別に、その支払金額を期間別に一覧表としてプリンタ３００へ出力することができる。

【０４２１】これらの出力は操作表示ボードのキー入力により随時出力できるが、メイン制御ボード内のマイコンのタイマ機能により定期的に出力をさせてもよい。

Petitioner Apple Inc. - Exhibit 1012, p. 1479

59

週、月極めにより自動出力させてキー入力の手間を省く事ができる。

【0422】ところで、このMFDSに接続されたプリンタ300側で、コピー用紙がジャムした場合には、このプリンタ300側からMFDSのメイン制御ボード310へ、シリアル通信によりジャム発生コードが送信される。

【0423】これによって、MFDS側は、プリンタジャムリカバリー動作を行なう。

【0424】このリカバリー動作の一部に、先のジャム発生コードの送信タイミングにより、図63、および図69で示したように、読み取り動作が終了して、既に、IDコード・バーコードカウント動作済みであるならば、マイナスカウントを行なう。　また、ここで、IDコード・バーコードカウント動作済みでなければ、このときのカウント値をそのまま保持する。

【0425】一方、本実施例では、ブック原稿読み取りモードルーチン内に、IDコード・バーコード別カウント動作処理サブルーチンを組み込んだ例を示したが、プリンタ300から送信されてくる排出OKコード（転写紙がプリンタ300から排出されたときにMFDSへ出力されるコード）を受信したときに、先のサブルーチンコールを実行するように組み込んでもよい。

【0426】このように、プリンタ300から送信されてくる排出OKコード（転写紙がプリンタ300から排出されたときにMFDSへ出力されるコード）を受信したときに、先のサブルーチンコールを実行するように組み込むことによって、ジャム時のマイナスカウントを行なう必要がなくなる。

【0427】ところで、上記実施例は、画像出力がリアルタイム処理される場合の例であるが、例えば、プリンタ300の処理速度が速い場合や、リピート複写の高速化および原稿保護のために、一旦、メモリに画像データを蓄えた後、このメモリから画像データを適時出力するように構成されている場合の実施例を以下に示す。

【0428】上記のように、例えば、図57において、画像メモリボード343にメモリコントローラ342を介してブック原稿の読み取り画像を一旦記憶し、この記憶された画像データをプリンタ300へ逐次出力する場合、MFDSのワンチップマイコン330がメモリコントローラ342に対してFGATE出力を要求する毎に、IDコード・バーコード別カウント動作サブルーチンを実行するように組み込むことにより、メモリリテンション時にも、先のカウント動作を行なうことができる。

【0429】〔請求項7に対応する説明〕また、上記実施例では、ブック原稿の背表紙部のバーコードパターン341cを読み取ることによって、複写の許可・不許可を判断したが、例えば、ブック原稿のページに貼られたり、押されたりしている、印紙、印鑑、シール等を読み

60

取り、そのパターンを認識することによって、そのブック原稿の複写の許可・不許可を判断することもできる。

【0430】このように、ブック原稿の印紙、印鑑、シール等を読み取り、そのパターンを認識することによって、そのブック原稿の複写の許可・不許可を判断する手段としては、画像メモリボード343に、ブック原稿の印紙、印鑑、シール等の読み取りデータをストアし、メモリ上の所定位置（所定アドレス）に複写許可マークがあるか無い可をパターンマッチングにより判断して、メモリからの複写許可あるいはカウント動作のするしないを決定する。

【0431】ここで、メモリボード343を使用しない場合には、プレスキャンにおいて、上記の判断を行なって、ブック原稿の読み取り動作の許可・不許可を決定するようにしてもよい。

【0432】〔請求項8に対応する説明〕ところで、このMFDSでは、読み取った画像情報をプリンタ300へ出力する場合、キャラクタジェネレータ344により、文字やマーク（読み取ったIDコードやバーコードパターン）等の付加情報をOR回路345によって、ブック原稿の読み取り画像データとともに、合成して出力することができる。これにより、著作権のあるブック原稿から複写したか否かが明らかとなり、誤った複写による著作権の更なる侵害を防止することができる。

【0433】例えば、著作権のあるブック原稿をじかに複写した場合には、このシステムによりその著作権料の徴収が可能となるが、このブック原稿のコピーを原本として複写した場合には、著作権料を算出するためのカウントができなくなる。

【0434】そこで、著作権のあるオリジナル原稿の複写時には、そのコピー画像として、読み取り画像データと複写禁止マークやコードとを予め合成して出力することによって、このようなブック原稿のコピーを原本とする複写時にも著作権料の徴収が可能となる。

【0435】また、本実施例では、IDカード認識手段により、ブック原稿の読み取りの許可・不許可を決定しているが、例えば、操作部からのパスワードや、暗証番号などのキー入力によって、読み取り動作の許可・不許可を決定してもよい。

【0436】さらに、ブック原稿の読み取りの許可・不許可や著作権料の徴収に際して、このMFDSにプリペイドカードの読み取り装置を接続することにより、ブック原稿の読み取り処理時に、著作権料を前払したプリペイドカードのポイントをダウンさせることによって、著作権料を徴収するようにしてもよい。

【0437】

【発明の効果】本発明によれば、許可された特定のブック原稿から、或いは、特定ユーザーによる画像読み取り（複写）のみを可能とすることにより、著作権問題への対処を図り得る画像読み取り装置を提供することができ

Petitioner Apple Inc. - Exhibit 1012, p. 1480

61

る。

【図面の簡単な説明】

【図１】本発明の実施に適するマルチ・ファンクション・ドキュメント・スキャナ（ＭＦＤＳ）の概略断面図である。

【図２】前記ＭＦＤＳの駆動系の概略横断面図である。

【図３】前記ＭＦＤＳの駆動系の概略平面図である。

【図４】前記ＭＦＤＳにおけるページめくり読取ユニットの端部の斜視図である。

【図５】前記ページめくり読取ユニットを構成するローラの支持構造を示すローラ端部の断面図である。

【図６】前記ＭＦＤＳにおける搬送部ロック装置のロック解除態様を示す側面図である。

【図７】前記搬送部ロック装置のロック開始作動態様を示す側面図である。

【図８】前記搬送部ロック装置のロック完了態様を示す側面図である。

【図９】前記ＭＦＤＳが搭載されたプリンタの外観を示す斜視図である。

【図１０】前記ＭＦＤＳが搭載されたプリンタの搬送部開放時の外観を示す斜視図である。

【図１１】前記ページめくり読取ユニット内に配設された第１読み取りセンサユニットの端部付近の斜視図である。

【図１２】前記第１読み取りセンサユニットの端部付近の側面図である。

【図１３】前記第１読み取りセンサユニットの端部の支持構造を示す部分拡大断面図である。

【図１４】前記ページめくり読取ユニットのめくりローラ２の奥側の側面図である。

【図１５】前記ＭＦＤＳにおける原稿載置面の中央基準位置決め部の構造を示す断面図である。

【図１６】前記ＭＦＤＳにおける操作表示ボードの平面図である。

【図１７】前記プリンタの概略断面図である。

【図１８】前記プリンタの書込部の平面図である。

【図１９】前記プリンタの転写紙搬送経路を切り換える切換爪の作動態様図である。

【図２０】前記ページめくり読取ユニットの概略断面図である。

【図２１】前記第１読み取りセンサユニットの構成を示す断面図である。

【図２２】前記ＭＦＤＳの作動態様を示す概略断面図である。

【図２３】前記ＭＦＤＳにおけるめくり搬送ベルトの説明図である。

【図２４】前記めくり搬送ベルトのページめくり動作を示す部分斜視図である。

【図２５】前記めくり搬送ベルトの搬送力のピッチ特性を示す線図である。

62

【図２６】前記めくり搬送ベルトの吸着力のピッチ特性を示す線図である。

【図２７】前記めくり搬送ベルトの搬送力の印加電圧特性を示す線図である。

【図２８】前記めくり搬送ベルトの吸着力の印加電圧特性を示す線図である。

【図２９】前記めくり搬送ベルトに不平等電荷を付与する他の手段の部分斜視図である。

【図３０】前記めくり搬送ベルトに不平等電荷を付与するさらに他の手段の部分斜視図である。

【図３１】前記めくり搬送ベルトに不平等電荷を付与するさらに他の手段の部分斜視図である。

【図３２】前記めくり搬送ベルトに不平等電荷を付与するさらに他の手段の部分斜視図である。

【図３３】前記めくり搬送ベルトに不平等電荷を付与するさらに他の手段の部分斜視図である。

【図３４】前記ＭＦＤＳの電装ブロック図である。

【図３５】前記ＭＦＤＳの著作権管理支援システムの動作モードの遷移図である。

【図３６】前記ＭＦＤＳの著作権管理支援システムの動作モードの遷移図である。

【図３７】前記ＭＦＤＳの著作権管理支援システムの動作モードの遷移図である。

【図３８】前記ＭＦＤＳの著作権管理支援システムの動作モードの遷移図である。

【図３９】前記各モードの切り換え動作を示すフローチャートである。

【図４０】前記ブック原稿読み取りモードの動作を示すフローチャートである。

【図４１】ブック原稿読み取りモードにおける見開き２ページ連続読み取りモードの動作を示すタイミングチャートである。

【図４２】ブック原稿読み取りモードにおける見開き１ページ区切り読み取りモードの動作を示すタイミングチャートである。

【図４３】前記見開き１ページ区切り読み取りモードにおいてブック原稿の右ページから読み取るようにセットした場合の動作を示すタイミングチャートである。

【図４４】前記見開き１ページ区切り読み取りモードにおいて読み取られたデータの転送タイミングを遅延させる回路のブロック図である。

【図４５】前記見開き１ページ区切り読み取りモードにおいて読み取られたデータの転送タイミングを遅延させる回路の動作を示すタイミングチャートである。

【図４６】前記見開き１ページ区切り読み取りモードにおける両面モードの動作を示すタイミングチャートである。

【図４７】前記シート原稿読み取りモードにおけるシート原稿スルーモードの切り換え動作を示すフローチャートである。

Petitioner Apple Inc. - Exhibit 1012, p. 1481

63

【図４８】前記シート原稿スルーモードにおける片面読み取りモードの動作を示すフローチャートである。

【図４９】前記片面読み取りモードの動作を示すタイミングチャートである。

【図５０】前記シート原稿スルーモードにおける同一位置読み取りモードの動作を示すフローチャートである。

【図５１】前記同一位置読み取りモードの動作を示すタイミングチャートである。

【図５２】前記シート原稿スルーモードにおける別位置読み取りモードの動作を示すフローチャートである。

【図５３】前記別位置読み取りモードの動作を示すタイミングチャートである。

【図５４】前記シート原稿読み取りモードにおけるシート原稿スキャンモードの動作を示すフローチャートである。

【図５５】前記シート原稿スキャンモードの動作を示すタイミングチャートである。

【図５６】前記シート原稿読み取りモードにおけるシート原稿手動開閉モードの動作を示すフローチャートである。

【図５７】前記シート原稿手動開閉モードの動作を示すタイミングチャートである。

【図５８】前記ページめくり読取ユニットの走査制御回路図である。

【図５９】前記ＭＦＤＳの著作権管理支援システムに関するブロック図である。

【図６０】前記著作権管理支援システムの動作モードの設定動作を示すフローチャートである。

【図６１】前記著作権管理支援システムのブック原稿読み取りモードのフローチャートである。

64

【図６２】前記著作権管理支援システムのブック原稿読み取りモードのフローチャートである。

【図６３】前記著作権管理支援システムのブック原稿読み取りモードのフローチャートである。

【図６４】前記著作権管理支援システムのＩＤカード認識モードのフローチャートである。

【図６５】前記著作権管理支援システムのバーコード認識モードのフローチャートである。

【図６６】前記ＭＦＤＳによって読み取られるブック原稿の斜視図である。

【図６７】本発明にかかる画像読み取り装置におけるバーコード読み取り装置を説明した概略斜視図である。

【図６８】本発明にかかる他の画像読み取り装置におけるバーコード読み取り装置を説明するための概略断面図である。

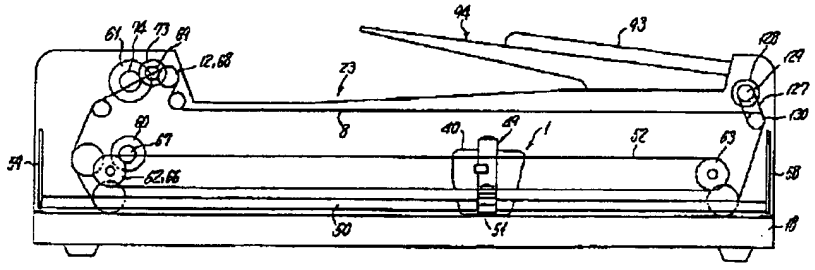
【図６９】前記著作権管理支援システムのＩＤコード・バーコード別カウント動作処理モードのフローチャートでである。

【図７０】本発明にかかる画像読み取り装置にセットされる中央綴じユニットを説明するための概略斜視図である。

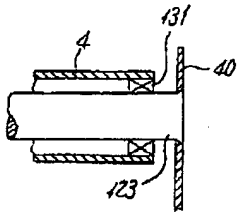
【符号の説明】

１	（読取手段としての）ページめくり読取ユニット
１ａ	（識別符号検知手段としての）バーコードスキャナ
１８	原稿台
９２	ブック原稿
３３０	（制御手段としての）ワンチップマイコン
３４１Ｃ	（識別符号としての）バーコードパターン

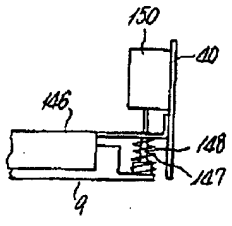
【図２】



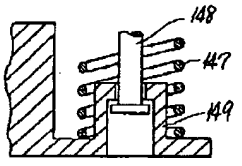
【図５】



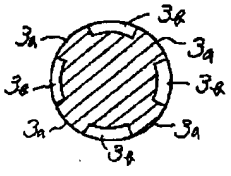
【図１２】



【図１３】

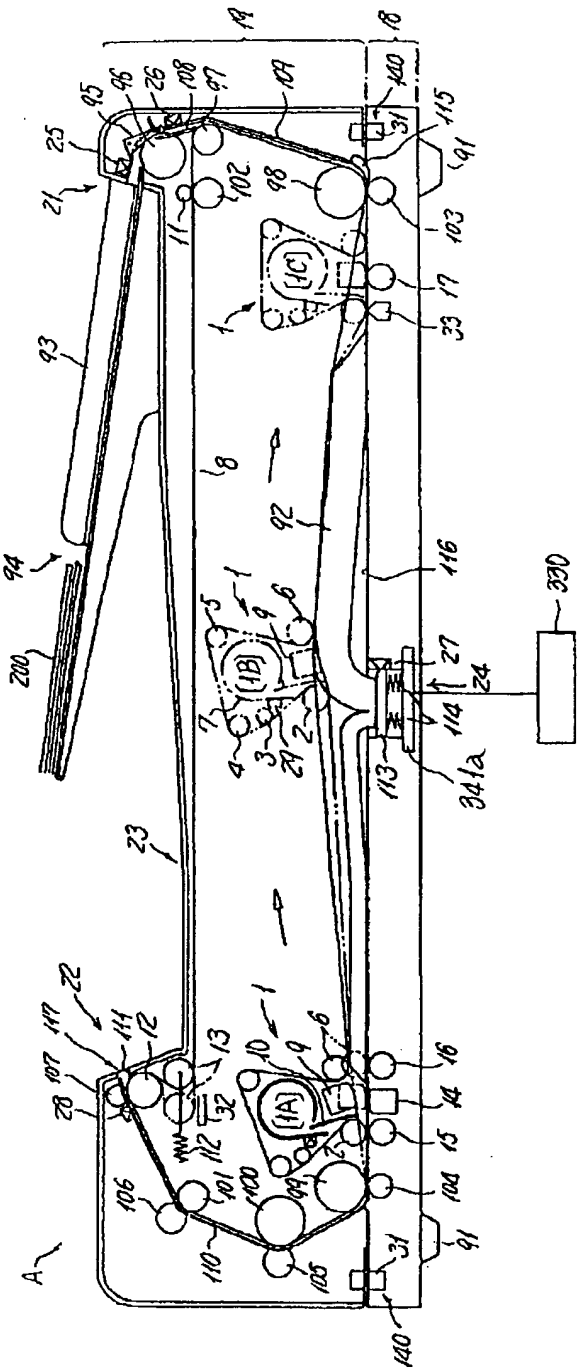


【図３０】

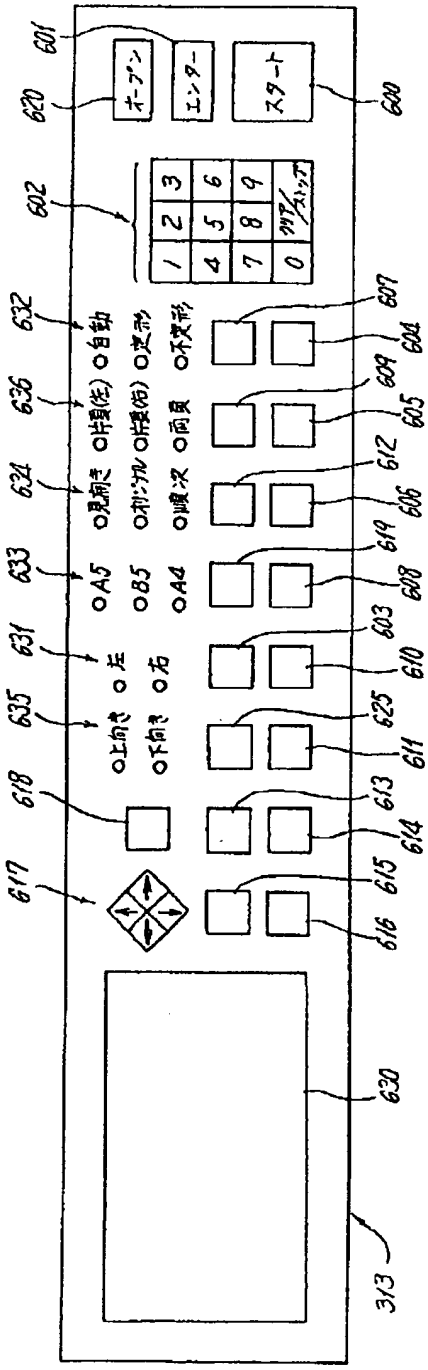


Petitioner Apple Inc. - Exhibit 1012, p. 1482

【図1】

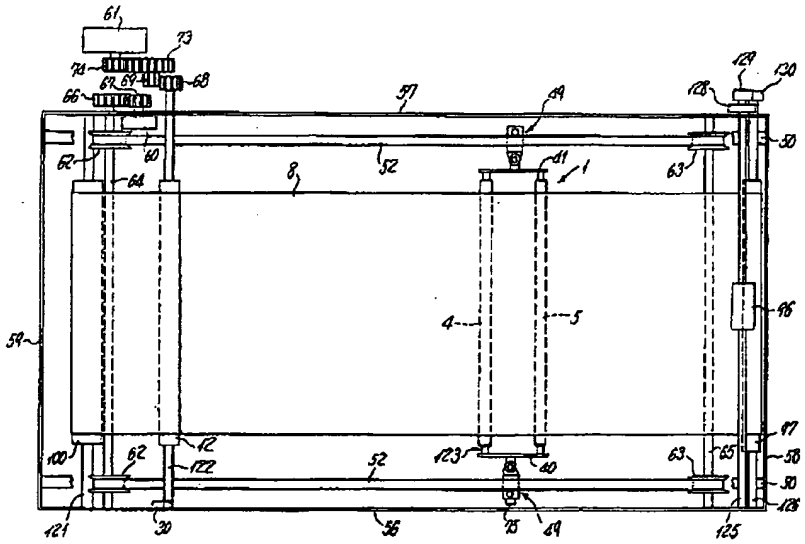


【図16】

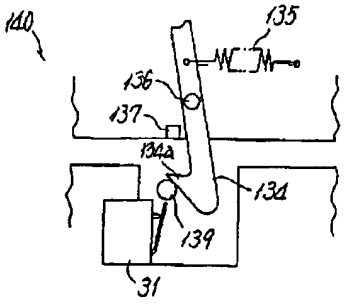


Petitioner Apple Inc. - Exhibit 1012, p. 1483

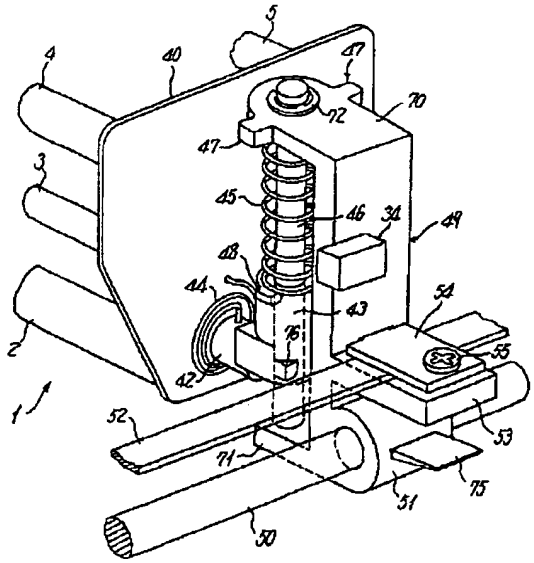
【図3】



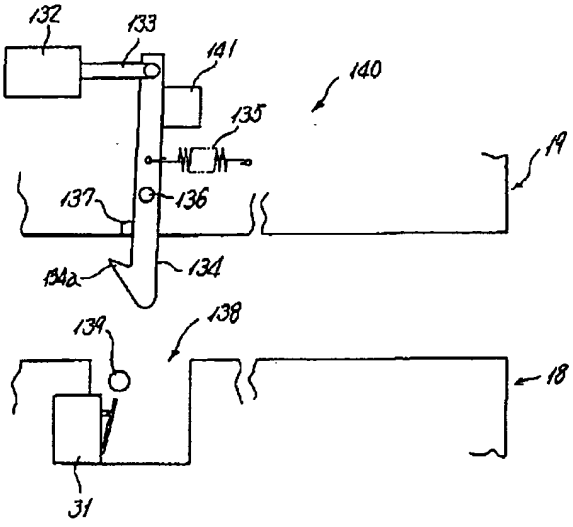
【図7】



【図4】



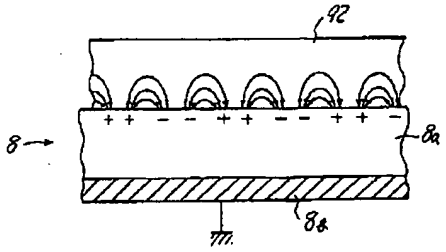
【図6】

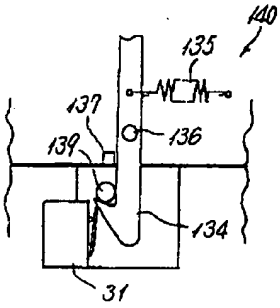


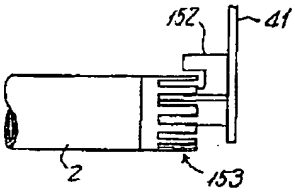
【図8】

【図14】

【図23】

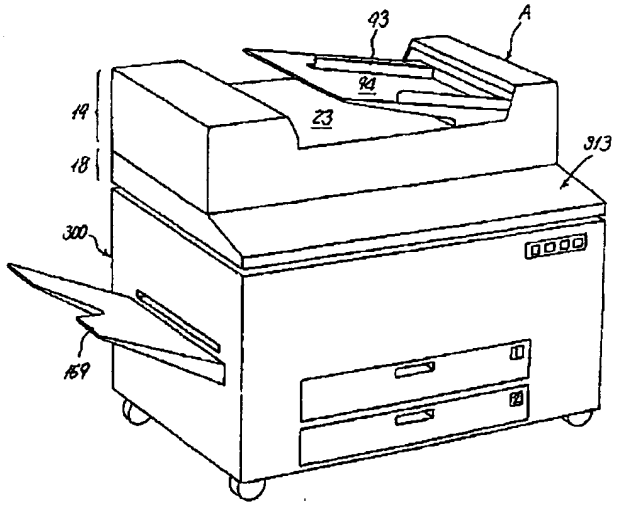




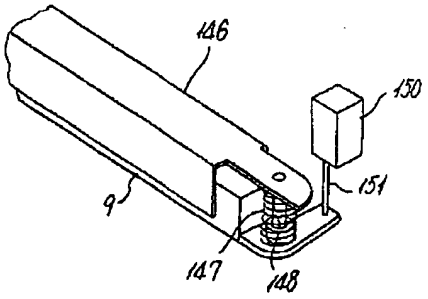


Petitioner Apple Inc. - Exhibit 1012, p. 1484

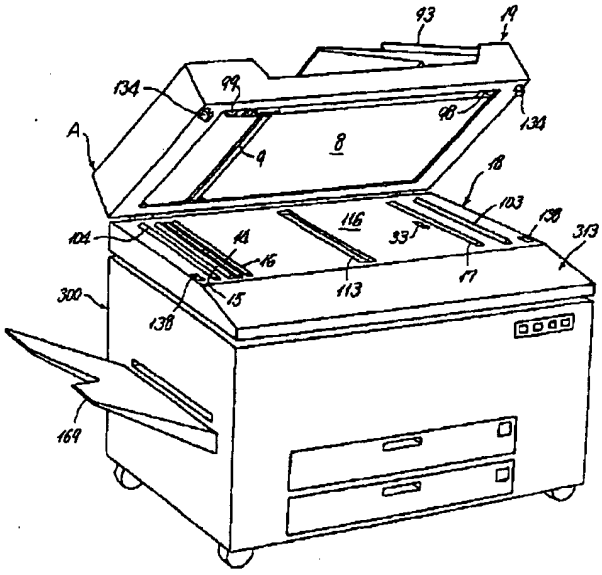
【図9】



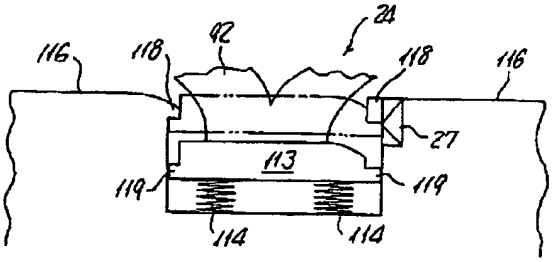
【図11】



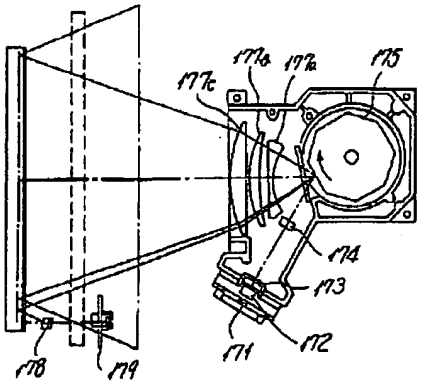
【図10】



【図15】

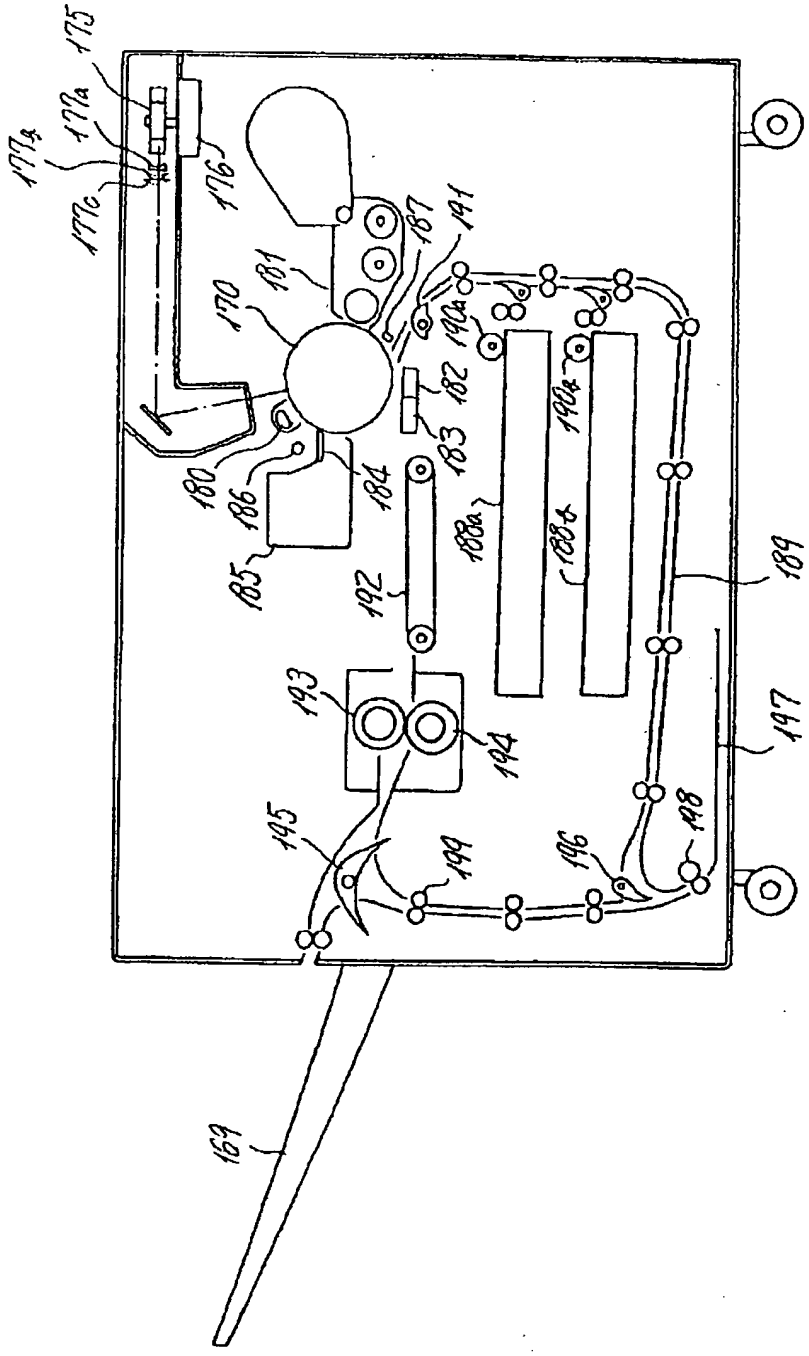


【図18】



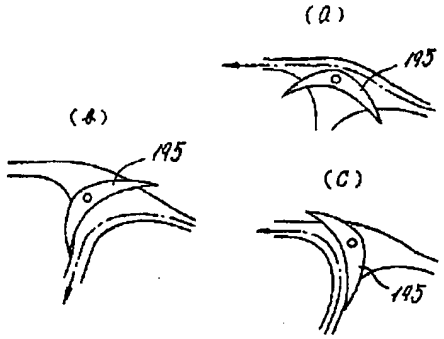
Petitioner Apple Inc. - Exhibit 1012, p. 1485

【図１７】

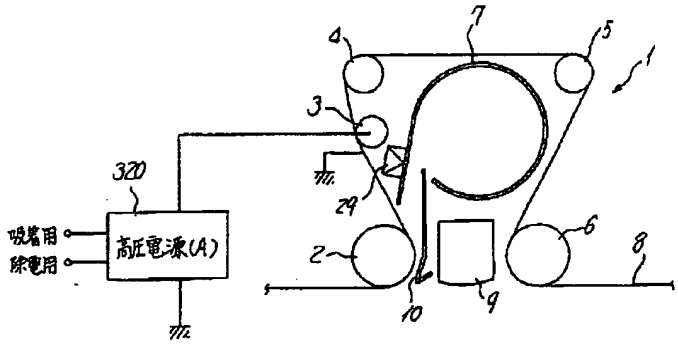


Petitioner Apple Inc. - Exhibit 1012, p. 1486

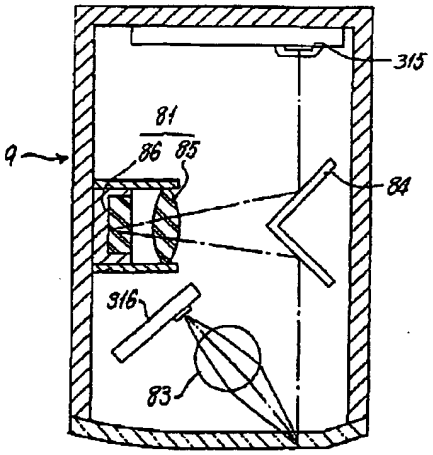
【図19】



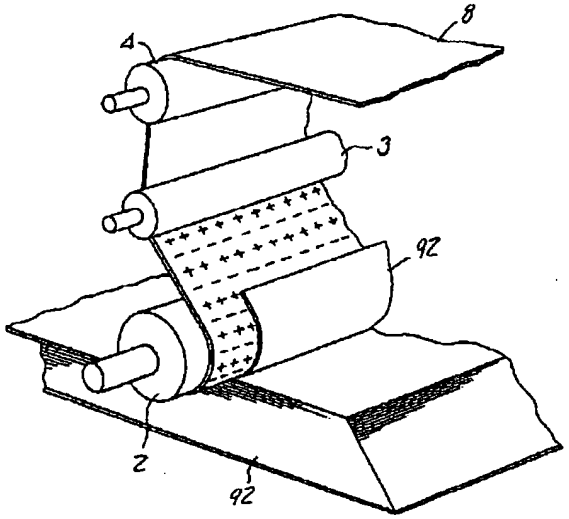
【図20】



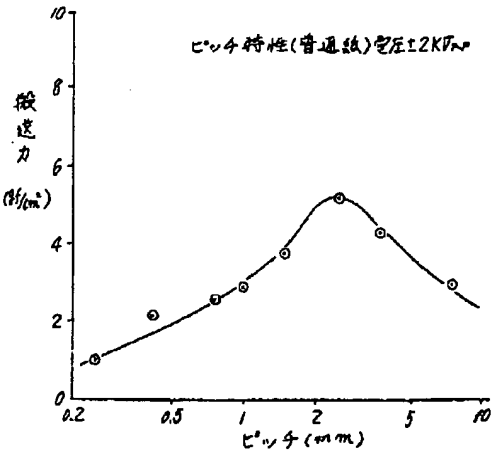
【図21】



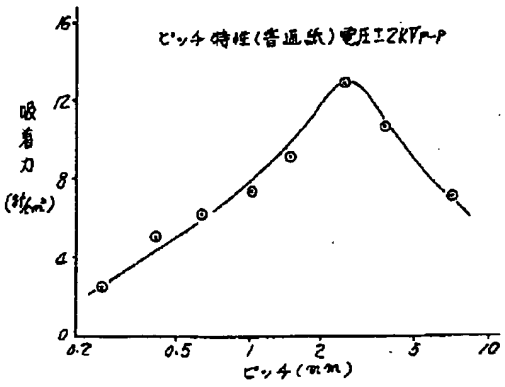
【図24】



【図25】

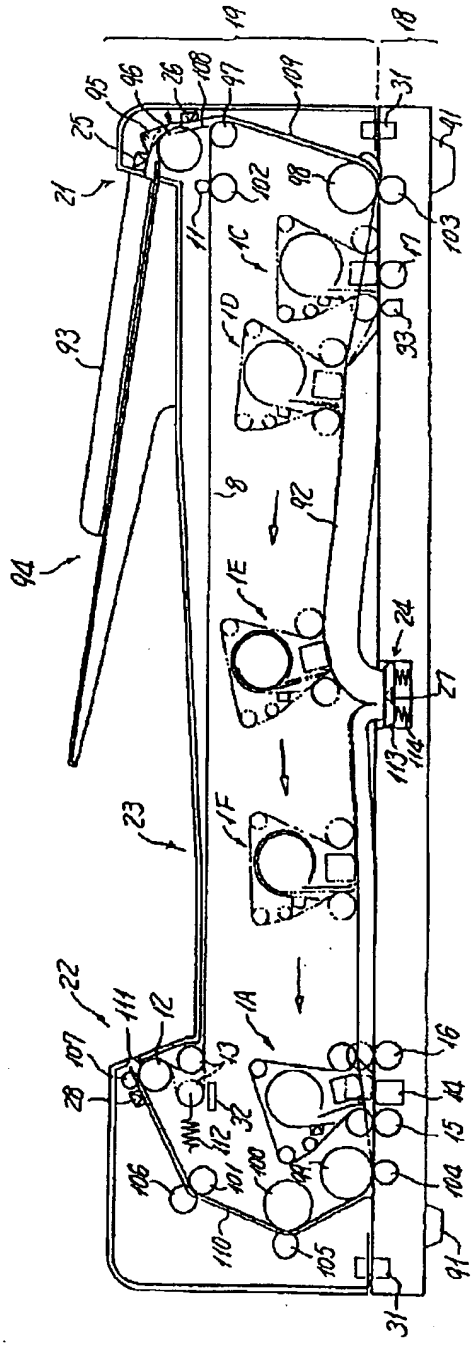


【図26】



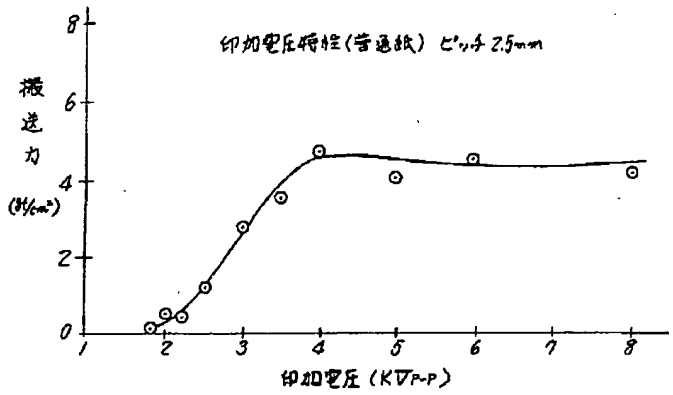
Petitioner Apple Inc. - Exhibit 1012, p. 1487

【図２２】

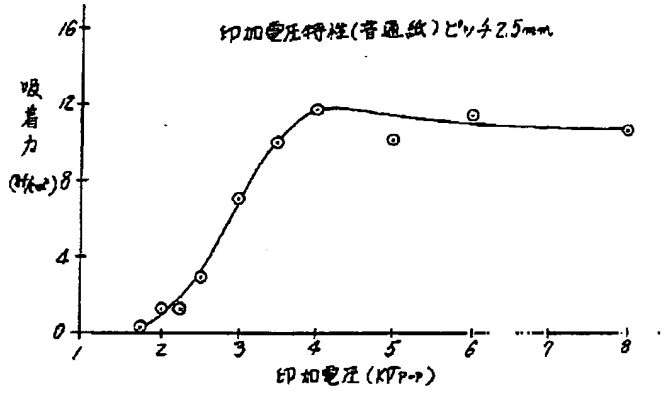


Petitioner Apple Inc. - Exhibit 1012, p. 1488

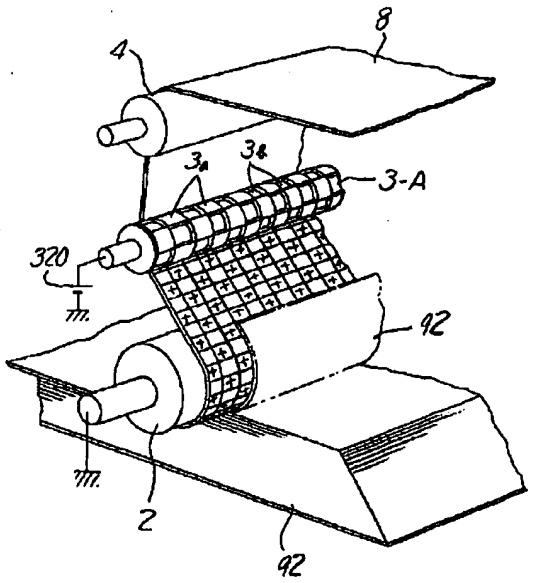
【図27】



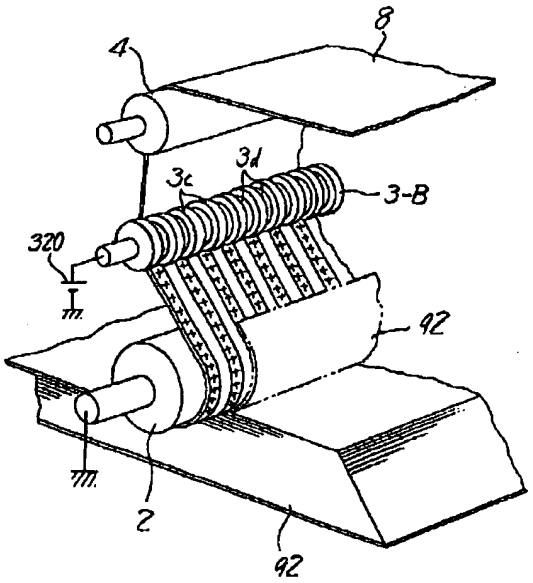
【図28】



【図29】

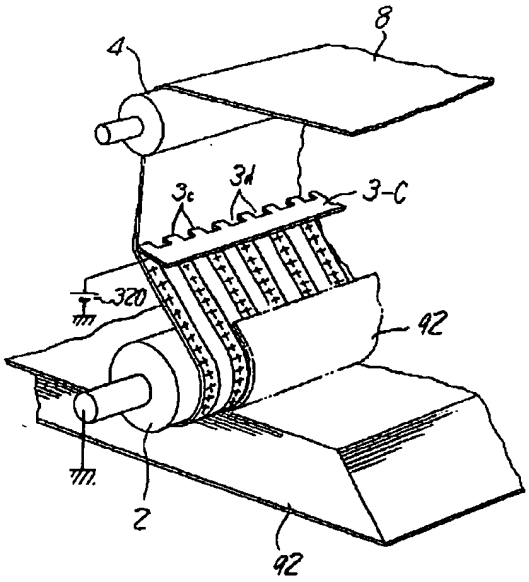


【図31】

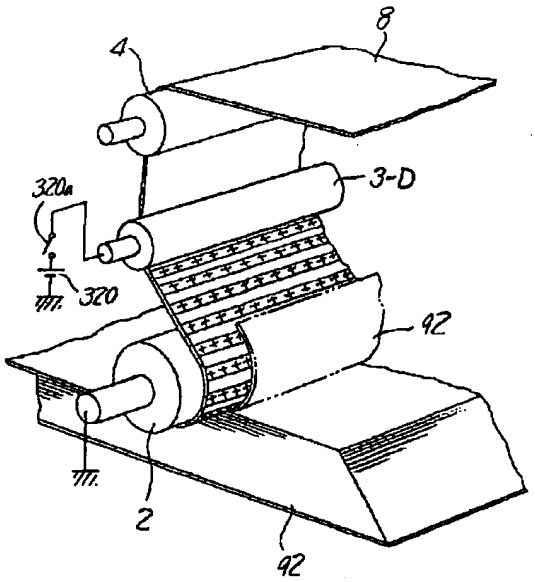


Petitioner Apple Inc. - Exhibit 1012, p. 1489

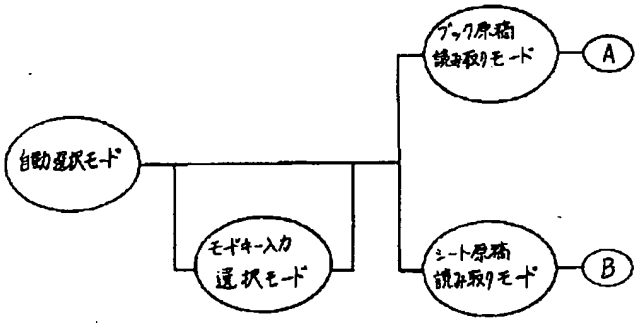
【図３２】



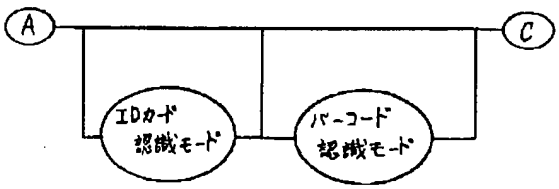
【図３３】



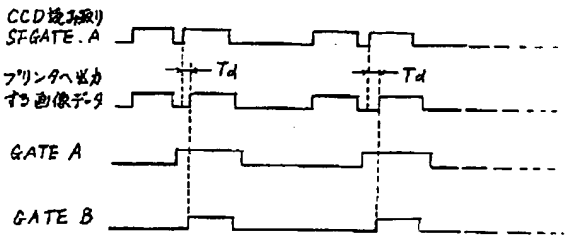
【図３５】



【図３６】

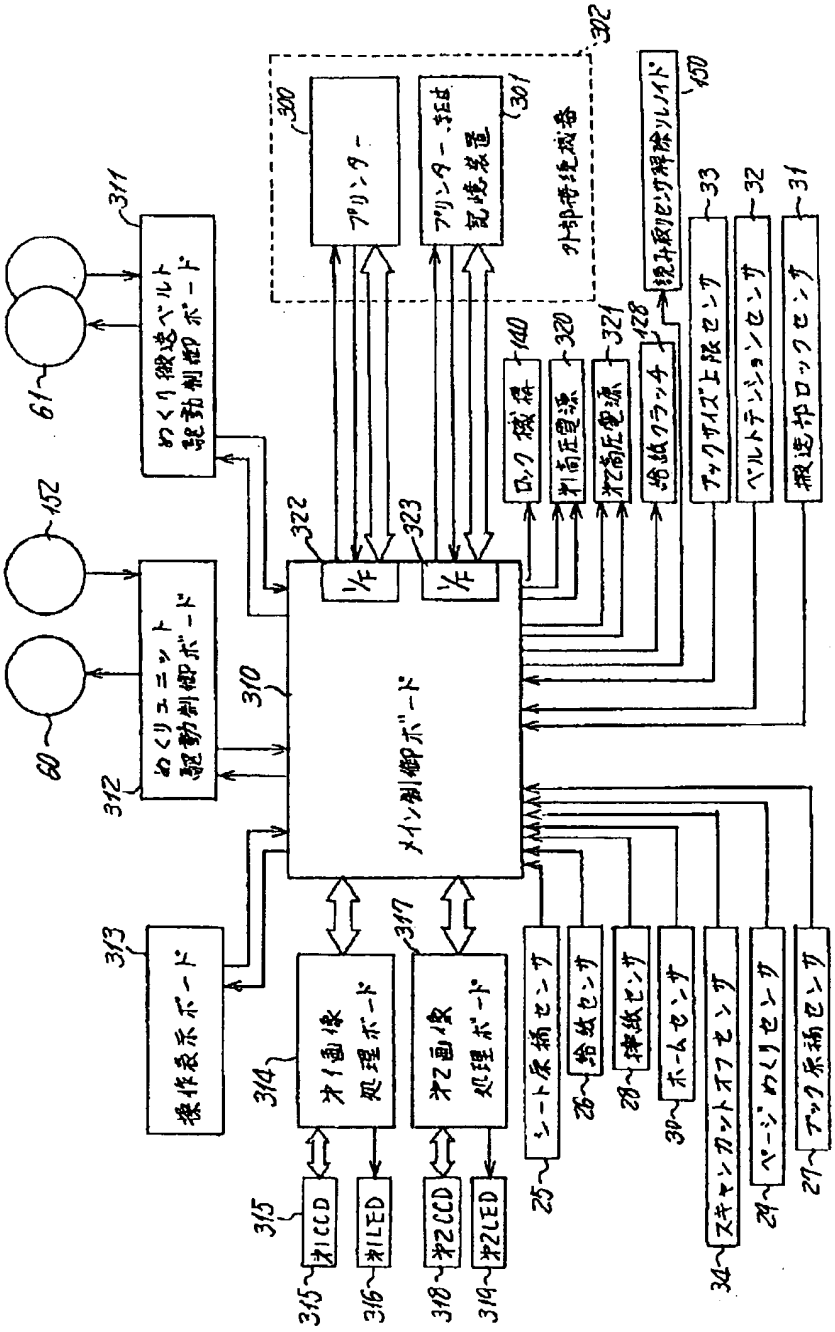


【図４５】



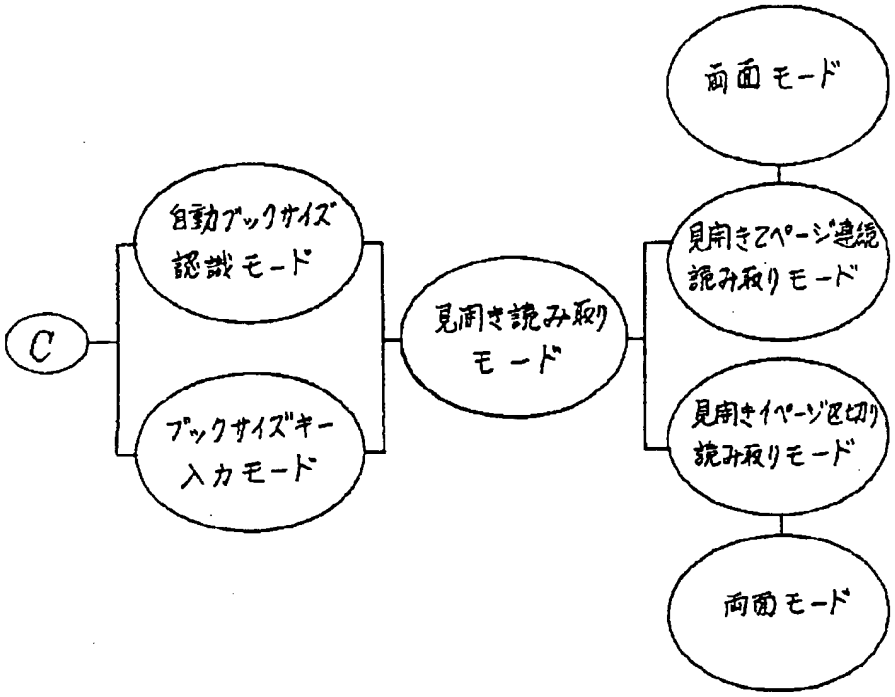
Petitioner Apple Inc. - Exhibit 1012, p. 1490

【図34】

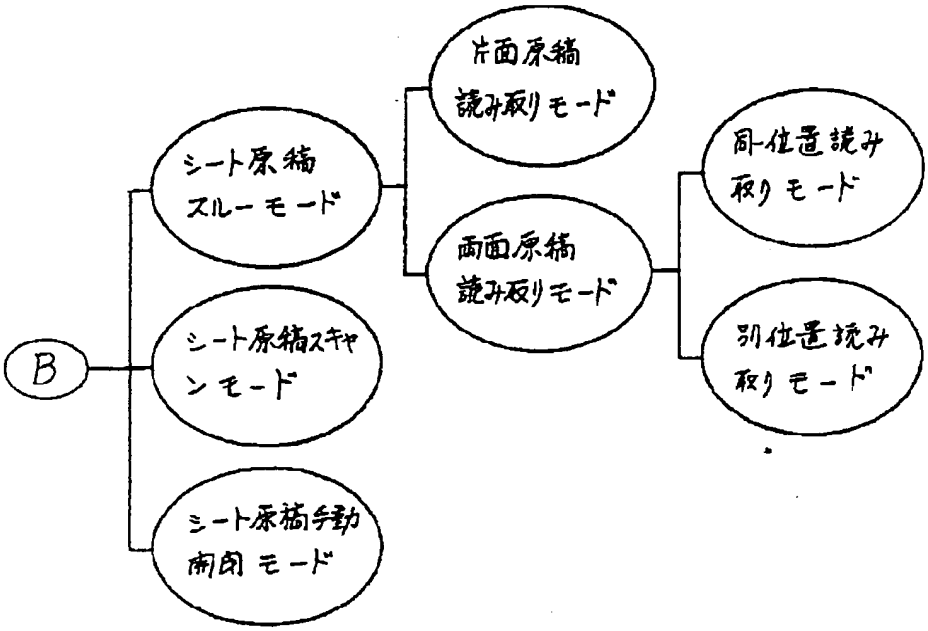


Petitioner Apple Inc. - Exhibit 1012, p. 1491

【図３７】

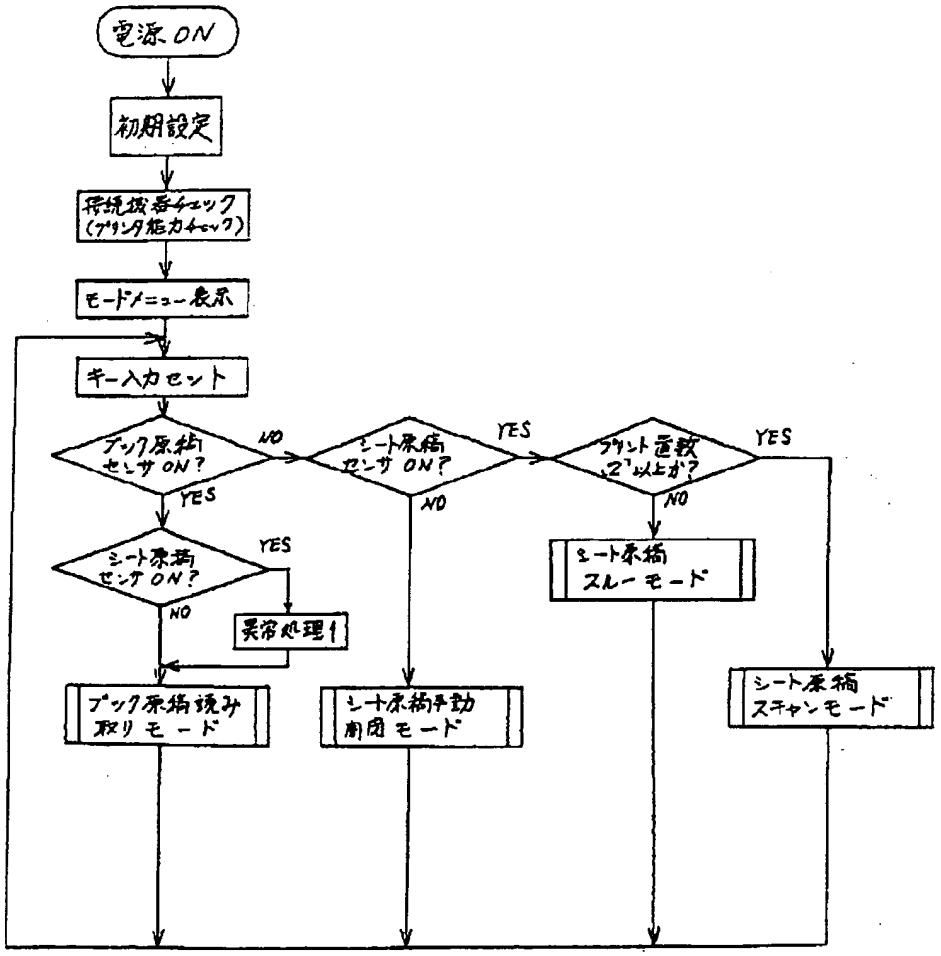


【図３８】

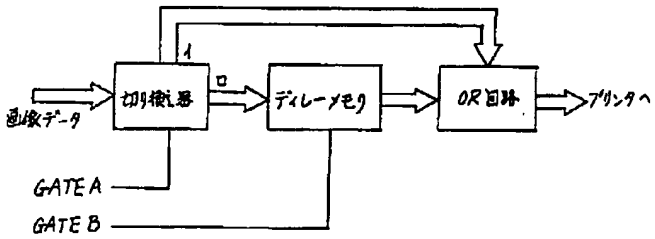


Petitioner Apple Inc. - Exhibit 1012, p. 1492

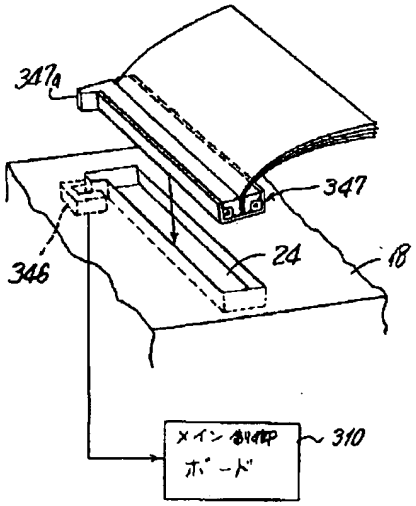
【図３９】



【図４４】

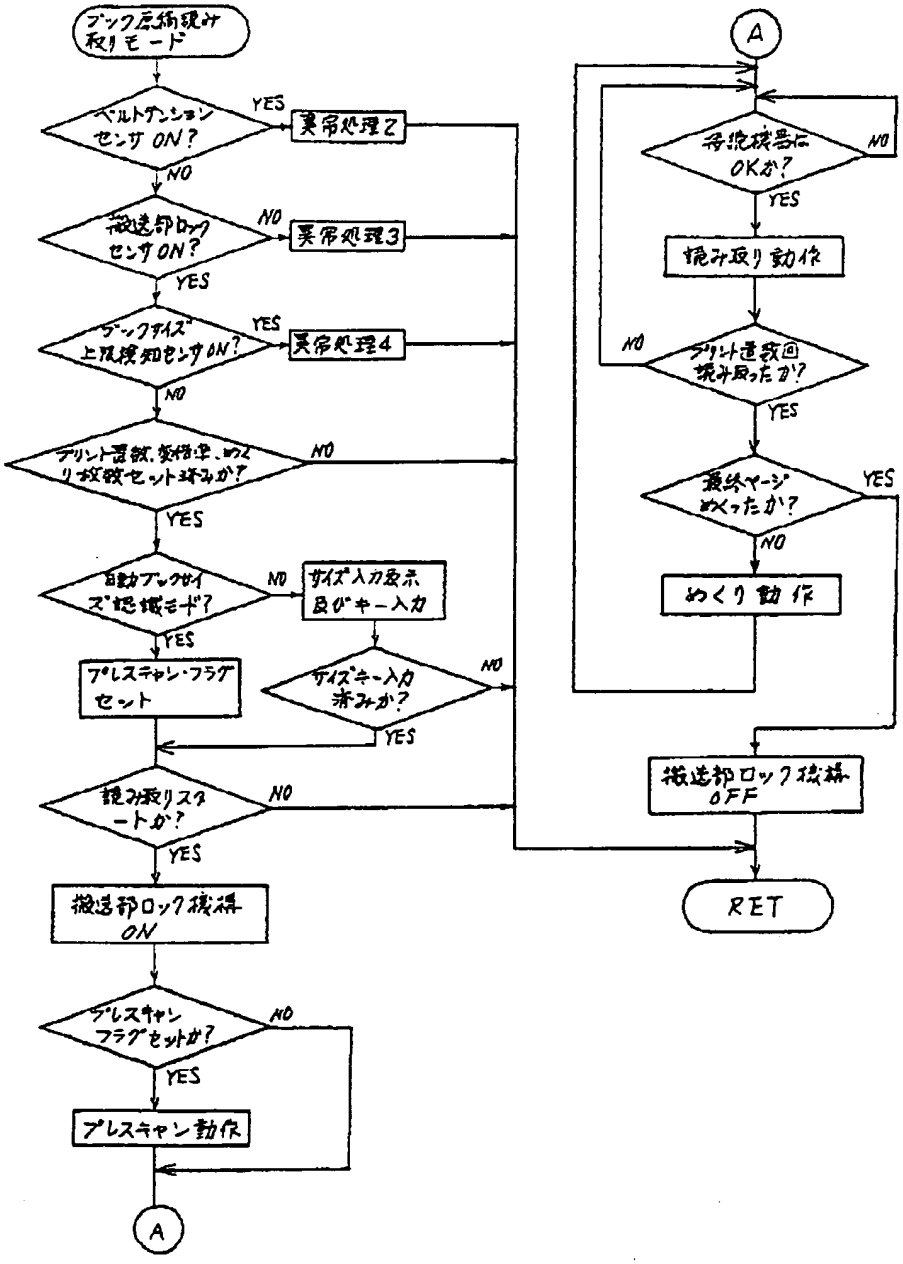


【図７０】



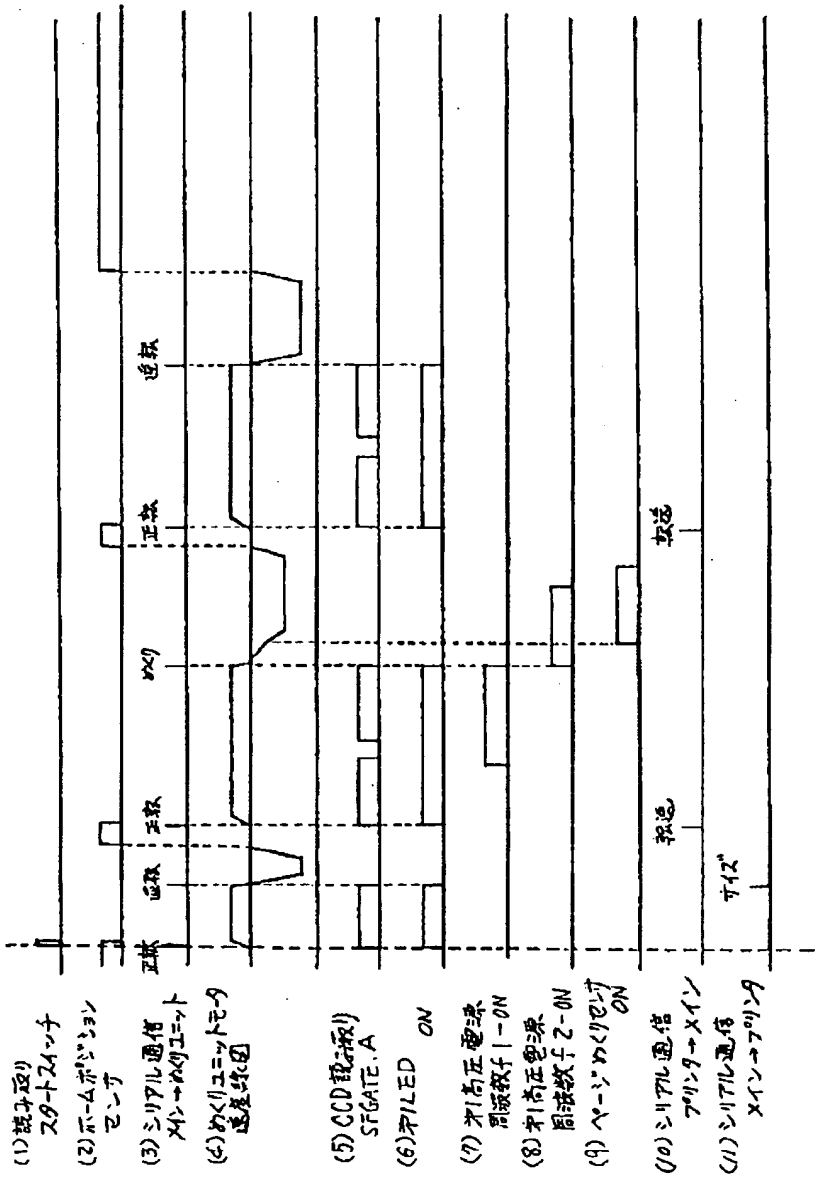
Petitioner Apple Inc. - Exhibit 1012, p. 1493

【図40】



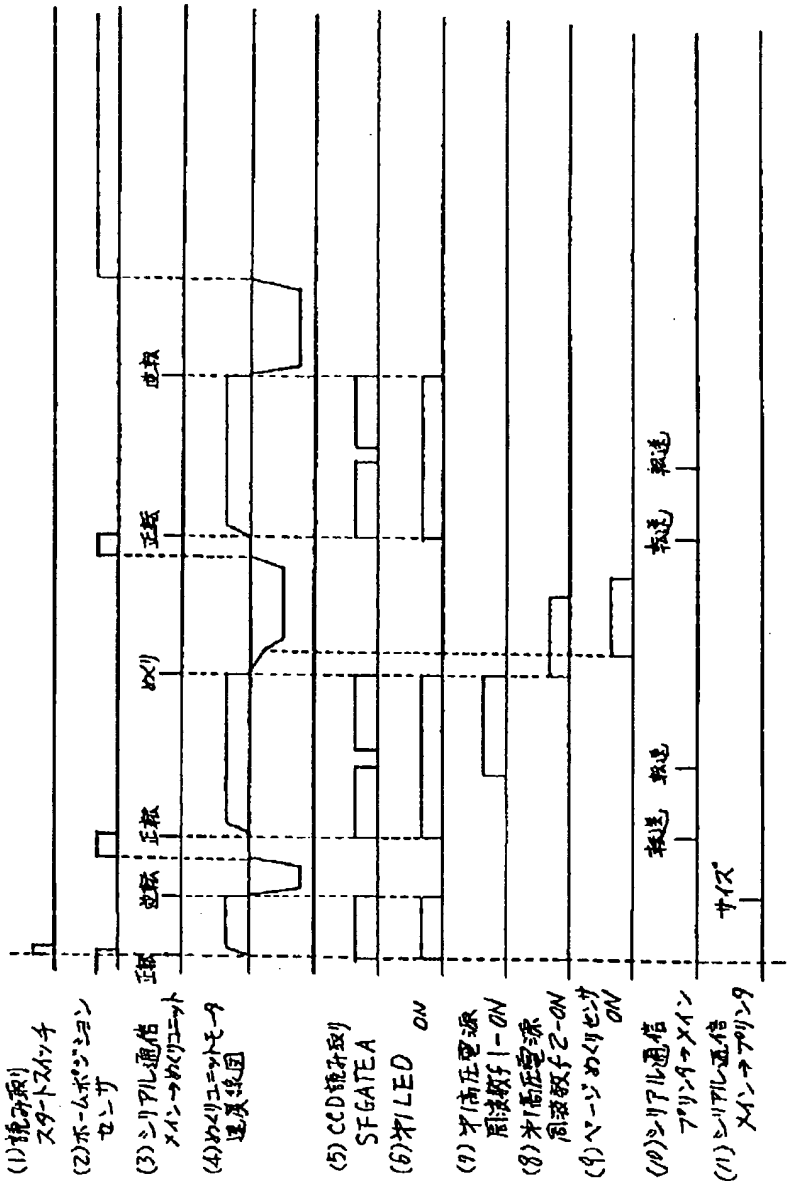
Petitioner Apple Inc. - Exhibit 1012, p. 1494

【図41】



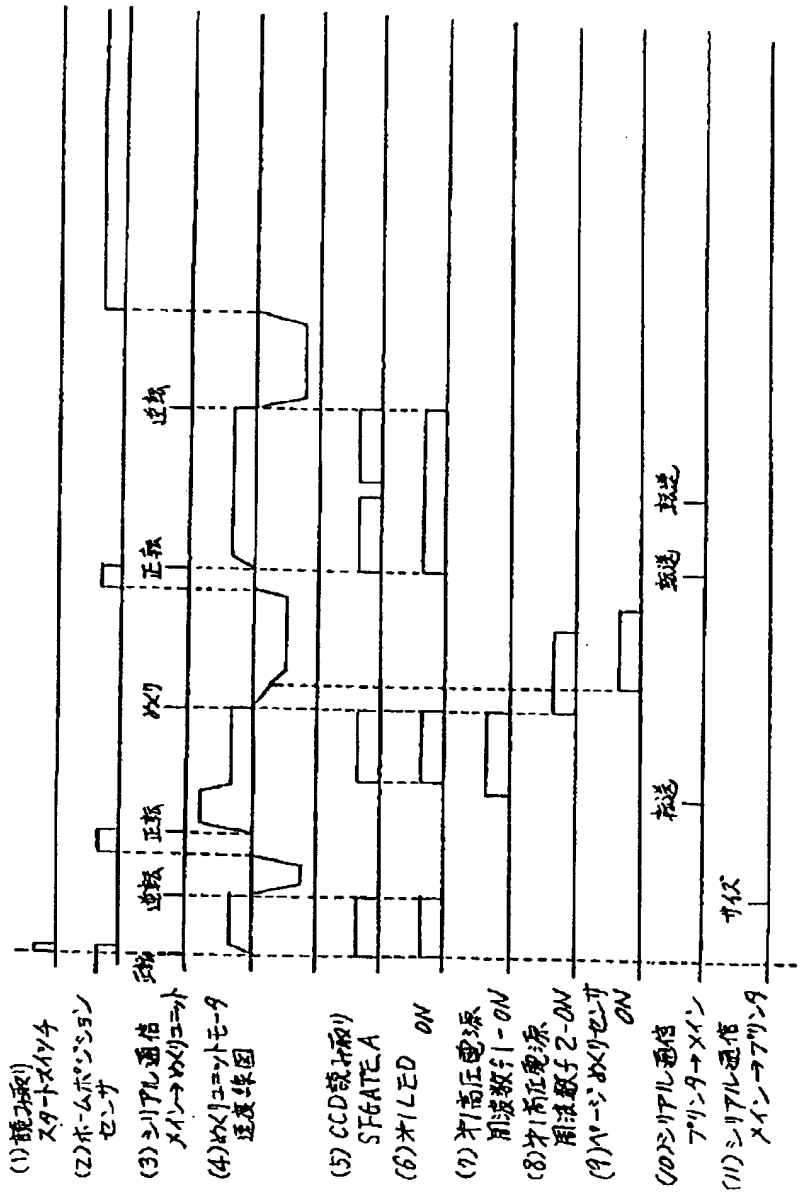
Petitioner Apple Inc. - Exhibit 1012, p. 1495

【図42】



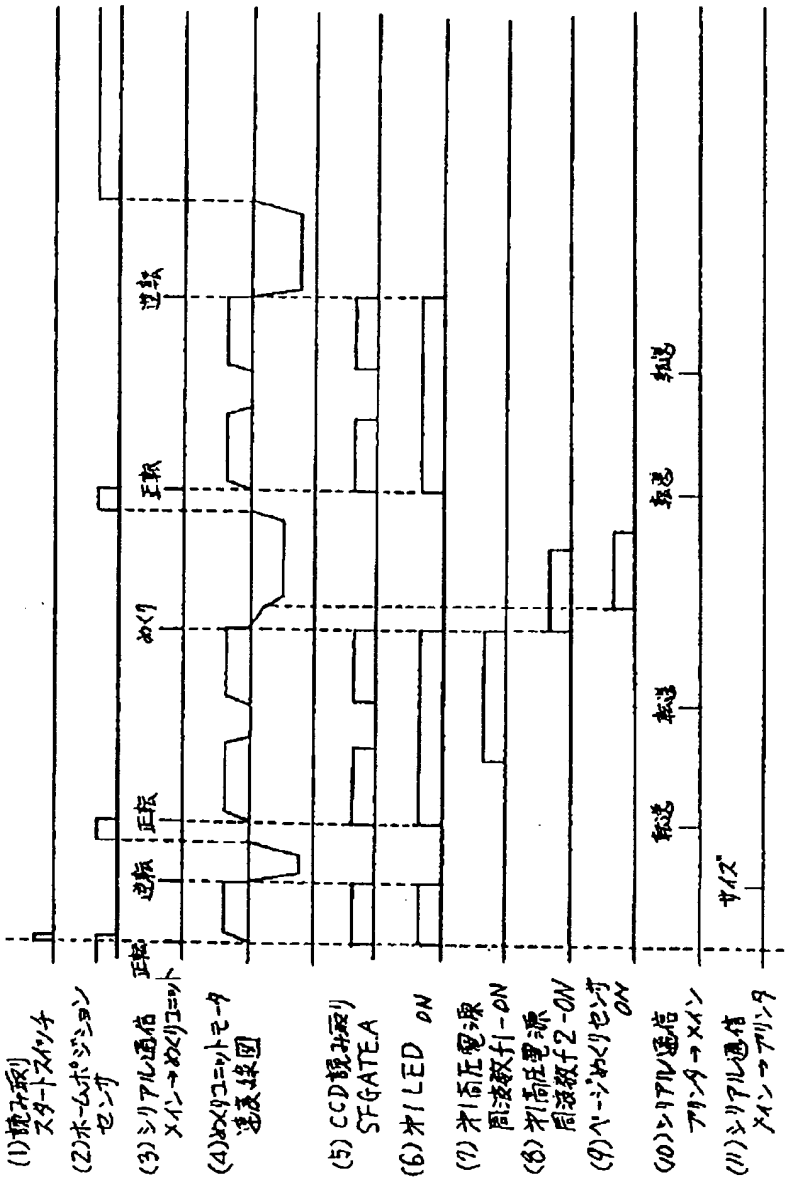
Petitioner Apple Inc. - Exhibit 1012, p. 1496

【図４３】



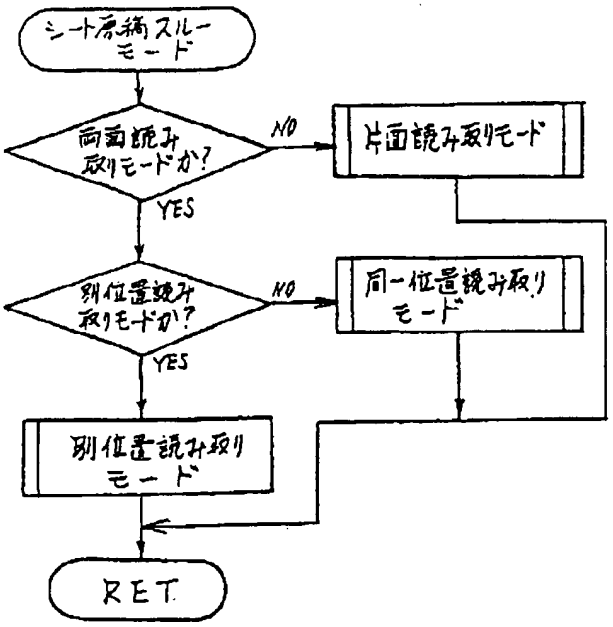
Petitioner Apple Inc. - Exhibit 1012, p. 1497

【図４６】

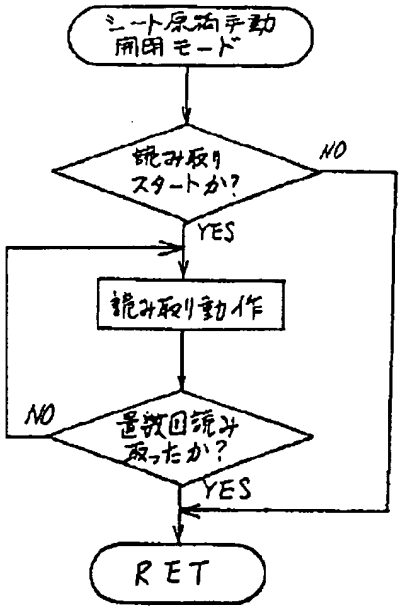


Petitioner Apple Inc. - Exhibit 1012, p. 1498

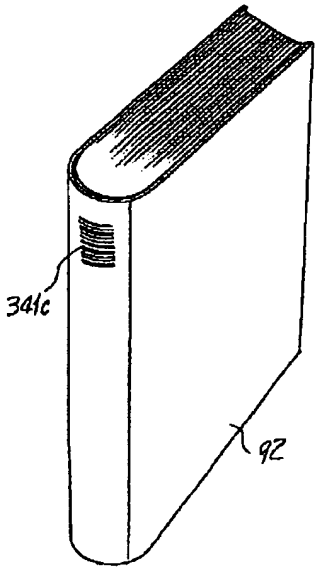
【図47】



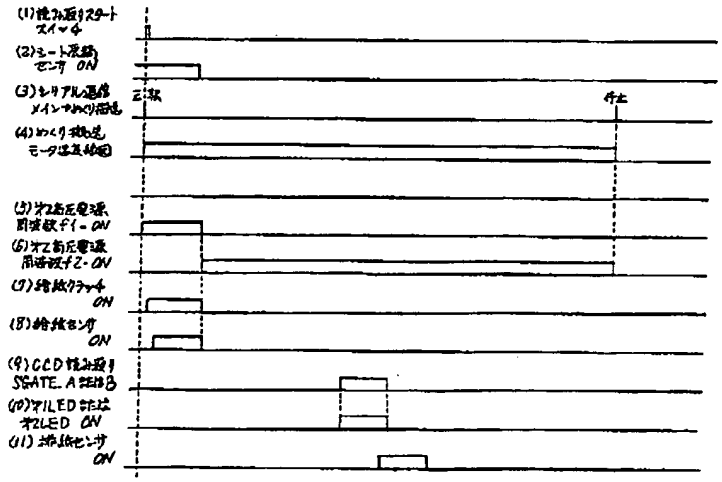
【図56】



【図66】

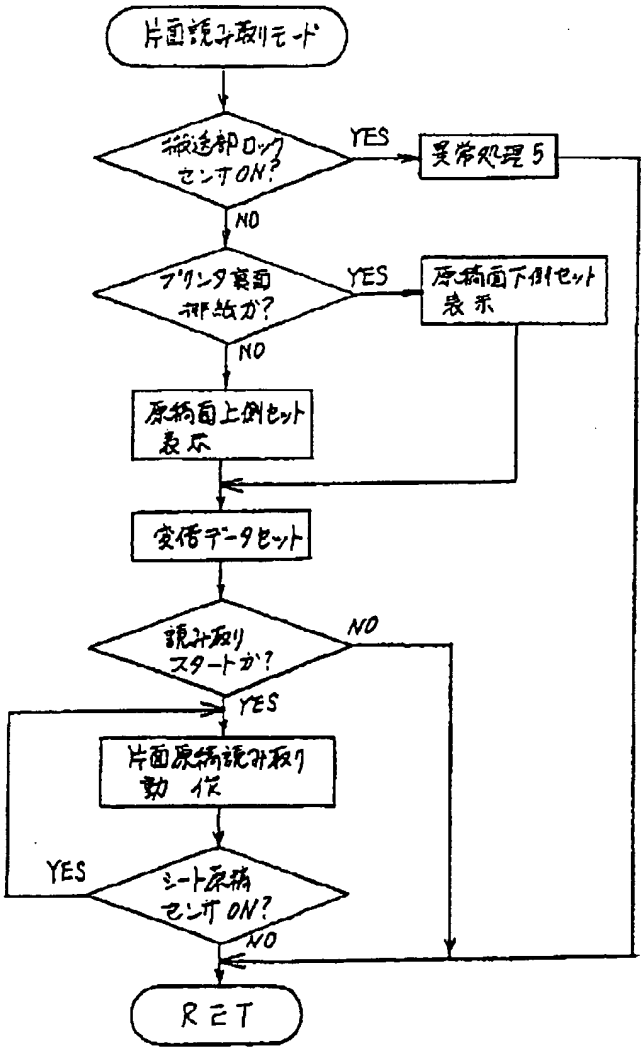


【図49】

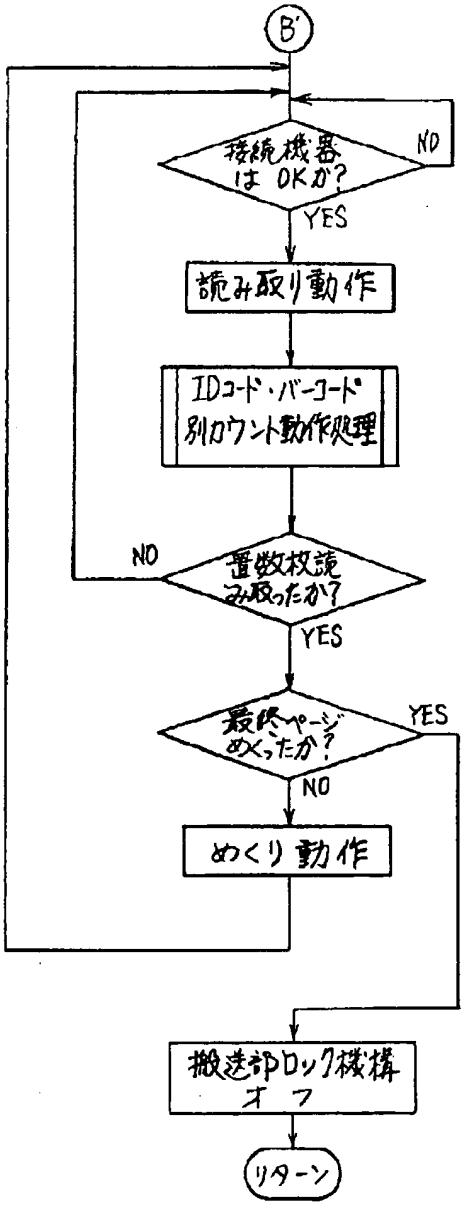


Petitioner Apple Inc. - Exhibit 1012, p. 1499

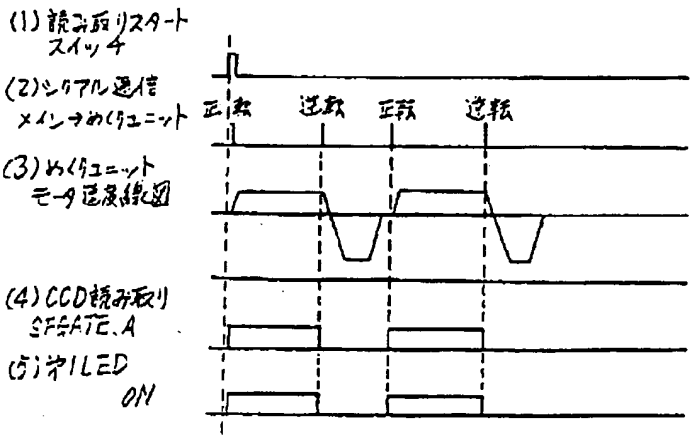
【図４８】



【図６３】

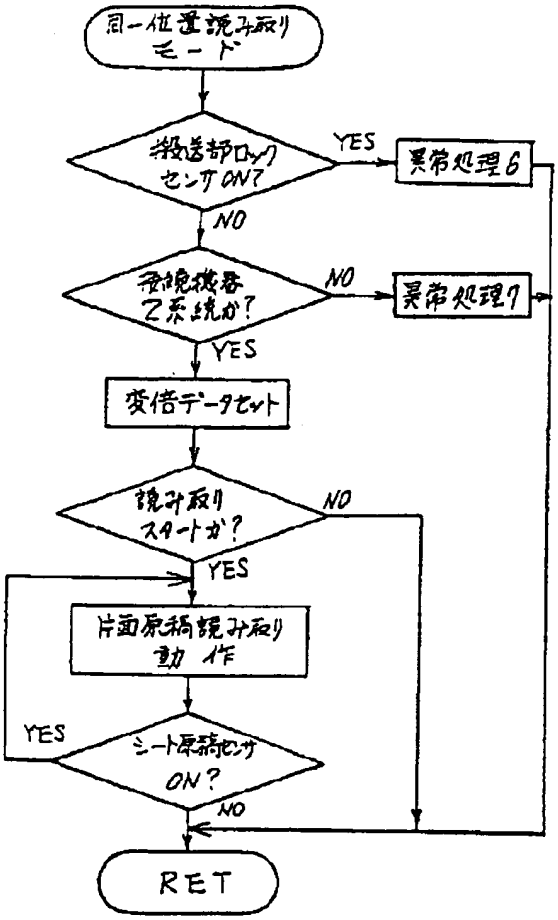


【図５７】

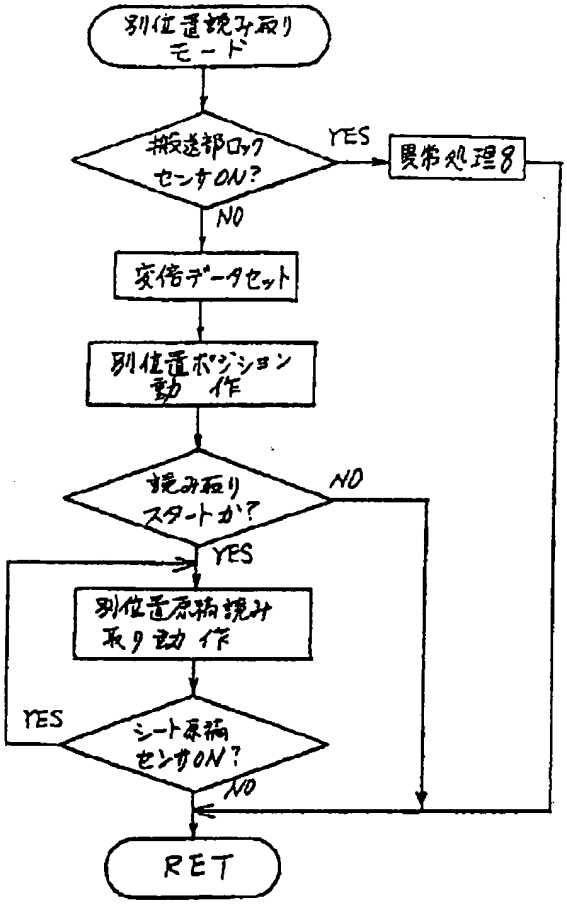


Petitioner Apple Inc. - Exhibit 1012, p. 1500

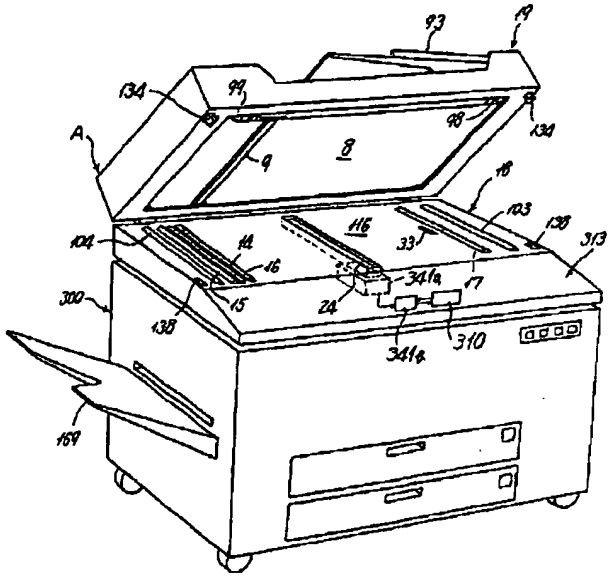
【図５０】



【図５２】

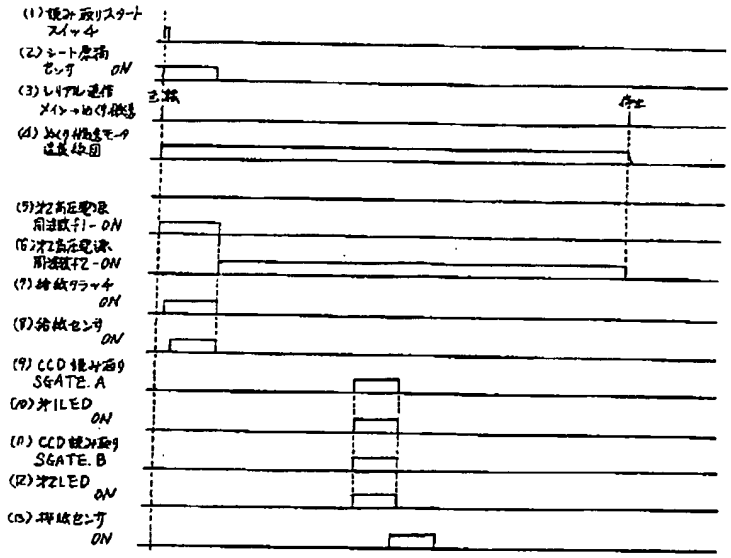


【図６７】

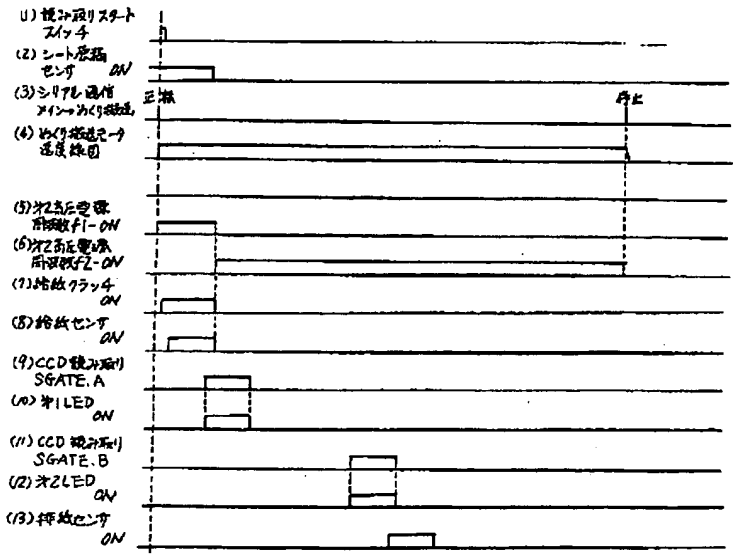


Petitioner Apple Inc. - Exhibit 1012, p. 1501

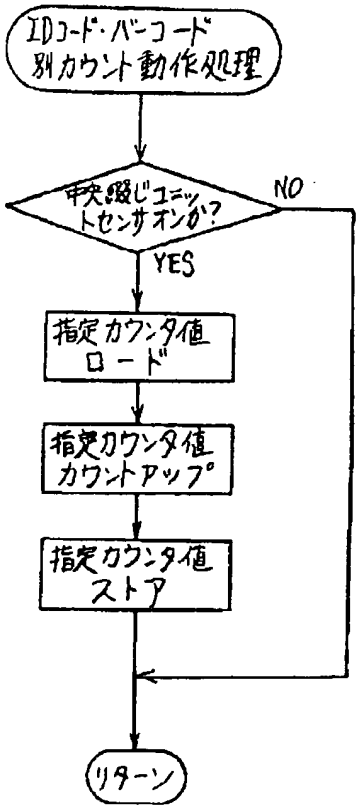
【図５１】



【図５３】

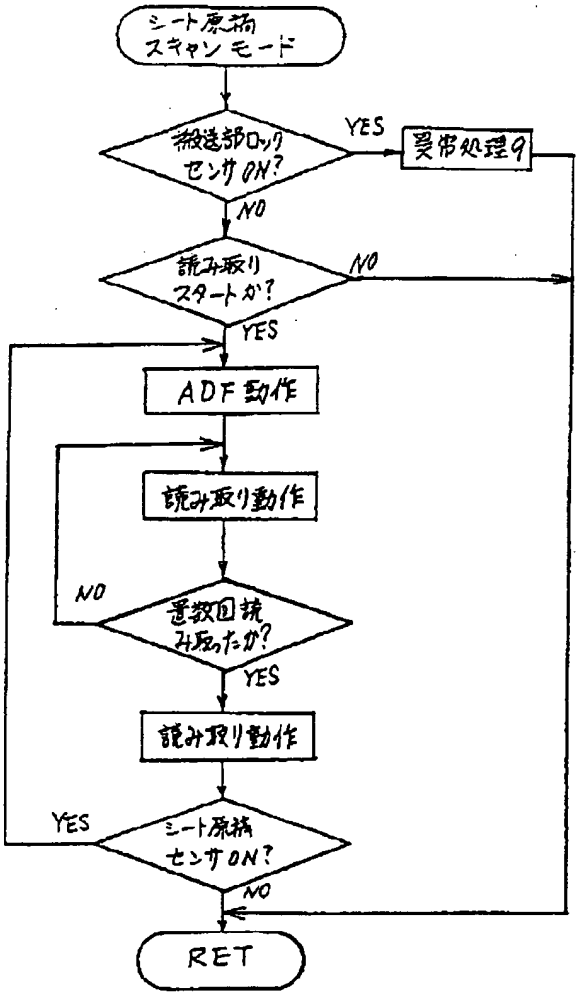


【図６９】

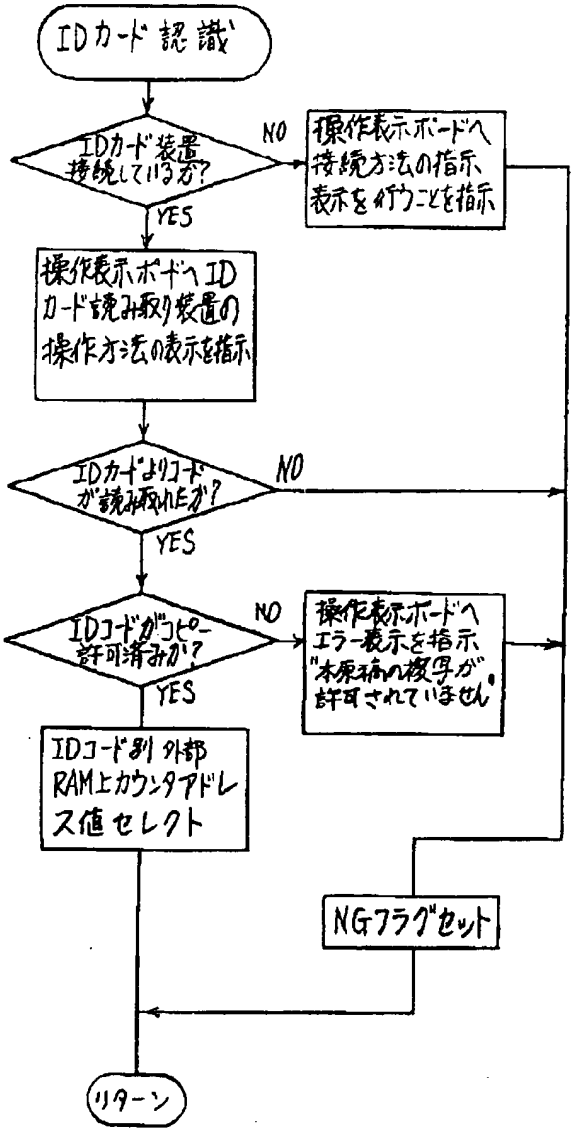


Petitioner Apple Inc. - Exhibit 1012, p. 1502

【図54】

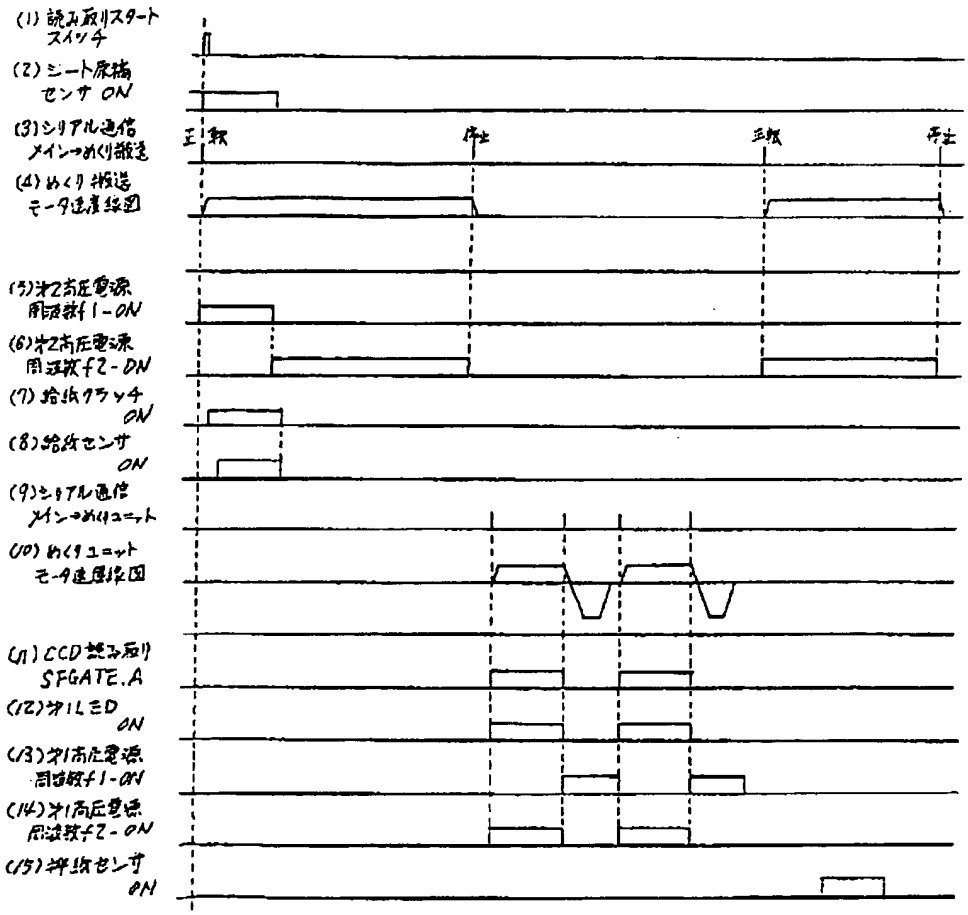


【図64】

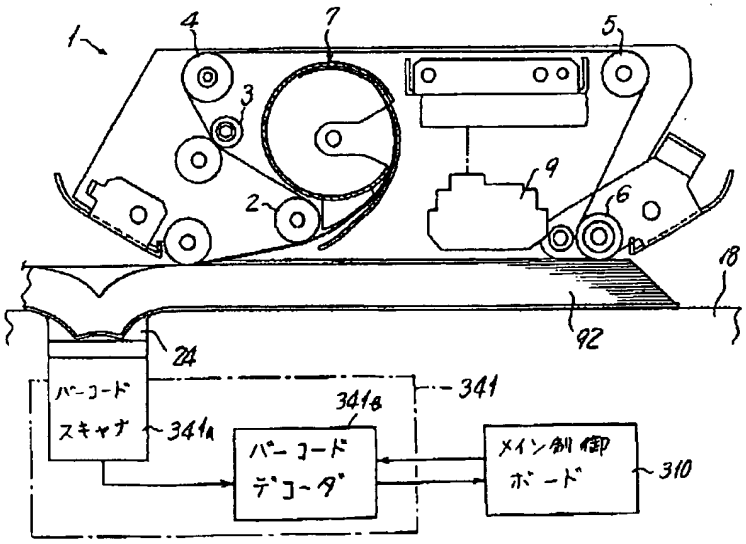


Petitioner Apple Inc. - Exhibit 1012, p. 1503

【図５５】

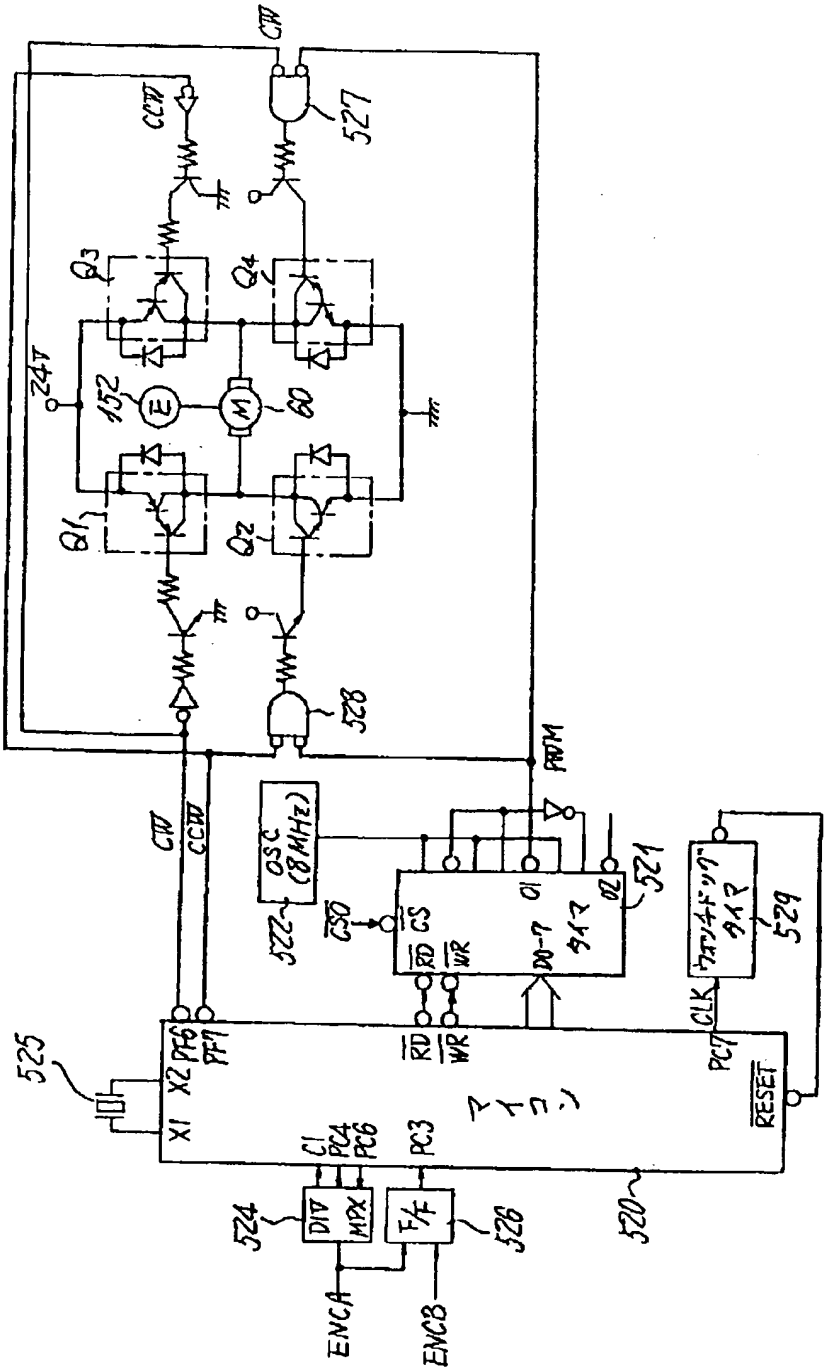


【図６８】



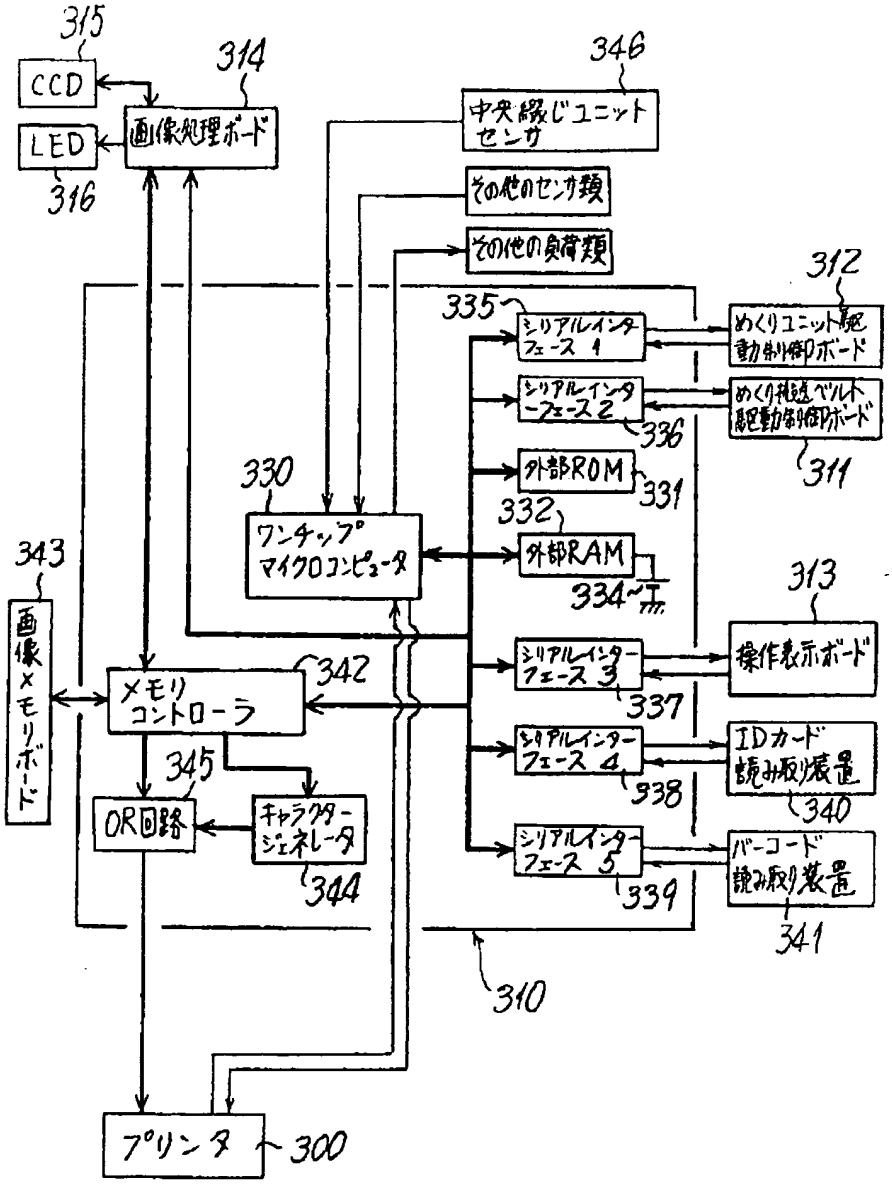
Petitioner Apple Inc. - Exhibit 1012, p. 1504

【図58】



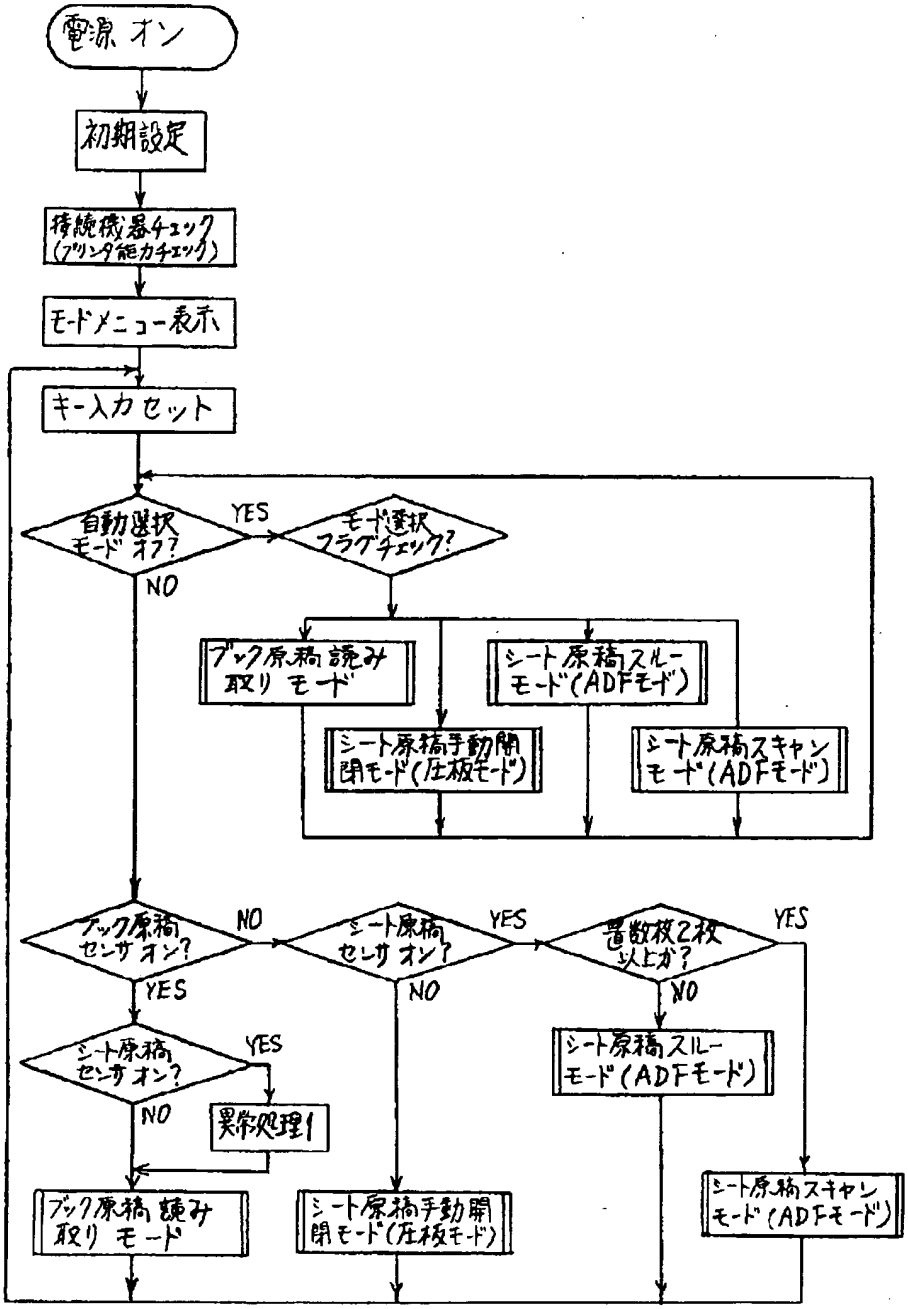
Petitioner Apple Inc. - Exhibit 1012, p. 1505

【図59】



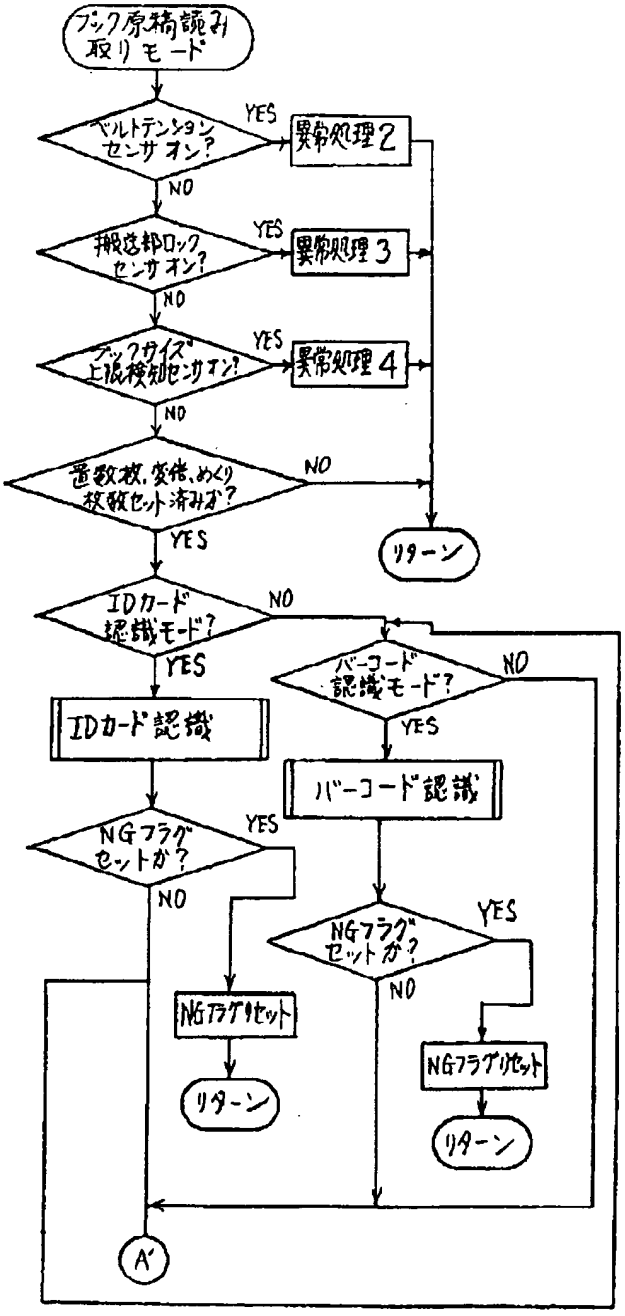
Petitioner Apple Inc. - Exhibit 1012, p. 1506

【図60】



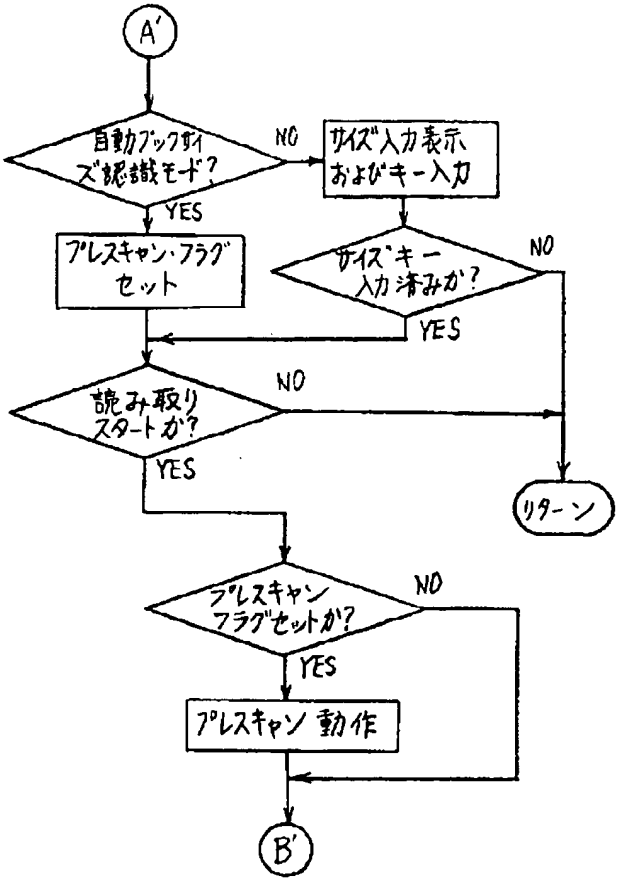
Petitioner Apple Inc. - Exhibit 1012, p. 1507

【図６１】



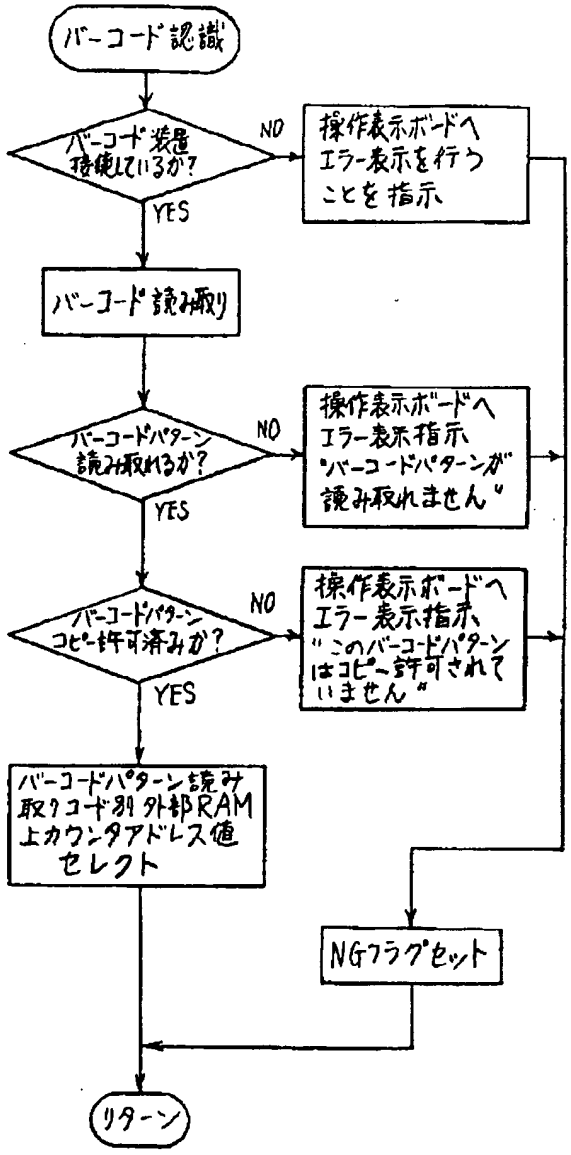
Petitioner Apple Inc. - Exhibit 1012, p. 1508

【図６２】



Petitioner Apple Inc. - Exhibit 1012, p. 1509

【図６５】



フロントページの続き

(51) Int. Cl.⁵		識別記号		庁内整理番号	FI	技術表示箇所
G03B	27/62			8106－2K		
G03G	15/00	102				
		107		8530－2H		
	15/04	119				
G06F	15/64	325	B	8840－5L		
H04N	1/00	108	M	7046－5C		
	1/10			7205－5C		

Petitioner Apple Inc. - Exhibit 1012, p. 1510

(72)発明者　坂内　和典
東京都大田区中馬込1丁目3番6号・株式会社リコー内

(72)発明者　椎名　将
東京都大田区中馬込1丁目3番6号・株式会社リコー内

Petitioner Apple Inc. - Exhibit 1012, p. 1511

Requested Patent: JP6175794A

Title: PRINT PROCESSING SYSTEM ;

Abstracted Patent: JP6175794 ;

Publication Date: 1994-06-24 ;

Inventor(s): TANAKA KOICHIRO ;

Applicant(s): FUJI XEROX CO LTD ;

Application Number: JP19920329533 19921209 ;

Priority Number(s): ;

IPC Classification: G06F3/12; B41J29/38 ;

Equivalents: ;

ABSTRACT:

PURPOSE:To prevent a third person from freely using and printing a print resource stored in a printer.

CONSTITUTION:When print is requested, a requester access right-acquiring part 22 acquires the requester access right from an access right management part 23, and a print resource use instruction in which this requester access right is built is issued. The requester access right built in this instruction is collated with a user access right added to a print resource 39 with access right by a printer 12. If it is discriminated as the result that the requester does not have the just right, the use of the print resource 39 is rejected, and the result is reported to a host computer 11. Deletion and update of the print resource are controlled in the same manner.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平6－175794

(43)公開日　平成６年(1994)６月24日

(51)Int.Cl.[5]	識別記号	庁内整理番号	Ｆ１	技術表示箇所
Ｇ０６Ｆ　3/12	A			
	B			
Ｂ４１Ｊ　29/38	Z	9113－2C		

審査請求　未請求　請求項の数４(全 29 頁)

(21)出願番号　特願平4－329533

(22)出願日　平成４年(1992)12月９日

(71)出願人　000005496
富士ゼロックス株式会社
東京都港区赤坂三丁目３番５号

(72)発明者　田中　浩一郎
埼玉県岩槻市府内３丁目７番１号　富士ゼロックス株式会社内

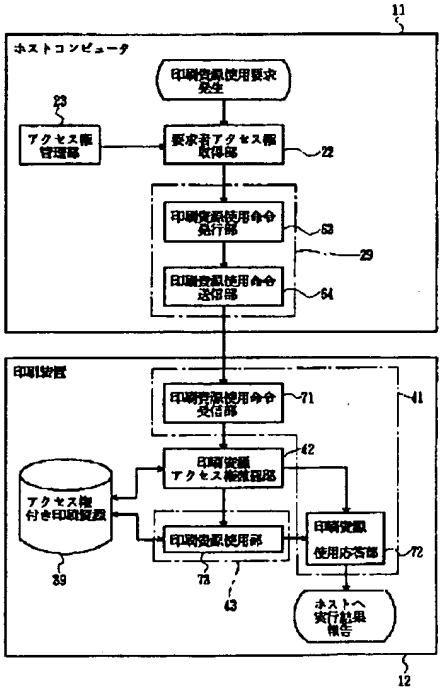
(74)代理人　弁理士　山内　梅雄

(54)【発明の名称】　印刷処理システム

(57)【要約】

【目的】　印刷装置に格納された印刷資源を第三者が勝手に使用して印刷できないようにする。

【構成】　印刷の要求があると、要求者アクセス権取得部２２がアクセス権管理部２３から要求者アクセス権を取得し、これを組み込んで印刷資源使用命令が発行される。この命令に組み込まれた要求者アクセス権は印刷装置１２でアクセス権付き印刷資源３９に付加されていた利用者アクセス権と照合される。この結果、要求者が正当な権限を有しないことが判別されたらその印刷資源の使用が拒否され、その結果がホストコンピュータ１１に報告される。印刷資源の使用の他、削除および更新についても同様の規制を行うことができる。



Petitioner Apple Inc. - Exhibit 1012, p. 1513

1

【特許請求の範囲】

【請求項1】　文字フォント等の印刷に必要とされる印刷資源を格納した送信側印刷資源格納手段と、印刷資源ごとにそれらを処理できる利用者を利用者アクセス権として規定した利用者管理テーブルと、印刷資源の処理要求者ごとに印刷資源のアクセス範囲を要求者アクセス権として規定した要求者管理テーブルと、前記送信側印刷資源格納手段に格納された印刷資源の送信が要求されたとき印刷資源ごとに対応する前記利用者アクセス権を付加して転送する印刷資源転送手段と、印刷資源の処理要求があったときその要求者アクセス権を組み込んだ印刷資源処理命令を発行する印刷資源使用命令発行手段とを備えたホストコンピュータと、

このホストコンピュータと回線によって接続され前記印刷資源が送られてきたときこれを格納する受信側印刷資源格納手段と、前記印刷資源処理命令を受信する印刷資源処理命令受信手段と、前記印刷資源処理命令が受信されたとき対象となる印刷資源の利用者アクセス権と受信した要求者アクセス権を比較する比較手段と、比較結果が一致しないときその印刷資源の処理を拒否する使用拒否手段とを備えた印刷装置とを具備することを特徴とする印刷処理システム。

【請求項2】　文字フォント等の印刷に必要とされる印刷資源を格納した送信側印刷資源格納手段と、印刷資源ごとにそれらを印刷時に使用できる利用者を利用者アクセス権として規定した利用者管理テーブルと、印刷資源の使用要求者ごとに印刷資源のアクセス範囲を要求者アクセス権として規定した要求者管理テーブルと、前記送信側印刷資源格納手段に格納された印刷資源の送信が要求されたとき印刷資源ごとに対応する前記利用者アクセス権を付加して転送する印刷資源転送手段と、印刷資源の使用要求があったときその要求者アクセス権を組み込んだ印刷資源使用命令を発行する印刷資源使用命令発行手段とを備えたホストコンピュータと、

このホストコンピュータと回線によって接続され前記印刷資源が送られてきたときこれを格納する受信側印刷資源格納手段と、前記印刷資源使用命令を受信する印刷資源使用命令受信手段と、前記印刷資源使用命令が受信されたとき対象となる印刷資源の利用者アクセス権と受信した要求者アクセス権を比較する比較手段と、比較結果が一致しないときその印刷資源の使用を拒否する使用拒否手段とを備えた印刷装置とを具備することを特徴とする印刷処理システム。

【請求項3】　文字フォント等の印刷に必要とされる印刷資源を格納した送信側印刷資源格納手段と、印刷資源ごとにそれらを削除できる利用者を利用者アクセス権として規定した利用者管理テーブルと、印刷資源の削除要求者ごとに印刷資源のアクセス範囲を要求者アクセス権として規定した要求者管理テーブルと、前記送信側印刷資源格納手段に格納された印刷資源の送信が要求されたとき印刷資源ごとに対応する前記利用者アクセス権を付加して転送する印刷資源転送手段と、印刷資源の削除要求があったときその要求者アクセス権を組み込んだ印刷資源削除命令を発行する印刷資源使用命令発行手段とを備えたホストコンピュータと、

このホストコンピュータと回線によって接続され前記印刷資源が送られてきたときこれを格納する受信側印刷資源格納手段と、前記印刷資源削除命令を受信する印刷資源削除命令受信手段と、前記印刷資源削除命令が受信されたとき対象となる印刷資源の利用者アクセス権と受信した要求者アクセス権を比較する比較手段と、比較結果が一致しないときその印刷資源の削除を拒否する使用拒否手段とを備えた印刷装置とを具備することを特徴とする印刷処理システム。

【請求項4】　文字フォント等の印刷に必要とされる印刷資源を格納した送信側印刷資源格納手段と、印刷資源ごとにそれらを更新できる利用者を利用者アクセス権として規定した利用者管理テーブルと、印刷資源の更新要求者ごとに印刷資源のアクセス範囲を要求者アクセス権として規定した要求者管理テーブルと、前記送信側印刷資源格納手段に格納された印刷資源の送信が要求されたとき印刷資源ごとに対応する前記利用者アクセス権を付加して転送する印刷資源転送手段と、印刷資源の更新要求があったときその要求者アクセス権を組み込んだ印刷資源更新命令を発行する印刷資源使用命令発行手段とを備えたホストコンピュータと、

このホストコンピュータと回線によって接続され前記印刷資源が送られてきたときこれを格納する受信側印刷資源格納手段と、前記印刷資源更新命令を受信する印刷資源更新命令受信手段と、前記印刷資源更新命令が受信されたとき対象となる印刷資源の利用者アクセス権と受信した要求者アクセス権を比較する比較手段と、比較結果が一致しないときその印刷資源の更新を拒否する使用拒否手段とを備えた印刷装置とを具備することを特徴とする印刷処理システム。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は印刷資源を備えたホストコンピュータ等の印刷資源格納手段と、必要に応じてこの印刷資源格納手段から印刷資源の供給を受けて文字あるいはグラフィック等からなる印刷情報の印刷を行う印刷装置とを備えた印刷処理システムに係わり、詳細には印刷装置側で印刷資源の利用や削除あるいは更新等の各種処理の管理を行うことのできる印刷処理システムに関する。

【0002】

【従来の技術】印刷装置は、文書あるいはグラフィック描画情報等の印刷情報を印刷する際に、個別に指定された文字フォントや文字パターン等の印刷資源を用いながら印刷処理を行うようになっている。このような印刷処

2

Petitioner Apple Inc. - Exhibit 1012, p. 1514

理システムでは、印刷の開始するたびにそのときの印刷情報に使われるすべての印刷資源をホストコンピュータから印刷装置に転送するようになっているものがある。このようなシステムでは、印刷情報が切り替わるたびに、前に転送した印刷資源をすべて削除して新たに印刷資源を転送しているので、転送に手間と時間がかかるという問題がある。

【０００３】そこで、特開昭６３－１３０３６２号公報ではこれを改良し、印刷装置側に例えば磁気ディスクのような比較的大容量の記憶手段を用意させ、これに最低限必要な印刷資源を格納させるようになっている。そして、新たに印刷を行う際にはその印刷情報に必要な印刷資源のみをホストコンピュータ等の印刷資源格納手段から転送してもらうようになっている。

【０００４】

【発明が解決しようとする課題】ところが、この提案された印刷処理システムでは、ホストコンピュータ等の印刷資源格納手段に格納された印刷資源が印刷を要求する者によって結果的に自由に引き出され各個人等が管理する印刷装置側に渡ってしまうことになる。したがって、その印刷資源が機密性を有するようなものである場合には、機密が漏洩するといった問題を発生させた。

【０００５】また、印刷装置に備えられた磁気ディスク等の記憶手段は印刷資源を無制限に格納することができないため、適宜整理する必要がある。このとき、印刷資源格納手段から転送しておいた印刷資源を第三者が誤って削除することがあった。この場合には、新たにホストコンピュータ等からその印刷資源を転送する必要があり、印刷に要する時間を実質的に長引かせるといった問題があった。

【０００６】更に、印刷資源格納手段から転送しておいた印刷資源を第三者が勝手に内容を訂正し更新してしまう場合もあった。この場合には、文字パターンが異なってしまったり、所定の文字コードの組み合わせに対応する語句または文章の内容が異なってしまうというように印刷に使用する印刷資源自体が変質してしまう。したがって、更新されたことを知らずにその印刷資源を使用すると、印刷された内容自体が予期しないものになるといった問題を生じさせた。

【０００７】そこで本発明の目的は、ホストコンピュータ等の印刷資源格納手段から供給を受けた印刷資源について機密の必要なものを保護できるようにした印刷処理システムを提供することにある。

【０００８】本発明の他の目的は、ホストコンピュータ等の印刷資源格納手段から供給を受けた印刷資源のうち所定のものを第三者が勝手に削除できないようにした印刷処理システムを提供することにある。

【０００９】本発明の更に他の目的は、ホストコンピュータ等の印刷資源格納手段から供給を受けた印刷資源のうち所定のものを第三者が勝手に更新することのできないようにした印刷処理システムを提供することにある。

【００１０】

【課題を解決するための手段】請求項１記載の発明では、（イ）文字フォント等の印刷に必要とされる印刷資源を格納した送信側印刷資源格納手段と、印刷資源ごとにそれらを処理できる利用者を利用者アクセス権として規定した利用者管理テーブルと、印刷資源の処理要求者ごとに印刷資源のアクセス範囲を要求者アクセス権として規定した要求者管理テーブルと、送信側印刷資源格納手段に格納された印刷資源の送信が要求されたとき印刷資源ごとに対応する利用者アクセス権を付加して転送する印刷資源転送手段と、印刷資源の処理要求があったときその要求者アクセス権を組み込んだ印刷資源処理命令を発行する印刷資源使用命令発行手段とを備えたホストコンピュータと、（ロ）このホストコンピュータと回線によって接続され印刷資源が送られてきたときこれを格納する受信側印刷資源格納手段と、印刷資源処理命令を受信する印刷資源処理命令受信手段と、印刷資源処理命令が受信されたとき対象となる印刷資源の利用者アクセス権と受信した要求者アクセス権を比較する比較手段と、比較結果が一致しないときその印刷資源の処理を拒否する使用拒否手段とを備えた印刷装置とを印刷処理システムに具備させる。

【００１１】すなわち請求項１記載の発明では、ホストコンピュータから印刷資源を印刷装置に送信してこれに格納する際には、印刷資源と併せてそれを処理することのできる利用者を表わした利用者アクセス権を付加して転送しておく。また、その印刷資源の使用を要求する者に対しては、その者がアクセスすることのできる印刷資源を表わした要求者アクセス権を印刷資源処理命令に組み込んでホストコンピュータが印刷装置に送信することにする。印刷装置側ではこの印刷資源処理命令から抽出された要求者アクセス権と該当する印刷資源に付加された利用者アクセス権を照合し、要求者に印刷資源の処理の権限がない場合には、その処理を拒絶することにして、印刷資源の利用、削除、更新等の処理の安全を図るようになっている。

【００１２】請求項２記載の発明では、（イ）文字フォント等の印刷に必要とされる印刷資源を格納した送信側印刷資源格納手段と、印刷資源ごとにそれらを印刷時に使用できる利用者を利用者アクセス権として規定した利用者管理テーブルと、印刷資源の使用要求者ごとに印刷資源のアクセス範囲を要求者アクセス権として規定した要求者管理テーブルと、送信側印刷資源格納手段に格納された印刷資源の送信が要求されたとき印刷資源ごとに対応する利用者アクセス権を付加して転送する印刷資源転送手段と、印刷資源の使用要求があったときその要求者アクセス権を組み込んだ印刷資源使用命令を発行する印刷資源使用命令発行手段とを備えたホストコンピュータと、（ロ）このホストコンピュータと回線によって接

Petitioner Apple Inc. - Exhibit 1012, p. 1515

5

続され印刷資源が送られてきたときこれを格納する受信側印刷資源格納手段と、印刷資源使用命令を受信する印刷資源使用命令受信手段と、印刷資源使用命令が受信されたとき対象となる印刷資源の利用者アクセス権と受信した要求者アクセス権を比較する比較手段と、比較結果が一致しないときその印刷資源の使用を拒否する使用拒否手段とを備えた印刷装置とを印刷処理システムに具備させる。

【００１３】すなわち請求項２記載の発明では、ホストコンピュータから印刷資源を印刷装置に送信してこれに格納する際には、印刷資源と併せてそれを利用することのできる利用者を表わした利用者アクセス権を付加して転送しておく。また、その印刷資源の使用を要求する者に対しては、その者がアクセスすることのできる印刷資源を表わした要求者アクセス権を印刷資源利用命令に組み込んでホストコンピュータが印刷装置に送信することにする。印刷装置側ではこの印刷資源利用命令から抽出された要求者アクセス権と該当する印刷資源に付加された利用者アクセス権を照合し、要求者に印刷資源の利用の権限がない場合には、その利用を拒絶することにして、印刷資源の利用の安全を図るようになっている。

【００１４】請求項３記載の発明では、（イ）文字フォント等の印刷に必要とされる印刷資源を格納した送信側印刷資源格納手段と、印刷資源ごとにそれらを削除できる利用者を利用者アクセス権として規定した利用者管理テーブルと、印刷資源の削除要求者ごとに印刷資源のアクセス範囲を要求者アクセス権として規定した要求者管理テーブルと、送信側印刷資源格納手段に格納された印刷資源の送信が要求されたとき印刷資源ごとに対応する利用者アクセス権を付加して転送する印刷資源転送手段と、印刷資源の削除要求があったときその要求者アクセス権を組み込んだ印刷資源削除命令を発行する印刷資源使用命令発行手段とを備えたホストコンピュータと、（ロ）このホストコンピュータと回線によって接続され印刷資源が送られてきたときこれを格納する受信側印刷資源格納手段と、印刷資源削除命令を受信する印刷資源削除命令受信手段と、印刷資源削除命令が受信されたとき対象となる印刷資源の利用者アクセス権と受信した要求者アクセス権を比較する比較手段と、比較結果が一致しないときその印刷資源の削除を拒否する使用拒否手段とを備えた印刷装置とを印刷処理システムに具備させる。

【００１５】すなわち請求項３記載の発明では、ホストコンピュータから印刷資源を印刷装置に送信してこれに格納する際には、印刷資源と併せてそれを削除することのできる削除者を表わした削除者アクセス権を付加して転送しておく。また、その印刷資源の使用を要求する者に対しては、その者がアクセスすることのできる印刷資源を表わした要求者アクセス権を印刷資源削除命令に組み込んでホストコンピュータが印刷装置に送信することにする。印刷装置側ではこの印刷資源削除命令から抽出された要求者アクセス権と該当する印刷資源に付加された削除者アクセス権を照合し、要求者に印刷資源の削除の権限がない場合には、その削除を拒絶することにして、印刷資源の削除の際の不都合の発生を防止している。

6

【００１６】請求項４記載の発明では、（イ）文字フォント等の印刷に必要とされる印刷資源を格納した送信側印刷資源格納手段と、印刷資源ごとにそれらを更新できる利用者を利用者アクセス権として規定した利用者管理テーブルと、印刷資源の更新要求者ごとに印刷資源のアクセス範囲を要求者アクセス権として規定した要求者管理テーブルと、送信側印刷資源格納手段に格納された印刷資源の送信が要求されたとき印刷資源ごとに対応する利用者アクセス権を付加して転送する印刷資源転送手段と、印刷資源の更新要求があったときその要求者アクセス権を組み込んだ印刷資源更新命令を発行する印刷資源使用命令発行手段とを備えたホストコンピュータと、（ロ）このホストコンピュータと回線によって接続され印刷資源が送られてきたときこれを格納する受信側印刷資源格納手段と、印刷資源更新命令を受信する印刷資源更新命令受信手段と、印刷資源更新命令が受信されたとき対象となる印刷資源の利用者アクセス権と受信した要求者アクセス権を比較する比較手段と、比較結果が一致しないときその印刷資源の更新を拒否する使用拒否手段とを備えた印刷装置とを印刷処理システムに具備させる。

【００１７】すなわち請求項４記載の発明では、ホストコンピュータから印刷資源を印刷装置に送信してこれに格納する際には、印刷資源と併せてそれを更新することのできる更新者を表わした更新者アクセス権を付加して転送しておく。また、その印刷資源の使用を要求する者に対しては、その者がアクセスすることのできる印刷資源を表わした要求者アクセス権を印刷資源更新命令に組み込んでホストコンピュータが印刷装置に送信することにする。印刷装置側ではこの印刷資源更新命令から抽出された要求者アクセス権と該当する印刷資源に付加された更新者アクセス権を照合し、要求者に印刷資源の更新の権限がない場合には、その更新を拒絶することにして、印刷資源の更新の際の不都合の発生を防止している。

【００１８】

【実施例】以下実施例につき本発明を詳細に説明する。

【００１９】第１の実施例

【００２０】図１は本発明の第１の実施例における印刷処理システムの原理的な構成を表わしたものである。この印刷処理システムは、印刷資源を格納したホストコンピュータ１１と、印刷装置１２およびこれらを接続する回線１３とによって構成されている。

【００２１】ホストコンピュータ１１側には、その制御

Petitioner Apple Inc. - Exhibit 1012, p. 1516

を行う制御部１５が配置されている。制御部１５は、ＣＰＵ（中央処理装置）１６を備えており、図示しないバスを介してＲＯＭ（リード・オンリ・メモリ）１７、ＲＡＭ（ランダム・アクセス・メモリ）１８と接続されている他、図示しない入出力回路を介して端末装置１９と接続されている。ここで端末装置１９は、ＣＲＴ等の出力装置やキーボード等の入力装置によって構成されている。

【００２２】制御部１５は、利用者アクセス権設定部２１、要求者アクセス権取得部２２およびアクセス権管理部２３の制御を行うようになっている。ここで、利用者アクセス権設定部２１とは、磁気ディスク装置２４内に格納されている図示しない利用者アクセス権のついていない印刷資源に対して利用者アクセス権を付け、アクセス権付き印刷資源２５とするための機能部品をいう。ここで利用者アクセス権とは、印刷資源を利用可能な者の範囲を定める情報である。印刷資源の中には、利用者を限定する必要がないもの、すなわち誰でも自由に利用することができる印刷資源も存在するが、本明細書ではこれに対しても“誰でもアクセスできるというアクセス権”を付けるものとして、その設定を利用者アクセス権設定部２１が行うようになっている。アクセス権付き印刷資源２５は、必要に応じて印刷資源送信部２６から回線１３を通じて印刷装置１２側に送出されるようになっている。

【００２３】利用者アクセス権および要求者アクセス権の設定に関する管理はアクセス権管理部２３が行うようになっている。この管理のために、アクセス権管理部２３は磁気ディスク装置２４内にアクセス権管理テーブル２８を備えている。なお、磁気ディスク装置２４には制御部１５が各種制御を行うために必要なプログラムも格納されている。

【００２４】要求者アクセス権取得部２２は、印刷資源の使用時に要求者アクセス権を取得する機能部品である。ここで要求者アクセス権とは、印刷資源の使用を要求するものが有しているアクセス権であり、文書等の印刷情報のアクセスを行うのに必要とされるアクセス権と等しい。印刷資源使用命令部２９は印刷資源の使用が要求されたとき、アクセス権管理部２３の管理の下で要求者アクセス権を取得し、これを付加した印刷資源使用命令を発行する。この印刷資源使用命令は回線１３を通じて印刷装置１２へ送出されるようになっている。

【００２５】次に印刷装置１２の説明を行う。印刷装置１２にも、その制御を行う制御部３１が配置されている。制御部３１は、ＣＰＵ３２を備えており、図示しないバスを介してＲＯＭ３３、ＲＡＭ３４と接続されている。ホストコンピュータ１１の印刷資源送信部２６から送られてきたアクセス権付き印刷資源は、印刷資源受信部３６で受信される。そして、制御部３１の制御を受ける印刷資源格納部３７によって磁気ディスク装置３８内

にアクセス権付き印刷資源３９として格納される。なお、磁気ディスク装置３８は、図示しないディスク制御装置を介して制御部３１と接続されており、アクセス権付き印刷資源３９の他に、この制御部３１を制御するための各種のプログラムも格納している。

【００２６】一方、ホストコンピュータ１１から回線１３を通じて送られてくる印刷資源使用命令は印刷資源使用命令応答部４１で受信され、印刷資源アクセス権確認部４２に送られるようになっている。印刷資源アクセス権確認部４２はこの要求者アクセス権をアクセス権付き印刷資源３９に付けられている利用者アクセス権と比較する。そして、要求者にその使用しようとする印刷資源の利用者アクセスが存在する場合にはその印刷資源の使用を許可する。これ以外の場合には、その印刷資源の使用が許可されない。その印刷資源の使用が許可された場合、印刷処理部４３はそのアクセス権付き印刷資源３９を使用して印刷情報の印刷を行う。

【００２７】その印刷資源の使用が許可されなかった場合には、要求者が使用できる範囲の印刷資源を用いて印刷情報の印刷が行われることになる。例えば特殊な文字フォントについて利用者が限定されていて印刷情報の印刷を行う者がその使用を要求した場合に、その使用が認められなかったとする。この際には、その要求者の使用できる他の文字フォントを用いれば印刷が可能である。

【００２８】図２は、この印刷処理システムで印刷資源が印刷装置側に転送されるときの処理の流れを表わしたものである。アクセス権なし印刷資源５１のうち利用者アクセスの付与が求められたものについては、利用者アクセス権設定部２１によって、アクセス権付き印刷資源２５に変更される。このとき、アクセス権管理部２３がその管理を行う。

【００２９】図３は、利用者アクセス権設定部の具体的な構成を表わしたものである。利用者アクセス権設定部２１は、利用者アクセス権の取得をアクセス権管理部２３に対して要求する利用者アクセス権取得要求部５３と、アクセス権なし印刷資源５１に対して利用者アクセス権を設定する印刷資源アクセス権設定部５４と、これらの制御を行う利用者アクセス権設定制御部５５から構成されている。利用者アクセス権設定制御部５５は、制御部１５の制御の下に利用者アクセス権設定部２１の制御を行うことになる。

【００３０】図４は、アクセス権管理部の具体的な構成を表わしたものである。アクセス権管理部２３は、アクセス権の取得要求を利用者アクセス権設定部２１から受信するアクセス権取得要求受信部５７と、アクセス権の取得要求があったときアクセス権管理テーブル２８を用いてアクセス権を取得するアクセス権取得部５８と、取得したアクセス権を図３の利用者アクセス権取得要求部５３に送出するアクセス権送信部５９を有している。アクセス権管理制御部６１は、制御部１５の制御の下で、

Petitioner Apple Inc. - Exhibit 1012, p. 1517

これら各部の制御を行うようになっている。

【0031】すなわち、アクセス権管理部23はアクセス権なし印刷資源51についてアクセス権の付加が要求されたときには、どのような印刷資源についてはどのようなアクセスを付与するかを示したアクセス権管理テーブル28を参照して該当するアクセス権を読み出し、これをその印刷資源に付加してアクセス権付き印刷資源25を作成することになる。このアクセス権付き印刷資源25は印刷資源送信部26から送出され、印刷装置12の印刷資源受信部36に受信される。そして、印刷資源格納部37によってアクセス権付き印刷資源39として磁気ディスク装置38（図1）内に格納されることになる。

【0032】図5は、印刷資源の使用時における印刷処理システムの処理の流れを表わしたものである。印刷装置12に印刷を行わせるために、ホストコンピュータ11で印刷資源使用要求が発生すると、要求者アクセス権取得部22はアクセス権管理部23の管理の下で要求者アクセス権を取得する。この要求者アクセス権は、印刷資源使用命令部29に送られ、その印刷資源使用命令発行部63で印刷資源使用命令が発行される。この印刷資源使用命令は、印刷資源使用命令送信部64から印刷装置12へ送信される。

【0033】図6は、要求者アクセス権取得部の具体的な構成を表わしたものである。要求者アクセス権取得部22は要求者アクセス権の取得をアクセス権管理部23に対して要求する要求者アクセス権取得要求部66と、取得された要求者アクセス権を印刷資源使用命令に付加して印刷資源使用命令部29に送出するための使用命令アクセス権設定部67を備えている。要求者アクセス権取得制御部68は、制御部15の制御の下でこれら要求者アクセス権取得要求部66および使用命令アクセス権設定部67の制御を行うようになっている。

【0034】図5に戻って説明を続ける。ホストコンピュータ11の印刷資源使用命令送信部64から送信された印刷資源使用命令は、印刷装置12の印刷資源使用命令応答部41内の印刷資源使用命令受信部71で受信され、印刷資源アクセス権確認部42に送られる。印刷資源アクセス権確認部42は、アクセス権付き印刷資源39を用いてアクセス権の確認を行い、アクセス権がないとされた場合には印刷資源使用命令応答部41内の印刷資源使用応答部72を介してホストコンピュータ11へそれを報告する。

【0035】ホストコンピュータ11はこれに基づいて代替の印刷資源を使用する等の措置を採るか、印刷を中止することになる。また、印刷資源アクセス権確認部42はその印刷資源のアクセス権があると判別した場合には、該当のアクセス権付き印刷資源39の使用を許可し、その印刷資源が印刷処理部43内の印刷資源使用部73に送られて印刷情報の印刷に使用されることになる。

【0036】図7は、印刷資源アクセス権確認部の具体的な構成を表わしたものである。印刷資源アクセス権確認部42は、印刷資源使用命令応答部41を介して印刷資源の使用要求者のアクセス権を取得する要求者アクセス権取得部71と、アクセス権付き印刷資源39を用いて利用者アクセス権を取得する利用者アクセス権取得部72の2つの取得部を備えている。アクセス権確認部73は、これら2種類のアクセス権を比較し、印刷資源についてのアクセス権が存在するかどうかの確認を行う。アクセス権確認結果送信部74はこの結果を印刷資源使用命令応答部41を介してホストコンピュータ11に送信することになる。印刷資源アクセス権確認部42内の印刷資源アクセス権確認制御部75は、印刷装置12側の制御部31によって制御され各部71～74の制御を行う他、印刷資源の使用が許可されたときには該当の印刷資源を印刷処理部43に送出する制御も行うようになっている。

【0037】図8は、このような印刷処理システムにおける印刷資源転送時の処理の流れを表わしたものである。印刷資源を図1に示したホストコンピュータ11から印刷装置12に転送する場合、図3に示した利用者アクセス権設定部21は利用者アクセス権取得要求部53にて利用者アクセス権の取得を要求する。アクセス権管理部23は、図4に示したアクセス権取得要求受信部57でこの要求を受信し、アクセス権取得部58でアクセス権管理テーブル28を参照して該当するアクセス権を取得する（図8ステップS101）。

【0038】アクセス権送信部59は、この利用者アクセス権を利用者アクセス権設定部21に返信した後、制御をこの利用者アクセス権設定部21に返す。利用者アクセス権設定部21では、アクセス権管理部23から受け取った利用者アクセス権を印刷資源アクセス権設定部54において転送対象の印刷資源に付加する。そして、印刷資源送信部26に印刷装置12への印刷資源の転送を依頼する。これにより、利用者アクセス権が付加された印刷資源が印刷装置12に転送される（ステップS102）。

【0039】印刷資源送信部26から転送されてきた利用者アクセス権付き印刷資源は、印刷資源受信部36で受信され（ステップS103）、磁気ディスク装置38に格納される（ステップS104）。

【0040】図9は、転送されてきた印刷資源を使用して印刷情報の印刷を行う場合の処理の流れを表わしたものである。印刷資源の使用要求が発生すると（ステップS201；Y）、要求者アクセス権取得部22はその要求者アクセス権取得要求部66にてアクセス権管理部23に対して要求者アクセス権の取得を要求する。アクセス権管理部23はそのアクセス権取得要求受信部57でこの要求を受信し、アクセス権取得部58でアクセス権

Petitioner Apple Inc. - Exhibit 1012, p. 1518

管理テーブル２８を用いて該当使用要求者に対する要求者アクセス権を取得する（ステップＳ２０２）。そしてアクセス権送信部５９から要求者アクセス権取得部２２にこれを返信して、制御を要求者アクセス権取得部２２に返す。

【００４１】要求者アクセス権取得部２２では、アクセス権管理部２３から受け取った要求者アクセス権を使用命令アクセス権設定部６７で印刷資源使用命令に付加する。そして、印刷資源使用命令部２９の印刷資源使用命令発行部６３に印刷装置１２への印刷資源使用命令の発行を依頼する。印刷資源使用命令発行部６３はこれを基に印刷資源使用命令を発行する（ステップＳ２０３）。

【００４２】この発行された要求者アクセス権付き印刷資源使用命令は、印刷資源使用命令応答部４１で受信され（ステップＳ２０４）、印刷資源アクセス権確認部４２に渡される。印刷資源アクセス権確認部４２では、要求者アクセス権取得部７１で印刷資源使用命令から要求者アクセス権を取得する（ステップＳ２０５）。また、利用者アクセス権取得部７２では印刷装置１２の磁気ディスク装置３８に格納されたアクセス権付き印刷資源３９から利用者アクセス権を取得する（ステップＳ２０６）。アクセス権確認部７３は以上により取得した要求者アクセス権と利用者アクセス権とを照合確認する（ステップＳ２０７）。そして、確認の結果、要求者が印刷資源を使用できると判別された場合には（ステップＳ２０８；Ｙ）、印刷処理部４３において該当の印刷資源を使用して印刷が行われる（ステップＳ２０９）。

【００４３】これに対して、その要求者が該当する印刷資源の使用を許されていない場合には（ステップＳ２０８；Ｎ）、その印刷資源の使用が拒否される（ステップＳ２１０）。いずれの場合にも、印刷資源使用命令応答部４１は要求に対する応答情報を作成し（ステップＳ２１１）、これを回線１３を通じてホストコンピュータ１１側に送信することになる（ステップＳ２１２）。印刷資源を使用することができないことで印刷を行うことができない場合には、応答情報としてその旨の情報が組み込まれることになる。

【００４４】第２の実施例

【００４５】図１０は本発明の第２の実施例における印刷処理システムの原理的な構成を表わしたものである。この印刷処理システムは、印刷資源を格納したホストコンピュータ１１Ａと、印刷装置１２Ａおよびこれらを接続する回線１３とによって構成されている。なお、この印刷処理システムはその構成が第１の実施例のそれと共通した箇所が多いので、回路装置の内容が同一の箇所には図１等と同一の符号を付し、これらの説明を適宜省略する。また、回路装置の内容自体は異なるが、第１の実施例と対応させて説明することが便利であるような回路装置についてはそれらの箇所に用いた符号の末尾に“Ａ”という符号を付加することにする。

【００４６】ホストコンピュータ１１Ａは、第１の実施例の印刷資源使用命令部２９の代わりに印刷資源削除命令部２９Ａを備えている。印刷装置１２Ａは第１の実施例の印刷資源使用命令応答部４１の代わりに印刷資源削除命令応答部４１Ａを、また印刷処理部４３の代わりに印刷資源削除部４３Ａを備えている。

【００４７】ここで、印刷資源削除命令部２９Ａは、印刷資源の削除が要求されたとき、アクセス権管理部２３の管理の下で要求者アクセス権を取得し、これを付加した印刷資源削除命令を発行するためのもである。この印刷資源削除命令は回線１３を通じて印刷装置１２Ａ送出されるようになっている。

【００４８】一方、ホストコンピュータ１１Ａから回線１３を通じて送られてくる印刷資源削除命令は印刷資源削除命令応答部４１Ａで受信され、印刷資源アクセス権確認部４２に送られるようになっている。印刷資源アクセス権確認部４２はこの要求者アクセス権をアクセス権付き印刷資源３９に付けられている利用者アクセス権と比較する。そして、要求者にその削除しようとする印刷資源の利用者アクセスが存在する場合にはその印刷資源の削除を許可する。これ以外の場合には、その印刷資源の削除が許可されない。その印刷資源の削除が許可された場合、印刷資源削除部４３Ａはアクセス権付き印刷資源３９内の該当する印刷資源を削除することになる。

【００４９】図１１は、この印刷処理システムで印刷資源が印刷装置側に転送されるときの処理の流れを表わしたものである。アクセス権なし印刷資源５１のうち利用者アクセスの付与が求められたものについては、利用者アクセス権設定部２１によって、アクセス権付き印刷資源２５に変更される。このとき、アクセス権管理部２３がその管理を行う。

【００５０】図１２は、利用者アクセス権設定部の具体的な構成を表わしたものである。利用者アクセス権設定部２１は、利用者アクセス権の取得をアクセス権管理部２３に対して要求する利用者アクセス権取得要求部５３と、アクセス権なし印刷資源５１に対して利用者アクセス権を設定する印刷資源アクセス権設定部５４と、これらの制御を行う利用者アクセス権設定制御部５５から構成されている。利用者アクセス権設定制御部５５は、制御部１５Ａの制御の下に利用者アクセス権設定部２１の制御を行うことになる。

【００５１】図１３は、アクセス権管理部の具体的な構成を表わしたものである。アクセス権管理部２３は、アクセス権の取得要求を利用者アクセス権設定部２１から受信するアクセス権取得要求受信部５７と、アクセス権の取得要求があったときアクセス権管理テーブル２８Ａを用いてアクセス権を取得するアクセス権取得部５８と、取得したアクセス権を図１２の利用者アクセス権取得要求部５３に送出するアクセス権送信部５９を有している。アクセス権管理制御部６１は、制御部１５Ａの制

Petitioner Apple Inc. - Exhibit 1012, p. 1519

13

御の下で、これら各部の制御を行うようになっている。

【0052】すなわち、アクセス権管理部23はアクセス権なし印刷資源51についてアクセス権の付加が要求されたときには、どのような印刷資源についてはどのようなアクセスを付与するかを示したアクセス権管理テーブル28Aを参照して該当するアクセス権を読み出し、これをその印刷資源に付加してアクセス権付き印刷資源25を作成することになる。このアクセス権付き印刷資源25は印刷資源送信部26から送出され、印刷装置12Aの印刷資源受信部36に受信される。そして、印刷資源格納部37によってアクセス権付き印刷資源39として磁気ディスク装置38（図10）内に格納されることになる。

【0053】図14は、印刷資源の削除時における印刷処理システムの処理の流れを表わしたものである。印刷資源の削除を行わせるために、ホストコンピュータ11Aで印刷資源削除要求が発生すると、要求者アクセス権取得部22Aはアクセス権管理部23の管理の下で要求者アクセス権を取得する。この要求者アクセス権は、印刷資源削除命令部29Aに送られ、その印刷資源削除命令発行部63Aで印刷資源削除命令が発行される。この印刷資源削除命令は、印刷資源削除命令送信部64から印刷装置12Aへ送信される。

【0054】図15は、要求者アクセス権取得部の具体的な構成を表わしたものである。要求者アクセス権取得部22Aは要求者アクセス権の取得をアクセス権管理部23に対して要求する要求者アクセス権取得要求部66と、取得された要求者アクセス権を印刷資源削除命令に付加して印刷資源削除命令部29Aに送出するための削除命令アクセス権設定部67を備えている。要求者アクセス権取得制御部68は、制御部15Aの制御の下でこれら要求者アクセス権取得要求部66および削除命令アクセス権設定部67の制御を行うようになっている。

【0055】図14に戻って説明を続ける。ホストコンピュータ11Aの印刷資源削除命令送信部64Aから送信された印刷資源削除命令は、印刷装置12Aの印刷資源削除命令応答部41A内の印刷資源削除命令受信部71Aで受信され、印刷資源アクセス権確認部42に送られる。印刷資源アクセス権確認部42は、アクセス権付き印刷資源39を用いてアクセス権の確認を行い、アクセス権がないとされた場合には印刷資源削除命令応答部41A内の印刷資源削除応答部72Aを介してホストコンピュータ11Aへそれを報告する。また、印刷資源アクセス権確認部42はその印刷資源のアクセス権があると判別した場合には、該当のアクセス権付き印刷資源39の削除を許可する。この場合にも、削除の実行結果がホストコンピュータ11Aに報告される。

【0056】図16は、印刷資源アクセス権確認部の具体的な構成を表わしたものである。印刷資源アクセス権確認部42は、印刷資源削除命令応答部41Aを介して

14

印刷資源の削除要求者のアクセス権を取得する要求者アクセス権取得部71Aと、アクセス権付き印刷資源39を用いて利用者アクセス権を取得する利用者アクセス権取得部72Aの2つの取得部を備えている。アクセス権確認部73は、これら2種類のアクセス権を比較し、印刷資源についてのアクセス権が存在するかどうかの確認を行う。

【0057】アクセス権確認結果送信部74はこの結果を印刷資源削除命令応答部41Aを介してホストコンピュータ11Aに送信することになる。印刷資源アクセス権確認部42内の印刷資源アクセス権確認制御部75は、印刷装置12A側の制御部31Aによって制御され各部71A～74の制御を行う他、印刷資源の削除が許可されたときには印刷資源削除部43Aが印刷資源を削除する際の制御も行うようになっている。

【0058】なお、先の第1の実施例ではその図8で印刷処理システムにおける印刷資源転送時の処理の流れを表わしたが第2の実施例ではこの点について実質的な変更がないので、これについての説明を省略する。

【0059】図17は、転送されてきた印刷資源を削除する場合の処理の流れを表わしたものである。印刷資源の削除要求が発生すると（ステップS301；Y）、要求者アクセス権取得部22Aはその要求者アクセス権取得要求部66にてアクセス権管理部23に対して要求者アクセス権の取得を要求する。アクセス権管理部23はそのアクセス権取得要求受信部57でこの要求を受信し、アクセス権取得部58でアクセス権管理テーブル28Aを用いて該当削除要求者に対する要求者アクセス権を取得する（ステップS302）。そしてアクセス権送信部59から要求者アクセス権取得部22Aにこれを返信して、制御を要求者アクセス権取得部22Aに返す。

【0060】要求者アクセス権取得部22Aでは、アクセス権管理部23から受け取った要求者アクセス権を削除命令アクセス権設定部67で印刷資源削除命令に付加する。そして、印刷資源削除命令部29Aの印刷資源削除命令発行部63Aに印刷装置12Aへの印刷資源削除命令の発行を依頼する。印刷資源削除命令発行部63Aはこれを基に印刷資源削除命令を発行する（ステップS303）。

【0061】この発行された要求者アクセス権付き印刷資源削除命令は、印刷資源削除命令応答部41Aで受信され（ステップS304）、印刷資源アクセス権確認部42に渡される。印刷資源アクセス権確認部42では、要求者アクセス権取得部71Aで印刷資源削除命令から要求者アクセス権を取得する（ステップS305）。また、利用者アクセス権取得部72Aでは印刷装置12Aの磁気ディスク装置38に格納されたアクセス権付き印刷資源39から利用者アクセス権を取得する（ステップS306）。アクセス権確認部73は以上により取得した要求者アクセス権と利用者アクセス権とを照合確認す

Petitioner Apple Inc. - Exhibit 1012, p. 1520

15

る（ステップＳ３０７）。そして、確認の結果、要求者が印刷資源を削除できると判別された場合には（ステップＳ３０８；Ｙ）、印刷資源削除部４３Ａにおいて該当の印刷資源を削除する（ステップＳ３０９）。

【００６２】これに対して、その要求者が該当する印刷資源の削除を許されていない場合には（ステップＳ３０８；Ｎ）、その印刷資源の削除が拒否される（ステップＳ３１０）。いずれの場合にも、印刷資源削除命令応答部４１Ａは要求に対する応答情報を作成し（ステップＳ３１１）、これを回線１３を通じてホストコンピュータ１１Ａ側に送信することになる（ステップＳ３１２）。

【００６３】第３の実施例

【００６４】図１８は本発明の第３の実施例における印刷処理システムの原理的な構成を表わしたものである。この印刷処理システムは、印刷資源を格納したホストコンピュータ１１Ｂと、印刷装置１２Ｂおよびこれらを接続する回線１３とによって構成されている。なお、この印刷処理システムはその構成が第１の実施例のそれと共通した箇所が多いので、回路装置の内容が同一の箇所には図１等と同一の符号を付し、これらの説明を適宜省略する。また、回路装置の内容自体は異なるが、第１の実施例と対応させて説明することが便利であるような回路装置についてはそれらの箇所に用いた符号の末尾に“Ｂ”という符号を付加することにする。

【００６５】ホストコンピュータ１１Ｂは、第１の実施例の印刷資源使用命令部２９の代わりに印刷資源確認命令部２９Ｂを備えている。また、利用者アクセス権設定部２１は印刷資源転送・更新部８１を介して制御部１５Ｂと接続されている。印刷装置１２Ｂは第１の実施例の印刷資源使用命令応答部４１の代わりに印刷資源確認命令応答部４１Ｂを備えている。

【００６６】ここで、印刷資源転送・更新部８１は、印刷資源の転送指示と更新指示を行うようになっている。印刷資源確認命令部２９Ｂは、印刷資源の更新が要求されたとき、アクセス権管理部２３の管理の下で要求者アクセス権を取得し、これを付加した印刷資源確認命令を発行するためのものである。この印刷資源確認命令は回線１３を通じて印刷装置１２Ｂへ送出されるようになっている。

【００６７】一方、ホストコンピュータ１１Ｂから回線１３を通じて送られてくる印刷資源確認命令は印刷資源確認命令応答部４１Ｂで受信され、印刷資源アクセス権確認部４２に送られるようになっている。印刷資源アクセス権確認部４２はこの要求者アクセス権をアクセス権付き印刷資源３９に付けられている利用者アクセス権と比較する。そして、要求者にその更新しようとする印刷資源の利用者アクセスが存在する場合にはその印刷資源の更新を許可する。これ以外の場合には、その印刷資源の更新が許可されない。

【００６８】図１９は、この印刷処理システムで印刷資源が印刷装置側に転送・更新されるときの処理の流れを表わしたものである。アクセス権なし印刷資源５１のうち利用者アクセスの付与が求められたものについては、利用者アクセス権設定部２１によって、アクセス権付き印刷資源２５に変更される。このとき、アクセス権管理部２３がその管理を行う。

16

【００６９】図２０は、利用者アクセス権設定部の具体的な構成を表わしたものである。利用者アクセス権設定部２１は、利用者アクセス権の取得をアクセス権管理部２３に対して要求する利用者アクセス権取得要求部５３と、アクセス権なし印刷資源５１に対して利用者アクセス権を設定する印刷資源アクセス権設定部５４と、これらの制御を行う利用者アクセス権設定制御部５５から構成されている。制御部１５Ｂは、印刷資源転送・更新部８１を介して利用者アクセス権設定制御部５５を制御している。

【００７０】図２１は、アクセス権管理部の具体的な構成を表わしたものである。アクセス権管理部２３は、アクセス権の取得要求を利用者アクセス権設定部２１から受信するアクセス権取得要求受信部５７と、アクセス権の取得要求があったときアクセス権管理テーブル２８Ｂを用いてアクセス権を取得するアクセス権取得部５８と、取得したアクセス権を図２０の利用者アクセス権取得要求部５３に送出するアクセス権送信部５９を有している。アクセス権管理制御部６１は、制御部１５Ｂの制御の下で、これら各部の制御を行うようになっている。

【００７１】すなわち、アクセス権管理部２３はアクセス権なし印刷資源５１についてアクセス権の付加が要求されたときには、どのような印刷資源についてはどのようなアクセスを付与するかを示したアクセス権管理テーブル２８Ｂを参照して該当するアクセス権を読み出し、これをその印刷資源に付加してアクセス権付き印刷資源２５を作成することになる。このアクセス権付き印刷資源２５は印刷資源送信部２６から送出され、印刷装置１２Ｂの印刷資源受信部３６に受信される。そして、印刷資源転送時には印刷資源格納部３７によってアクセス権付き印刷資源３９として磁気ディスク装置３８（図１８）内に格納される。これに対して印刷資源更新時には、印刷資源更新部８３によって更新され、その内容がアクセス権付き印刷資源３９として磁気ディスク装置３８内に格納されることになる。

【００７２】図２２は、印刷資源の更新時における印刷処理システムの処理の流れを表わしたものである。印刷資源の更新を行わせるために、ホストコンピュータ１１Ｂで印刷資源更新要求が発生すると、要求者アクセス権取得部２２Ｂはアクセス権管理部２３の管理の下で要求者アクセス権を取得する。この要求者アクセス権は、印刷資源確認命令部２９Ｂに送られ、その印刷資源確認命令発行部６３Ｂで印刷資源確認命令が発行される。この印刷資源確認命令は、印刷資源確認命令送信部６４から

Petitioner Apple Inc. - Exhibit 1012, p. 1521

印刷装置１２Ｂへ送信される。

【００７３】図２３は、要求者アクセス権取得部の具体的な構成を表わしたものである。要求者アクセス権取得部２２Ｂは要求者アクセス権の取得をアクセス権管理部２３に対して要求する要求者アクセス権取得要求部６６と、取得された要求者アクセス権を印刷資源確認命令に付加して印刷資源確認命令部２９Ｂに送出するための確認命令アクセス権設定部６７を備えている。要求者アクセス権取得制御部６８は、制御部１５Ｂの制御の下でこれら要求者アクセス権取得要求部６６および確認命令アクセス権設定部６７Ｂの制御を行うようになっている。

【００７４】図２２に戻って説明を続ける。ホストコンピュータ１１Ｂの印刷資源確認命令送信部６４Ｂから送信された印刷資源確認命令は、印刷装置１２Ｂの印刷資源確認命令応答部４１Ｂ内の印刷資源確認命令受信部７１Ｂで受信され、印刷資源アクセス権確認部４２に送られる。印刷資源アクセス権確認部４２は、アクセス権付き印刷資源３９を用いてアクセス権の確認を行い、アクセス権がないとされた場合には印刷資源確認命令応答部４１Ｂ内の印刷資源更新応答部７２Ｂを介してホストコンピュータ１１Ｂへそれを報告する。また、印刷資源アクセス権確認部４２はその印刷資源のアクセス権があると判別した場合には、印刷資源更新応答部７２Ｂを介してホストコンピュータ１１Ｂへ更新する印刷資源の転送を要求する。

【００７５】図２４は、印刷資源アクセス権確認部の具体的な構成を表わしたものである。印刷資源アクセス権確認部４２は、印刷資源確認命令応答部４１Ｂを介して印刷資源の更新要求者のアクセス権を取得する要求者アクセス権取得部７１Ｂと、アクセス権付き印刷資源３９を用いて利用者アクセス権を取得する利用者アクセス権取得部７２Ｂの２つの取得部を備えている。アクセス権確認部７３は、これら２種類のアクセス権を比較し、印刷資源についてのアクセス権が存在するかどうかの確認を行う。アクセス権確認結果送信部７４はこの結果を印刷資源確認命令応答部４１Ｂを介してホストコンピュータ１１Ｂに送信することになる。印刷資源アクセス権確認部４２内の印刷資源アクセス権確認制御部７５は、印刷装置１２Ｂ側の制御部３１Ｂによって制御され各部７１Ｂ～７４の制御を行う。

【００７６】なお、先の第１の実施例ではその図８で印刷処理システムにおける印刷資源転送時の処理の流れを表わしたが第３の実施例でもこの点について実質的な変更がないので、これについての説明を省略する。

【００７７】図２５は、転送されてきた印刷資源を更新する場合の処理の流れを表わしたものである。印刷資源の更新要求が発生すると（ステップＳ４０１；Ｙ）、要求者アクセス権取得部２２Ｂはその要求者アクセス権取得要求部６６にてアクセス権管理部２３に対して要求者アクセス権の取得を要求する。アクセス権管理部２３はそのアクセス権取得要求受信部５７でこの要求を受信し、アクセス権取得部５８でアクセス権管理テーブル２８Ｂを用いて該当更新要求者に対する要求者アクセス権を取得する（ステップＳ４０２）。そしてアクセス権送信部５９から要求者アクセス権取得部２２Ｂにこれを返信して、制御を要求者アクセス権取得部２２Ｂに返す。

【００７８】要求者アクセス権取得部２２Ｂでは、アクセス権管理部２３から受け取った要求者アクセス権を確認命令アクセス権設定部６７Ｂで印刷資源確認命令に付加する。そして、印刷資源確認命令部２９Ｂの印刷資源確認命令発行部６３Ｂに印刷装置１２Ｂへの印刷資源確認命令の発行を依頼する。印刷資源確認命令発行部６３Ｂはこれを基に印刷資源確認命令を発行する（ステップＳ４０３）。

【００７９】この発行された要求者アクセス権付き印刷資源確認命令は、印刷資源確認命令応答部４１Ｂで受信され（ステップＳ４０４）、印刷資源アクセス権確認部４２に渡される。印刷資源アクセス権確認部４２では、要求者アクセス権取得部７１Ｂで印刷資源確認命令から要求者アクセス権を取得する（ステップＳ４０５）。また、利用者アクセス権取得部７２Ｂでは印刷装置１２Ｂの磁気ディスク装置３８に格納されたアクセス権付き印刷資源３９から利用者アクセス権を取得する（ステップＳ４０６）。アクセス権確認部７３は以上により取得した要求者アクセス権と利用者アクセス権とを照合確認する（ステップＳ４０７）。そして、確認の結果、要求者が印刷資源を更新できると判別された場合には（ステップＳ４０８；Ｙ）、印刷資源の更新を許可する（ステップＳ４０９）。

【００８０】これに対して、その要求者が該当する印刷資源の更新を許されていない場合には（ステップＳ４０８；Ｎ）、その印刷資源の更新が拒否される（ステップＳ４１０）。印刷資源の更新が拒否された場合には、要求に対する応答情報を作成してホストコンピュータ１１Ｂへ報告し（ステップＳ４１１）、処理を終了させる（エンド）。

【００８１】印刷資源の更新が許可された場合には（ステップＳ４０９）、この要求に対する応答情報が作成されてアクセス権確認結果送信部７４からホストコンピュータ１１Ｂへの報告が行われ（ステップＳ４１２）、印刷資源転送・更新部８１にて該当する印刷資源の更新が依頼される。これにより、印刷資源の更新が行われることになる（ステップＳ４１３）。

【００８２】なお、以上説明した第１～第３の実施例ではアクセス権管理テーブルから要求者アクセス権と利用者アクセス権双方を取得するようにしたが、２つのテーブルを用意し、取得先を異ならせるようにしてもよい。

【００８３】また、実施例では印刷資源の印刷時の使用と、印刷資源自体の削除あるいは更新を例に挙げて説明したが、これ以外の印刷資源の処理についても本発明が

Petitioner Apple Inc. - Exhibit 1012, p. 1522

19

適用されることはもちろんである。

【0084】

【発明の効果】以上説明したように請求項1記載の発明によれば、ホストコンピュータが必要な印刷資源を印刷装置に転送してその受信側印刷資源格納手段に格納された印刷資源を処理させるようにした印刷処理システムにおいて、印刷資源には利用者アクセス権を付けて印刷装置に転送するようにし、印刷資源の処理の要求があったときにはその要求者のアクセス権を印刷装置に送出するようにした。したがって、印刷装置側ではこれらのアクセス権を照合するだけで該当する印刷資源の処理が妥当であるかどうかを判別することができ、アクセス権を持たない第三者の不適当な要求を拒絶することができる。これにより、第三者の印刷資源処理の乱用を防止し、印刷資源適切な保護が可能になる。

【0085】また請求項2記載の発明によれば、ホストコンピュータが必要な印刷資源を印刷装置に転送してその受信側印刷資源格納手段に格納された印刷資源を印刷のために使用させるようにした印刷処理システムにおいて、印刷資源には利用者アクセス権を付けて印刷装置に転送するようにし、印刷資源の使用の要求があったときにはその要求者のアクセス権を印刷装置に送出するようにした。したがって、印刷装置側ではこれらのアクセス権を照合するだけで該当する印刷資源の使用が妥当であるかどうかを判別することができ、アクセス権を持たない第三者の不適当な要求を拒絶することができる。これにより、第三者の印刷資源利用の乱用を防止し、印刷資源適切な保護が可能になる。

【0086】更に請求項3記載の発明によれば、ホストコンピュータが必要な印刷資源を印刷装置に転送してその受信側印刷資源格納手段に格納された印刷資源を必要に応じて削除させるようにした印刷処理システムにおいて、印刷資源には利用者アクセス権を付けて印刷装置に転送するようにし、印刷資源の削除の要求があったときにはその要求者のアクセス権を印刷装置に送出するようにした。したがって、印刷装置側ではこれらのアクセス権を照合するだけで該当する印刷資源の削除が妥当であるかどうかを判別することができ、アクセス権を持たない第三者の不適当な要求を拒絶することができる。これにより、第三者の印刷資源利用の乱用を防止し、印刷資源適切な保護が可能になる。

【0087】また請求項4記載の発明によれば、ホストコンピュータが必要な印刷資源を印刷装置に転送してその受信側印刷資源格納手段に格納された印刷資源を必要に応じて更新させるようにした印刷処理システムにおいて、印刷資源には利用者アクセス権を付けて印刷装置に転送するようにし、印刷資源の更新の要求があったときにはその要求者のアクセス権を印刷装置に送出するようにした。したがって、印刷装置側ではこれらのアクセス権を照合するだけで該当する印刷資源の更新が妥当であるかどうかを判別することができ、アクセス権を持たない第三者の不適当な要求を拒絶することができる。これにより、第三者の印刷資源利用の乱用を防止し、印刷資源適切な保護が可能になる。

20

【図面の簡単な説明】

【図1】　本発明の第1の実施例における印刷処理システムの原理的な構成を表わしたブロック図である。

【図2】　この印刷処理システムで印刷資源が印刷装置側に転送されるときの処理の流れを表わした説明図である。

【図3】　第1の実施例の利用者アクセス権設定部の具体的な構成を表わしたブロック図である。

【図4】　第1の実施例のアクセス権管理部の具体的な構成を表わしたブロック図である。

【図5】　印刷資源の使用時における印刷処理システムの処理の流れを表わした説明図である。

【図6】　第1の実施例の要求者アクセス権取得部の具体的な構成を表わしたブロック図である。

【図7】　第1の実施例の印刷資源アクセス権確認部の具体的な構成を表わしたブロック図である。

【図8】　第1の実施例の印刷処理システムにおける印刷資源転送時の処理の流れを表わした流れ図である。

【図9】　第1の実施例で転送されてきた印刷資源を使用して印刷情報の印刷を行う場合の処理の流れを表わした流れ図である。

【図10】　本発明の第2の実施例における印刷処理システムの原理的な構成を表わしたブロック図である。

【図11】　第2の実施例の印刷処理システムで印刷資源が印刷装置側に転送されるときの処理の流れを表わした説明図である。

【図12】　第2の実施例の利用者アクセス権設定部の具体的な構成を表わしたブロック図である。

【図13】　第2の実施例のアクセス権管理部の具体的な構成を表わしたブロック図である。

【図14】　印刷資源の削除時における第2の実施例の印刷処理システムの処理の流れを表わした説明図である。

【図15】　第2の実施例の要求者アクセス権取得部の具体的な構成を表わしたブロック図である。

【図16】　第2の実施例の印刷資源アクセス権確認部の具体的な構成を表わしたブロック図である。

【図17】　第2の実施例で転送されてきた印刷資源を削除する場合の処理の流れを表わした流れ図である。

【図18】　本発明の第3の実施例における印刷処理システムの原理的な構成を表わしたブロック図である。

【図19】　この印刷処理システムで印刷資源が印刷装置側に転送・更新されるときの処理の流れを表わした説明図である。

【図20】　第3の実施例の利用者アクセス権設定部の具体的な構成を表わしたブロック図である。

Petitioner Apple Inc. - Exhibit 1012, p. 1523

21

【図２１】　第３の実施例のアクセス権管理部の具体的な構成を表わしたブロック図である。

【図２２】　印刷資源の更新時における第３の実施例の印刷処理システムの処理の流れを表わした説明図である。

【図２３】　第３の実施例の要求者アクセス権取得部の具体的な構成を表わしたブロック図である。

【図２４】　第３の実施例の印刷資源アクセス権確認部の具体的な構成を表わしたブロック図である。

【図２５】　第３の実施例で転送されてきた印刷資源を更新する場合の処理の流れを表わした流れ図である。

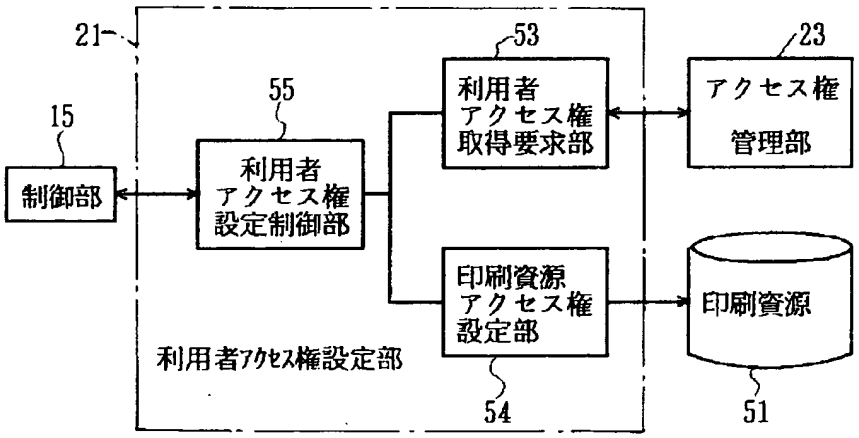
【符号の説明】

１１、１１Ａ、１１Ｂ…ホストコンピュータ、１２、１２Ａ、１２Ｂ…印刷装置、１３…回線、１５、１５Ａ、１５Ｂ…（ホストコンピュータの）制御部、１６…ＣＰＵ、１７…ＲＯＭ、１８…ＲＡＭ、１９…端末装置、２

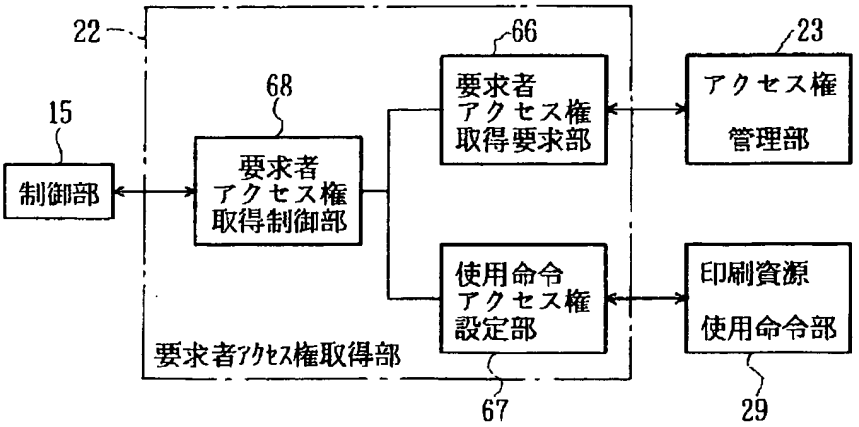
22

１…利用者アクセス権設定部、２２…要求者アクセス権設定部、２３…アクセス権管理部、２４、３８…磁気ディスク装置、２５…アクセス権付き印刷資源、２６…印刷資源送信部、２８、２８Ａ、２８Ｂ…アクセス権管理テーブル、２９…印刷資源使用命令部、２９Ａ…印刷資源削除命令部、２９Ｂ…印刷資源確認命令部、３１、３１Ａ、３１Ｂ…（印刷装置の）制御部、３６…印刷資源受信部、３７…印刷資源格納部、３９…アクセス権付き印刷資源、４１…印刷資源使用命令応答部、４１Ａ…印刷資源削除命令応答部、４１Ｂ…印刷資源確認命令応答部、４２…印刷資源アクセス権確認部、４３…印刷処理部、４３Ａ…印刷資源削除部、５１…アクセス権なし印刷資源、７１…要求者アクセス権取得部、７２…利用者アクセス権取得部、８１…印刷資源転送・更新部、８３…印刷資源更新部

【図３】

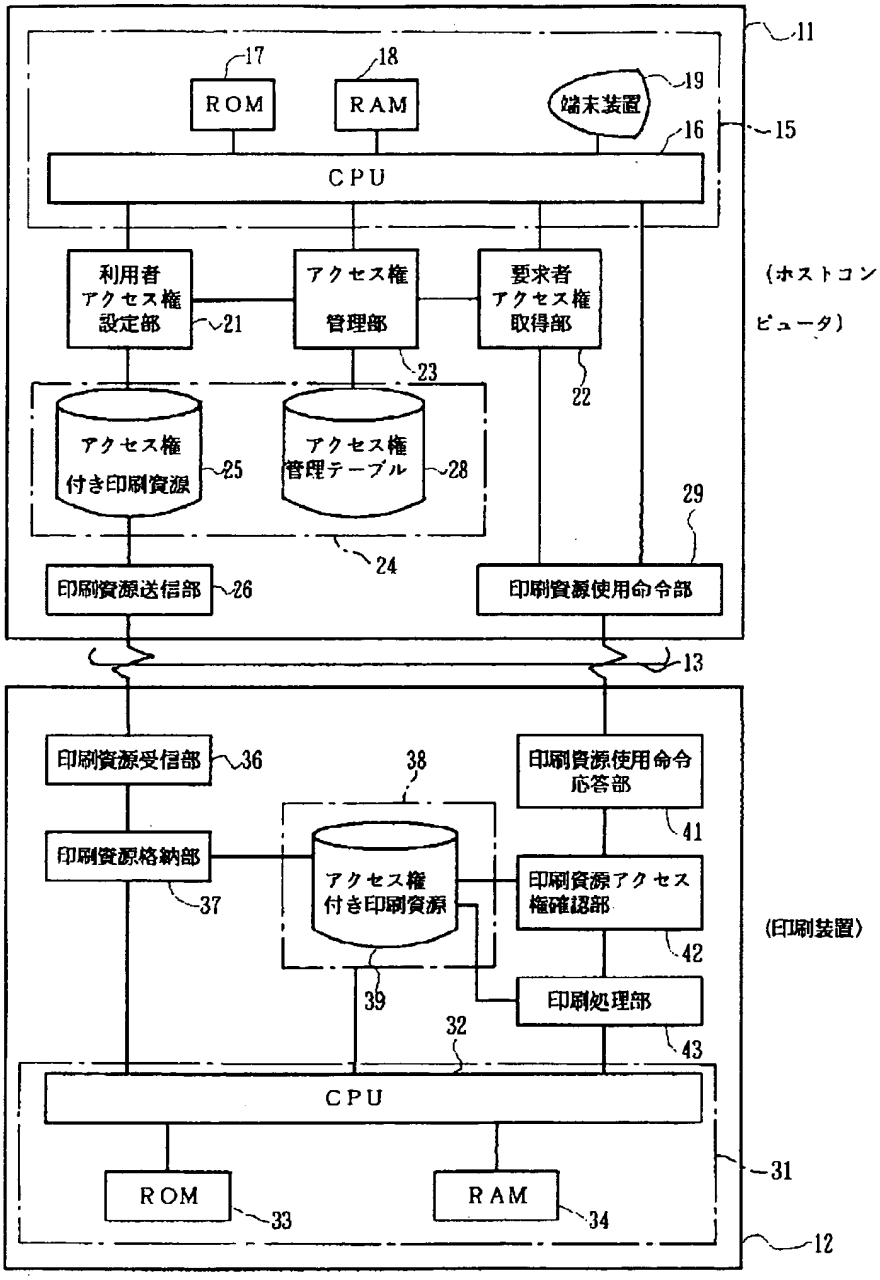


【図６】



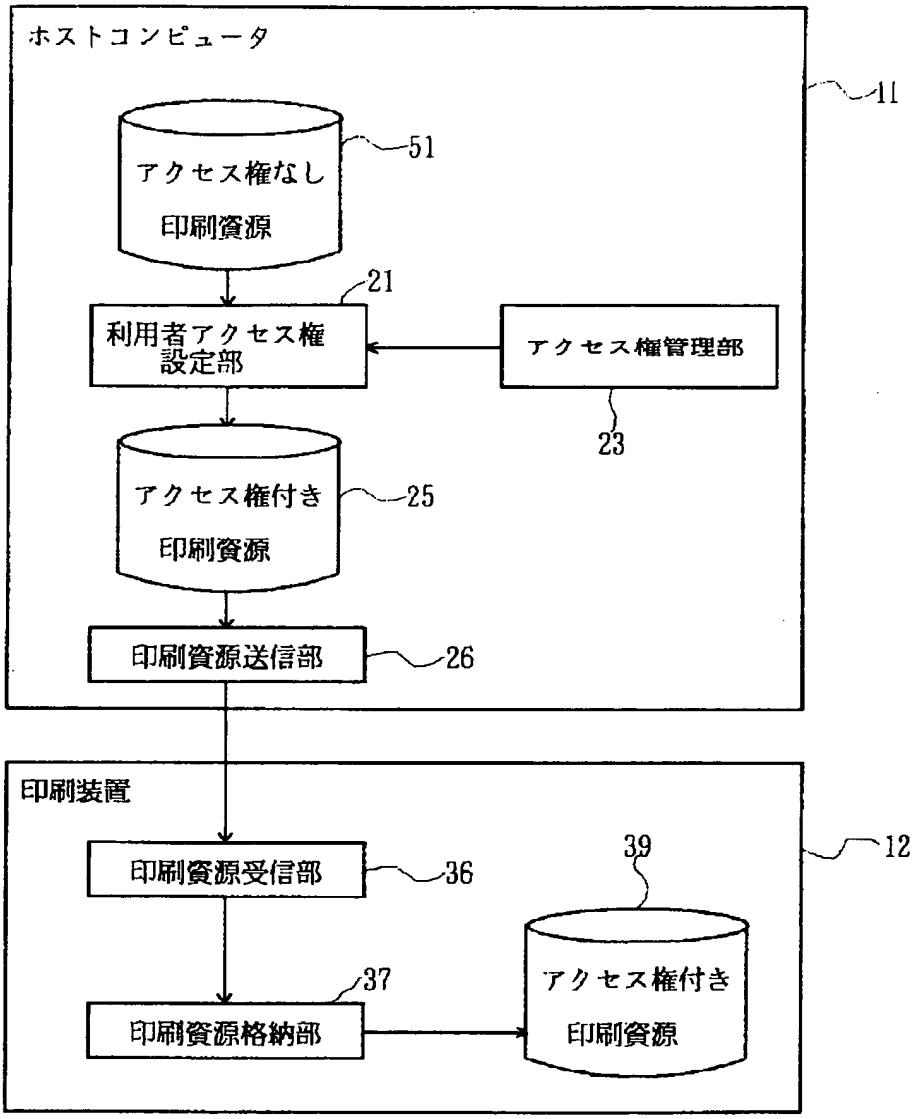
Petitioner Apple Inc. - Exhibit 1012, p. 1524

【図1】



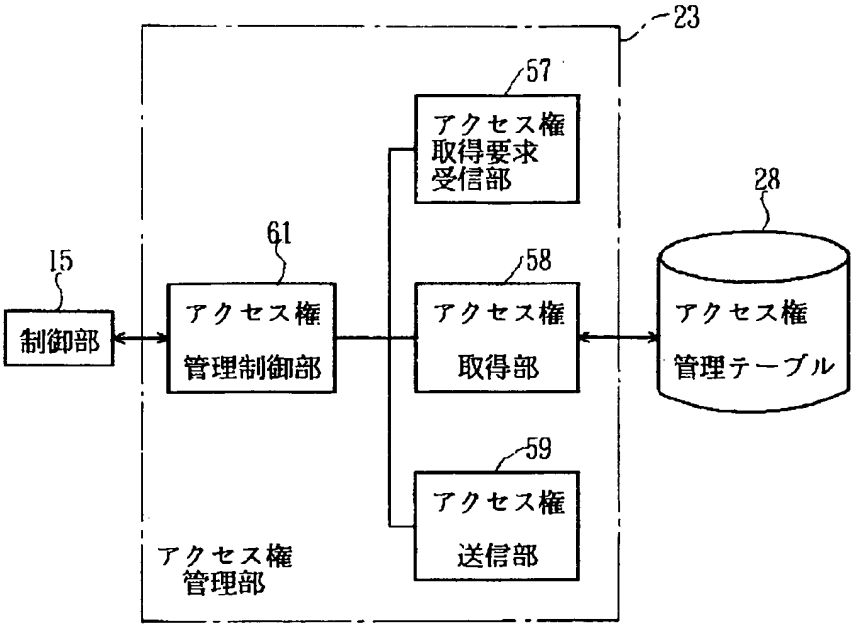
Petitioner Apple Inc. - Exhibit 1012, p. 1525

【図2】

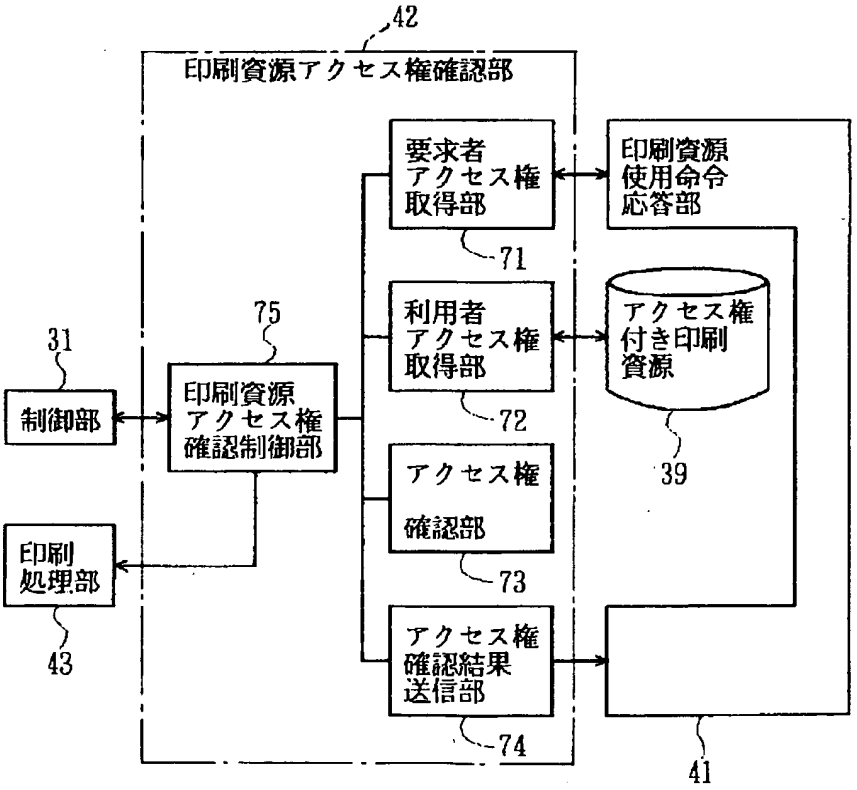


Petitioner Apple Inc. - Exhibit 1012, p. 1526

【図4】

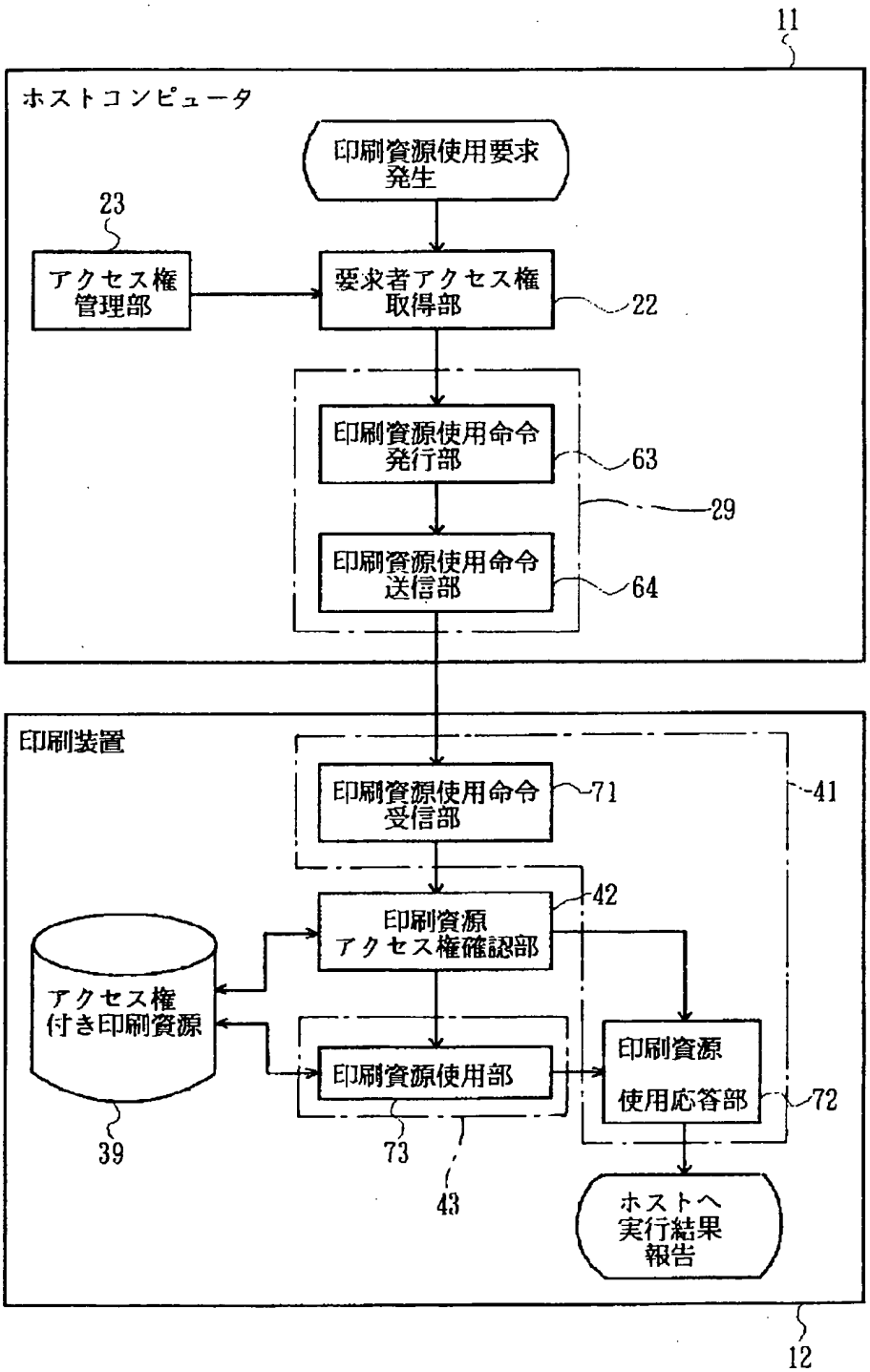


【図7】



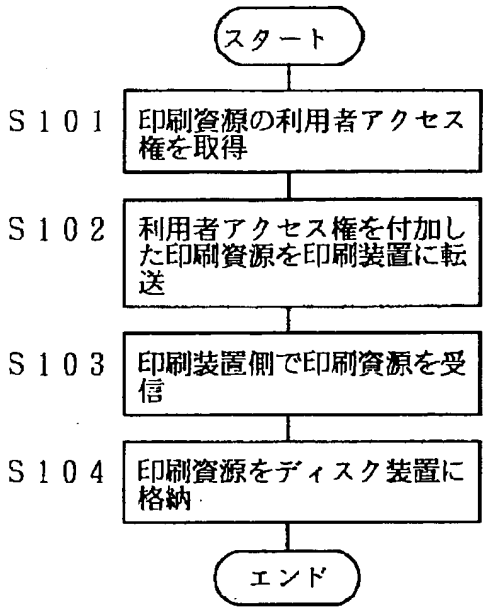
Petitioner Apple Inc. - Exhibit 1012, p. 1527

【図5】

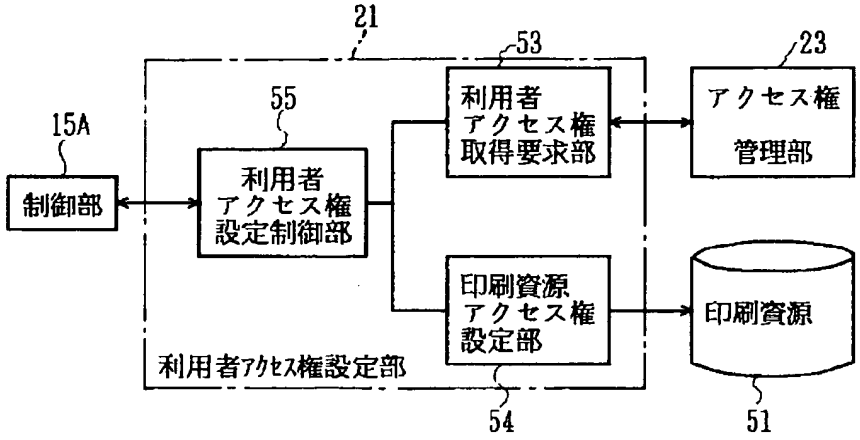


Petitioner Apple Inc. - Exhibit 1012, p. 1528

【図8】

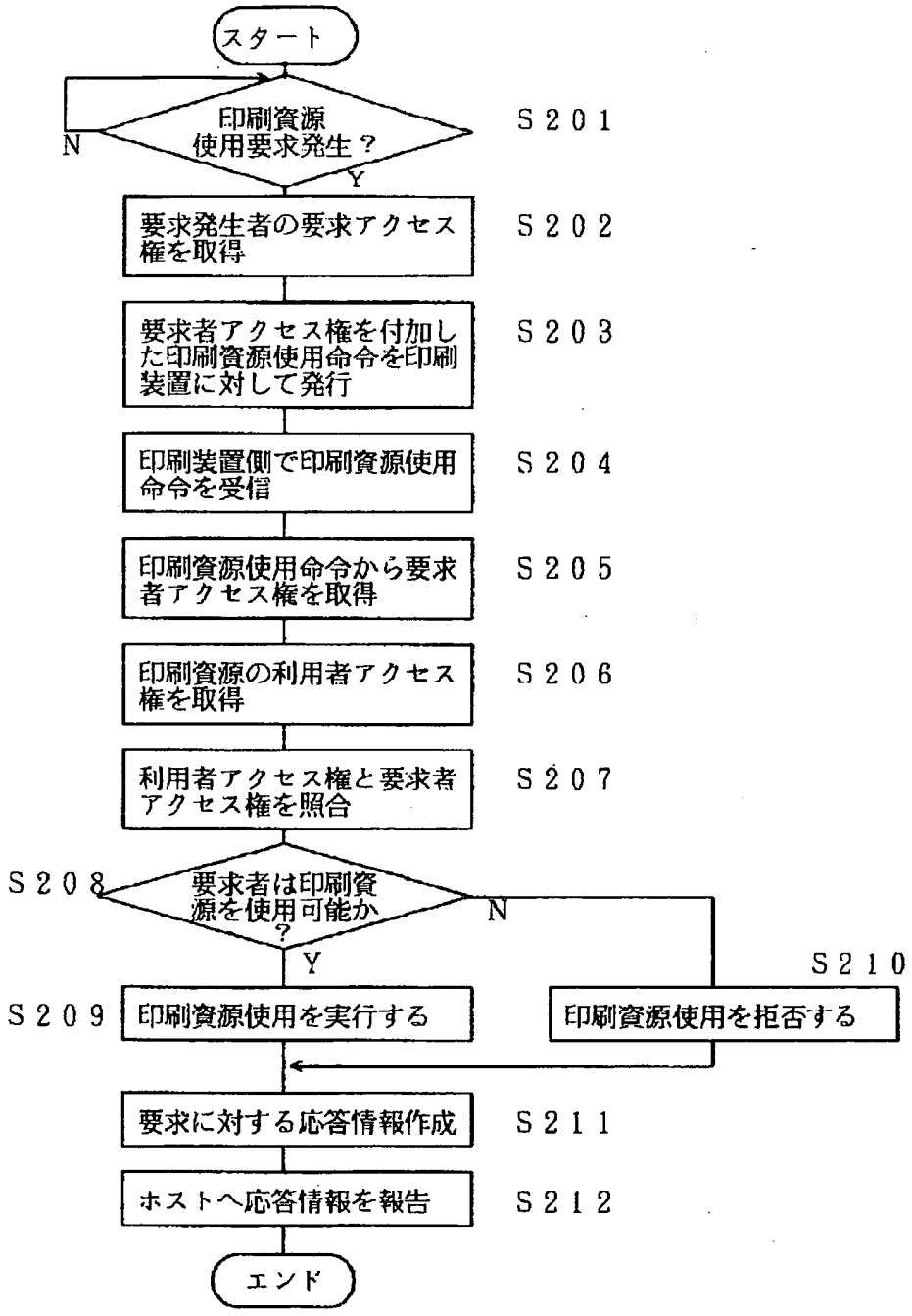


【図12】



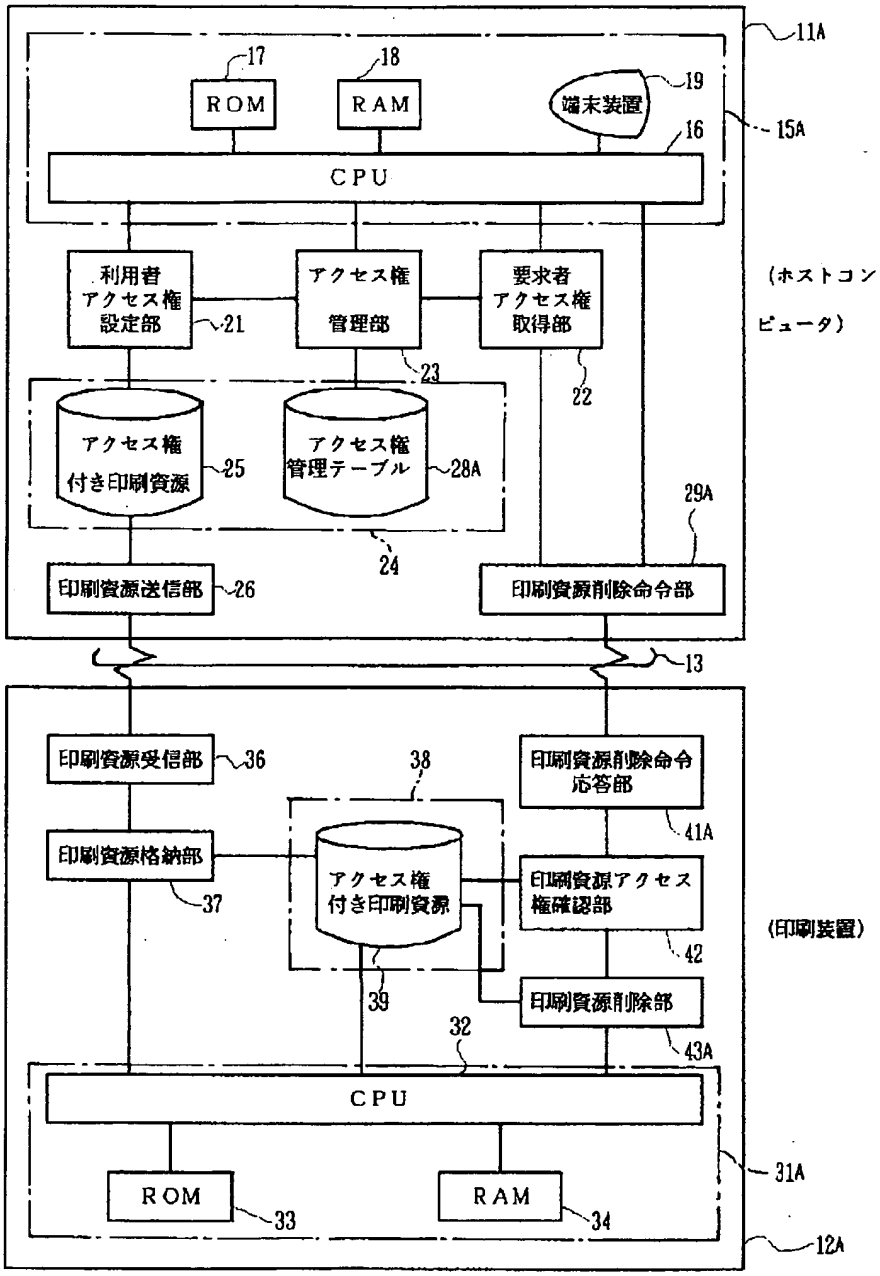
Petitioner Apple Inc. - Exhibit 1012, p. 1529

【図9】



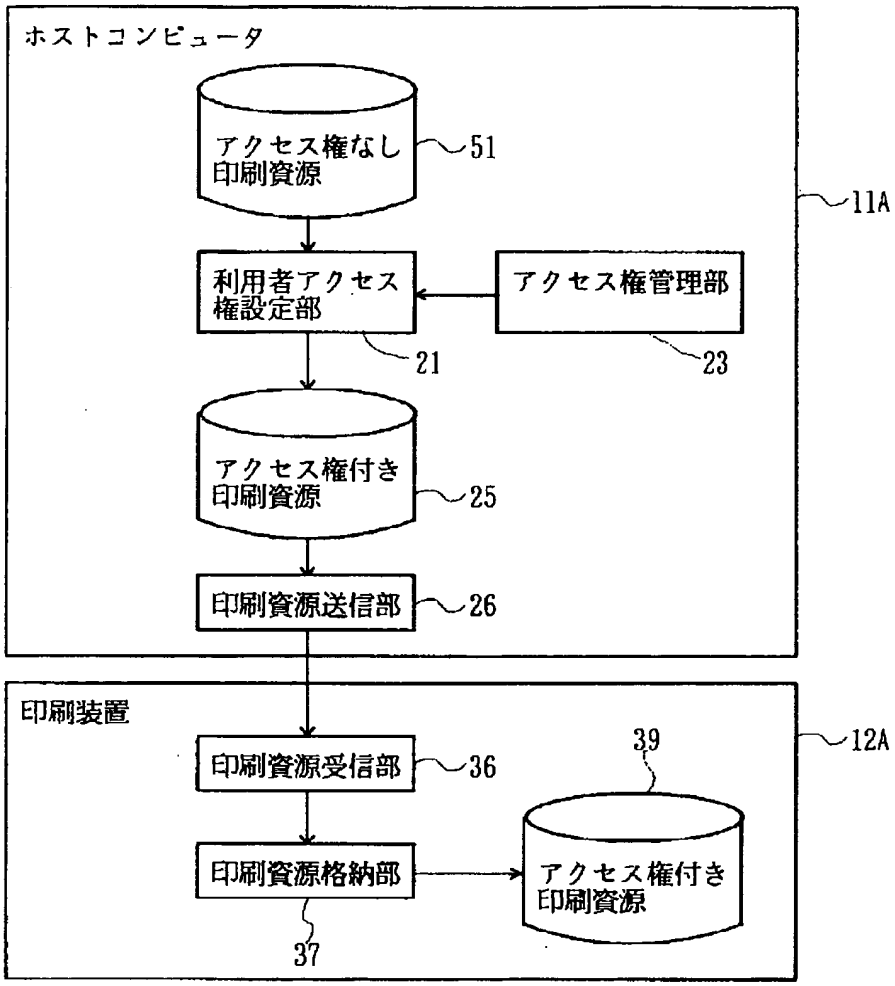
Petitioner Apple Inc. - Exhibit 1012, p. 1530

【図10】

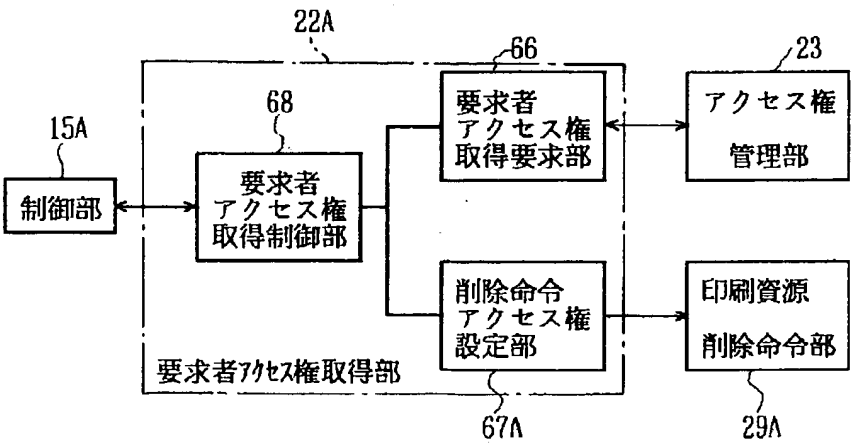


Petitioner Apple Inc. - Exhibit 1012, p. 1531

【図１１】

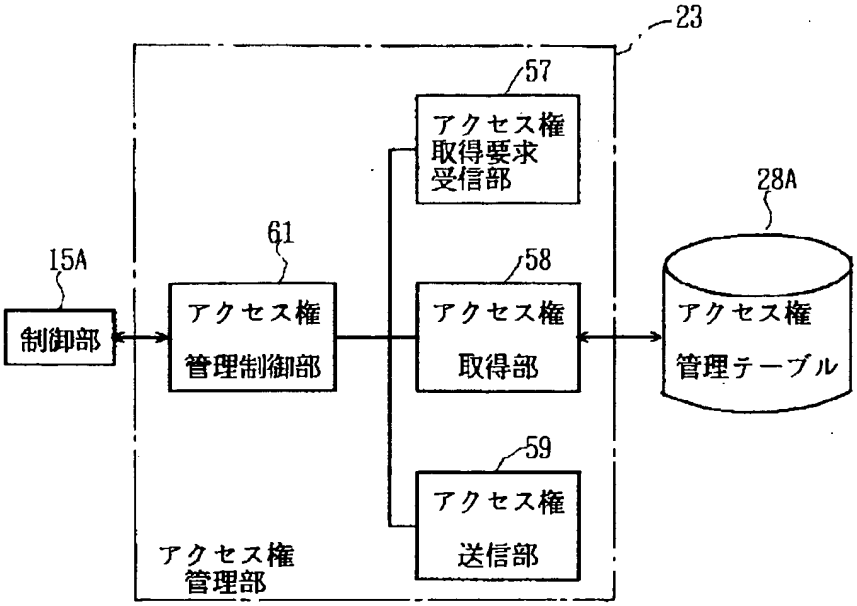


【図１５】

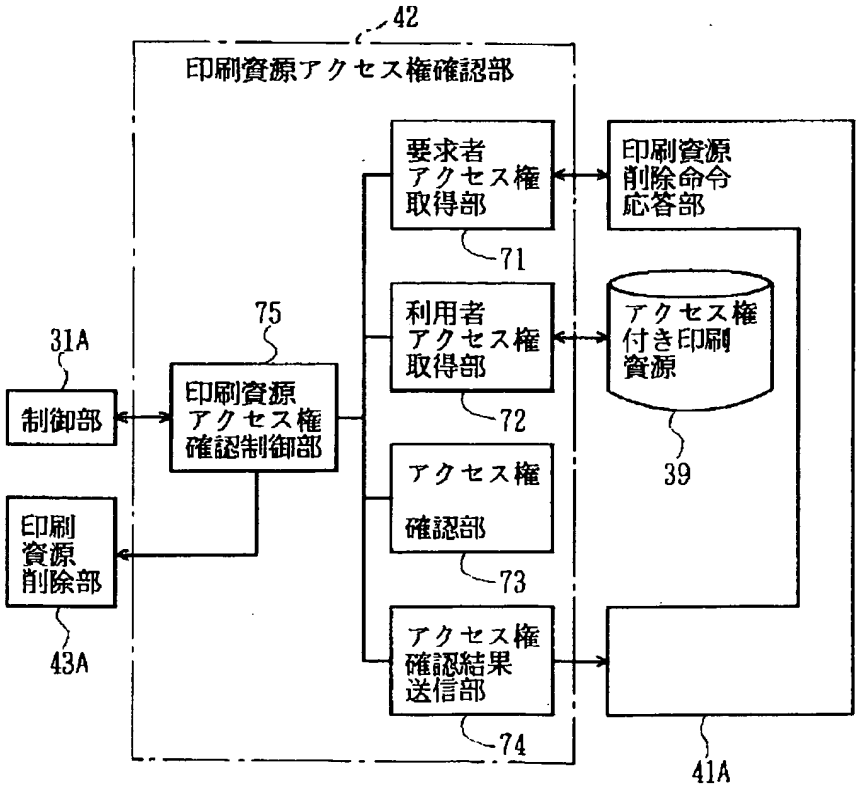


Petitioner Apple Inc. - Exhibit 1012, p. 1532

【図１３】

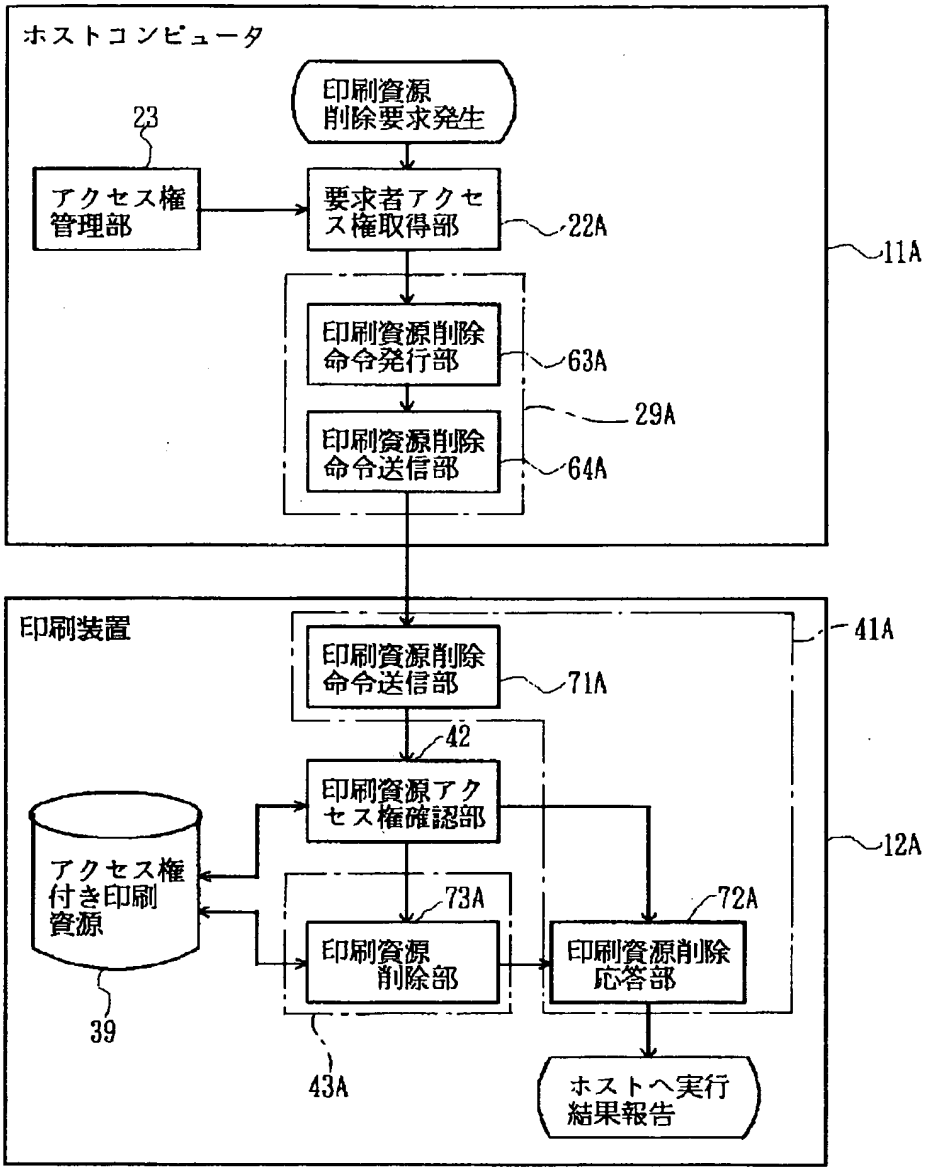


【図１６】



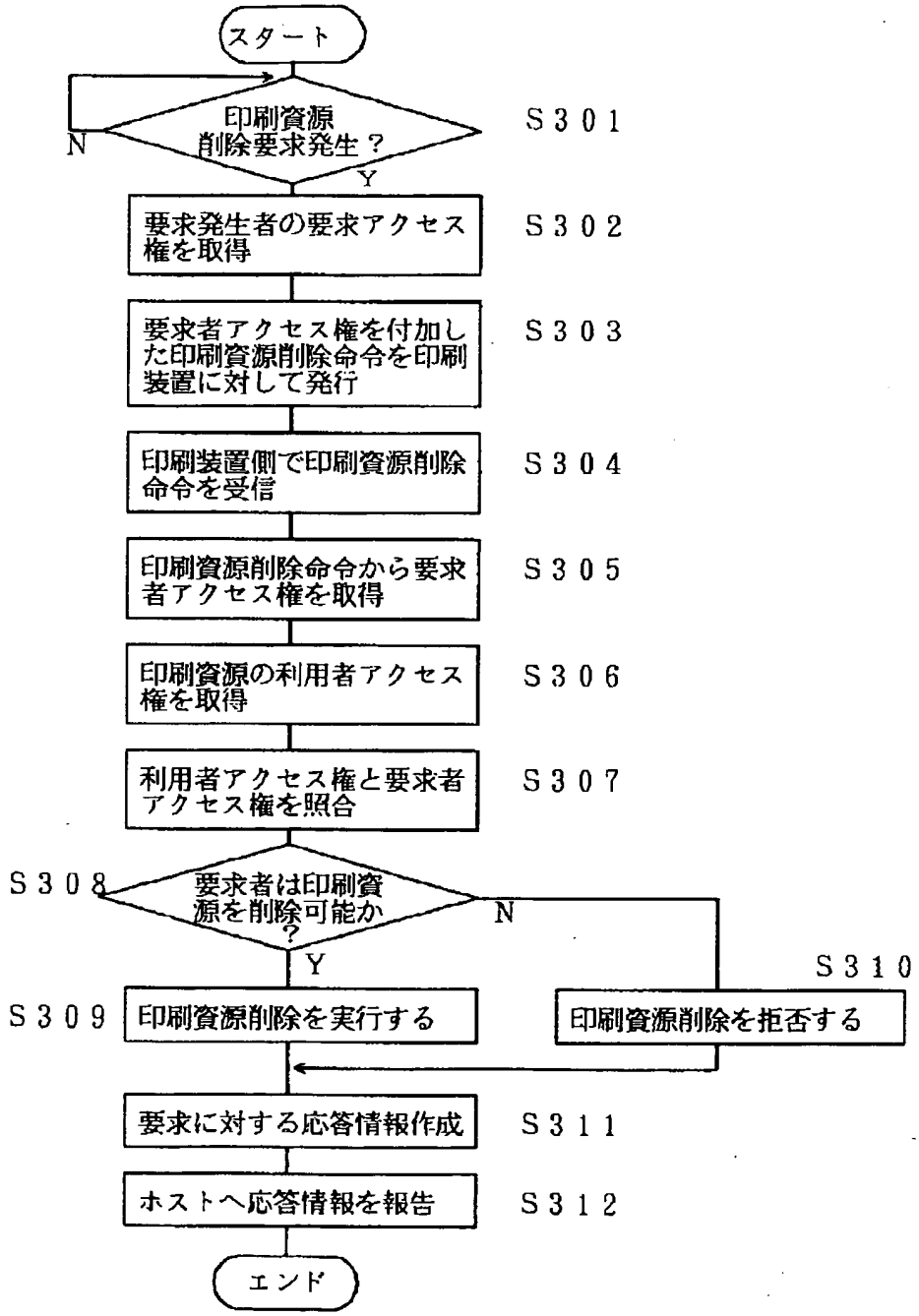
Petitioner Apple Inc. - Exhibit 1012, p. 1533

【図14】



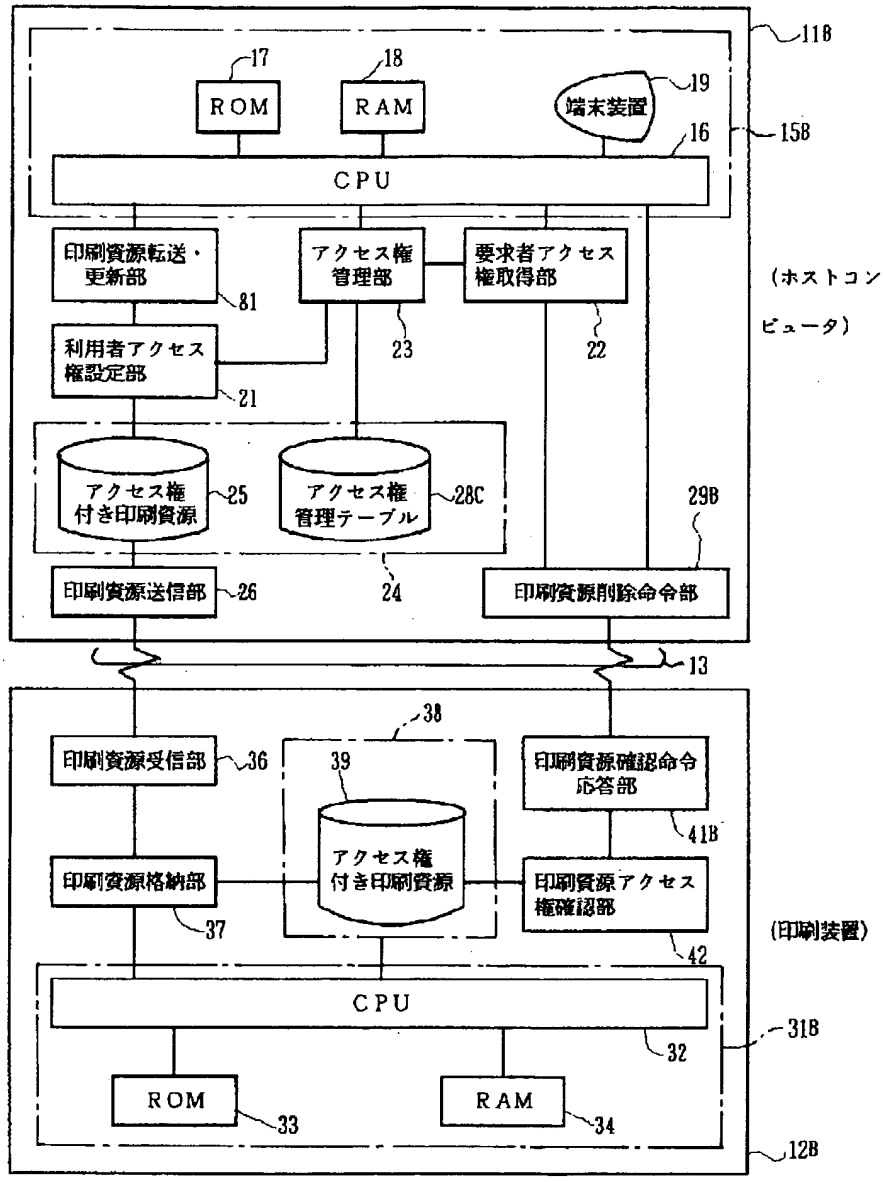
Petitioner Apple Inc. - Exhibit 1012, p. 1534

【図１７】



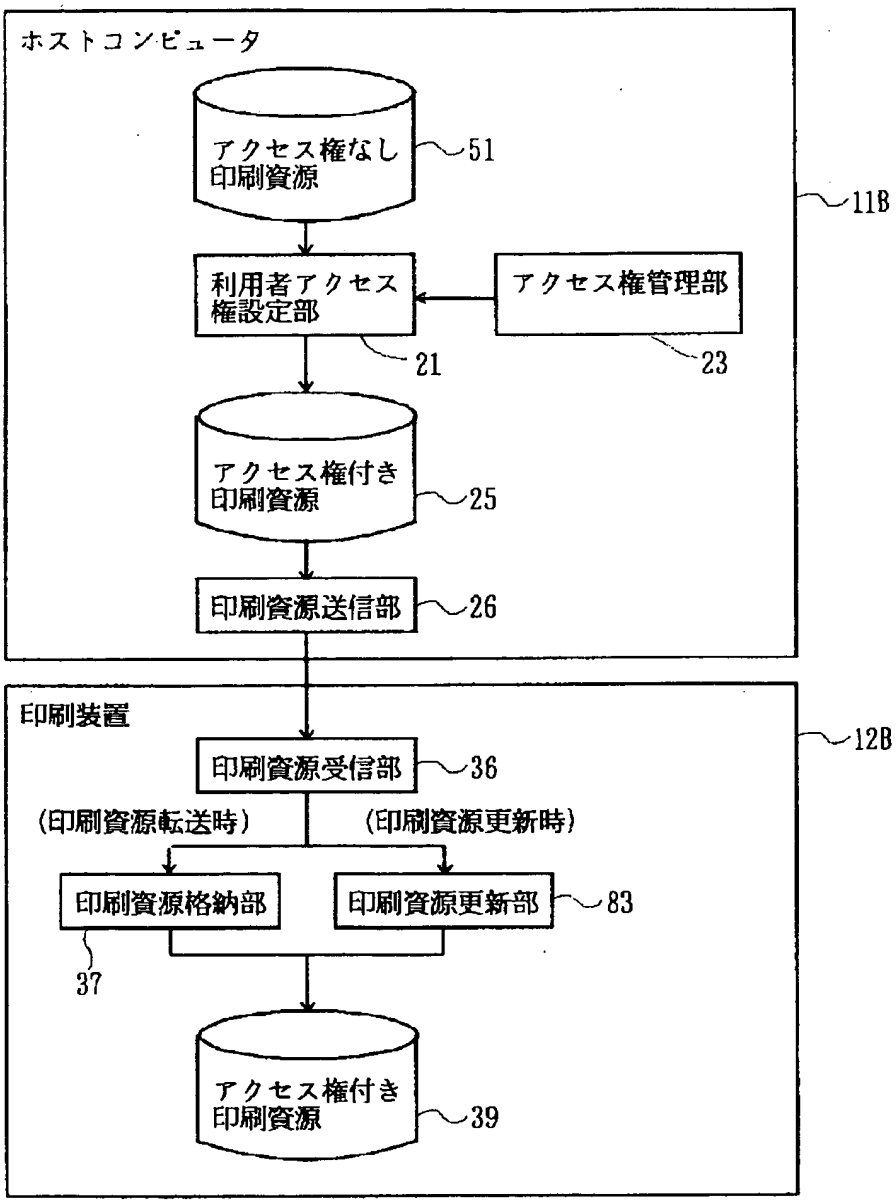
Petitioner Apple Inc. - Exhibit 1012, p. 1535

【図18】



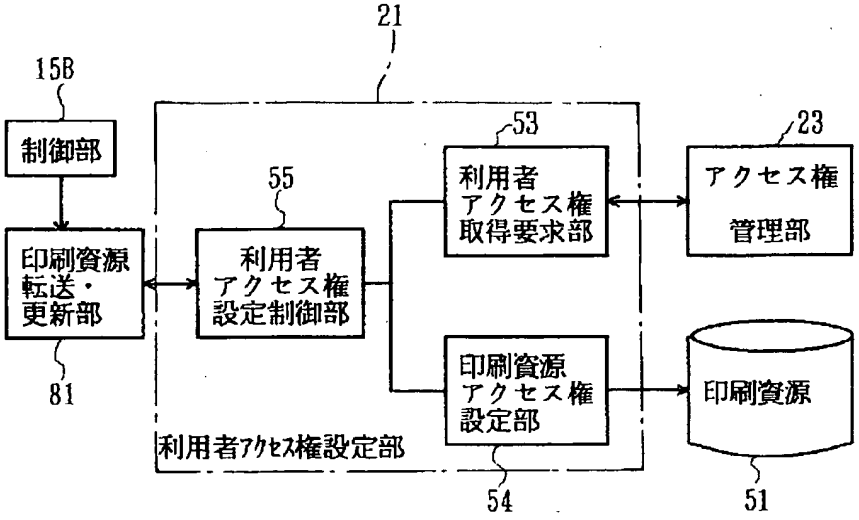
Petitioner Apple Inc. - Exhibit 1012, p. 1536

【図19】

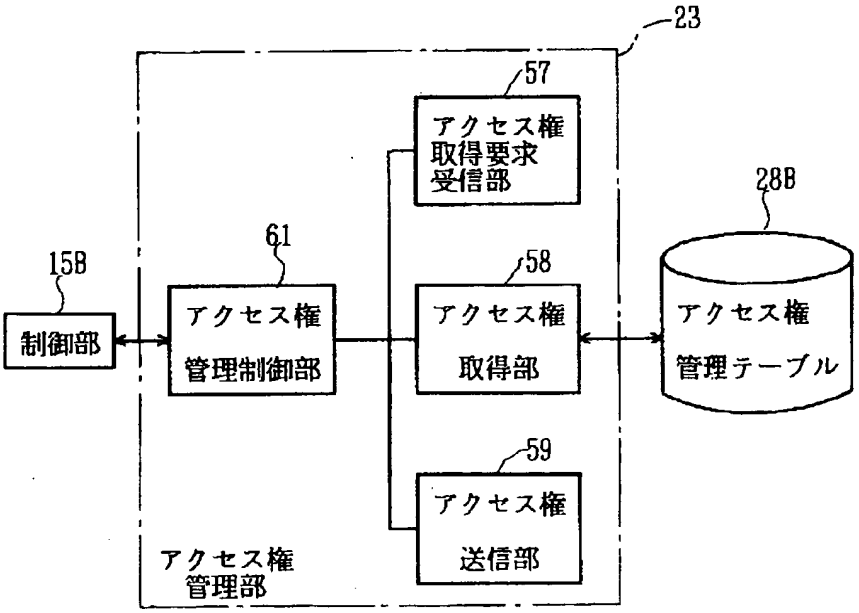


Petitioner Apple Inc. - Exhibit 1012, p. 1537

【図２０】

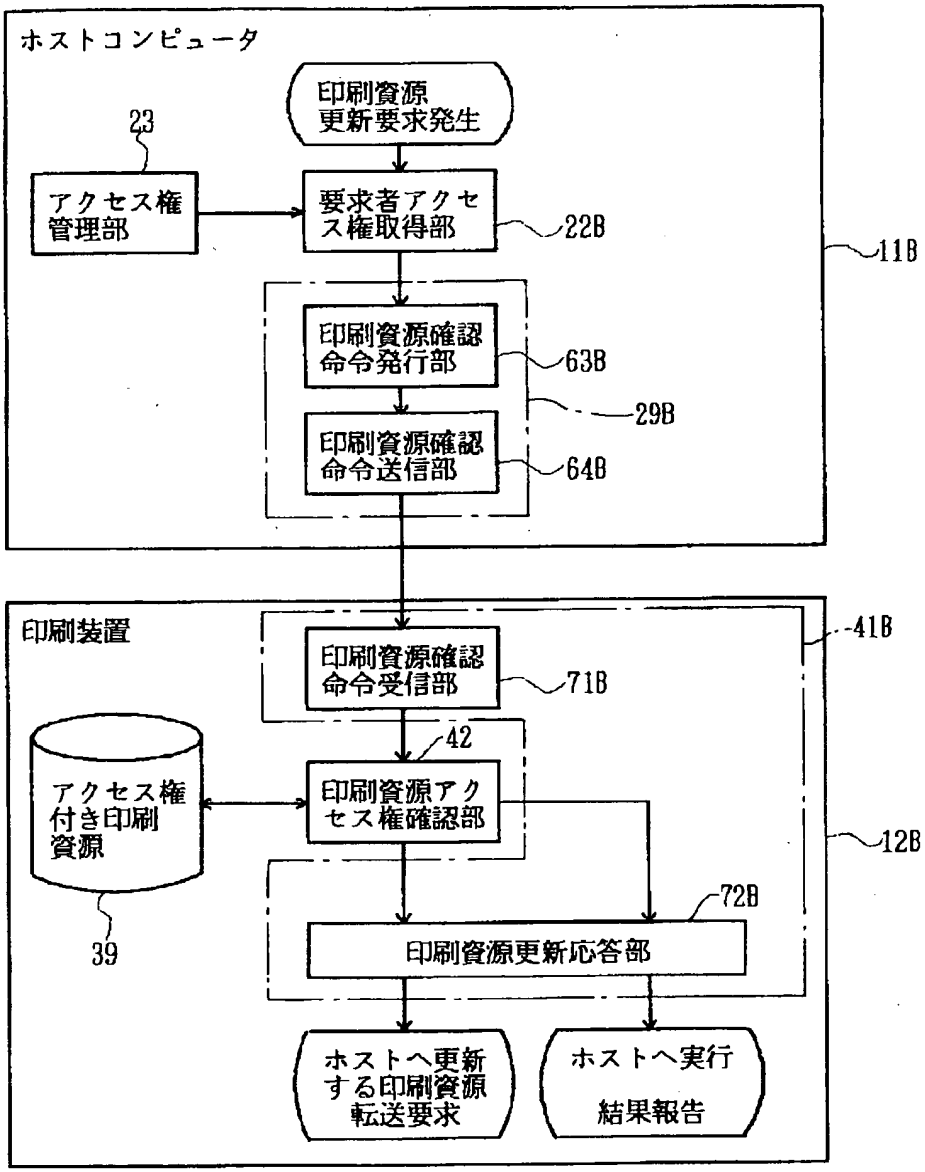


【図２１】



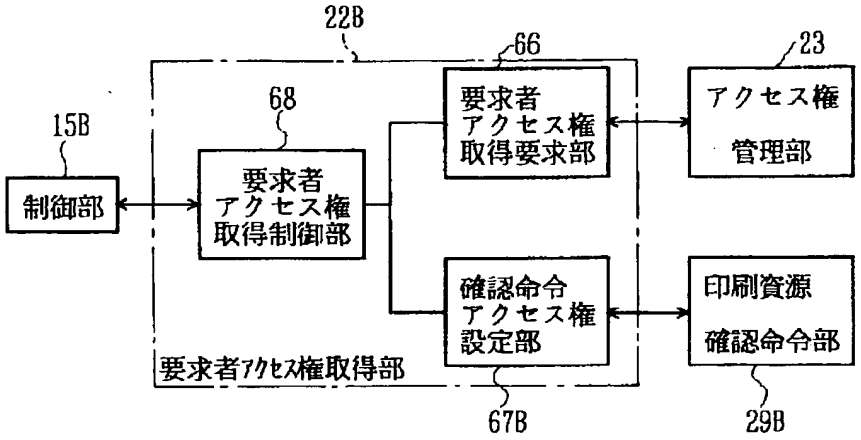
Petitioner Apple Inc. - Exhibit 1012, p. 1538

【図22】

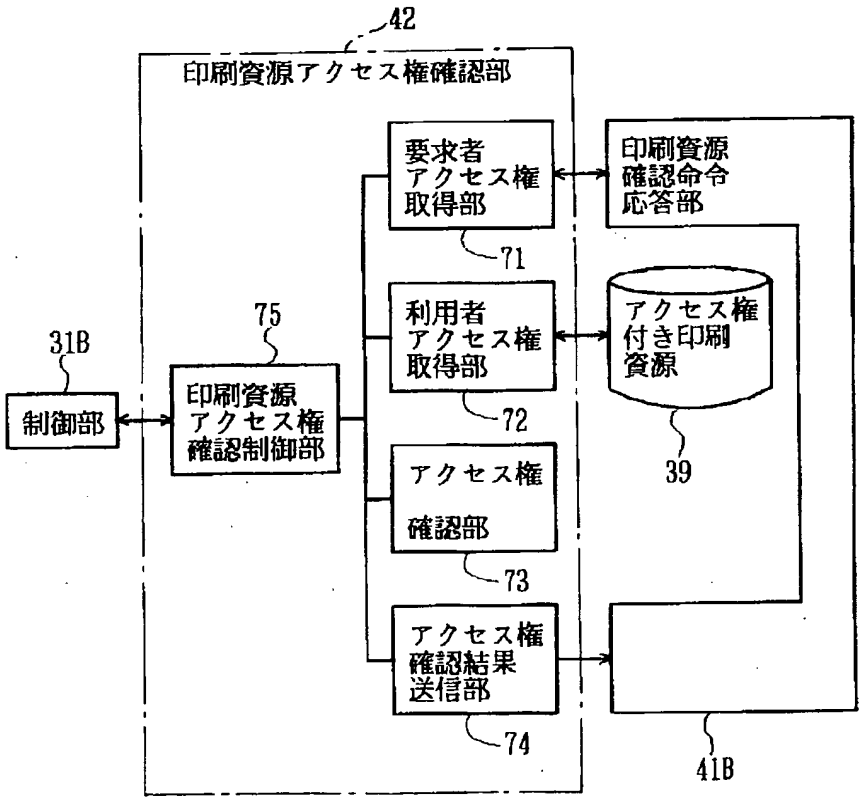


Petitioner Apple Inc. - Exhibit 1012, p. 1539

【図２３】

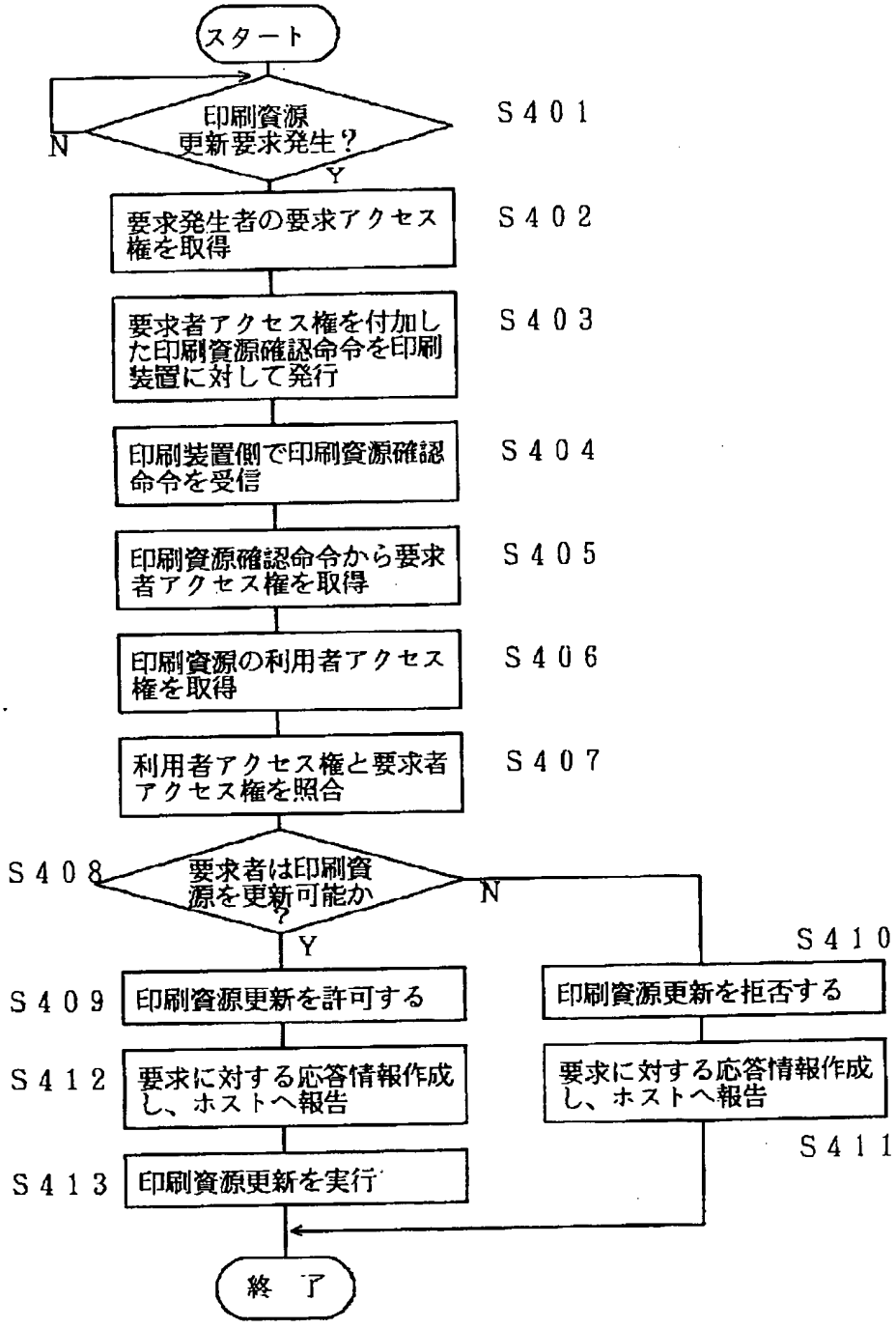


【図２４】



Petitioner Apple Inc. - Exhibit 1012, p. 1540

【図25】



Petitioner Apple Inc. - Exhibit 1012, p. 1541

Requested Patent: JP6215010A

Title: INFORMATION ACQUIRING DEVICE ;

Abstracted Patent: JP6215010 ;

Publication Date: 1994-08-05 ;

Inventor(s): TSUTSUI KIYOUYA ;

Applicant(s): SONY CORP ;

Application Number: JP19930021729 19930114 ;

Priority Number(s): ;

IPC Classification: G06F15/21; G06F7/58; G06K17/00; G06K19/00; G07F7/08 ;

Equivalents: ;

ABSTRACT:

PURPOSE:To copy the information of news or music by inserting an information recording and reproducing device such as an IC card to an information acquiring device.

CONSTITUTION:The information acquiring device copies the information of news or music to an information recorder A by inserting the information recorder A such as the IC card to the information acquiring device installed at a station or on the street of a shopping town. The information recorder A copying these kinds of information is mounted at an information reproducing device B and viewed by a display B2 and an earphone B4, etc. Prepaid information is previously written in the information recorder A by a right management information updating device and therefore, it is not necessary to adjust compensation in the case of copying information from the information acquiring device to the information recorder A.

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平6－215010

(43)公開日　平成６年(1994)８月５日

(51)Int.Cl.[5]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　15/21	３５０	8724－5L		
7/58	Ｚ	9188－5B		
Ｇ０６Ｋ　17/00	Ｌ	7459－5L		
		8623－5L	Ｇ０６Ｋ　19/ 00	Ｑ
		9256－3E	Ｇ０７Ｆ　7/ 08	Ｓ

審査請求　未請求　請求項の数10　ＦＤ　（全 14 頁）　最終頁に続く

(21)出願番号　特願平5－21729

(22)出願日　平成５年(1993)１月14日

(71)出願人　000002185
ソニー株式会社
東京都品川区北品川６丁目７番35号

(72)発明者　筒井　京弥
東京都品川区北品川６丁目７番35号　ソニー株式会社内

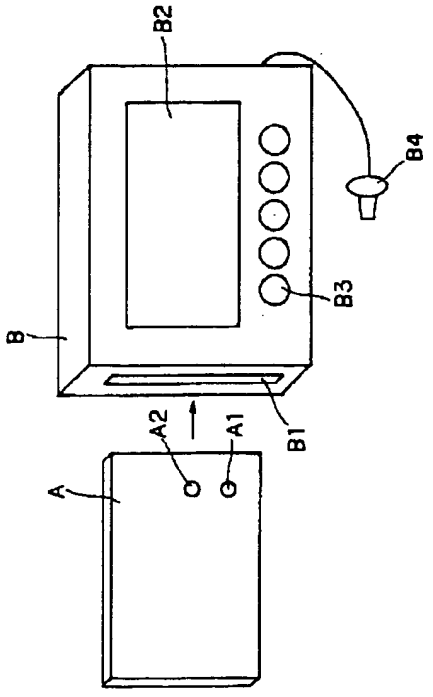
(74)代理人　弁理士　稲本　義雄

(54)【発明の名称】　情報取得装置

(57)【要約】

【目的】　情報提供装置に対してＩＣカード等の情報記録再生装置を挿入することで、ニュース或いは音楽等の情報をコピー出来るようにする。

【構成】　駅或いはショッピング街等の街頭に設置された情報提供装置に対して、ＩＣカード等の情報記録装置Ａを挿入することで、情報提供装置より情報記録装置Ａに対してニュース或いは音楽等の情報をコピーさせる。これらの情報をコピーした情報記録装置Ａは、情報再生装置Ｂに装着され、表示体Ｂ２およびイアホンＢ４等で視聴される。情報記録装置Ａには、予め権利管理情報更新装置によってプリペイド情報が書き込まれており、従って情報提供装置より情報記録装置Ａに対して情報をコピーする際には対価の精算の必要はない。



Petitioner Apple Inc. - Exhibit 1012, p. 1543

1

【特許請求の範囲】

【請求項1】　識別情報に基づいて権利管理情報を送出する権利管理情報更新手段と、識別情報に基づいて提供すべき情報を送出する情報提供手段との間でそれぞれ情報交換が成される情報取得装置であって、

前記権利管理情報更新手段と情報交換を行う際に、識別情報に基づいて権利管理情報更新手段からの権利管理情報を管理情報記録媒体に格納する管理情報格納制御手段と、

前記管理情報記録媒体に権利管理情報が格納された状態において、前記情報提供手段と情報交換を行う際に、識別情報に基づいて情報提供手段から提供される情報を情報記録媒体に格納する情報格納制御手段とを具備したことを特徴とする情報取得装置。

【請求項2】　前記情報記録媒体に蓄積された情報を読み出し再生する情報再生手段をさらに具備したことを特徴とする請求項1に記載の情報取得装置。

【請求項3】　前記管理情報記録媒体には、前記権利管理情報に加え、さらに識別情報と、第1の鍵情報と、第2の鍵情報とが格納されるように成されたことを特徴とする請求項1または請求項2に記載の情報取得装置。

【請求項4】　前記権利管理情報更新手段には、前記管理情報記録媒体に格納された第1の鍵情報と同一の鍵情報が格納された鍵情報テーブルが具備されて成ることを特徴とする請求項3に記載の情報取得装置。

【請求項5】　前記権利管理情報更新手段は、前記管理情報記録媒体に格納された第1の鍵情報と同一の鍵情報を通信手段によって管理センタより取得するようにして成る請求項3に記載の情報取得装置。

【請求項6】　前記管理情報記録媒体に格納される権利管理情報は前記権利管理情報更新手段との情報交換によって書き替え可能に成されていることを特徴とする請求項1乃至請求項5に記載の情報取得装置。

【請求項7】　前記権利管理情報の書き替えは前記第1の鍵情報に基づいて正当であると認証された権利管理情報更新手段からの情報に基づいてのみ可能であることを特徴とする請求項6に記載の情報取得装置。

【請求項8】　前記正当であると認証する手段は、情報取得装置に内蔵された乱数発生手段によって発生された乱数に基づいて行われることを特徴とする請求項7に記載の情報取得装置。

【請求項9】　前記情報提供手段には、前記管理情報記録媒体に格納された第2の鍵情報と同一の鍵情報が格納された鍵情報テーブルが具備されて成ることを特徴とする請求項3に記載の情報取得装置。

【請求項10】　前記情報提供手段は、前記管理情報記録媒体に格納された第2の鍵情報と同一の鍵情報を通信手段によって管理センタより取得するようにして成る請求項3に記載の情報取得装置。

【発明の詳細な説明】

2

【0001】

【産業上の利用分野】本発明はニュース、或いは音楽等の情報を迅速に取得することができる情報取得装置に関する。

【0002】

【従来の技術】例えば、特開平3－118690号には、ニュース或いは音楽等の各種の情報が格納された装置に対して、手持ちのＩＣカード或いはカセットテープ等の情報記録媒体を装着し、対価として必要な金額に相当するコインを装置のコインボックスに投入することで、前記情報記録媒体に対して装置よりニュース或いは音楽等の各種の情報を選択的にダビングできるように成された情報提供装置が開示されている。

【0003】従って、これらの情報提供装置を駅前或いはショッピング街等の人通りの多い各所に設置しておけば、利用者が必要な時に前記情報提供装置に向かって手持ちのＩＣカード或いはカセットテープ等の情報記録媒体を装着し、情報の対価としてのコインをコインボックスに投入することで、即座に必要な情報を得ることができるようになる。

【0004】

【発明が解決しようとする課題】ところで、前記した従来の装置においては、手持ちのＩＣカード或いはカセットテープ等の情報記録媒体に対して必要な情報をダビングさせる際に、所定の金額をコインボックスに対してその都度投入する等の操作が必要である。情報記録媒体としては、将来ＩＣカードの普及が見込まれており、情報記録媒体としてＩＣカードを利用するようにした場合には、ＩＣカードに対しての情報のダビングは略瞬時に行うことが可能であるにもかかわらず、対価として必要なコインを投入するなどの操作を余儀無くされることとなる。従って、例えば駅構内において、電車を待つ間の限られた時間内にダビング操作を行おうとしても、コインボックス等にコインを投入する等の金額的な精算が必要となり、この精算による時間が必要となるため、情報を取得できる人数は限られたものになる。

【0005】本発明は、この様な点に着目して成されたものであり、情報提供手段としての情報提供装置に対して、情報記録（再生）手段を装着させることで、必要な情報を即座にダビング出来るようにし、前記した従来のものの不都合を解消した情報取得装置を提供することを課題とするものである。

【0006】

【課題を解決するための手段】前記課題を達成するために成された請求項1に記載の情報取得装置は、識別情報に基づいて権利管理情報を送出する権利管理情報更新手段としての権利管理情報更新装置と、識別情報に基づいて提供すべき情報を送出する情報提供手段としての情報提供との間でそれぞれ情報交換が成される情報取得装置であって、権利管理情報更新装置と情報交換を行う際

Petitioner Apple Inc. - Exhibit 1012, p. 1544

に、識別情報に基づいて権利管理情報更新装置からの権利管理情報を管理情報記録媒体に格納する管理情報格納制御手段と、管理情報記録媒体に権利管理情報が格納された状態において、情報提供手段としての情報提供装置と情報交換を行う際に、識別情報に基づいて情報提供装置から提供される情報を情報記録媒体に格納する情報格納制御手段とを備えることを特徴とする。

【０００７】また、請求項２に記載の情報取得装置は、情報記録媒体に蓄積された情報を読み出し再生する情報再生手段をさらに具備することを特徴とする。

【０００８】また、請求項３に記載の情報取得装置は、管理情報記録媒体に対して権利管理情報に加え、識別情報と、第１の鍵情報と、第２の鍵情報とをさらに格納するようにした点を特徴とする。

【０００９】また、請求項４に記載の情報取得装置は、権利管理情報更新手段としての権利管理情報更新装置に、管理情報記録媒体に格納された第１の鍵情報と同一の鍵情報が格納された鍵情報テーブルを備えることを特徴とする。

【００１０】また、請求項５に記載の情報取得装置は、権利管理情報更新手段としての権利管理情報更新装置が、管理情報記録媒体に格納された第１の鍵情報と同一の鍵情報を通信手段によって管理センタより取得するよう構成した点を特徴とする。

【００１１】また、請求項６に記載の情報取得装置は、管理情報記録媒体に格納される権利管理情報が権利管理情報更新手段としての権利管理情報更新装置との情報交換によって書き替え可能に成されるよう構成した点を特徴とする。

【００１２】また、請求項７に記載の情報取得装置は、権利管理情報の書き替えが第１の鍵情報に基づいて正当であると認証された権利管理情報更新手段としての権利管理情報更新装置からの情報に基づいてのみ可能であるよう構成した点を特徴とする。

【００１３】また、請求項８に記載の情報取得装置は、前記正当であると認証する手段が、情報取得装置に内蔵された乱数発生手段としての乱数発生器によって発生される乱数に基づいて行われるよう構成した点を特徴とする。

【００１４】また、請求項９に記載の情報取得装置は、管理情報記録媒体に格納された第２の鍵情報と同一の鍵情報が格納された鍵情報テーブルが情報提供手段としての情報提供装置に具備されたことを特徴とする。

【００１５】また、請求項１０に記載の情報取得装置は、情報提供手段としての情報提供装置に、管理情報記録媒体に格納された第２の鍵情報と同一の鍵情報を通信手段によって管理センタより取得できるように構成した点を特徴とする。

【００１６】

【作用】請求項１に記載の情報取得装置においては、は

じめに権利管理情報更新装置と情報交換を行う際に、識別情報に基づいて権利管理情報更新装置からの権利管理情報を管理情報記録媒体に予め格納する。この時、情報に対する対価をプリペイドする。次いで管理情報記録媒体に権利管理情報が格納された状態において、情報提供装置と情報交換を行うように成され、情報提供装置からの情報を取得する毎に例えば権利管理情報が残度数情報として書き替えられる。

【００１７】また請求項２に記載の情報取得装置においては、情報記録媒体に蓄積された情報を読み出し再生する情報再生手段としての再生装置がさらに具備されており、この再生装置によって情報を視聴することが可能となる。

【００１８】また請求項３に記載の情報取得装置においては、管理情報記録媒体に対して権利管理情報に加え、識別情報と、第１の鍵情報と、第２の鍵情報とがさらに格納され、これらの識別情報および鍵情報によって情報の授受の安全性が確保される。

【００１９】また請求項４に記載の情報取得装置においては、権利管理情報更新手段としての権利管理情報更新装置に、管理情報記録媒体に格納された第１の鍵情報と同一の鍵情報が格納された鍵情報テーブルが備えられる。

【００２０】また請求項５に記載の情報取得装置においては、権利管理情報更新手段としての権利管理情報更新装置が、管理情報記録媒体に格納された第１の鍵情報と同一の鍵情報を通信手段によって管理センタより取得するよう構成される。

【００２１】また請求項６に記載の情報取得装置においては、管理情報記録媒体に格納される権利管理情報が権利管理情報更新手段としての権利管理情報更新装置との情報交換によって書き替え可能に成される。

【００２２】また請求項７に記載の情報取得装置においては、権利管理情報の書き替えが第１の鍵情報に基づいて正当であると認証された権利管理情報更新手段としての権利管理情報更新装置からの情報に基づいてのみ可能であるよう構成される。

【００２３】また請求項８に記載の情報取得装置においては、前記正当であると認証する手段が、情報取得装置に内蔵された乱数発生手段としての乱数発生器によって発生される乱数に基づいて行われるよう構成される。

【００２４】また請求項９に記載の情報取得装置においては、管理情報記録媒体に格納された第２の鍵情報と同一の鍵情報が格納された鍵情報テーブルが情報提供手段としての情報提供装置に具備される。

【００２５】また請求項１０に記載の情報取得装置においては、情報提供手段としての情報提供装置に、管理情報記録媒体に格納された第２の鍵情報と同一の鍵情報を通信手段によって管理センタより取得できるように構成される。

Petitioner Apple Inc. - Exhibit 1012, p. 1545

5

【0026】

【実施例】本発明の情報取得装置は、ニュース、或いは音楽等の情報を視聴しようとする利用者が、自分が所持している情報取得装置、すなわち情報記録（再生）装置に対して情報提供手段としての情報提供装置より必要な情報をコピー（ダビング）し、即座にその情報を視聴できるようにするものである。この場合、情報提供装置より情報を受ける権利、すなわち権利管理情報を権利管理情報更新手段としての権利管理情報更新装置により予め更新しておくことで、情報記録（再生）装置は情報提供装置より必要な情報を入手するに際し、その都度現金等の情報料の精算を行う必要をなくすように成される。

【0027】ここで言う権利管理情報とは、その情報使用者が情報提供装置から情報を入手する権利を表す情報のことを言い、例えばその情報使用者の会員情報や、情報入手時毎に減じられる残度数情報等をその例として挙げることができる。

【0028】以下、本発明の実施例について図面を参照して説明する。図1は、本発明の情報取得装置を構成する情報記録装置Aと、この情報記録装置が装着され、情報記録装置Aに記録された情報を再生することができる情報再生装置Bの外観図を示したものである。

【0029】前記情報記録装置Aは、例えばICカードにより構成されており、この情報記録装置Aには、情報の再生時に、情報再生装置Bとの間でデータおよび制御信号の交換をするための端子として情報再生装置結合端子A1が設けられている。また、情報記録装置AとしてのICカードの一部には、後述する情報提供装置との間でデータおよび制御信号の交換をするための端子として情報提供装置結合端子A2も設けられている。前記情報再生装置結合端子A1および情報提供装置結合端子A2は、実際には一つの端子を切り替えて使用するように構成することもできる。

【0030】前記情報再生装置Bは、携帯に便利なように偏平箱型形状に成され、その左側壁部には、ICカードより成る前記情報記録装置Aが挿入されるスリット状の挿入口B1が形成されており、また正面中央部には、表示手段としての例えば液晶表示体B2が配置され、さらに正面下側部には、再生選択手段としての複数個の押釦スイッチB3が横一線に配置されている。そして、その右側壁部からはイアホンB4が導出されている。

【0031】前記液晶表示体B2は、前記情報記録装置A内に記録された情報の内容を表示することができ、この液晶表示体B2に表示される、例えば情報リストに基づいて押釦スイッチB3のいずれかを押圧操作することで、選択された情報が液晶表示体B2に視覚情報として再生され、また前記イアホンB4によって音声情報として再生される。情報の内容は、テキスト情報、映像情報、コンピュータプログラムおよび音声情報等を含み、特に限定されない。

6

【0032】なお、図1の実施例には図示していないが、イアホンの代わりに、或いはイアホンに加えて情報再生装置Bにスピーカを装備していてもよく、その場合には、スピーカに音声情報の再生結果を出力してもよい。さらに再生信号は、やはり図1には描かれていないが、外部出力端子を経由させて、外部のCRTやスピーカ等に接続してもよい。

【0033】図2は、本発明の情報取得装置の他の実施例である情報記録再生装置の外観図を示したものである。すなわち、図1に示した情報記録装置Aに相当するものが、情報再生装置Bに内臓された構成となっており、外観上は前記図1における情報再生装置Bと略同一形状に成されている。従って、図2において、図1に相当する部分は同一符号を付し、その詳細な説明は省略する。

【0034】ただし、図2に示す情報記録再生装置Cにおいては、その左側壁部に後述する情報提供装置への結合端子C1が設けられており、この端子C1を経由して情報が取得される。なお、図2に示した情報記録再生装置Cに内蔵される情報記録媒体の種類は特に限定されることはないが、高速にコピー（ダビング）が可能であり、かつ、記録媒体へのランダムアクセスが容易で、携帯性にも優れたICメモリを使用すると便利である。

【0035】図3は、本発明の情報取得装置に対して情報を提供する情報提供手段としての情報提供装置の外観図を示している。情報提供装置D内には、後述する情報記録媒体が内蔵され、情報取得装置に対して提供するための各種の情報が蓄積されている。そして、箱型の情報提供装置Dの正面パネルには、蓄積されている情報の内容や提供価格等を表示する表示手段としての液晶表示体D11乃至D16が配置され、どの情報を情報提供装置Dから供給を受けるかを選択する出力選択手段としての複数個の押釦スイッチD11乃至D16がそれぞれ前記各液晶表示体D11乃至D16の近傍に配置されている。そして、その正面右下側部には、ICカードより成る前記情報記録装置Aの挿入排出口D3が配置されている。

【0036】従って、情報を入手しようとする場合には、ICカードより成る情報記録装置Aを前記挿入排出口D3に挿入し、液晶表示体D11乃至D16に表示された入手しようとする情報に対応する前記押釦スイッチD11乃至D16を択一的に押圧操作することで、情報記録装置Aに対して情報がコピーされる。そしてコピー済みの情報記録装置Aは、挿入排出口D3より排出される。

【0037】なお、図3に示す例は、ICカードより成る情報記録装置Aを直接挿入し、コピーを行うようにする場合を示しているが、例えば前記図2に示したような情報記録再生装置Cに対しては、ワイヤ（図示せず）を情報提供装置結合端子C1に接続し、リクエストされた

Petitioner Apple Inc. - Exhibit 1012, p. 1546

情報を電気的に供給するように成される。

【００３８】図４は、本発明の情報取得装置に対して情報を提供する情報提供装置の他の例を示した外観図である。この図４に示した情報提供装置Ｅにおいては、ＩＣカードより成る情報記録装置Ａに対して情報を供給するものであり、情報記録装置Ａの挿入口Ｅ１と排出口Ｅ２とが距離をおいて分離されており、情報入手希望者Ｆは矢印方向に歩きながら、ＩＣカードより成る情報記録装置Ａに対して情報をコピーさせることができる。この例は、多くの人に対して迅速に情報を提供する場合に便利である。

【００３９】図５は、権利管理情報更新手段としての権利管理情報更新装置の外観図を示している。箱型の権利管理情報更新装置Ｇの正面パネルには、ＩＣカードより成る情報記録装置Ａの挿入排出口Ｇ１およびコイン投入口Ｇ２が設けられている。権利管理情報の更新を希望する場合には、情報記録装置Ａを挿入排出口Ｇ１に挿入すると共に、コイン投入口Ｇ２に必要な対価を投入することで情報記録装置Ａの権利管理情報の更新が成される。

【００４０】図６は、権利管理情報更新装置の他の例を示した外観図である。この例に示す権利管理情報更新装置Ｈは人手によって管理されるものである。すなわち、管理者が、更新希望者より対価ならびに情報記録装置Ａを受けとり、その対価に応じた更新情報を入力手段としてのテンキーＨ１を操作する。テンキーＨ１の操作により、更新情報が表示装置Ｈ２に表示され、情報記録装置Ａを挿入排出口Ｈ２に挿入することで、情報記録装置Ａは対価に応じた権利管理情報の更新が成される。

【００４１】なお、図５および図６に示した権利管理情報更新装置は、いずれも図１に示したようなＩＣカードより成る情報記録装置Ａに対して権利管理情報を更新させるタイプであるが、例えば前記図２に示したような情報記録再生装置Ｃに対しては、ワイヤ（図示せず）によって電気的に接続し、権利管理情報を更新させるように成される。

【００４２】次に、図７は、情報記録再生装置の電気的な内部構成をブロック図で示したものである。この例は、例えば前記図２に示すような情報記録装置と情報再生装置が一体となった状態を示しており、図１においては、情報再生装置Ｂに対して情報記録装置Ａが装着された状態で示している。

【００４３】図７において、情報記録再生装置１００１は、情報提供装置からライン１０３を介して転送された情報を情報記録媒体１００３に格納し、格納された情報は伝送ライン１０２を介して情報再生手段１００２によって読み出され、再生される。そして、ライン１０１を介して、図１または図２に示す表示手段Ｂ２およびイアホンＢ４等に出力される。

【００４４】情報提供装置からの情報を受けるに先立って、制御手段としての制御装置１００４は、情報格納制御手段として作用し、後に詳述するが、情報提供装置との間でライン１０４を介して通信（情報交換）を行い、管理情報記録媒体１００６に記録された情報に基づいて、その情報記録再生装置が情報の伝送を受けることができることを証明する。ここで、管理情報記録媒体１００６に格納された権利管理情報は、ライン１０７を介して制御装置１００４に接続されており、さらに権利管理情報は、後に詳述するが、ライン１０５を介して権利管理情報更新装置との間で記録／更新される。この場合、前記制御装置１００４は、管理情報格納制御手段として作用する。

【００４５】前記ライン１０４および１０５を介した情報提供装置および権利管理情報更新装置との通信には、管理情報記録媒体１００６に格納された識別情報Ｉ、第１の鍵情報１、第２の鍵情報２の情報が使用される。これらの値は、全ての情報記録再生装置について同一であってもよいが、後で述べるように、情報記録再生装置によって異なっていると都合が良い。また前記制御装置１００４には、ライン１０６を介して接続された乱数発生手段としての乱数発生回路１００５より乱数が供給されている。

【００４６】次に、図８は、権利管理情報更新装置の電気的な内部構成をブロック図で示したものである。権利管理情報更新装置１０１１には、制御手段としての制御装置１０１２が内蔵されており、この制御装置１０１２には、第１の鍵情報が格納された鍵情報１テーブル１０１４がライン１１２を介して接続され、また更新情報記録媒体１０１３がライン１１１を介してそれぞれ接続されている。そして権利管理情報更新装置１０１１は、後に詳述するが、情報記録再生装置との間でライン１０５を介して通信（情報交換）を行うことにより、情報記録再生装置に記録されている権利管理情報を更新することができる。また、この更新手続の記録は更新情報記録媒体１０１３に記録され、これにより権利管理情報の更新に伴う金銭の授受が人手によって行われた場合にも、正確な決済処理を行うことができる。また、この更新情報をライン１１３を介して管理センタＪに送信することにすれば、権利管理更新装置が設置されている場所まで行って決済のための手続きを行わなくても、金銭授受者との決済を行うことが可能である。

【００４７】図９は、情報提供装置の電気的な内部構成をブロック図で示したものである。情報提供装置１０２１には、制御手段としての制御装置１０２３が内蔵されており、この制御装置１０２３には、まず第２の鍵情報が格納された鍵情報２テーブル１０２５がライン１２４を介して接続され、また乱数発生手段としての乱数発生回路１０２５がライン１２３を介して接続されている。さらに制御装置１０２３には、ライン１２５を介して情報伝送記録媒体１０２６が接続されている。そして前記制御装置１０２３からは、ライン１２２によって情報記

Petitioner Apple Inc. - Exhibit 1012, p. 1547

録媒体１０２２に対して制御信号が出力される構成となっている。

【００４８】情報提供装置の情報記録媒体１０２２には、ライン１２１によって管理センタＪから伝送された情報が記録され、情報記録装置に対してライン１０３を介して情報の転送がなされる。その転送に先立ち、制御手段１０２３は、情報記録再生装置との間でライン１０４を介して通信（情報交換）を行ない、その情報転送要求が正当なものであるかどうかの確認を行なう。また、この情報転送に関する記録を情報転送記録媒体１０２６に記録することができ、この情報転送に関するデータをライン１２６を介して管理センタＪに送信することも可能である。

【００４９】ここで、権利管理情報の記録／更新に関する処理フローについて、図１０に示すフローチャートに基づいて説明する。権利管理情報の記録／更新は、正当に管理されている権利管理情報更新装置、すなわち各情報記録装置に記録されている秘密の鍵情報１の内容を知っている権利管理情報更新装置のみによって行なうことができるものでなければならない。

【００５０】図１０において、権利管理情報更新装置１０１１に挿入された情報記録再生装置１００１は、まず識別情報Ｉを権利管理情報更新装置に送信（ステップＳ１）すると共に、乱数Ｒを発生（ステップＳ２）して、権利管理情報更新装置１０１１に送信（ステップＳ３）する。前記識別情報Ｉを受信（ステップＳ４）し、また、乱数Ｒを受信（ステップＳ５）した権利管理情報更新装置１０１１は、まず識別情報Ｉの値から鍵情報１のテーブル１０１４を検索して、その情報記録再生装置１００１に対応する鍵情報１、Ｋ１［Ｉ］を得、Ｋ１［Ｉ］と乱数ＲからＥ２を算出（ステップＳ６）して、情報記録再生装置１００１に送信（ステップＳ７）する。

【００５１】一方、情報記録再生装置１００１においても、Ｋ１［Ｉ］と乱数Ｒから権利管理情報更新装置が成した方法と同一の方法でＥ１を算出（ステップＳ８）する。そして、権利管理情報更新装置１０１１よりＥ２を受信（ステップＳ９）し、ステップＳ８で算出したＥ１と、ステップＳ９で受信したＥ２の比較（ステップＳ１０）を行なう。この比較結果が一致しない（Ｎｏ）場合には、不正な権利管理情報更新装置１０１１からの記録／更新要求があったものと判断して、権利管理情報の記録／更新を停止（ステップＳ１１）させる。また、この比較結果が一致した（Ｙｅｓ）ならば、正当な権利管理情報更新装置１０１１からの記録／更新要求があったものと判断する。この場合には、権利管理情報更新装置１０１１より権利管理情報が送信（ステップＳ１２）され、これを受けて、情報記録再生装置１００１は権利管理情報の記録／更新を行なう（ステップＳ１３）。

【００５２】なお、この時、図８において、権利管理情

報更新の記録を更新情報記録媒体１０１３に記録したり、ライン１１３を介して管理センタＪに送信することで、決済処理をセンタで行なわせ、また統計処理の集計も行なわせることが可能となる。

【００５３】次に、情報提供装置より情報記録再生装置に対して情報を転送する処理フローについて、図１１に示すフローチャートに基づいて説明する。情報の提供は、情報提供を受ける権利を証明することのできる情報記録再生装置、すなわち識別情報Ｉに対応した鍵情報２の値を知っている事実と、情報提供を受けることを表わす権利管理情報の両者を提示できる情報記録再生装置のみに対して行なわれるものでなければならない。

【００５４】情報提供装置１０２１に挿入された情報記録再生装置１００１は、まず識別情報Ｉを情報提供装置１０２１に送信（ステップＳ２１）し、情報提供装置１０２１は、これを受信（ステップＳ２２）する。次いで情報提供装置１０２１は、乱数Ｐを発生（ステップＳ２３）し、これを情報記録再生装置１００１に送信（ステップＳ２４）する。情報記録再生装置１００１では、乱数Ｐを受信（ステップＳ２５）し、受信した乱数Ｐと鍵情報２の値、Ｋ２［Ｉ］からＦ２を算出（ステップＳ２６）して、Ｆ２を情報提供装置１０２１に送信（ステップＳ２７）する。

【００５５】一方、情報提供装置１０２１においても、受信した識別情報Ｉの値から鍵情報２のテーブル１０２５を検索して、その情報記録再生装置１００１に対応する鍵情報２、Ｋ２［Ｉ］を得、Ｋ２［Ｉ］と乱数Ｐから情報記録再生装置がＦ２を算出したのと同じ方法でＦ１を算出（ステップＳ２８）する。そして、情報記録再生装置１００１よりＦ２を受信（ステップＳ２９）し、ステップＳ２８で算出したＦ１と、ステップＳ２９で受信したＦ２の比較（ステップＳ３０）を行なう。

【００５６】この比較結果が一致しない（Ｎｏ）場合には、不正な情報記録再生装置１００１からの情報提供要求であったと判断して、情報提供装置１０２１から情報記録再生装置１００１への情報の送信を停止（ステップＳ３１）させる。また、この比較結果が一致した（Ｙｅｓ）ならば、正当な情報記録再生装置１００１からの情報提供要求であったと判断する。この場合には、情報記録再生装置１００１より送信（ステップＳ３２）される権利管理情報を受信（ステップＳ３３）して、その情報記録再生装置１００１が実際にその情報提供を受ける権利があるのかどうか、会員情報等の権利管理情報を調べる（ステップＳ３４）。

【００５７】ステップＳ３４において、権利が有効でない（Ｎｏ）と判断された場合には、情報の送信を停止（ステップＳ３１）させる。権利が有効である（Ｙｅｓ）と判断されれば、情報の送信（ステップＳ３５）を行ない、情報記録再生装置１００１は、情報の受信／記録（ステップＳ３６）がなされる。なお、この情報転送

Petitioner Apple Inc. - Exhibit 1012, p. 1548

の記録を情報転送記録媒体１０２６に記録したり、ライン１２５を介して管理センタＪに送信することで、各種の統計処理に役立たせることができる。

【００５８】以上の構成および作用において、ライン１０４および１０５の通信処理で、鍵情報１や鍵情報２を直接送信せず、鍵情報で乱数を符号化したものを送信するのは、送信時にこれらの秘密情報が盗まれることを防ぐためのものであり、もしそうした危険性を考慮しなくてよい場合には、これらの情報を直接送信して正当性を証明するようにしてもよい。また逆に、さらに安全性を高めるために、識別情報等の情報に関しても別の鍵情報を使って送信することにしてもよい。また、鍵情報１と２は別々なものとして説明したが、これらは勿論同一のものであってもよい。

【００５９】ここで、前記した実施例における情報の授受の安全性について述べるが、情報提供装置から不正に情報が転送されるのは次の二つの場合である。

（１）不正な情報記録再生装置に情報の転送が行なわれる。

（２）正当な情報記録再生装置に不正な権利管理情報が記録され、情報提供装置から情報の転送が行なわれる。

【００６０】前記（１）に関して言えば、情報記録再生装置は大量に生産され、不特定多数の使用者に比較的安価に供給されるもので、ハードウエア的にその偽造を行なうことは困難である。しかし万一情報記録再生装置が偽造された場合に、その情報記録再生装置には少なくともある識別情報に対応した鍵情報２が記録されていなければ、情報提供装置からの情報の転送を受けることはできない。

【００６１】そこで偽造者は鍵情報２を盗み出す必要があるが、情報提供装置は厳重に管理することが比較的容易であるので、鍵情報２は情報記録再生装置から盗み出される危険性の方が高い。しかし鍵情報２は、信号としてそのまま情報記録再生装置から外部に出ることはないので、これを盗み出すのは非常に困難である。また万一これを盗み出し、その鍵情報２を持った情報記録再生装置が大量に出回った場合には、情報提供装置および管理センタでの統計的な処理により、そのことを認知し、その情報記録再生装置への情報転送を一時的に中断する等の処理を施すことができる。

【００６２】また、前記（２）に関して言えば、不正な権利管理情報更新装置を作るためには、その装置によって権利管理情報の更新が行なわれるすべての情報記録再生装置の鍵情報１についての情報が必要になる。しかし権利管理情報更新装置は厳重に管理することが比較的容易であり、ここから鍵情報１を盗み出すことは難しい。また鍵情報１の内容は直接外部に出力されない上、各情報記録再生装置によって異なっているので、結局不特定多数の情報記録再生装置に対して不正に権利管理情報の記録／更新を行なう装置を構成することは極めて困難なものとなる。

【００６３】

【発明の効果】以上の説明で明らかなように、請求項１に記載の情報取得装置によれば、はじめに権利管理情報更新装置と情報交換を行う際に、識別情報に基づいて権利管理情報更新装置からの権利管理情報を管理情報記録媒体に予め格納する。この時、情報に対する対価の精算が成される。次いで管理情報記録媒体に権利管理情報が格納された状態において、情報提供装置と情報交換を行うように成され、情報提供装置からの情報を取得（コピー）する毎に例えば権利管理情報が残度数情報として書き替えられる。従って情報を取得する毎に、その場で情報の対価として金銭を授受する必要がなく情報提供装置より情報取得装置に対して能率良く情報を提供することが可能となる。

【００６４】また請求項２に記載の情報取得装置によれば、情報記録媒体に蓄積された情報を読み出し再生する情報再生手段としての再生装置がさらに具備されており、この再生装置によって情報を即座に視聴することが可能となる。

【００６５】また請求項３に記載の情報取得装置によれば、管理情報記録媒体に対して権利管理情報に加え、識別情報と、第１の鍵情報と、第２の鍵情報とがさらに格納される。従ってこれらの識別情報および鍵情報によって情報の授受の安全性が確保される。

【００６６】また請求項４に記載の情報取得装置によれば、権利管理情報更新手段としての権利管理情報更新装置に、管理情報記録媒体に格納された第１の鍵情報と同一の鍵情報が格納された鍵情報テーブルが備えられており、従って正当な情報取得装置に対してのみ権利管理情報の更新が約束される。

【００６７】また請求項５に記載の情報取得装置においては、権利管理情報更新手段としての権利管理情報更新装置が、管理情報記録媒体に格納された第１の鍵情報と同一の鍵情報を通信手段によって管理センタより取得するよう構成される。この構成によると、権利管理情報更新装置には相当な数の複数の第１の鍵情報を格納するための鍵情報記録媒体を具備する必要がなくなる。

【００６８】また請求項６に記載の情報取得装置においては、管理情報記録媒体に格納される権利管理情報が権利管理情報更新手段としての権利管理情報更新装置との情報交換によって書き替え可能に成される。従って情報取得装置におけるＩＣカード等の記録媒体は、反復して使用可能となる。

【００６９】また請求項７に記載の情報取得装置においては、権利管理情報の書き替えが第１の鍵情報に基づいて正当であると認証された権利管理情報更新手段としての権利管理情報更新装置からの情報に基づいてのみ可能であるよう構成される。

【００７０】また請求項８に記載の情報取得装置におい

Petitioner Apple Inc. - Exhibit 1012, p. 1549

13

ては、前記正当であると認証する手段が、情報取得装置に内蔵された乱数発生手段としての乱数発生器によって発生される乱数に基づいて行われるよう構成される。従って前記鍵情報が表面上現れることがないため、鍵情報の秘密性が向上する。

【００７１】また請求項９に記載の情報取得装置においては、管理情報記録媒体に格納された第２の鍵情報と同一の鍵情報が格納された鍵情報テーブルが情報提供手段としての情報提供装置に具備される。従って正当な情報取得装置に対してのみ情報の提供が約束される。

【００７２】また請求項１０に記載の情報取得装置においては、情報提供手段としての情報提供装置に、管理情報記録媒体に格納された第２の鍵情報と同一の鍵情報を通信手段によって管理センタより取得できるように構成される。この構成によると、情報提供手段には相当な数の複数の第２の鍵情報を格納するための鍵情報記録媒体を具備する必要がなくなる。

【図面の簡単な説明】

【図１】本発明における情報取得装置の一実施例の示す外観図である。

【図２】本発明における情報取得装置の他の実施例を示す外観図である。

【図３】本発明における情報取得装置と情報交換される情報提供装置を示した外観図である。

【図４】本発明における情報取得装置と情報交換される情報提供装置の他の例を示した外観図である。

14

【図５】本発明における情報取得装置と情報交換される権利管理情報更新装置を示した外観図である。

【図６】本発明における情報取得装置と情報交換される権利管理情報更新装置の他の例を示した外観図である。

【図７】図１または図２に示した情報取得装置としての情報記録再生装置の電気的な構成を示したブロック図である。

【図８】図５または図６に示した権利管理情報更新装置の電気的な構成を示したブロック図である。

【図９】図５または図６に示した情報提供装置の電気的な構成を示したブロック図である。

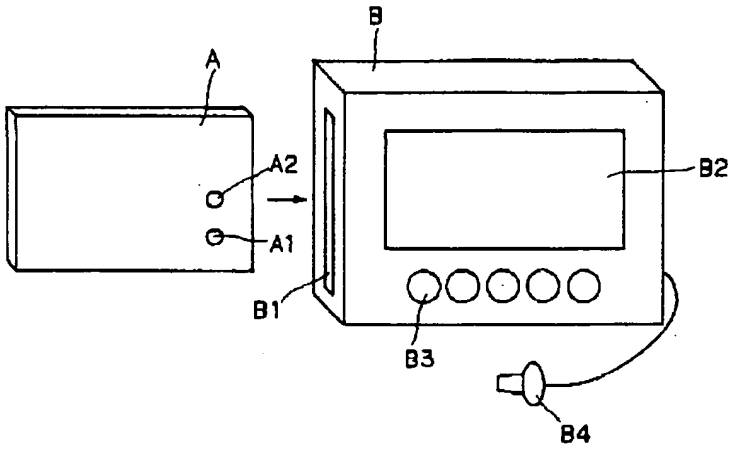
【図１０】本発明における情報取得装置と権利管理情報更新装置との交信作用を説明するフローチャートである。

【図１１】本発明における情報取得装置と情報提供装置との交信作用を説明するフローチャートである。

【符号の説明】

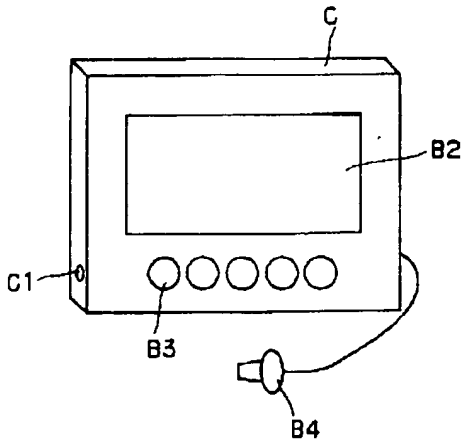
A　情報取得装置（情報記録装置）
B　情報再生装置
C　情報取得装置（情報記録再生装置）
D　情報提供装置（情報提供手段）
E　情報提供装置（情報提供手段）
F　情報入手希望者
G　権利管理情報更新装置（権利管理情報更新手段）
H　権利管理情報更新装置（権利管理情報更新手段）
J　管理センタ

【図１】

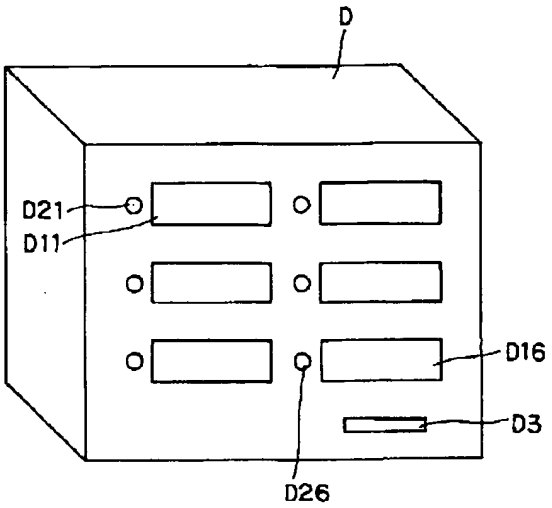


Petitioner Apple Inc. - Exhibit 1012, p. 1550

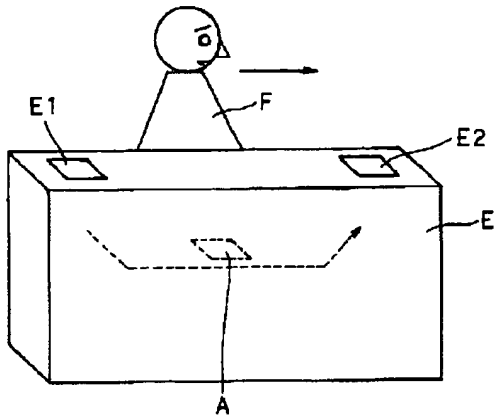
【図2】



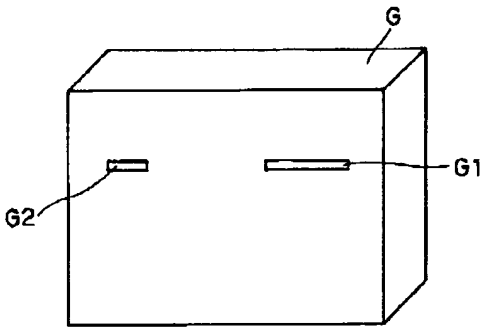
【図3】



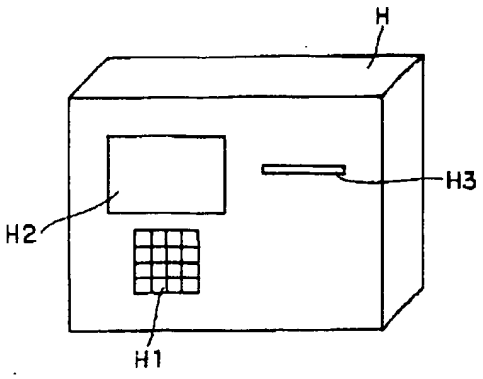
【図4】



【図5】

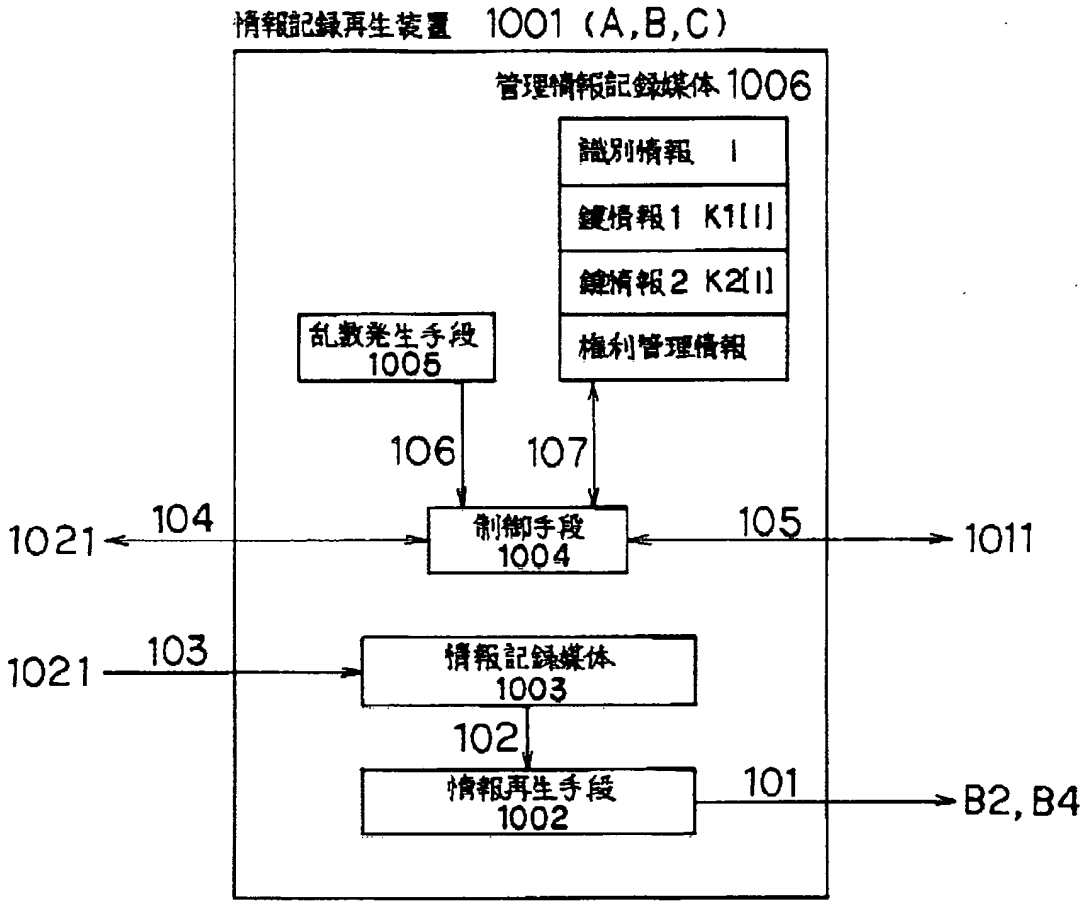


【図6】



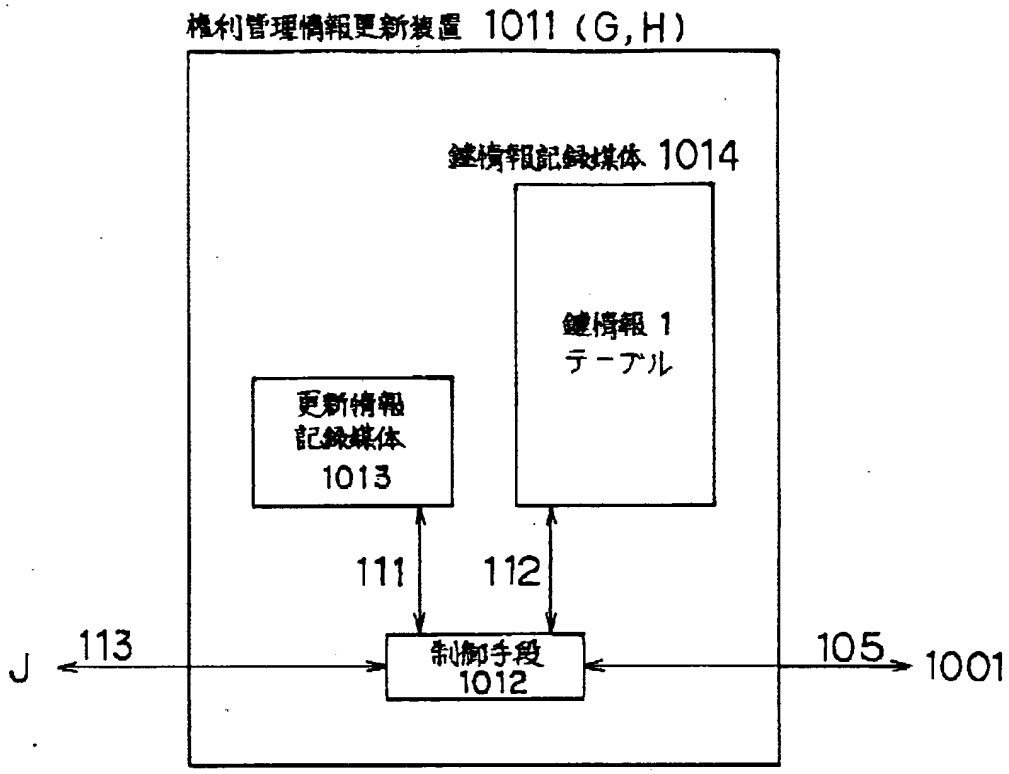
Petitioner Apple Inc. - Exhibit 1012, p. 1551

【図7】



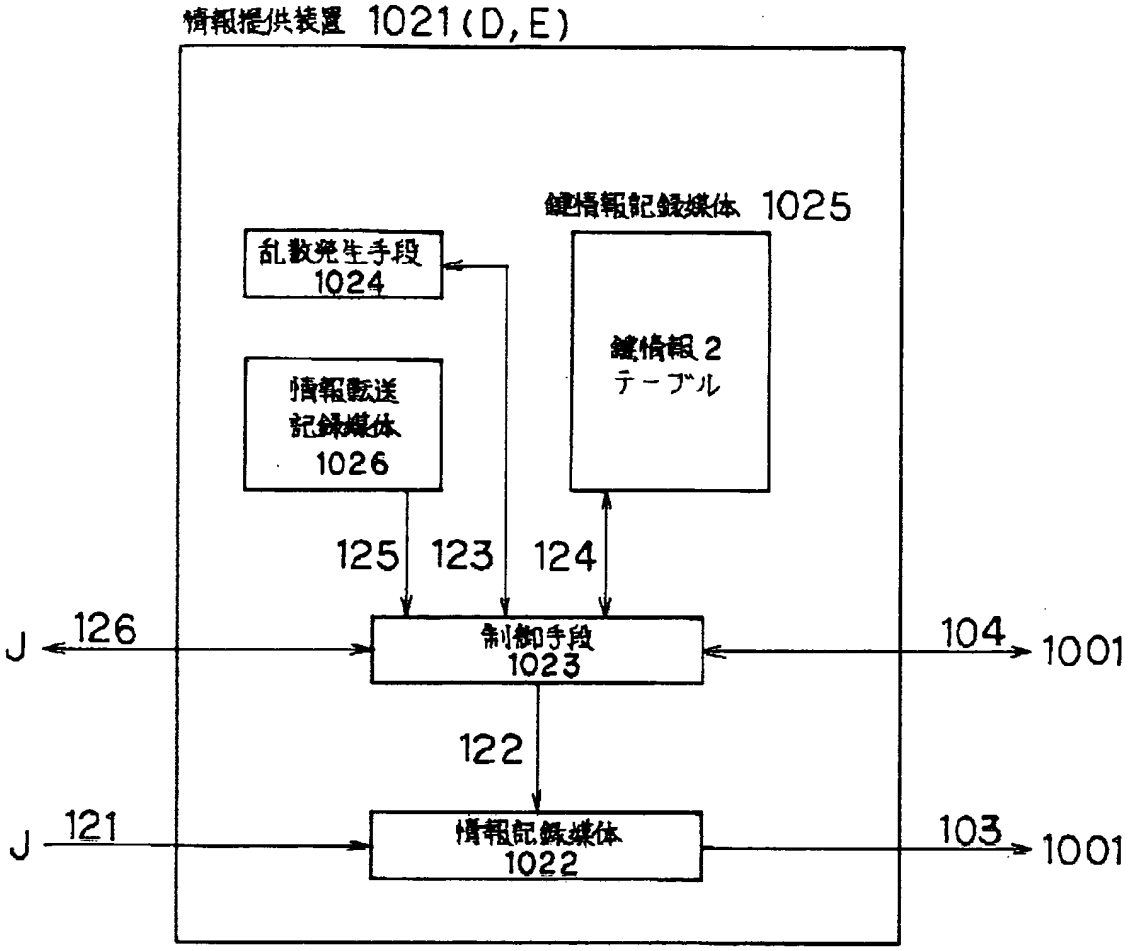
Petitioner Apple Inc. - Exhibit 1012, p. 1552

【図8】



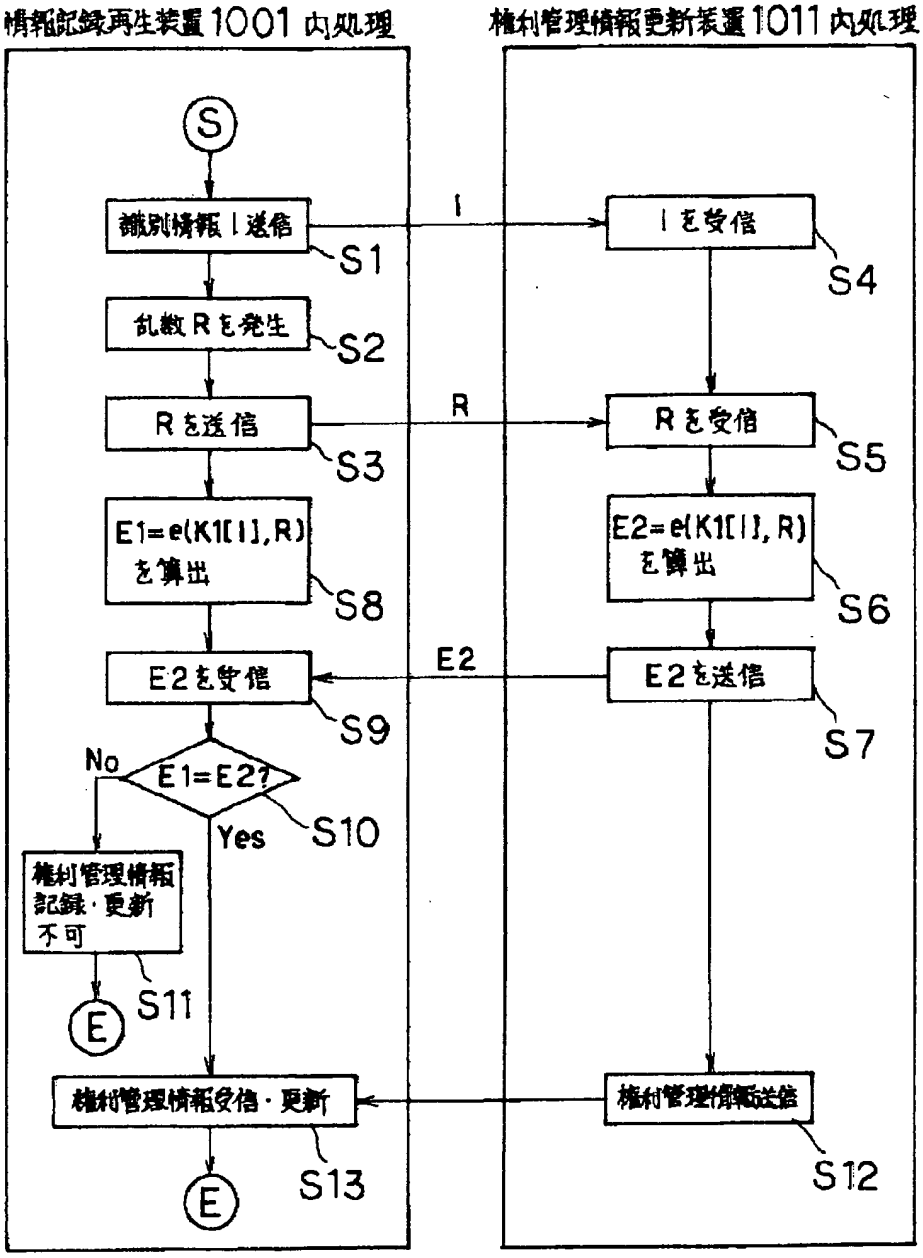
Petitioner Apple Inc. - Exhibit 1012, p. 1553

【図9】



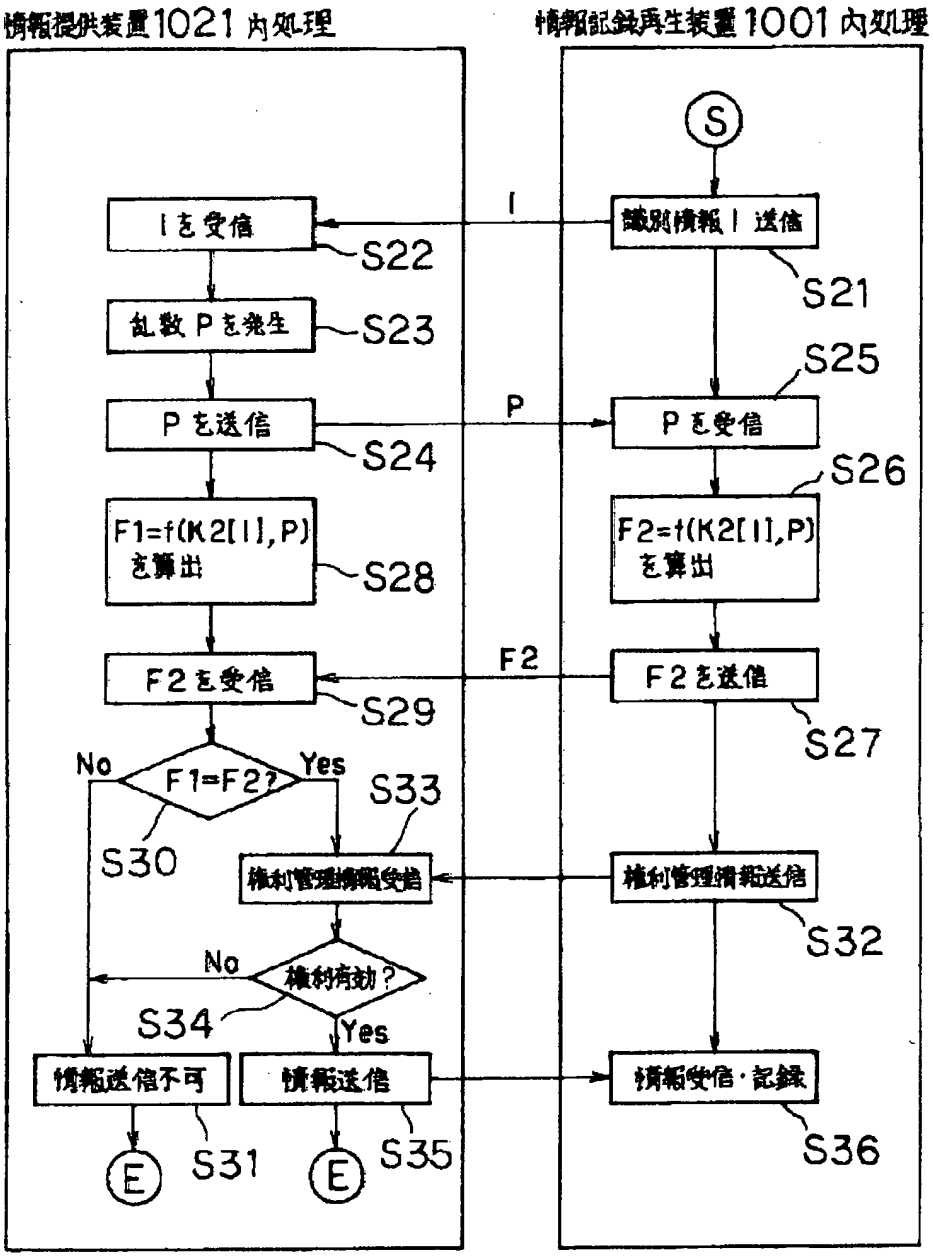
Petitioner Apple Inc. - Exhibit 1012, p. 1554

【図10】



Petitioner Apple Inc. - Exhibit 1012, p. 1555

【図11】



フロントページの続き

(51)Int.Cl.[5]	識別記号	庁内整理番号	F I	技術表示箇所
G06K 19/00				
G07F 7/08				

Petitioner Apple Inc. - Exhibit 1012, p. 1556

Requested Patent: JP7084852A

Title: SECURITY SYSTEM FOR INFORMATION ;

Abstracted Patent: JP7084852 ;

Publication Date: 1995-03-31 ;

Inventor(s): TANAKA KAZUAKI; others: 02 ;

Applicant(s): HITACHI LTD ;

Application Number: JP19930225440 19930910 ;

Priority Number(s): ;

IPC Classification: G06F12/00; G06F3/14; G06F12/14 ;

Equivalents: ;

ABSTRACT:

PURPOSE:To offer information to limited users and to restrict the takeout of a copy of the information and also prevent it by providing a program, which controls a read of displayed screen data, with a function which limits the read.

CONSTITUTION:This system is provided with a database server 1, a client work station 2, and a network 3, and the window server 22 of the client work station 2 performs an input/output process on a display screen at a request made by a user interface program 13 in the server 1. Then a document management file while managing a document file itself wherein substance data on a document are stored manages whether the document can be referred to or copied. At this time, a reference management program checks a reference right management file for a document file whose reference management attribute indicates 'limited' to check whether or not a referring person has the right to refer or copy, thereby deciding whether the the person is allowed to refer to or copy the document file.

(19)日本国特許庁（ＪＰ）　(12) **公開特許公報（A）**　(11)特許出願公開番号

特開平7－84852

(43)公開日　平成７年(1995)３月31日

(51)Int.Cl.[6]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	12/00	５３７　Ｍ	8944－5Ｂ		
	3/14	３４０　Ａ			
	12/14	３２０　Ａ			

審査請求　未請求　請求項の数９　ＯＬ　（全７頁）

(21)出願番号　特願平5－225440

(22)出願日　平成５年(1993)９月10日

(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地

(72)発明者　田中　和明
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(72)発明者　能見　誠
茨城県勝田市市毛1070番地　株式会社日立製作所水戸工場内

(72)発明者　岩崎　一正
神奈川県川崎市麻生区王禅寺1099番地　株式会社日立製作所システム開発研究所内

(74)代理人　弁理士　小川　勝男

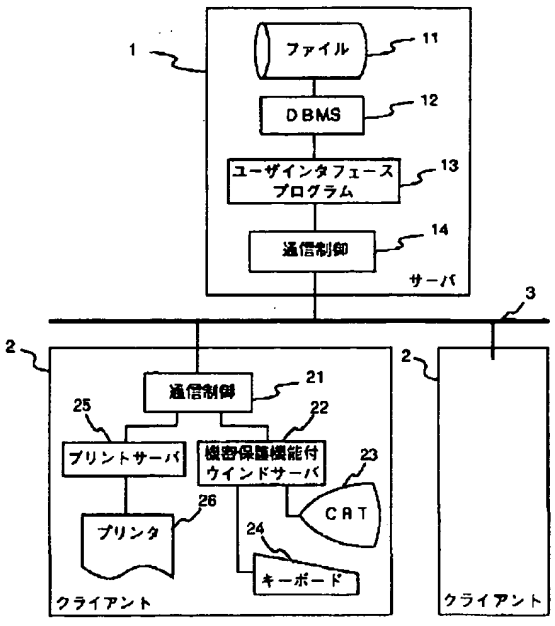
(54)【発明の名称】　情報の機密保護方式

(57)【要約】

【構成】データベースサーバ１，クライアントワークステーション等により構成し、ファイル参照管理で参照の可否，複写の可否を管理し、特に複写の可否によって他の媒体への複写を禁止する機能を備え、更に、画面表示を司るウインドサーバ２２に画面のハードコピーを制限する機能を設けた。

【効果】限られた範囲のユーザにデータベースの情報を提供し、かつ、その情報の複写持出しを制限，防止する上に大きな効果がある。

図１



Petitioner Apple Inc. - Exhibit 1012, p. 1558

1

【特許請求の範囲】

【請求項１】文書，データのファイルを蓄積し、それを利用する計算機システムにおいて、ファイルの参照と共に複写の可否を登録し、その可否によって参照，複写を制限することを特徴とする情報の機密保護方式。

【請求項２】請求項１において、情報を表示する端末の表示制御機能に表示画面の読みだしを制限する機能を付加することによって表示画面のハードコピーを制限する情報の機密保護方式。

【請求項３】請求項１において、情報の複写媒体ごとに複写の可否を制限する機能を備えた情報の機密保護方式。

【請求項４】請求項１において、複写の可否を参照者もしくは参照者グループ対応に登録し、その登録情報に基づいて複写を制限する情報の機密保護方式。

【請求項５】請求項１において、複写の可否を情報種別対応に登録し、その登録情報に基づいて複写を制限する情報の機密保護方式。

【請求項６】請求項２において、マルチウインドを表示する機能を備えた端末を具備し、前記端末においてウインド毎に読みだし可否の属性を管理する機能を備え、少なくも一つの読みだし禁止ウインドを表示している間は画面の表示データを読みだすことを禁止する機能を備えた情報の機密保護方式。

【請求項７】請求項６において、情報を送り出すプログラムより端末の表示ウインドに読みだし禁止属性を設定した後に、その読みだしを指示し、読みだしが不可能であれば禁止機能がはたらいていると判断して、複写禁止の対象となっている情報を表示する情報の機密保護方式。

【請求項８】請求項６において，情報を送り出す機能と表示する端末を一つの計算機で実現した情報の機密保護方式。

【請求項９】計算機のマルチウインドシステムのウインドサーバにおいて、各ウインド単位のウインド管理情報の中に複写可否を指定するための複写可否属性を付与し、ウインドサーバへの表示画面データ読みだし要求があったとき、表示中の全てのウインドの複写可否属性をチェックし、少なくも一つのウインドが複写可否属性が否を示す場合、画面表示データの読みだしを禁止する機能をこと備えたことをを特徴とするウインドサーバシステム。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明はコンピュータ上に蓄積され、端末等によってそのデータを参照する情報システムに係り、その参照，複写等の制限を設けて情報の保安を管理する方法に関する。

【０００２】

【従来の技術】従来、計算機上の情報の参照を制限する

2

最も単純な方法は、例えばワークステーションのオペレーティングシステム（以下ＯＳと略す）であるユニックス（Unix）の場合、利用者に識別コード、いわゆる、ＩＤコードを与え、かつ、そのＩＤコードに対応する個人のパスワードを与え、このパスワードを当人、あるいは特定のグループ以外に秘密とすることで、他人が管理する情報を許可無く参照することを禁止する方法がある。この方法では、このＩＤコード，パスワードの他に、プログラム，情報ファイルに参照権利属性を付与して書き込み，読みだしの権利を個人，グループ，その他の複数のレベルで管理できるようにしているのが一般的である。

【０００３】この方法の拡張として、更に、特定の情報、例えば、データベース等を限定的に参照許可を与える方法として、ファイルのアクセス権ではなく、データベースへの接続権を限定し、更に特定のＩＤとパスワードを与え、階層的な保護を図る方法が利用されている。

【０００４】一方、重要な情報の機密保護等を必要とする場合は、上記一般的な方法に加えて、参照の手続き、及び情報そのものを暗号化して特定の暗号化、復号機構を備えた端末等によりアクセスし、かつ暗号の鍵を特定者に与えることによってそれ以外の者が参照，解読，盗聴不可能なシステムが提供されている。

【０００５】一方、著作権に基づく不法なプログラム，データの複写を防止するためには、コピープロテクトのための情報を付加し、その格納された媒体上に参照プログラムを同居させ、その参照プログラムによって目的とするプログラム，データを参照するもので、その参照プログラム以外のＯＳ等では直接参照出来ないようにすることによってプロテクトを実現する方法が一般的である。

【０００６】

【発明が解決しようとする課題】以上のような保護方法を用い、汎用のUnixワークステーションあるいは汎用パーソナルコンピュータを用いて、例えば、企業内の情報システムを構築した場合、企業内の社員は自由、あるいは緩やかな制限で参照できる必要のある情報を扱った場合、参照そのものは問題無いが、それを物理的な媒体、例えばフロッピーディスクにコピーしたもの、あるいはプリントアウトした書類は外部には持ち出してはならない情報が存在する。製品の開発，設計，製造に関わる技術情報はその種の情報の一例である。

【０００７】このような情報は、他の媒体に複写，印刷するのを防止することは、それを参照するプログラムを専用のものにすることにより比較的容易に実現することが可能である。

【０００８】しかし、一般のワークステーション，パーソナルコンピュータは表示された画面をそのまま印刷する機能を持っているか、持っていなくても他のプログラムを動作させて表示されている画面を容易に印刷するこ

Petitioner Apple Inc. - Exhibit 1012, p. 1559

3

とが出来るようになっているため、自由に表示画面を印刷可能となり、一方、その画面印刷機能が無ければ通常の利用で不都合が生じることになり、その機能を無くすことは出来ないという問題がある。

【０００９】

【課題を解決するための手段】以上の問題を解決するために、表示された画面データの読みだしを司るプログラムに読みだしを制限する機能を設け、かつ、読みだしを制限すべき情報の表示領域（ウインドー）に読みだし制限の属性を持たせることによって解決する。

【００１０】

【作用】以上のような手段を設け、特定情報を表示するプログラムは上記読みだし制限の属性を表示ウインドーに与えて、表示し、一方、画面の読みだしを行うプログラムは読みだしを制限されたウインドーが少なくも一つ表示画面上に存在する場合は、その全面を読みだし禁止とするか、あるいは、読みだしを制限されたウインドーの領域のみ読みだし不可能として白地に抜いたデータを読みだし要求のあったプログラムに渡す等の手続きを実行することによって機密保護情報の印刷を防ぐことが出来る。

【００１１】

【実施例】以下、本発明の実施例を図に従って説明する。

【００１２】図１は本発明を実施する情報システム全体の構成例を示したもので、１は情報を蓄積し、要求に応じて情報を提供するデータベースサーバ、２はその情報を参照するためのクライアントワークステーション、３はネットワークである。

【００１３】更に、データベースサーバ１の内部を機能的に表現したものとして、１１はデータベースファイルであり文書等のデータ及びその管理情報が格納されている。１２はデータベース管理システム（以下ＤＢＭＳ）、１３はユーザインタフェースプログラム、１４は通信制御機能である。

【００１４】一方、クライアントワークステーション２の内部を機能的に表現したものとして、２１はサーバ内の通信制御と対になってコマンド，データの授受を行うための通信制御機能である。２２はウインドーサーバでUnixシステムのＸ－windowサーバ等がこれに相当し、サーバ１の中のユーザインタフェースプログラム１３の要求に応じて表示画面上での入出力処理を行う。又、２３はプリントサーバで１３の要求に応じて文書や表示画面の印刷処理を行う。

【００１５】このようなデータベースシステムにおいて、情報の機密管理は、通常計算機システムを利用する上でのＩＤ，パスワード管理と、データベースを利用する上でのＩＤ，パスワード管理が多重に行われ、情報の機密管理はＤＢＭＳ１２又はユーザインタフェースプログラム１３、あるいはその双方において後者を主体に行

4

われているが、参照の可否を管理しているに過ぎず、本発明では参照可否の他に参照結果の複写をも管理する。

【００１６】図２はその複写管理方法の例を説明したもので、文書管理ファイルは文書の実体データの格納されている文書ファイル自身を管理すると同時に、その参照及び複写可否の管理を行う。

【００１７】この時、参照管理プログラムはファイルの参照管理属性が「制限」を示している文書ファイルＷａの場合は、参照権管理ファイルをチェックして参照者が参照権，複写権を得ているかどうかをチェックしてその参照，複写を許可するかどうかを判定する。

【００１８】図２の例の場合はＩＤが「ＮＮＮＮＮ」の参照者は参照権が「許可」であるが、複写権が「不許可」となっているため複写要求を出してもそれは受け付けられないのに対して、ＩＤが「ＭＭＭＭ」の参照者は複写権が「許可」と登録されているため、複写要求は受け付けられ、複写サービスを受けることが出来る。

【００１９】一方、文書ファイルＦｂは参照管理属性がファイルそのものを複写不可とする「複写禁止」となっているため、参照者の権利のいかんに関わらず複写は許可されない。

【００２０】他方、参照管理属性が「無制限」となっている文書ファイルＦｃとＦｄは参照のみならず複写の制限もなく、無条件に複写サービスを受けることが可能であることを示している。

【００２１】このように、ファイルの参照，複写サービスを提供するか否かの管理を行うことが可能となる。

【００２２】この場合、「複写」の持つ意味は、データとしてファイルをフロッピーディスク等の他のメディアや他のワークステーションの磁気ディスク等の外部記憶装置への複写のみならず、プリンタへの出力も含まれるが、何に複写するかまでも細かく管理したい場合は、複写権管理ファイルの管理項目をきめ細かくすることによって可能である。

【００２３】しかし、以上のような管理を行っても、Unix等のＯＳ，Ｘ－windowのウインドサーバを搭載したワークステーションシステムの場合は、全く異なるプログラムを並行して動作させ、かつ、同一のディスプレイにマルチウインドで複数の画面を同時に表示することが出来、複写禁止の文書を一つのウインドで表示し、それとは関係のないプログラムを動かし今一つのウインドを表示し、そこから表示画面のハードコピーをウインドサーバ，プリントサーバを経由して複写禁止の画面をコピーすることは可能で、従来のウインドサーバ，プリントサーバをそのまま利用する限りこれを防止することは出来ない。

【００２４】それを示したのが図３で、ウインドＷａは複写禁止の文書を表示しており、他方、ウインドＷｂ，Ｗｃ，Ｗｄは複写を禁止されていない情報を表示している場合を示したもので、例えば、ウインドＷｂより画面

Petitioner Apple Inc. - Exhibit 1012, p. 1560

5

のハードコピーを要求するプログラムを動かせば、複写禁止ウインドを含めて画面全体をプリントアウトすることが出来る。

【0025】もちろん、ウインドWaを全面に表示し、ウインドWbを一時消去して、複写禁止文書の画面のみをプリントアウトすることも可能である。

【0026】そこで本発明は更に、画面（ウインド）を表示する時に、ウインドの属性として複写管理属性を持たせ、それが「複写禁止」となっているウインドが表示されている場合は、表示画面の読み取り，複写を禁止する機構を設けてそれを防止するものである。

【0027】図4はその属性を付加したウインド管理テーブルの一例を示したもので、一つのウインド管理テーブルには複写権の有無を設定する項目を追加し、既にある表示状態管理情報とを用いてその管理制御を行う。

【0028】図4で示す例は、ウインドWaが複写禁止属性を持ち、他のウインドWb，Wc，Wdは複写禁止となっていない。

【0029】従って、この場合は、ウインドWaが画面上に表示されている限りは他のウインドから画面コピーを要求しても、ウインドを管理しているウインドサーバが画面データを渡さないようにしておけば以上の問題を解決することが出来る。

【0030】図5は、参照者の要求に基づいて例えば文書ファイルを検索し、それを表示するユーザインタフェースプログラムのフローチャートの一例を示したもので、ステップ301，302は参照権チェックのためのユーザID，パスワードの入力である。この場合、ユーザID、及びパスワードの入力はワークステーションを利用開始時に入力するものをそのまま使用しても良いし、管理を厳しくするために別に設けても良い。又、ステップ301，302でユーザID、及びパスワードの入力だけではなく、このデータベースシステムのサービスを提供すべきユーザであるかどうかをチェックしてもよい。

【0031】次に303で検索項目を入力し、それに基づいてステップ304でデータベースに登録されたファイルを検索し、該当なファイルが存在しない場合は終了とし、ファイルがあった場合は次のステップ306，307で参照権，複写権のチェックを行う。

【0032】この時のチェックは図2に示す文書管理ファイル，参照管理ファイルのデータに基づいて行う。

【0033】ここで一般のデータベースと同様に、ユーザに参照権が与えられていない場合は、ここでは省略しているが、許可されていないことをユーザにメッセージを出して終了する。

【0034】一方、参照権が与えられている場合は、更にステップ307で複写権が与えられているかチェックし、複写権が与えられている場合はステップ310で複写許可の属性を持つウインドを生成し、他方、複写権の

6

無い場合はステップ309でウインドサーバが画面読み出しを禁止出来ているかどうかを確認し、読み出し可能であれば禁止機能がないとして表示を打切り、禁止出来ていれば読みだし保護が可能であると判断してステップ311以降の処理に入る。

【0035】そのあとでステップ311でファイルを読みだし、ステップ312でその表示データをクライアントワークステーション2のウインドサーバに送信することでユーザが利用しているワークステーションの表示画面上に文書ファイルが図3の例のように表示されることになる。

【0036】次に、図6はこの画面のハードコピーを他のプログラム等からプリントサーバに要求したときのプリントサーバのハードコピープログラムの一例を示したもので、印刷要求によって処理を開始し、ステップ401で表示画面の読みだし受渡しをウインドサーバに要求し、ステップ402でリターン情報でそれが正常に受け渡されたか、あるいは、複写禁止ウインドが含まれているかをチェックし、禁止されていなければ、ステップ403でその画面データをプリンタへ送り、ステップ404で印刷完了を待って終了する。

【0037】一方、画面の表示データを要求されたウインドサーバは、図7の例に示すように、ステップ501でウインド管理テーブルをチェックし、複写禁止属性を持つウインドが表示されていないときのみステップ502で画面データを読みだし、ステップ503で要求元にそのでデータを受け渡す。

【0038】以上のように、ウインドサーバが表示画面データの読みだしをウインド管理情報の複写権属性と表示状態を監視し、その読みだし可否によって受渡しを管理制御出来るようにすることによって表示画面の複写を制限する機能を実現することが可能となる。

【0039】次に、図8は文書ファイルをデータベースに登録する際の参照管理を行うときの処理を示したもので、ステップ601で参照属性を入力し、ステップ602でその属性を判断し、参照が禁止の場合はステップ603で参照禁止属性を付与し、参照制限であればステップ604で参照制限属性を付与し、ステップ605でその参照を管理するための参照管理ファイルを生成する。無制限であればステップ606で参照無制限属性を付与して、ステップ607でファイルを格納する。

【0040】この場合、基本の管理は参照のみとしそのもとで複写の可否を制限したものを示したが、情報の性格から無条件に複写が禁止されるべきものもあり、この場合は属性情報に複写禁止属性を追加すればその管理を行うことが出来る。

【0041】更にユーザごとの参照権登録処理のフローチャートとを示したものが図9である。図9において、データベース管理者は登録対象者と参照対象文書ファイルを指定し、システムはステップ701，702でそれ

Petitioner Apple Inc. - Exhibit 1012, p. 1561

7

を入力する。次にそれに対応した参照権をステップ７０３で入力し、ステップ７０４でそれをチェックし、参照権が与えられている場合はステップ７０５で参照許可属性を設定し、不許可であればステップ７０９で不許可属性を設定する。

【００４２】更に、参照権が与えられている場合は複写権をチェックし、複写権を与えている場合はステップ７０７で複写許可を設定し、与えない場合は不許可を設定する。その結果をステップ７１０で参照管理ファイルに登録して終了する。

【００４３】尚、図９では文書，参照者毎に参照権の設定を行っているが、文書の種類，参照者グループ毎の単位で設定，管理を行っても良い。

【００４４】

【発明の効果】本発明によれば、限られた範囲のユーザにデータベースの情報を提供し、かつ、その情報の複写持出しを制限，防止する上で大きな効果がある。

【図面の簡単な説明】

【図１】本発明の一実施例のブロック図。

【図２】本発明の文書管理ファイルの実施例の説明図。

【図３】本発明の画面表示例の説明図。

8

【図４】本発明のウインド管理テーブルの実施例の説明図。

【図５】本発明のデータベース検索処理実施例のフローチャート。

【図６】本発明の一実施例の画面印刷プログラムのフローチャート。

【図７】本発明の一実施例のウインドサーバの画面読み出し機能のフローチャート。

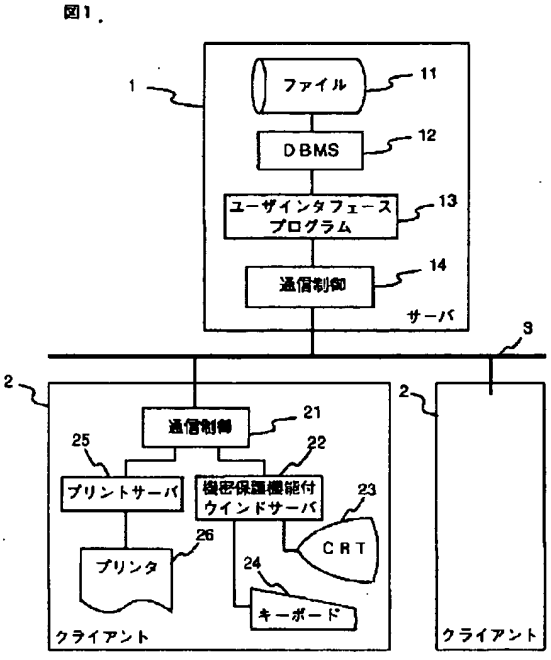
【図８】本発明の一実施例のデータベース参照，複写管理属性設定処理のフローチャート。

【図９】本発明の一実施例の参照者単位の参照権，複写権登録プログラムのフローチャート。

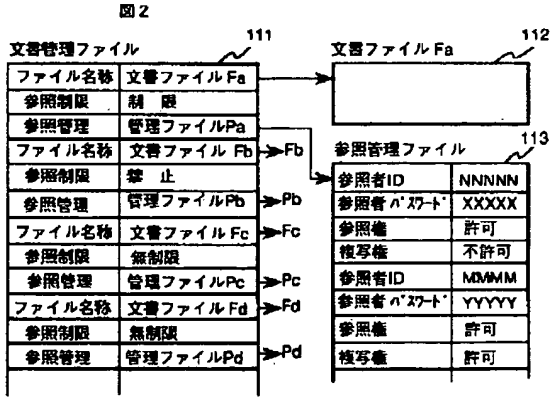
【符号の説明】

１…データベースサーバ、１１…その中のファイルシステム、１２…データベース管理システム、１３…ユーザインタフェースプログラム、１４…通信制御機能、２…クライアントシステム、２１…通信制御機能、２２…機密保護付きウインドサーバ、２３…ディスプレイ装置、２４…キーボード、２５…プリントサーバ、２６…プリンタ、３…サーバとクライアントを結ぶネットワーク。

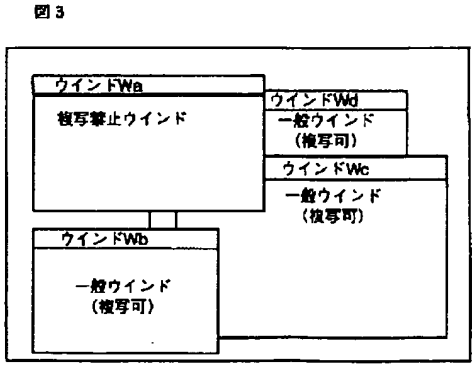
【図１】



【図２】



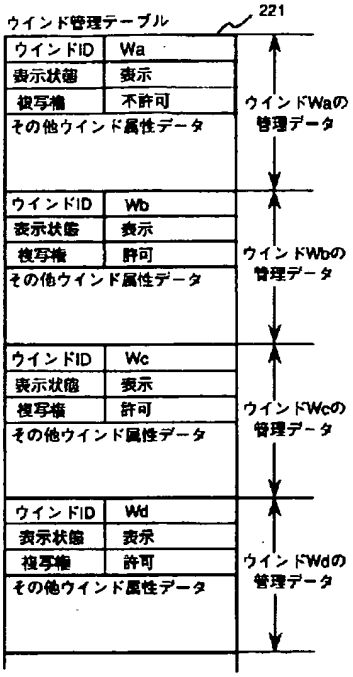
【図３】



Petitioner Apple Inc. - Exhibit 1012, p. 1562

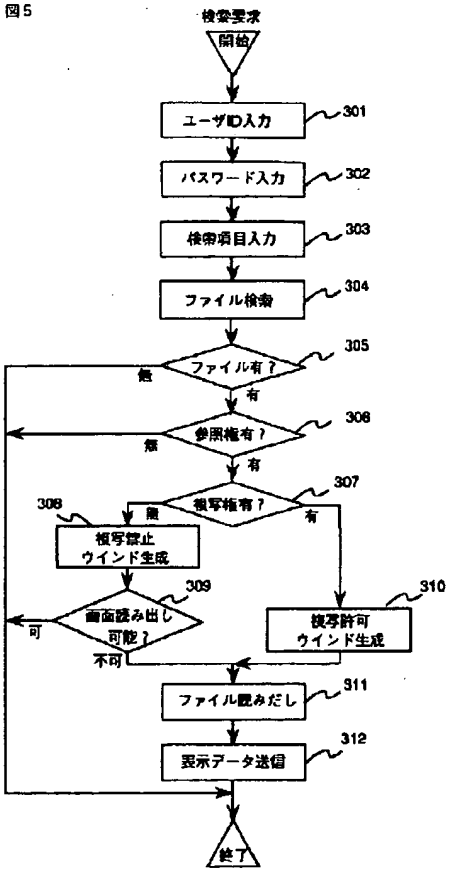
【図４】

図4



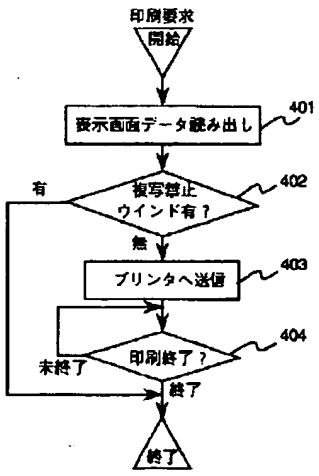
【図５】

図5



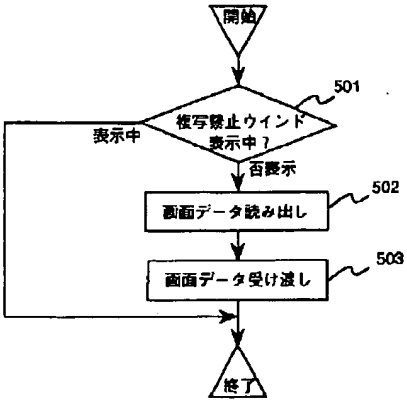
【図６】

図6



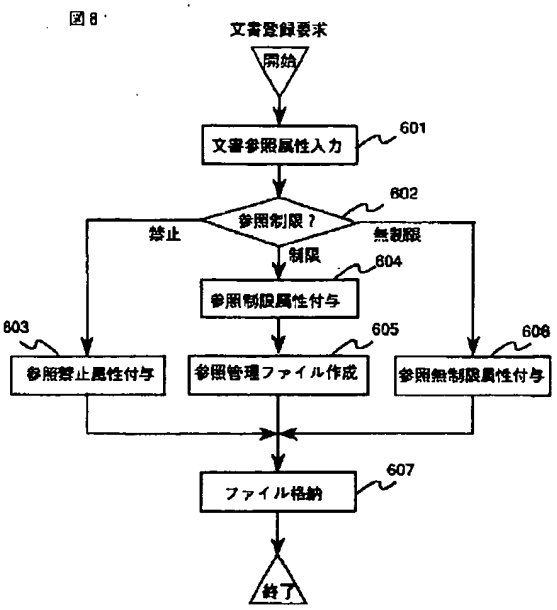
【図７】

図7

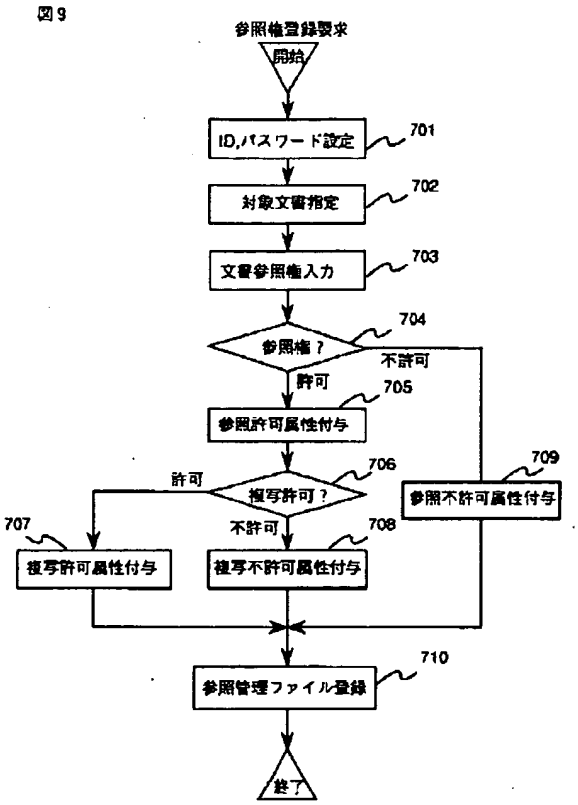


Petitioner Apple Inc. - Exhibit 1012, p. 1563

【図８】



【図９】



Petitioner Apple Inc. - Exhibit 1012, p. 1564

Requested Patent: JP7244639A

Title: ACCESS RIGHT MANAGEMENT DEVICE ;

Abstracted Patent: JP7244639 ;

Publication Date: 1995-09-19 ;

Inventor(s): OURA MASAHIKO ;

Applicant(s): FUJITSU LTD ;

Application Number: JP19940032713 19940303 ;

Priority Number(s): ;

IPC Classification: G06F15/00 ;

Equivalents: ;

ABSTRACT:

PURPOSE:To flexibly change the right to access and facilitate its management as to access right management for managing the adequacy of a process request in an information system which offers plural information process services to plural users.

CONSTITUTION:The access right management device has a user qualification file 41 which holds records consisting of user IDs and qualification IDs as items, an access right files 42 consisting of service IDs, qualification IDS or user IDs, the kinds of access and whether or not the access is allowed, and the priority of records as items, a request acceptance means 1, an access right determination means 2, an access right holding means 3, and a service start means 5. The access right determination means 2 takes a qualification ID out of the user qualification file 41 based on the user ID as a key, retrieves the access right file 42 based on the qualification ID and the user ID as keys, and determines and holds whether or not final access is allowed with a high-priority record regarding the same service in the access right holding means 3.

(19)日本国特許庁（ＪＰ）　(12) 公開特許公報（A）　(11)特許出願公開番号

特開平7－244639

(43)公開日　平成７年(1995)９月19日

(51)Int.Cl.[6]	識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ　15/00	３３０　Ａ	7459－5Ｌ		

審査請求　未請求　請求項の数３　ＯＬ　（全７頁）

(21)出願番号　特願平6－32713

(22)出願日　平成６年(1994)３月３日

(71)出願人　000005223
富士通株式会社
神奈川県川崎市中原区上小田中1015番地

(72)発明者　大浦　雅彦
神奈川県川崎市中原区上小田中1015番地
富士通株式会社内

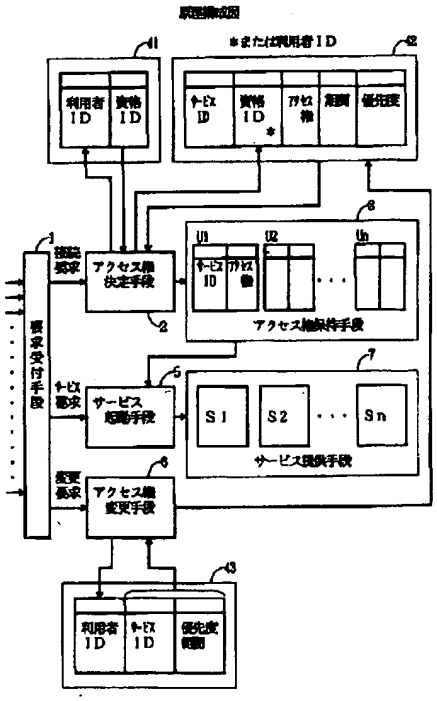
(74)代理人　弁理士　井桁　貞一

(54)【発明の名称】　アクセス権管理装置

(57)【要約】

【目的】多数の利用者を対象に複数の情報処理サービスを提供する情報システムでの処理要求の妥当性を管理するアクセス権管理に関し、アクセス権の変更を柔軟に、管理を容易にする。

【構成】利用者ＩＤと資格ＩＤとを項目とするレコードを保持する利用者資格ファイル41と、サービスＩＤと、資格ＩＤまたは利用者ＩＤと、アクセスの種類と可否と、レコードの優先度とを項目とするレコードを保持するアクセス権ファイル42と、要求受付手段１と、アクセス権決定手段２と、アクセス権保持手段３と、サービス起動手段５とを有する。アクセス権決定手段２は、利用者ＩＤをキーとして利用者資格ファイル41から資格ＩＤを取り出し、資格ＩＤと利用者ＩＤをキーとしてアクセス権ファイル42を検索して、同一のサービスについて優先度の高いレコードにより最終的なアクセスの可否を決定しアクセス権保持手段３に保持する。



Petitioner Apple Inc. - Exhibit 1012, p. 1566

1

【特許請求の範囲】

【請求項1】　複数の利用者に対し複数の処理サービスを提供する情報システムにおける利用者のサービスへのアクセス権を管理する装置であって、

利用者資格ファイル（41）と、アクセス権ファイル（42）と、要求受付手段（1）と、アクセス権決定手段（2）と、アクセス権保持手段（3）と、サービス起動手段（5）とを有し、

利用者資格ファイル（41）は、利用者ＩＤと、その利用者のサービスへのアクセスに関する資格を表す資格ＩＤとを項目とするレコードを保持し、

アクセス権ファイル（42）は、サービスＩＤと、資格ＩＤまたは利用者ＩＤと、アクセスの種類とその可否と、そのレコードの優先度とを項目とするレコードを保持し、

要求受付手段（1）は、利用者からの要求を受付けて、接続要求をアクセス権決定手段（2）へ、サービス要求をサービス起動手段（5）へ伝え、

アクセス権決定手段（2）は、利用者からの接続要求があると、利用者ＩＤをキーとして利用者資格ファイル（41）を検索してその利用者ＩＤの存在の確認と、対応する資格ＩＤの取り出しとを行い、資格ＩＤおよび利用者ＩＤをキーとしてアクセス権ファイル（42）を検索して、同一のサービスについて複数のレコードがある場合には、優先度の高いレコードのアクセス権の指定により最終的なアクセスの可否を決定して、利用者ＩＤごとにサービスＩＤとアクセスの可否とをアクセス権保持手段（3）に保持し、

サービス起動手段（5）は、受け付けた利用者からのサービスへのアクセス要求があると、利用者ＩＤとサービスＩＤとアクセス種類とを受け取り、その内容が、アクセス権保持手段の内容に合致する場合に指定されたサービス提供手段を起動し、合致しなければ拒絶するように構成したアクセス権管理装置。

【請求項2】　アクセス権ファイル（42）は、サービスＩＤと、資格ＩＤまたは利用者ＩＤと、アクセスの種類とその可否と、そのレコードの優先度と、そのレコードの有効期間とを項目とするレコードを保持し、アクセス権決定手段（2）は、アクセス権ファイル（42）のレコードにより最終的なアクセスの可否を決定する場合に、有効期間外のレコードは無視することを特徴とする請求項1に記載のアクセス権管理装置。

【請求項3】　管理者情報ファイル（43）とアクセス権変更手段（6）とを設け、

管理者情報ファイル（43）には、アクセス権ファイル（42）の更新を行なう権限をもつ利用者の利用者ＩＤとサービスＩＤと優先度範囲とを項目とするレコードを保持し、

アクセス権変更手段（6）は、要求受付手段（1）からアクセス権ファイル（42）の内容の変更要求を受ける

2

と、管理者情報ファイル（43）を検索し、その利用者が設定可能なサービスと優先度範囲をチェックし、それを許可するか否かを決定することを特徴とする請求項1または請求項2に記載のアクセス権管理装置。

【発明の詳細な説明】

【０００１】

【産業上の利用分野】本発明は多数の利用者を対象に複数の情報処理サービスを提供する情報システムに関する。特にその処理要求の妥当性を管理するアクセス権管理装置に関する。

【０００２】多数の利用者を対象に複数の情報処理サービスを提供する情報システムにおいては、サービスに対する要求（アクセスの種類・アクセス権）の管理・規制を行なっている。運用中に、利用者のアクセス権の変更・追加、特に一時的な変更や、サービスの追加・変更、特に一時的変更・試験的提供等の処理を行なうことが必要であり、それをシステムの安全性を損なわずに、かつ利用者の不便をきたさないように行なうことが要求されている。

【０００３】

【従来の技術】サービスには、例えば、電子伝票、会議室予約、旅費精算等の全員がアクセスできるものや、人事情報・評価のように特定の資格者のみアクセスできるものがある。

【０００４】サービスに対する要求の管理・規制の方法として、利用者個々に対して利用できるサービスとその処理内容（参照・更新等）や期間等を定義しておく方法が考えられるが、管理情報の量が膨大になるので、利用者の資格によるグループ設定を行い、このグループに対してアクセス権の内容を設定するやり方がある。グループはサービス毎に設定することができ、さらに、一般利用者、管理職、サービスの管理者あるいは処理の開発者等により分けることができる。

【０００５】予算申請を受け付けて登録するサービスのように、ある期間を設け、申請期限を過ぎてからの新規申請や申請データの修正は特定者以外には禁止する場合、従来の技術でも利用者の属するグループによるアクセス権の管理は実現可能である。ところで、そのサービスの管理者が、申請データを処理（例えば集計）する際に、申請データに誤りを発見し、その申請を行なった利用者に再申請を指示する必要がある場合を考える。このとき、申請期限は過ぎているので、他の利用者に対しては受け付けないようにする必要がある。従来の技術では、このような場合、その特定の利用者をその属するグループから一時的に外し、別のグループに（申請可能なグループ）に入れることになるが、特定の利用者は一時的に元のグループから外されるため、そのグループに許されていた他のサービスへのアクセスが制限されたり、逆に、本来制限されるはずのアクセスができてしまったりする可能性ができる。

Petitioner Apple Inc. - Exhibit 1012, p. 1567

3

【0006】

【発明が解決しようとする課題】従って、このような副作用を起こさないようにするには、この処理はかなり面倒な管理を必要とするものとなる。すなわち、関連するアクセス権情報を矛盾のないようにすべて修正し、さらに一時的な処置が済んだ時点で早急にもとに戻す必要がある。

【0007】本発明は、個々のアクセス権情報に優先度表示を付けて複数のアクセス権情報を同時に存在させ、優先度の高い情報によって実際のアクセス権を決定することにより、一時的な変更を含めてアクセス権の変更を柔軟にでき、かつ管理が容易なアクセス権管理装置を実現することを目的としている。

【0008】

【課題を解決するための手段】図1は本発明の原理構成図である。複数の利用者に対し複数の処理サービスを提供する情報システムにおける利用者のサービスへのアクセス権を管理する装置であって、第1の発明は、利用者資格ファイル41と、アクセス権ファイル42と、要求受付手段1と、アクセス権決定手段2と、アクセス権保持手段3と、サービス起動手段5とを有する。

【0009】利用者資格ファイル41は、利用者ＩＤと、その利用者のサービスへのアクセスに関する資格を表す資格ＩＤとを項目とするレコードを保持する。アクセス権ファイル42は、サービスＩＤと、資格ＩＤまたは利用者ＩＤと、アクセスの種類とその可否と、そのレコードの優先度とを項目とするレコードを保持する。

【0010】要求受付手段1は、利用者からの要求を受付けて、接続要求をアクセス権決定手段2へ、サービス要求をサービス起動手段5へ伝える。アクセス権決定手段2は、利用者からの接続要求があると、利用者ＩＤをキーとして利用者資格ファイル41を検索してその利用者ＩＤの存在の確認と、対応する資格ＩＤの取り出しとを行い、資格ＩＤおよび利用者ＩＤをキーとしてアクセス権ファイル42を検索して、同一のサービスについて複数のレコードがある場合には、優先度の高いレコードのアクセス権の指定により最終的なアクセスの可否を決定して、利用者ＩＤごとに、サービスＩＤとアクセスの可否とをアクセス権保持テーブルとしてアクセス権保持手段3に保持する。

【0011】サービス起動手段5は、受け付けた利用者からのサービスへのアクセス要求があると、利用者ＩＤとサービスＩＤとアクセス種類とを受け取り、その内容が、アクセス権保持テーブルの内容に合致する場合に指定されたサービス提供手段を起動し、合致しなければ拒絶する。

【0012】第2の発明は、アクセス権ファイル42は、サービスＩＤと、資格ＩＤまたは利用者ＩＤと、アクセスの種類とその可否と、そのレコードの優先度と、そのレコードの有効期間とを項目とするレコードを保持する。そして、アクセス権決定手段2は、アクセス権ファイル42のレコードにより最終的なアクセスの可否を決定する場合に、有効期間外のレコードは無視する。

4

【0013】第3の発明は、管理者情報ファイル43とアクセス権変更手段6とを設け、管理者情報ファイル43は、アクセス権ファイル42の更新を行なう権限をもつ利用者の利用者ＩＤとサービスＩＤと優先度範囲とを項目とするレコードを保持する。

【0014】アクセス権変更手段6は、要求受付手段1からアクセス権ファイル42の内容の変更要求を受けると、管理者情報ファイル43を検索し、その利用者が設定可能なサービスと優先度範囲をチェックし、それを許可するか否かを決定する。

【0015】

【作用】利用者が情報システムにログインしてきたとき、要求受付手段1は接続要求として利用者ＩＤ（例えばＵ1）をアクセス権決定手段に渡す。アクセス権決定手段2は、利用者ＩＤをキーとして利用者資格ファイル41を検索し、資格ＩＤを得る。さらに、資格ＩＤと、利用者ＩＤとをキーとしてアクセス権ファイル42を検索して、どちらかを含むレコードを抽出する。ここで、もし同一サービスに対するレコードが複数ある場合は、優先度の値が一番大きなレコードのアクセス可否項目をアクセス権として採用する。このようにしてサービスＩＤとアクセス権とを対応させたアクセス権保持テーブルを生成してアクセス権保持手段3に保持する。この対応テーブルは利用者ＩＤごとに区別しておく。利用者がログアウトした場合は、その利用者ＩＤのアクセス権保持テーブルは削除することになる。

【0016】利用者からのサービスＳ1へのアクセス要求を受けて、要求受付手段1は利用者ＩＤとサービスＩＤとをサービス起動手段5へ渡す。サービス起動手段5は、アクセス権保持手段に保持されたアクセス権保持テーブルを参照してアクセス可能と判断したらサービス提供手段の所定のサービスを起動する。

【0017】このように構成することにより、アクセス権ファイルには、同じサービスに対する同じ利用者の異なるアクセス権を指定したレコードが複数存在することになるが、どちらの指定を採るかが優先度によって決定され一意に定まる。従って、部分的に、または一時的にアクセス権を変更する場合に、変更したい内容にした（優先度の値は大きい）レコードを追加することができる。もとにもどす場合にはそれを削除するだけでよい。

【0018】第2の発明では、アクセス権を指定したレコードの有効期間を項目の1つにして指定してあるので、その期間外であれば、そのレコードは無いのと同じであり、前もって追加しておいたり、削除を延ばしたりしても問題がなく、アクセス権管理が容易になる。

【0019】第3の発明では、アクセス権ファイル42の内容更新を要求された場合には、更新要求者の利用者Ｉ

Petitioner Apple Inc. - Exhibit 1012, p. 1568

5

Ｄをキーとして管理者情報43を検索し、該当する項目が存在しなければ、更新要求を拒絶し、存在するならば変更対象のサービスＩＤと設定可能な優先度の範囲を限度としてアクセス権の更新を許可する。従って、アクセス権の変更を適正に行なうことができる。

【００２０】

【実施例】以下、図面を参照して本発明の実施例を説明する。図２は本発明の一実施例の構成図である。図１と同一の機能のものは、同一の符号を付して示す。

【００２１】図２において、利用者用の端末装置91は回線90を通じて情報システム92に接続されている。情報システム92は、メモリ81、プロセサ82、ファイル装置83、通信制御装置84よりなる。メモリ81には、全体を制御するオペレーティングシステム70と、利用者から要求されたサービスを実行するサービスプログラム７と、図１の原理構成図に示したアクセス権管理のための手段を実現したプログラムとがある。アクセス権管理のための手段を実現したプログラムは、端末装置91から入力されたコマンドを受け付けたり、サービスの実行結果を端末装置91に表示する制御を行なう要求受付部１と、利用者毎のアクセス権を決定するアクセス権決定部２と、アクセス権のチェックを行なってサービスプログラムを起動するサービス起動部５と、アクセス権を変更するためのアクセス権変更部６とよりなる。

【００２２】利用者の情報を格納した利用者資格ファイル41と、各サービスのアクセス権情報を格納したアクセス権ファイル42と、アクセス権情報を管理する管理者の情報を格納した管理者情報ファイル43とはファイル装置83に保持され、利用者毎のアクセス権の内容を保持するアクセス権保持部３はメモリ81またはファイル装置に保持される。これらのファイルやテーブルの操作、端末装置91とのやり取り等はオペレーティングシステム70を通して行なうが、自明のこととして以下の説明では省略する。

【００２３】図３は本実施例のファイル構成図である。図３（１）は利用者資格ファイル41の構成を示す。各利用者には、利用者ＩＤ、パスワード、所属グループが定義してある。

【００２４】図３（２）は、アクセス権ファイル42の構成を示す。アクセス権情報はそれぞれ、対象となるサービス、グループ、処理（参照、更新毎の可否）、期間、優先度の各項目で構成されている。項目の値が‘ ALL ’の場合は、その項目についてはすべてが対象となることを示す。また、グループの項目には、グループＩＤ（資格ＩＤ）の他に、利用者ＩＤを設定することもできる。期間の項目は、そのアクセス権情報レコードが適用される期間を示している。優先度の項目は、同一サービス、同一利用者に対してレコードが複数あるとき数値が大きいレコードが優先して使用されることを示す。

【００２５】図３（３）は、管理者情報ファイル43の構成を示す。管理者情報ファイル43は、管理対象となるサービスのＩＤと、管理者の利用者ＩＤと設定可能な優先度の範囲を示す値が定義してある。

6

【００２６】情報システムのサービスの例として、本実施例では電子伝票Ｓ１、会議室予約Ｓ２、旅費精算Ｓ３等が提供されている。上記サービスを提供するため、サービスプログラム７は、各サービスを実現するプログラムモジュール（Ｓ１，Ｓ２，Ｓ３，・・・）から成り、各サービスはサービス起動部５によって対応するプログラムモジュールが起動されることによって行なわれる。

【００２７】以下に、本実施例の動作について説明する。まず利用者（ＩＤ：Ｕ１）は、端末装置91を操作して、接続要求をする。具体的には、端末装置91から利用者ＩＤとパスワードを入力する。すると要求受付部１は、入力された利用者のＩＤとパスワードの組を渡してアクセス権決定部２を起動する。アクセス権決定部２は利用者資格ファイル41から抽出した情報と照合して、もし、照合の結果が一致すれば接続要求を受理し、そうでなければ拒絶する。この段階はいわゆるログイン処理である。接続要求が受理された利用者については、以下の手順でアクセス権の調査が行なわれ、その結果がアクセス権保持テーブルとしてアクセス権保持部３に書き込まれ、その利用者が情報システム92との接続を開放（ログアウト）するまで保持される。そして、利用者からのサービスへのアクセス要求があるたびに、サービス起動部５は、このアクセス権保持テーブルの内容をチェックし、利用者が所望するサービスと処理に関するアクセス権が‘可’であれば、対応するプログラムモジュールを起動し、‘否’であれば利用できない旨のメッセージを端末装置91に送る処理を行なう。

【００２８】アクセス権保持部３への利用者のアクセス権の格納の手順を、図３、図４を参照しながら以下に説明する。アクセス権決定部３は、要求受付部１からの要求を受けてまず利用者資格ファイル41から利用者Ｕ１が所属するグループ（資格ＩＤ）を抽出する（この例ではＧ１とＧ３に属している）。

【００２９】次に、情報システムで提供されている各サービスについて以下の処理を行なう。サービスＳ１に対するアクセス権を求めるために、先ずアクセス権ファイル42から、サービスの値が‘ ALL ’または‘Ｓ１’であり、かつグループの値が‘ ALL ’または利用者Ｕ１が所属するグループ（Ｇ１，Ｇ３）または利用者のＩＤ（この場合Ｕ１）と一致するレコードで、期間の指定があればその期間内であるものを抽出し、優先度の値が最大であるレコードの値を各処理（更新、参照）ごとに求め、アクセス権保持部３に格納する。この操作をすべてのサービスについて繰り返す。

【００３０】図４（１）は、アクセス権ファイル42に、図３（２）のａ～ｃのレコードが登録され有効である場合（すなわちレコードｄがない場合または指定期間外）

Petitioner Apple Inc. - Exhibit 1012, p. 1569

に、アクセス権保持部３に格納される利用者ＩＤ＝Ｕ１の利用者に関する情報すなわちアクセス権保持テーブルの内容の例である。

【００３１】図４（２）は、アクセス権ファイル42に図３（２）のａ～ｄのレコードが登録され有効である場合（すなわちレコードｄがあり指定期間内の場合）に、アクセス権保持部３に格納される利用者ＩＤ＝Ｕ１の利用者に関する情報すなわちアクセス権保持テーブルの内容の例である。

【００３２】このアクセス権ファイルのレコードｄは、従来技術の項で述べた電子伝票の誤りを訂正するような場合に、利用者Ｕ１のみ更新できるように一時的に追加した項目であり、利用者Ｕ１が更新を完了したらこの項目を削除することにより、本来のアクセス権設定状態に戻すことができる。なお、削除しなくても指定期間外になれば自動的に無効になる。

【００３３】なお、図３（２）のアクセス権ファイルの内容を説明する。レコードａは、すべてのサービスをすべての利用者に開放することを意味する。このレコードだけであれば、なんの制約もなくアクセスできる。レコードｂが追加されると、サービスＳ１についてはグループＧ１とＧ２に属する利用者にのみ更新アクセスが期間を限って許されなくなる。レコードｃが追加されると、指定された期間の間は、それまで全員がアクセスできたサービスＳ３がアクセスできなくなる。これは例えば、サービスＳ３の内容の変更のため一時的にサービスを中止する場合である。レコードｄが追加された場合は、先に説明した通りである。

【００３４】一方、利用者が端末装置91からアクセス権ファイル42の更新を要求した場合、要求受付部１はアクセス権変更部６を起動する。アクセス権変更部６は、管理者情報ファイル43に、更新を要求している利用者ＩＤと更新を要求しているサービスＩＤの組が登録されていれば、そこに登録されている優先度の範囲でそのサービスについてのアクセス権管理情報のレコードをアクセス権ファイル42に追加・削除・更新を許可する。これにより、アクセス権の変更がみだりに行なわれたり、誤って他のサービスに影響するようなことを防ぐことができる。

【００３５】

【発明の効果】以上説明したように、情報システムの運用中にアクセス権の変更を柔軟にでき、かつ管理が容易なアクセス権管理装置を実現することができる。システムの安全性を損なわずに、かつ利用者の不便をきたさないように、利用者のアクセス権の変更・追加、特に一時的な変更や、サービスの追加・変更、特に一時的変更・試験的提供等の処理を行なうことができる。

【図面の簡単な説明】

【図１】　本発明の原理構成図

【図２】　本発明の実施例の構成図

【図３】　実施例のファイル構成図

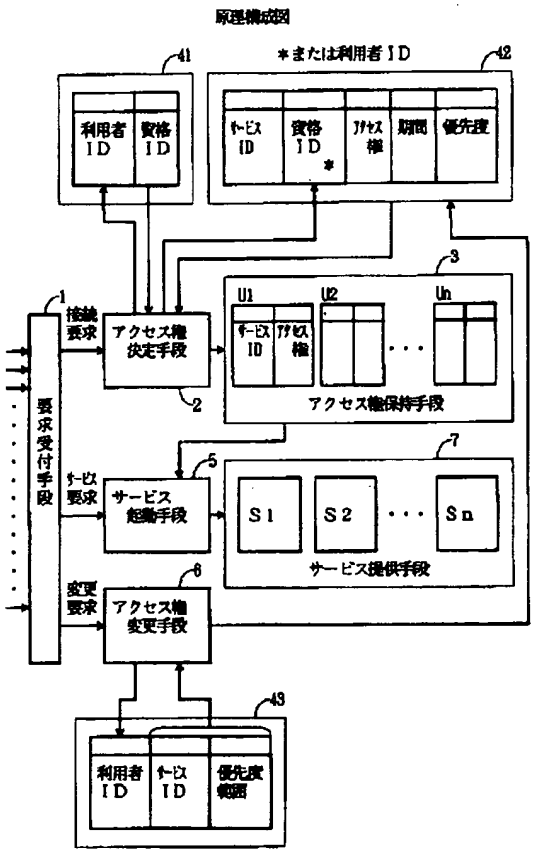
【図４】　アクセス権保持テーブルの内容の例

【符号の説明】

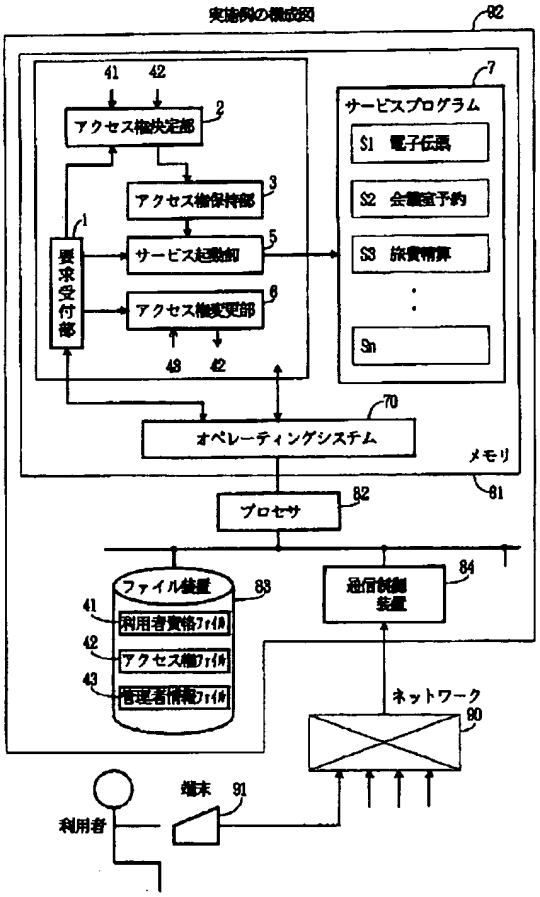
1　要求受付手段（要求受付部）
2　アクセス権決定手段（アクセス権決定部）
3　アクセス権保持手段（アクセス権保持部）
41　利用者資格ファイル
42　アクセス権ファイル
43　管理者情報ファイル
5　サービス起動手段（サービス起動部）
6　アクセス権変更手段（アクセス権変更部）
7　サービス提供手段（サービスプログラム）
70　オペレーティングシステム
81　メモリ
82　プロセサ
83　ファイル装置
84　通信制御装置
90　ネットワーク
91　端末装置
92　情報システム

Petitioner Apple Inc. - Exhibit 1012, p. 1570

【図1】



【図2】



【図4】

アクセス権保持テーブルの内容の例　（ID：U1の場合）

（1）レコードdがない場合または指定期間外の場合

サービス	参照	更新
S1	可	否
S2	可	可
S3	否	否
：		

（2）レコードdがあり指定期間内の場合

サービス	参照	更新
S1	可	可
S2	可	可
S3	否	否
：		

Petitioner Apple Inc. - Exhibit 1012, p. 1571

【図3】

実施例のファイル構成図

(1) 利用者資格ファイル

利用者ID	パスワード	グループ(資格)
U1	ABCD	G1, G3
U2	DEFG	G1, G2
U3	GHIJ	G1
M11	XYZA	G1, G10
・		

(2) アクセス権ファイル

	サービス	グループ	参照	更新	期間	優先度
a	ALL	ALL	可	可		10
b	S1	G1, G2		否	94/7/21 ～95/7/20	100
c	S3	ALL	否	否	94/7/20 ～94/7/22	50
d	S1	U1		可	94/7/21 ～94/7/21	200
	・					
	・					

(3) 管理者情報ファイル

サービス	利用者ID	優先度範囲
S1	M11	1～200
S2	M12, M13	1～100
S3	M31	1～100
S3	M32	1～500
・		
・		

Petitioner Apple Inc. - Exhibit 1012, p. 1572

EP 17024 C

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00 — A1

(11) International Publication Number: **WO 98/11690**

(43) International Publication Date: 19 March 1998 (19.03.98)

(21) International Application Number: PCT/US97/16223

(22) International Filing Date: 12 September 1997 (12.09.97)

(30) Priority Data:

60/025,991	12 September 1996 (12.09.96)	US
08/887,723	3 July 1997 (03.07.97)	US

(71)(72) Applicant and Inventor: GLOVER, John, J. [US/US]; 26 Amaranth Avenue, Medford, MA 02155 (US).

(74) Agent: GORDON, Peter, J.; Wolf, Greenfield & Sacks, P.C., 600 Atlantic Avenue, Boston, MA 02210 (US).

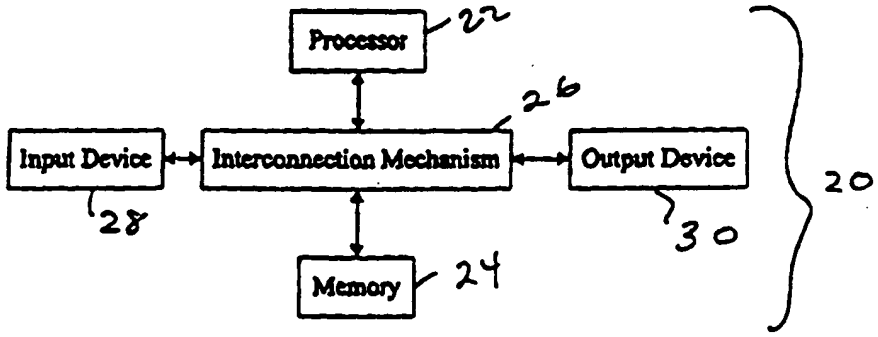
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published

With international search report.

Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SELF-DECRYPTING DIGITAL INFORMATION SYSTEM AND METHOD



(57) Abstract

The claimed data protection device (20) includes a processor (22) connected to a memory system (24) through an interconnection mechanism (26). An input device (28) is also connected to the processor (22) and memory system (24) through the interconnection mechanism (26). The interconnection mechanism (26) is typically a combination of one or more buses and one or more switches. The output device (30) may be a display, and the input device (28) may be a keyboard and/or mouse or other cursor control device.

BNSDOCID <WO___9811690A1_I_>

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

BNSDOCID <WC__9811690A1_I_>

SELF-DECRYPTING DIGITAL INFORMATION SYSTEM AND METHOD

Field of the Invention

The present invention is related to mechanisms for protecting digital information from being copied. In particular, the present invention is related to mechanisms which permit authorized execution of computer program code or access to other digital information which is encrypted or otherwise encoded.

Background of the Invention

A serious problem which faces the electronic publishing and software industries is the ease with which digital information can be copied without authorization from the publisher. Digital information also may be used or modified without authorization. For example, computer software may be reverse engineered or attacked by computer viruses.

There are many mechanisms available which may be used to limit or prevent access to digital information. Such mechanisms often either restrict the ability of the user to make back-up copies or involve the use of special purpose hardware to limit access to the digital information. For example, some mechanisms restrict the use of digital information to a particular machine. See, for example, U.S. Patent 4,817,140. Other mechanisms require the digital information to be stored on a particular recording medium in order to be used. See, for example, U.S. Patent 5,412,718. Yet other mechanisms allow only a certain number of uses of the digital information. See for example, U.S. Patent 4,888,798. Many of these access control mechanisms cause distribution to be more costly.

Several other patents describe a variety of systems for encryption, compression, licensing and royalty control and software distribution such as: U.S. Pat. No. 4,405,829, U.S. Pat. No. 4,864,616, U.S. Pat. No. 4,888,800, U.S. Pat. No. 4,999,806, U.S. Pat. No. 5,021,997, U.S. Patent No. 5,027,396, U.S. Pat. No. 5,033,084, U.S. Pat. No. 5,081,675, U.S. Pat. No. 5,155,847, U.S. Pat. No. 5,166,886, U.S. Pat. No. 5,191,611, U.S. Pat. No. 5,220,606, U.S. Pat. No. 5,222,133, U.S. Pat. No. 5,272,755, U.S. Pat. No. 5,287,407, U.S. Pat. No. 5,313,521, U.S. Pat. No. 5,325,433, U.S. Pat. No. 5,327,563, U.S. Pat. No. 5,337,357, U.S. Pat. No. 5,351,293, U.S. Pat. No. 5,341,429, U.S. Pat. No. 5,351,297, U.S. Pat. No. 5,361,359, U.S. Pat. No. 5,379,433, U.S. Pat. No. 5,392,351, U.S. Pat. No. 5,394,469, U.S. Pat. No. 5,414,850, U.S. Pat. No. 5,473,687, U.S. Pat. No. 5,490,216, U.S. Pat. No. 5,497,423, U.S. Pat. No. 5,509,074, U.S.

Petitioner Apple Inc. - Exhibit 1012, p. 1575

Pat. No. 5,,511,123, U.S. Pat. No. 5,524,072, U.S. Pat. No. 5,532,920, U.S. Pat. No. 5,555,304, U.S. Pat. No. 5,557,346, U.S. Pat. No. 5,557,765, U.S. Pat. No. 5,592,549, U.S. Pat. No. 5,615,264, U.S. Pat. No. 5,625,692, and U.S. Pat. No. 5,638,445.

Computer programs or other digital information also may be encrypted in order to prevent an individual from making a useful copy of the information or from reverse engineering a program. Even with such encryption, however, a computer program must be decrypted in order for a computer to load and execute the program. Similarly, other digital information must be decrypted before it can be accessed and used. Generally, digital information is decrypted to disk, and not to main memory of the computer which is more protected by the operating system, because decryption to main memory results in a significant loss of memory resources. If the purpose for using encryption is to prevent users from copying the digital information, then decryption of the information to accessible memory for use defeats this purpose.

One way to protect digital information using encryption has been made available by International Business Machines (IBM) and is called a "CRYPTOLOPE" information container. This technology is believed to be related to U.S. Patent Nos. 5,563,946 and 5,598,470 (to Cooper et al.), and published European patent applications 0679977, 0679978, 0679979 and 0681233. The CRYPTOLOPE system requires a user to have a "helper application" and a key. The CRYPTOLOPE information container is generated by IBM. The content provider submits data to IBM, which in turn encrypts and packages the data in a CRYPTOLOPE information container. The helper application is a form of memory resident program, called a terminate and stay resident (TSR) program, which is a form of input/output (I/O) device driver installed in the operating system and which monitors requests from the operating system for files on specified drives and directories. Because the TSR program must know the directory, and/or file name to be accessed, that information also is available to other programs. Other programs could use that information to manipulate the operation of the TSR program in order to have access to decrypted contents of the information container. The encrypted information container includes an executable stub which is executed whenever the application is run without the installed TSR program or from a drive not monitored by the TSR program to prevent unpredictable activity from executing encrypted code. This stub may be used to install decryption and cause the application be executed a second time, or to communicate with the TSR program to instruct the TSR program to monitor the drive. It may be preferable from the point of view of the content provider however to maintain an encryption process and keys independently of any third party.

Petitioner Apple Inc. - Exhibit 1012, p. 1576

Multimedia content, such as a movie or hypertext presentation also may be stored on a digital versatile disk (DVD), sometimes called a digital video disk, compact disk read-only memory (CD-ROM), rewriteable compact disks (CD-RW) or other medium in an encrypted digital format for use with special-purpose devices. For example, concern about illegal copying of content from digital video disks or other digital media has resulted in a limited amount of content being available for such devices. This problem has caused representatives of both multimedia providers and digital video disk manufacturers to negotiate an agreement on an encryption format for information stored on DVDs. This copy protection scheme is licensed through an organization called the CSS Interim Licensing organization. However, in this arrangement, the content provider is limited to using the agreed upon encryption format and a device manufacturer is limited to using a predetermined decryption system.

Encryption has also been used to protect and hide computer viruses. Such viruses are typically polymorphic, i.e., they change every time they infect a new program, and are encrypted. The virus includes a decryption program that executes to decrypt the virus every time the infected program is run. Such viruses are described, for example, in "Computer Virus-Antivirus Coevolution" by Carey Nachenberg, Communications of the ACM, Vol. 40, No. 1, (Jan. 1997), p. 46 et seq. Such viruses include decryption keys within them since, clearly, their execution is not carried out by the user and a user would not be asked for authorization keys to permit execution of the viruses. Additionally, such viruses are typically only executed once at the start of execution of an infected program and permanently return control to the infected program after execution.

Summary of the Invention

Some of these problems with digital information protection systems may be overcome by providing a mechanism which allows a content provider to encrypt digital information without requiring either a hardware or platform manufacturer or a content consumer to provide support for the specific form of corresponding decryption. This mechanism can be provided in a manner which allows the digital information to be copied easily for back-up purposes and to be transferred easily for distribution, but which should not permit copying of the digital information in decrypted form. In particular, the encrypted digital information is stored as an executable computer program which includes a decryption program that decrypts the encrypted information

Petitioner Apple Inc. - Exhibit 1012, p. 1577

to provide the desired digital information, upon successful completion of an authorization procedure by the user.

In one embodiment, the decryption program is executed as a process within a given operating system and decrypts the digital information within the memory area assigned to that process. This memory area is protected by the operating system from copying or access by other processes. Even if access to the memory area could be obtained, for example through the operating system, when the digital information is a very large application program or a large data file, a copy of the entire decrypted digital information is not likely to exist in the memory area in complete form.

By encrypting information in this manner, a platform provider merely provides a computer system with an operating system that has adequate security to define a protected memory area for a process and adequate functionality to execute a decryption program. The content provider in turn may use any desired encryption program. In addition, by having a process decrypt information within a protected memory area provided by the operating system, the decrypted information does not pass through any device driver, memory resident program or other known logical entity in the computer system whose behavior may be controlled to provide unauthorized access to the data. The ability to reverse engineer or attack a computer program with a computer virus also may be reduced.

In another embodiment, the decryption program is part of a dynamically loaded device driver that responds to requests for data from the file containing the encrypted data. When the digital information product is first executed, this device driver is extracted from the file and is loaded into the operating system. The executed digital information product then informs the loaded device driver of the location of the hidden information in the file, any keys or other passwords, and the name of a phantom directory and file to be called that only the digital information product and the device driver know about. The name of this directory may be generated randomly. Each segment of hidden information in the digital information product may be assigned its own unique file name in the phantom directory. The digital information product then makes a call to the operating system to execute one of the files in the phantom directory. The loaded driver traps these calls to the operating system, accesses the original file, decrypts the desired information and outputs the desired information to the operating system.

In combination with other mechanisms that track distribution, enforce royalty payments and control access to decryption keys, the present invention provides an improved method for

Petitioner Apple Inc. - Exhibit 1012, p. 1578

identifying and detecting sources of unauthorized copies. Suitable authorization procedures also enable the digital information to be distributed for a limited number of uses and/or users, thus enabling per-use fees to be charged for the digital information.

Accordingly, one aspect of the invention is a digital information product including a computer-readable medium with digital information stored thereon. The digital information includes computer program logic having a first portion of executable computer program logic and a second portion of digital information. The first portion of executable program logic, when executed, defines a mechanism for responding to requests for digital information from an operating system of a computer. This mechanism, when used to access the second portion of the encrypted digital information, decrypts the encrypted digital information, and provides the encrypted digital information to the operating system.

In the foregoing aspect of the invention, the digital information may be executable computer program logic. Hence, one aspect of the invention is a computer program product, including a computer readable medium with computer program logic stored thereon. The computer program logic includes a first portion of executable computer program logic and a second portion of encrypted computer program logic. The first portion of executable computer program logic, when executed, defines a mechanism for responding to requests for computer program logic from an operating system of a computer. This mechanism accesses the second portion of encrypted computer program logic, decrypts the encrypted computer program logic, and provides the decrypted computer program logic to the operating system.

Another aspect of the present invention is a computer program product, a computer system and a process which produce a computer program or digital information product in accordance with other aspects of the invention, using executable program code for the first and second portions of the desired computer program product.

Another aspect of the present invention is a computer program product including a self-decrypting encrypted executable computer program. The product includes a computer readable medium having computer program logic stored thereon. The computer program logic defines first, second and third modules, wherein the third module defines the encrypted executable computer program. The first module, when executed by a computer, defines a mechanism for loading the second module into memory of the computer. The second module, when executed by a computer, defines a mechanism for communicating with an operating system of the computer to receive requests for program code from the encrypted executable computer program from the

Petitioner Apple Inc. - Exhibit 1012, p. 1579

third module, and for processing the requests to access and decrypt the encrypted executable computer program and for providing the decrypted executable code from the third module to the operating system.

Another aspect of the invention is a process for executing encrypted executable computer programs on a computer system having a processor, memory and operating system. The process involves receiving computer program logic having a first module defining a start up routine, a second module, and a third module containing the encrypted executable computer program. The first module of the received computer program logic is executed using the processor. When the first module is executed, the second module is caused to be loaded into the memory of the computer system. Requests are generated from the operating system for data from the encrypted executable computer program and are received by the second module. The second module accesses and decrypts the encrypted executable computer program in response to these requests and returns the decrypted executable computer program to the operating system.

These and other aspects, advantages and features of the present invention and its embodiments will be more apparent given the following detailed description.

Brief Description of the Drawing

In the drawing,

Fig. 1 is a block diagram of a typical computer system with which the present invention may be implemented;

Fig. 2 is a block diagram of a memory system in the computer system of Fig. 1;

Fig. 3 is a diagram of a computer program or digital information product which may be recorded on a computer readable and writable medium, such as a magnetic disc;

Fig. 4 is a flowchart describing how the computer program or digital information product of Fig. 3 is used;

Fig. 5 is a flowchart describing operation of an example unwrap procedure as shown in Fig. 3 in one embodiment of the invention;

Fig. 6 is a flowchart describing operation of an example device driver as shown in Fig. 3 in one embodiment of the invention;

Fig. 7 is a block diagram of a computer system in the process of executing a computer program product in accordance with one embodiment of the invention;

Petitioner Apple Inc. - Exhibit 1012, p. 1580

Fig. 8 is a flowchart describing operation of an example unwrap procedure in another embodiment of the invention; and

Fig. 9 is a flowchart describing how a computer program product such as shown in Fig. 3 is constructed.

Detailed Description

The present invention will be more completely understood through the following detailed description which should be read in conjunction with the attached drawing in which similar reference numbers indicate similar structures.

Embodiments of the present invention may be implemented using a general purpose digital computer or may be implemented for use with a digital computer or digital processing circuit. A typical computer system 20 is shown in Fig. 1, and includes a processor 22 connected to a memory system 24 via an interconnection mechanism 26. An input device 28 also is connected to the processor and memory system via the interconnection mechanism, as is an output device 30. The interconnection mechanism 26 is typically a combination of one or more buses and one or more switches. The output device 30 may be a display and the input device may be a keyboard and/or a mouse or other cursor control device.

It should be understood that one or more output devices 30 may be connected to the computer system. Example output devices include a cathode ray tube (CRT) display, liquid crystal display (LCD), television signal encoder for connection to a television or video tape recorder, printers, communication devices, such as a modem, and audio output. It also should be understood that one or more input devices 28 may be connected to the computer system. Example input devices include a keyboard, keypad, trackball, mouse, pen and tablet, communication device, audio or video input and scanner. It should be understood that the invention is not limited to the particular input or output devices used in combination with the computer system or to those described herein.

The computer system 20 may be a general purpose computer system, which is programmable using a high level computer programming language, such as "C++," "Pascal," "VisualBasic." The computer system also may be implemented using specially programmed, special purpose hardware. In a general purpose computer system, the processor is typically a commercially available processor, such as the Pentium processor from Intel Corporation. Many other processors are also available. Such a processor executes a program called an operating

Petitioner Apple Inc. - Exhibit 1012, p. 1581

system, such as Windows 95 or Windows NT 4.0, both available from Microsoft Corporation, which controls the execution of other computer programs and provides scheduling, debugging, input output control, accounting compilation, storage assignment, data management and memory management, and communication control and related services. Other examples of operating systems include: MacOS System 7 from Apple Computer, OS/2 from IBM, VMS from Digital Equipment Corporation, MS-DOS from Microsoft Corporation, UNIX from AT&T, and IRIX from Silicon Graphics, Inc.

The computer system 20 also may be a special purpose computer system such as a digital versatile disk or digital video disk (DVD) player. In a DVD player, there is typically a decoder controlled by some general processor which decodes an incoming stream of data from a DVD. In some instances, the DVD player includes a highly integrated DVD decoder engine. Such devices generally have a simple operating system which may be modified to include the capabilities described and used herein in connection with the typical operating systems in a general purpose computer. In particular, some operating systems are designed to be small enough for installation in an embedded system such as a DVD player, including the WindowsCE operating system from Microsoft Corporation and the JavaOS operating system from SunSoft Corporation. The operating system allows a content provider to provide its own programs that define some of the content, which is particularly useful for interactive multimedia. This capability also can be used to provide encryption and decryption, in accordance with the invention.

The processor and operating system define a computer platform for which application programs in a programming language such as an assembly language or a high level programming language are written. It should be understood that the invention is not limited to a particular computer platform, operating system, processor, or programming language. Additionally, the computer system 20 may be a multi-processor computer system or may include multiple computers connected over a computer network.

An example memory system 24 will now be described in more detail in connection with Fig. 2. A memory system typically includes a computer readable and writable non-volatile recording medium 40, of which a magnetic disk, a flash memory, rewriteable compact disk (CD-RW) and tape are examples. The recording medium 40 also may be a read only medium such as a compact disc-read only memory (CD-ROM) or DVD. A magnetic disk may be removable, such as a "floppy disk" or "optical disk," and/or permanent, such as a "hard drive." The disk,

Petitioner Apple Inc. - Exhibit 1012, p. 1582

which is shown in Fig. 2, has a number of tracks, as indicated at 42, in which signals are stored, in binary form, i.e., a form interpreted as a sequence of 1's and 0's, as shown at 44. Such signals may define an application program to be executed by the microprocessor, or information stored on the disk to be processed by the application program. Typically, in the operation of a general purpose computer, the processor 22 causes data to be read from the non-volatile recording medium 40 into an integrated circuit memory element 46, which is typically a volatile random access memory, such as a dynamic random access memory (DRAM) or static random access memory (SRAM). The integrated circuit memory element 46 allows for faster access to the information by the processor than disk 40, and is typically called the system or host memory. The processor generally causes the data to be manipulated within the integrated circuit memory 46 and may copy the data to the disk 40, if modified, when processing is completed. A variety of mechanisms are known for managing data movement between the disk 40 and the integrated circuit memory 46, and the invention is not limited thereto. It should also be understood that the invention is not limited to a particular memory system.

The file system of a computer generally is the mechanism by which an operating system manages manipulation of data between primary and secondary storage, using files. A file is a named logical construct which is defined and implemented by the operating system to map the name and a sequence of logical records of data to physical storage media. An operating system may specifically support various record types or may leave them undefined to be interpreted or controlled by application programs. A file is referred to by its name by application programs and is accessed through the operating system using commands defined by the operating system. An operating system provides basic file operations provided by for creating a file, opening a file, writing a file, reading a file and closing a file.

In order to create a file, the operating system first identifies space in the storage media which is controlled by the file system. An entry for the new file is then made in a directory which includes entries indicating the names of the available files and their locations in the file system. Creation of a file may include allocating certain available space to the file. Opening a file returns a handle to the application program which it uses to access the file. Closing a file invalidates the handle.

In order to write data to a file, an application program issues a command to the operating system which specifies both an indicator of the file, such as a file name, handle or other descriptor, and the information to be written to the file. Given the indicator of the file, the

Petitioner Apple Inc. - Exhibit 1012, p. 1583

operating system searches the directory to find the location of the file. The directory entry stores a pointer, called the write pointer, to the current end of the file. Using this pointer, the physical location of the next available block of storage is computed and the information is written to that block. The write pointer is updated in the directory to indicate the new end of the file.

In order to read data from a file, an application program issues a command to the operating system specifying the indicator of the file and the memory locations assigned to the application where the next block of data should be placed. The operating system searches its directory for the associated entry given the indicator of the file. The directory may provide a pointer to a next block of data to be read, or the application may program or specify some offset from the beginning of the file to be used.

A primary advantage of using a file system is that, for an application program, the file is a logical construct which can be created, opened, written to, read from and closed without any concern for the physical storage used by the operating system.

The operating system also allows for the definition of another logical construct called a process. A process is a program in execution. Each process, depending on the operating system, generally has a process identifier and is represented in an operating system by a data structure which includes information associated with the process, such as the state of the process, a program counter indicating the address of the next instruction to be executed for the process, other registers used by process and memory management information including base and bounds registers. Other information also may be provided. The base and bounds registers specified for a process contain values representing the largest and smallest addresses that can be generated and accessed by an individual program. Where an operating system is the sole entity able to modify these memory management registers, adequate protection from access to the memory locations of one process from another process is provided. As a result, this memory management information is used by the operating system to provide a protected memory area for the process. A process generally uses the file system of the operating system to access files.

The present invention involves storing encrypted digital information, such an audio, video, text or an executable computer program, on a computer readable medium such that it can be copied easily for back-up purposes and transferred easily for distribution, but also such that it cannot be copied readily in decrypted form during use. In particular, the digital information is stored as a computer program that decrypts itself while it is used to provide the digital information, e.g., to provide executable operation code to the operating system of a computer, as

Petitioner Apple Inc. - Exhibit 1012, p. 1584

the digital information is needed. Any kind of encryption or decryption may be used and also may include authorization mechanisms and data compression and decompression. In one embodiment of the present invention, decrypted digital information exists only in memory accessible to the operating system and processes authorized by the operating system. When the digital information is a large application program, a copy of the entire decrypted application program is not likely to exist in the main memory at any given time, further reducing the likelihood that a useful copy of decrypted code could be made. The decryption operation also is performed only if some predetermined authorization procedure is completed successfully.

One embodiment of the invention, in which the decryption program is a form of dynamically loaded device driver, will first be described. Fig. 3 illustrates the structure of digital information as stored in accordance with one embodiment of the present invention, which may be stored on a computer readable medium such as a magnetic disc or compact disc read only memory (CD-ROM) to form a computer program product. The digital information includes a first portion 50, herein called an unwrap procedure or application, which is generally unencrypted executable program code. The purpose of the unwrap procedure is to identify the locations of the other portions of the digital information, and may perform other operations such as verification. In particular, the unwrap procedure identifies and extracts a program which will communicate with the operating system, herein called a virtual device driver 52. The unwrap procedure may include decryption and decompression procedures to enable it to decrypt/decompress the driver, and/or other content of this file. The program 52 need not be a device driver. The virtual device driver 52 typically follows the unwrap procedure 50 in the file container, the digital information. The virtual device driver, when executed, decrypts and decodes the desired digital information such as an executable computer program code from hidden information 54, which may be either encrypted and/or encoded (compressed). It is the decrypted hidden information which is the desired digital information to be accessed. This hidden information may be any kind of digital data, such as audio, video, text, and computer program code including linked libraries or other device drivers.

In this embodiment of the computer program product, labels delineate the boundaries between the device driver and the hidden files. These labels may or may not be encrypted. A first label 56 indicates the beginning of the code for the virtual device driver 52. A second label 58 indicates the end of the virtual device driver code. Another label 60 indicates the beginning of the hidden information and a label 62 indicates the end of that application. There may be one

Petitioner Apple Inc. - Exhibit 1012, p. 1585

or more blocks of such hidden information, each of which can be given a different name. It may be advantageous to use the name of the block of information in its begin and end tags. This computer program product thus contains and is both executable computer program code and one or more blocks of digital information. A table of locations specifying the location of each portion of the product could be used instead of labels. Such a table could be stored in a predetermined location and also may be encrypted.

The overall process performed using this computer program product in one embodiment of the invention will now be described in connection with Fig. 4. This embodiment may be implemented for use with the Windows95 operating system and is described in more detail in connection with Figs. 5-7. An embodiment which may be implemented for use on the WindowsNT 4.0 operating system is described in more detail below in connection with Fig. 8. In both of these described embodiments, the digital information is an executable computer program which is read by the operating system as data from this file and is executed. The same principle of operation would apply if the data were merely audio, video, text or other information to be conveyed by a user. In the embodiment of Fig. 4, the computer program is first loaded into memory in step 70, and the unwrap procedure 50 is executed by the operating system, as any typical executable computer program is executed. The unwrap procedure may perform authorization, for example by checking for a required password or authentication code, and may receive any data needed for decryption or decompression, for example keys or passwords, in step 72. Suitable authorization procedures may provide the ability to distribute software for single use. The unwrap procedure locates the virtual device driver 52 within the computer program in step 74, and then locates the hidden application in step 76. The virtual device driver 52 is then extracted by the unwrap procedure from the computer program, copied to another memory location and loaded for use by the operating system in step 78. An advantage of an operating system like Windows95 is that it allows such device drivers to be loaded dynamically without restarting the computer.

The executed unwrap procedure 50, in step 80, informs the loaded virtual device driver 52 of the location of the hidden information in the file, any keys or other passwords, and a name of a phantom directory and file to be called that only the unwrap procedure and the virtual device driver know about. The name of this phantom directory may be generated randomly. Each segment information hidden in the digital information product may be assigned its own unique file name in the phantom directory.

Petitioner Apple Inc. - Exhibit 1012, p. 1586

After the loaded virtual device driver 52 receives all communications from the unwrap procedure, it opens the original application file for read only access in step 82. The unwrap procedure then makes a call to the operating system in step 84 to execute the file in the phantom directory for which the name was transmitted to the loaded virtual device driver. One function of the loaded virtual device driver 52 is to trap all calls from the operating system to access files in step 86. Any calls made by the operating system to access files in the phantom directory are processed by the virtual device driver, whereas calls to access files in other directories are allowed to proceed to their original destination. In response to each call from the operating system, the virtual device driver obtains the bytes of data requested by the operating system from the original computer program file in step 88. These bytes of data are then decrypted or decompressed in step 90 and returned to the operating system. When processing is complete, the phantom application is unloaded from the operating system in step 92, and may be deleted from the memory.

A more detailed description of the process of Fig. 4 will now be described in connection with Figs. 5-7. Fig. 5 is a flowchart describing the operation of one embodiment of the unwrap procedure in more detail. The first step performed by this procedure is identifying the operating system being used, in step 100. This step is useful because different methods may be used with different operating systems. All code that may be used to run in various operating systems may be placed in this unwrap procedure. This procedure also may contain the decompression/decryption code, for example or any other computer program code to be executed.

The executed application then opens the original executable file as a data file and searches for the begin and end tags of the device driver and hidden files in step 102. The device driver code is copied into memory and loaded into the operating system in step 104. The unwrap procedure then informs the device driver of the name of the original application file, offsets of the hidden files and the name of a phantom directory, which is typically randomly generated (step 106). This communication may be performed using a "DeviceIOControl" function call in the Windows95 operating system. The unwrap procedure then makes a call to the operating system to execute the hidden file in the phantom directory, in step 108.

The operation of one embodiment of a device driver will now be described in connection with Fig. 6. After the device driver is loaded into the operating system, it hooks into a position between the operating system and a file system driver (FSD), in step 110, to intercept

Petitioner Apple Inc. - Exhibit 1012, p. 1587

calls made by the operating system to the FSD for data from files in the phantom directory. The FSD is the code within the operating system that performs physical reading and writing of data to disk drives. The operating system makes requests to the FSD for data from files in directories on the disk drives. The driver then receives information from the unwrap procedure including the name of the original file, the location of hidden files within the original file, and the name of the phantom directory created by the unwrap procedure (step 112). The device driver opens the original file as a read only data file. The device driver now traps calls, in step 114, made from the operating system for files in the phantom directory. Calls to other directories are ignored and passed on to the original destination. The device driver then reads the data from the original data file, decrypts and decompresses it, and returns the decrypted/decompressed data to the operating system in step 116.

For example, if the offset for the hidden application in the original data file is 266,270 bytes and the operating system asks for 64 bytes starting at offset 0 of the hidden application in the phantom directory, the device driver reads 64 bytes from the original file starting at offset 266,270, decrypts/decompresses those 64 bytes, and returns the first 64 decrypted/decompressed bytes back to the operating system. From the point of view of the operating system, the 64 bytes appear to have come from the file in the phantom directory. Steps 114 and 116 are performed on demand in response to the operating system.

A block diagram of the computer system in this embodiment, with a device driver loaded and in operation, will now be described in more detail in connection with Fig. 7. Fig. 7 illustrates the operating system 120, the loaded device driver 122, a file system driver 124, the original executable file 126 as it may appear on disk and the unwrap procedure 128. The executable file may in fact be on a remote computer and accessed through a network by the device driver. The unwrap procedure causes the operating system to begin execution of the hidden file by issuing an instruction to execute the file in the phantom directory, as indicated at 130. This command is issued after the device driver 122 is informed of the file name of the original executable file 126, offsets of the hidden files within that file and the name of the phantom directory, as indicated at 132. The operating system then starts making calls to the phantom directory as indicated at 134. The device driver 122 traps these calls and turns them into requests 136 to the file system driver to access the original executable file 126. Such requests actually are made to the operating system 120, through the device driver 122 to the file system driver 124. The file system driver 124 returns encrypted code 138 to the device driver

Petitioner Apple Inc. - Exhibit 1012, p. 1588

122. The encrypted code 138 actually passes back through the device driver 122 to the operating system 120 which in turn provides the encrypted code 138 to the device driver 122 as the reply to the request 136 for the original file. The device driver 122 then decrypts the code to provide decrypted code 140 to the operating system 120.

Another embodiment of the invention will now be described in connection with Fig. 8. This embodiment may be implemented using the WindowsNT 4.0 operating system, for example. In this embodiment, the device driver portion 52 of the computer program product is not used. The unwrap procedure for this embodiment begins by identifying the operating system being used similar, which is step 100 in Fig. 5. If the operating system is Windows NT 4.0, for example, a different unwrap procedure for this embodiment is performed. Before describing this unwrap procedure, a brief description of some of the available operating system commands will be provided.

Currently, under all versions of the Window operating system or operating environment from Microsoft Corporation (such as Windows 3.1, Windows 95 and Windows NT 3.51 and 4.0) all executable files (.exe) or dynamic link library (.dll and .ocx) files, which are executable files with different header and loading requirements than .exe files, that are loaded into memory by the operating system must reside as a file either locally, e.g., on a disk drive or remotely, e.g., over a network or communications port. All further references herein to loading an executable will be using the Win32 function calls used in Windows 95 and NT 3.51 and 4.0 operating systems. The CreateProcess() function which loads files with an .exe extension takes ten parameters:

```
BOOL CreateProcess(// Prototype from Microsoft Visual C++ Help Documentation
  LPCTSTR lpApplicationName,                  // pointer to name of executable module
  LPTSTR lpCommandLine,                       // pointer to command line string
  LPSECURITY_ATTRIBUTES lpProcessAttributes,  // pointer to process security attributes
  LPSECURITY_ATTRIBUTES lpThreadAttributes,   // pointer to thread security attributes
  BOOL bInheritHandles,                       // handle inheritance flag
  DWORD dwCreationFlags,                      // creation flags
  LPVOID lpEnvironment,                       // pointer to new environment block
  LPCTSTR lpCurrentDirectory,                 // pointer to current directory name
  LPSTARTUPINFO lpStartupInfo,                // pointer to STARTUPINFO
  LPPROCESS_INFORMATION lpProcessInformation  // pointer to PROCESS_INFORMATION
);
```


Petitioner Apple Inc. - Exhibit 1012, p. 1589

Three of these parameters are pointers to strings that contain an application file name, command line parameters, and the current directory. The other parameters are security, environmental, and process information. The LoadLibrary() function takes one parameter that is a pointer to a string that contains the application file name:

```
HINSTANCE LoadLibrary(// Prototype from Microsoft Visual C++ Help Documentation
  LPCTSTR lpLibFileName      // address of filename of executable module
);
```

The LoadLibraryEx() function takes three parameters the first being the same as LoadLibrary(), the second parameter must be null, and the third tells the operating system whether to load the file as an executable or as a data file in order to retrieve resources such as icons or string table data from it and not load it as an executable:

```
HINSTANCE LoadLibraryEx(// Prototype from Microsoft Visual C++ Help Documentation
  LPCTSTR lpLibFileName,     // points to name of executable module
  HANDLE hFile,              // reserved, must be NULL
  DWORD dwFlags              // entry-point execution flag
);
```

The CreateFile() function is used to create and open files and to load files such as device drivers. This function also requires a pointer to a string that contains the name of a physical file:

```
HANDLE CreateFile(// Prototype from Microsoft Visual C++ Help Documentation
  LPCTSTR lpFileName,                          // pointer to name of the file
  DWORD dwDesiredAccess,                       // access (read-write) mode
  DWORD dwShareMode,                           // share mode
  LPSECURITY_ATTRIBUTES lpSecurityAttributes,  // pointer to security descriptor
  DWORD dwCreationDistribution,                // how to create
  DWORD dwFlagsAndAttributes,                  // file attributes
  HANDLE hTemplateFile                         // handle to file with attributes to copy
);
```


Petitioner Apple Inc. - Exhibit 1012, p. 1590

There are other functions such as MapViewOfFile() and MapViewOfFileEx() that map areas of memory to an already opened physical file through a handle to that file. They have the following parameters:

```
LPVOID MapViewOfFile(// Prototype from Microsoft Visual C++ Help Documentation
  HANDLE hFileMappingObject,        // file-mapping object to map into address space
  DWORD dwDesiredAccess,            // access mode
  DWORD dwFileOffsetHigh,           // high-order 32 bits of file offset
  DWORD dwFileOffsetLow,            // low-order 32 bits of file offset
  DWORD dwNumberOfBytesToMap        // number of bytes to map
 );

LPVOID MapViewOfFileEx(// Prototype from Microsoft Visual C++ Help Documentation
  HANDLE hFileMappingObject,        // file-mapping object to map into address space
  DWORD dwDesiredAccess,            // access mode
  DWORD dwFileOffsetHigh,           // high-order 32 bits of file offset
  DWORD dwFileOffsetLow,            // low-order 32 bits of file offset
  DWORD dwNumberOfBytesToMap,       // number of bytes to map
  LPVOID lpBaseAddress              // suggested starting address for mapped view
 );
```

All of the foregoing functions directly use a pointer to a string that is a physical file. The only file functions that do not directly use a physical filename are functions like CreateNamedPipe(), which has the following parameters:

```
HANDLE CreateNamedPipe(// Prototype from Microsoft Visual C++ Help Documentation
  LPCTSTR lpName,                          // pointer to pipe name
  DWORD dwOpenMode,                        // pipe open mode
  DWORD dwPipeMode,                        // pipe-specific modes
  DWORD nMaxInstances,                     // maximum number of instances
  DWORD nOutBufferSize,                    // output buffer size, in bytes
  DWORD nInBufferSize,                     // input buffer size, in bytes
  DWORD nDefaultTimeOut,                   // time-out time, in milliseconds
  LPSECURITY_ATTRIBUTES lpSecurityAttributes  // pointer to security attributes structure
 );
```

The string to which CreateNamedPipe() points using the first parameter is a string that both an existing executable and the operating system know about and does not exist physically. Unfortunately both of the executables that "know" this private name could only be loaded using one of the other procedures that required a physical file. Currently it is not possible to load an executable using a "named pipe" name. Both of or any executables that use the name of the "named pipe" already must have been loaded into memory.

All of the foregoing functions require a physical file because all of them use "file mapping" processes. File mapping allows large executable files to appear to be loaded rapidly since they are rarely completely loaded into memory but rather are mapped into memory. The detriment to this mapping capability is that executable code must remain in physical memory in a file in unencrypted form in order to be loaded, unless there is a middle layer or file system driver that the operating system uses as a physical layer and that decrypts the executable code to the operating system on demand. The potential weakness here is that another file system driver can hook into the operating system to monitor traffic between the operating system and all file system drivers and capture decrypted executable code passing from the file system driver to the operating system. Some operating systems allow such monitoring more than others. Many anti-viral software packages use this technique to prevent computer virus attacks.

One method of loading and executing encrypted executable computer program code is to use a stub executable having two parts. The first part is the normal front end loader code that all executables have. In addition, the first part would perform any authorization which may include receiving a password from the user, then allocate enough memory to hold hidden encrypted code when it is decrypted, either in its entirety or a portion of it, copy the encrypted code into that area of protected (and preferably locked so no disk swapping occurs) memory, decrypt it once it is in memory and only in memory, and then have the operating system load the code only from memory therefore bypassing any file system drivers or TSRs so they have access to only encrypted code.

Some of the file functions listed above and similar functions on other operating systems could be modified easily by a programmer having access to source code for those operating systems, or a new operating system may be made to provide functions which allow direct loading of executable code from memory rather than physical files. For example, in the Win32 commands, a command similar to CreateProcess() command could be provided. The command should have a few extra parameters including the process identifier of the process that contains

Petitioner Apple Inc. - Exhibit 1012, p. 1592

the now decrypted executable code, the memory address of the start of the decrypted code, and the size of the decrypted code. The command could also contain a parameter specifying a "call back" function within the first process that would provide decrypted code on demand directly to the operating system through a protected buffer, therefore allowing only a portion of the encrypted code to be decrypted at any one time instead of in its entirety, for better protection and less memory use. The second parameter of the LoadLibraryEx() command that now needs to be NULL could be expanded to hold a structure that contained the same information. Both of these and other similar functions could be changed or created to allow loading executable code either as an .exe, .dll, or other extensions or identifiers, such as by using a "named pipe" name that only the operating system and process that holds decrypted code know about and having the operating system load from the named pipe.

Alternatively, without having such additional capabilities in the operating system, an application program can be divided into two parts. The first part is code that is common to all applications such as code for allocating memory off the heap and code that provides some interaction with the user. This kind of code is generally not code that the content provider is concerned about copying. The second part is the code that the content provider believes is valuable. Typically this valuable code is a business logic code or what would be considered a middle tier of a three-tier environment. A content provider would like to protect this second part of the code, at least much more that the first part of the code. The content provider would place all of the important code to be protected inside a dynamic link library and the code that is not that important would reside in the front end "stub" executable. Both of these would be combined into another executable containing the .dll in encrypted form only, along with any other files, data, information, and/or tables for holding, for example, hardware identifiers. This other executable is the final digital information product.

The first part of the digital information product, i.e., the executable stub, would load and execute normally like any other application. It then would perform any authorization procedures. Once the proper authorization or password was completed successfully, an unwrap procedure would be performed as will now be described in connection with Fig. 8, it would then allocate enough protected memory using a function like VirtualAlloc() as shown in step 150:

```
DWORD nFileSize = 0;
DWORD nPhantomFileSize = 0;
```


Petitioner Apple Inc. - Exhibit 1012, p. 1593

```
DWORD exeOffset = 0;
DWORD nPreferredLoadAddress = GetPreCompiledLoadAddress();
CString cCommandFile = UnwrapGetNTCommandFile();
exeOffset = UnwrapGetDllOffset(cCommandFile);
nFileSize = UnwrapGetDllSize(cCommandFile);
nPhantomFileSize = nFileSize + 0x3000; // add any needed extra space
// Increase buffer size to account for page size (currently Intel page size).
DWORD nPageSize = GetPageSize();
nPhantomFileSize += (nPageSize -(nPhantomFileSize % nPageSize));
// Allocate the memory to hold the decrypted executable.
LPVOID lpvBlock = VirtualAlloc((LPVOID) nPreferredLoadAddress,
                    nPhantomFileSize,
                        MEM_RESERVE | MEM_COMMIT, PAGE_READWRITE);
```

This function can request a particular address space. Preferably, this address space is the preferred load address space to which the .dll was linked in order to minimize any needed relocation and fix up code. The stub executable may lock that area of memory in step 152, for example by using VirtualLock() to prevent any memory writes to a swap file, depending on the operating system, as shown below:

```
BOOL bVLock = VirtualLock((LPVOID) nPreferredLoadAddress, nPhantomFileSize);
```

The memory area still should be secure even without this preventive step since the Windows 95 and NT operating systems do not allow any user access to swap files.

The encrypted code is then copied from the digital information product into the allocated protected memory in step 154, for example by using the following command:

```
UnwrapCopyHiddenExeToMem(cCommandFile, exeOffset, nFileSize, (char *) lpvBlock);
```

Once in memory, the stub would then decrypt the code to that same portion of memory in step 156, for example by using the following commands:

Petitioner Apple Inc. - Exhibit 1012, p. 1594

```
CwrapDecryptSeed(cPassword.GetBuffer(0), cPassword.GetLength());
CwrapDecrypt((unsigned char *) lpvBlock, 0, nFileSize);
```

Any "fix up and relocation" type services would then be performed in step 158, for example by using the following command:

```
UnwrapFixUpAndRelocateDll(lpvBlock);
```

Possibly, the memory protection may be changed to execute only in step 160, for example by using the VirtualProtect() command as follows:

```
DWORD lpflOldProtect; // variable to get old protection
BOOL bVProtect = VirtualProtect((LPVOID) nPreferredLoadAddress,
                                nPhantomFileSize,
                                PAGE_EXECUTE,
                                &lpflOldProtect);
```

Function calls then can be made into that area of memory that now contains the decrypted code:

```
UnwrapDoDllAlgorithms();
```

Some of the "fix up" operations to be performed above include placing the addresses of external or stub.exe functions into the address place holders of the decrypted .dll or internal code, by using commands similar to the following:

```
WriteAddress((char*) 0x0a406104, (DWORD) &CallBackFunction1);
WriteAddress((char*) 0x0a406100, (DWORD) &CallBackFunction2);
```

For instance a wrapper function could be created in the outer stub.exe that received a size parameter, allocated that amount of memory off of the heap, and passed back the starting address of that block of memory. Another example would be to have encrypted algorithms within the hidden, encrypted .dll which would be called at run time from the front end stub once decrypted

Petitioner Apple Inc. - Exhibit 1012, p. 1595

within protected memory. The dynamic link library would be compiled and linked to expect a pointer to a function that took that parameter and/or returned a value by including prototypes in the header file as follows:

```
void (*lpCallBackFunc1)();
void (*lpCallBackFunc2)(unsigned long);
```

Function calls to "external" functions also could be added as follows:

```
(*lpCallBackFunc1)();
unsigned long z = x * x;
(*lpCallBackFunc2)(z);
```

At run time the "fix up" code would take the run time address of that "wrapper function" and place it into the pointer address within the .dll block of code as follows:

```
WriteAddress((char*) 0x0a406104, (DWORD) &CallBackFunction1);
WriteAddress((char*) 0x0a406100, (DWORD) &CallBackFunction2);
```

This information is readily available using the .cod output files from the compiler, an example of which follows:

```
_TestSum PROC NEAR                                          ; COMDAT
; Line 8
 00000      56              push   esi
; Line 23
 00001      ff 15 00 00 00
            00              call   DWORD PTR _lpCallBackFunc1
; Line 24
 00007      8b 44 24 08     mov    eax, DWORD PTR _a$[esp]
 0000b      50              push   eax
 0000c e8 00 00 00 00 call  _TestSquare
```


Petitioner Apple Inc. - Exhibit 1012, p. 1596

```
00011      83 c4 04       add    esp, 4
00014      8b f0          mov    esi, eax
; Line 25
00016      8b 44 24 0c    mov    eax, DWORD PTR _b$[esp]
0001a      50             push   eax
0001b      e8 00 00 00 00 call   _TestSquare
00020      83 c4 04       add    esp, 4
00023      03 c6          add    eax, esi
; Line 28
00025      5e             pop    esi
00026      c3             ret    0
_TestSum ENDP
_TEXT      ENDS
;       COMDAT_TestSquare
_TEXT      SEGMENT
_x$ = 8
_TestSquare PROC NEAR                                    ; COMDAT
; Line 30
00000      56             push   esi
; Line 32
00001      8b 74 24 08    mov    esi, DWORD PTR _x$[esp]
00005      0f af f6       imul   esi, esi
; Line 34
00008      56             push   esi
00009      ff 15 00 00 00
           00             call   DWORD PTR _lpCallBackFunc2
0000f 83 c4 04    add    esp, 4
00012      8b c6          mov    eax, esi
; Line 36
00014      5e             pop    esi
00015      c3             ret    0
_TestSquare ENDP
```


Petitioner Apple Inc. - Exhibit 1012, p. 1597

Such information also is available from .map output files from the linker where the "f" between the address (i.e., 0a406100) and the object file (i.e. Algorithms.obj) means it is a "flat" address (i.e., hard coded by the linker) and the lack of an "f" means that it is an address pointer to be supplied at run time (load time) where the address that is contained in that address location is used and not the actual address location (i.e., the address that is contained at address location 0a406100 and not 0a406100 itself):

```
0001:00000000   _TestSum            0a401000 f Algorithms.obj
0001:00000030   _TestSquare         0a401030 f Algorithms.obj

0003:00001100   _lpCallBackFunc2    0a406100   Algorithms.obj
0003:00001104   _lpCallBackFunc1    0a406104   Algorithms.obj
```

When the code inside the .dll makes a "call" to a dereferenced pointer, it would jump to the correct function in the outer code and return the expected return value (if any). For example:

```
void CallBackFunction1(){
// This is the first function that exists in the Stub executable
// whose address has been placed at the appropriate location inside the "dll" code
// that has now been decrypted in a block of memory. The code inside the "dll"
// makes a function call to this function. In its encrypted state, the "dll" does not contain
// this address, but merely has a placeholder for the address. The "dll" has enough space
allocated to hold an
// address of this size. After the "dll" has been decrypted at run time, its address is
// placed in that location so the code inside the "dll" that references (or more
// appropriately dereferences) that address can jump (which is function call) to this
// address.
AfxMessageBox(
_T("This is the FIRST Stub.exe call back function being called from the dll."));
        return;
}
```


Petitioner Apple Inc. - Exhibit 1012, p. 1598

```
void CallBackFunction2(DWORD nNumber){
// See comment for CallBackFunction1 except this function receives a parameter off
// of the stack.  It could also return a value as well.
        CString
        cString(
T("This is the SECOND Stub.exe call back function being called from the dll"));

        har buffer[20];
        ltoa(nNumber, buffer, 10);

        cString += _T(" with a parameter of ");
        cString += buffer;
        cString += _T(".");
        AfxMessageBox(cString.GetBuffer(0));
        return;
}
```

The outer stub.exe would make the same kinds of jumps or function calls into the now protected decrypted code block as follows:

```
DWORD c;

// This command declares a function pointer.  This command is different for different function
// calls.  Here the called function takes two integer parameters and
// passes back a DWORD.
DWORD (*lpFunc)(DWORD,DWORD);

// The function pointer is then pointed to the starting address of the function in the
// block of memory that now holds the decrypted DLL.
lpFunc = (DWORD (*)(DWORD,DWORD)) UnwrapFixUpAndRelocateDll();

// Now call that "function" which is really like all function calls, i.e., a jump to
```


Petitioner Apple Inc. - Exhibit 1012, p. 1599

```
// the address where that function exists. In this case, two
// variables are passed to that function and returning a value from that function. This function
illustrates that the function call
// can be more complicated than merely a simple jump
// to an address. Inline assembler code may be used to push the variables onto
// the stack frame and return the variable from the eax register, but this function enables
// the C++ compiler to do the same function.
c = (DWORD) (*lpFunc)(a, b);
```

This mechanism requires the unwrap procedure and the now decrypted code to have intimate knowledge about procedural interfaces of each other but no knowledge about each other's implementation. This is the way most executable .exe files and .dll files behave but with the addition of a series of "wrapper" functions on either side for communication. This method works under Windows 95 and Windows NT 4.0 operating systems and should work under Windows NT 3.51 and other operating systems.

Another modified version of this mechanism that works under the Windows NT 4.0 operating system because of functions specific to Windows NT 4.0 would be to have another hidden and/or encrypted executable within the digital information product. This executable would be copied to a physical disk in an unencrypted form, launched or loaded with the CreateProcess() command in its current form but called with a parameter to load the executable in suspended mode:

```
BOOL success = CreateProcess(cFrontEndExe.GetBuffer(0), 0, 0, 0, TRUE,
                    CREATE_NEW_CONSOLE | CREATE_SUSPENDED,
                0, 0, &startUpInfo, &processInfo);
```

Then the first process would copy the encrypted dll into its own process and decrypt it, allocate enough memory using VirtualAllocEx() in its current form in the second process that has just loaded the expendable front end executable in a suspended state as follows:

```
LPVOID lpvBlockEx = VirtualAllocEx(processInfo.hProcess,
```


Petitioner Apple Inc. - Exhibit 1012, p. 1600

```
(LPVOID) nPreferredLoadAddress, nPhantomFileSize,
MEM_RESERVE | MEM_COMMIT,
PAGE_READWRITE);
```

The decrypted code is copied from the first process to the second suspended process using WriteProcessMemory() in its current form:

```
BOOL bWriteProcessMemory = WriteProcessMemory((HANDLE) processInfo.hProcess,
(LPVOID) lpvBlockEx, (LPVOID) nPreferredAddress,
(DWORD) nPhantomFileSize, (LPDWORD) &nBytesWritten);
```

The primary thread of the previously launched second process is then resumed:

```
DWORD nResumed = ResumeThread(processInfo.hThread);
```

Any necessary function pointers are then placed in the correct locations by the second process, the area of memory is locked to prevent any writes to a swap file, and the memory protection is changed to execute only as follows:

```
WriteAddress((char*) 0x0a406104, (DWORD) &CallBackFunction1);
WriteAddress((char*) 0x0a406100, (DWORD) &CallBackFunction2);

BOOL bVLock = VirtualLock((LPVOID) nPreferredLoadAddress, nPhantomFileSize);
DWORD lpflOldProtect; // variable to get old protection
BOOL bVProtect = VirtualProtect((LPVOID) nPreferredLoadAddress,
nPhantomFileSize, PAGE_EXECUTE, &lpflOldProtect);
```

The program can continue running by making and receiving calls to and from the decrypted dynamic link library that now resides in the protected memory of its process using commands such as the following:

```
DWORD c;
```


Petitioner Apple Inc. - Exhibit 1012, p. 1601

```
DWORD (*lpFunc)(DWORD,DWORD);
lpFunc = (DWORD (*)(DWORD,DWORD)) ExpendableGetEntryAddress();
c = (DWORD) (*lpFunc)(a, b);
```

The first process can either close down or launch another instance of that same process.

In either of these implementations using the same process or launching into a second process, the hidden encrypted code never passes through a file system driver or memory resident program in decrypted form. Code can be split up among different dynamic link libraries so that no two would reside in memory at the same time in order to protect code further. Both of these systems can be implemented using the Win32 function calls. If additional functions, similar to a CreateProcess() command or a LoadLibrary() command but that take a process identifier and address location in memory to load in an executable instead of a physical file, are provided in an operating system then the entire executable and dynamic link library can be hidden, encrypted, and protected on the physical disk and then decrypted within protected memory and use the operating system loader to load it directly to the operating system from memory without residing in decrypted form on any physical medium.

Having described the operation and use of the computer program product in accordance with the invention, embodiments of which are described above in connection with Figs. 3-8, and the operation of the unwrap procedure and device driver it contains, the process of constructing such a computer program product will now be described in more detail. Referring now to Fig. 9, an embodiment of this process for creating a computer program product is shown. This process can be applied to any digital information including an arbitrary executable computer program, dynamic link libraries and related files of data. All digital information is treated as mere data by this process. Each separate data file is combined into a single file by this process, with an executable program for performing the unwrap procedure, and optionally executable program code for a virtual device driver, into the computer program product. Each file of hidden information has a unique location and is identified by its own begin and end markers as shown in Fig. 3. The first step of this process is opening a new data file for the computer program using a name that will be used to indicate an executable file (step 200). For example, an executable word processing program may be named "word_processor.exe" in the Windows95 operating system.

Petitioner Apple Inc. - Exhibit 1012, p. 1602

The three portions of the computer program product are then inserted into the open data file. First, the unwrap procedure is inserted at the beginning of the file in an executable format in step 202. The begin tag for the optional device driver is then inserted in step 204. The executable device driver program code is then inserted in step 206, followed by its corresponding end tag in step 208. For each hidden file to be inserted into this computer program product, steps 210 to 216 are performed. First, the begin tag is inserted in step 210. The begin tag also may include an indication of a unique name of the file which will be used as its name in the phantom directory created by the unwrap procedure. The hidden file is then encrypted and/or compressed in step 212 and inserted into the data file in step 214. The end tag for the hidden file is then inserted in step 216. The device driver and all of the tags may be encrypted also if the unwrap procedure has suitable decryption procedures. The computer program file is closed when the last hidden file is processed.

Using the present invention digital information, such as executable program code or various kinds of data, is loaded and unloaded as needed, and thus does not take up any more memory than is necessary. At no time does unencrypted digital information, such as computer program code, exist on disk in accessible and complete decrypted form. Because the original digital information is available as a read only file in one embodiment of the invention accessible only to the device driver, the digital information may be accessed over networks, from a CD-ROM or from a DVD, and can be made to have a limited number of uses. This mechanism is particularly useful for controlling distribution of computer programs, digitized movies or other information while reducing the cost of such distribution and control. For example, software may be distributed over a network on a single use basis, and charges may be levied on a per use basis. The ability to reverse engineer an application program also may be reduced.

One benefit with this system over some other systems for preventing unauthorized access to digital information is that the content provider maintains control of the encryption applied to the information how it may be decrypted. Any need for either a centralized facility or a predetermined decryption program is eliminated. An operating systems manufacturer or other platform vendor merely provides the capability for the information to be accessed and decrypted on the fly. Since the valuable information and any other tables of authorization codes, passwords, or hardware identifiers that the content provider may use to secure the information resides in one large encrypted file, it becomes difficult, if not impossible, for someone to determine just where any of this information exists.

Petitioner Apple Inc. - Exhibit 1012, p. 1603

A potential scenario with authorization procedure in which the present invention may be used is the following. A consumer purchases a DVD disk containing a movie. The user puts the disk into the player. This is the first time the disk is installed. The content provider's functions are loaded into the DVD chip, which looks in the encrypted table and sees that this is the first time this disk is being played. The player then displays on a screen a numeric identifier and toll free phone number. The consumer calls the toll free phone number and inputs the numeric identifier that was displayed on the screen. The content provider provides a numeric password based on the numeric identifier that the user inputs into the DVD. The content provider may develop a database of information about its consumers that also may be used to detect pirating of the digital information product. Now that this authorization has taken place, the software that the content provider wrote, and is now in the DVD chip, takes a hardware identifier from the DVD and encrypts it and puts it in the encrypted and buried table on the disk. Alteratively, the data may be decrypted in memory and re-encrypted back onto the disk using the hardware identifier as part of a key. Now that disk will run and show the movie and will only run on that DVD and no other. The content provider could allow for a table of hardware id's so they could limit the number of DVD's that disk would run on or a limited number of times it can be shown. It should be understood that many other authorization procedures may be used.

In the foregoing scenario, the movie is encrypted on the same disk inside of the encrypted file that contains the table and functions the content provider distributed. The movie is decrypted by the decryption functions contained in the file directly to the DVD chip. At no time does the movie reside anywhere in decrypted form. The content provider can protect the movie with any desired level of security (for both encryption and authorization).

In the present invention, the onus of protection of content does not reside with a hardware manufacturer or platform provider but in the hands of the content provider. The hardware manufacturer only provides the mechanism to protect the digital information through the operating system. The technique and implementation of protection resides in the hands of the content provider. This mechanism allows the content providers to change the level of security as needed without any modifications to the hardware. The security of the content is provided by the encryption/decryption algorithms, public/private keys, and authorization methods which are determined by the content provider. Even each individual product can have its own encryption/decryption algorithms and/or public/private keys. All of these can be changed and enhanced as the market demands.

Petitioner Apple Inc. - Exhibit 1012, p. 1604

The present invention also could be used for on-line or live use of digital information. For example, a movie could be retrieved on demand and recorded by a consumer. A set top box could receive the digital information, decrypt it, and then re-encrypt and store the information using, for example, a hardware identifier of the set top box. Since home movies digitally recorded would be encrypted using the hardware identifier of the device used in recording, that home movie could not be played on another or only on a limited number of other devices and/or for only a specified number of times depending on the wishes of the content provider. Since the algorithms are downloaded at the time of recording from a service provider, e.g., the cable company, the content provider (movie company) would provide the encrypted data to the service provider to present to their customers. The service provider need not be concerned with the encryption/decryption and authorization functions used by the content provider. Similar uses are possible with other data transmission systems including, but not limited to, telephone, cellular communications, audio transmission including communication and the like.

In another embodiment, the stub executable program is a first process that is implemented similar to a debugging tool such as the SoftIce debugger from NuMega Technologies or the WinDebug debugger from Microsoft Corporation for Ring 0 kernel level debugging for an Intel processor based architecture, or the CodeView debugger for ring 3 application level debugging. Such a debugger controls execution of a program to be debugged as a second process and steps through each program statement or opcode of the debugged program. The debugging tool could be modified to monitor each opcode that indicates a jump to a program fragment, such as each instruction or a block code. If the program fragment to be executed is not decrypted, the modified debugger decrypts the program fragment before the jump command is allowed to execute. Each program fragment may be re-encrypted after execution. Clearly, unnecessary debugging commands may be omitted from the modified debugger.

Having now described a few embodiments of the invention, it should be apparent to those skilled in the art that the foregoing is merely illustrative and not limiting, having been presented by way of example only. Numerous modifications and other embodiments are within the scope of one of ordinary skill in the art and are contemplated as falling within the scope of the invention as defined by the appended claims and equivalent thereto.

Petitioner Apple Inc. - Exhibit 1012, p. 1605

CLAIMS

1. A computer-implemented process for executing encrypted computer program logic while maintaining protection against copying of corresponding decrypted executable computer program logic, wherein the encrypted computer program logic is stored in association with first executable computer program logic, the process comprising the steps of:

through an operating system of a computer, reading, loading and executing the first executable computer program logic as a first process having a protected memory area defined by the operating system;

the first process decrypting the encrypted computer program logic into second executable computer program logic and storing the second executable computer program logic in the protected memory area; and

the first process causing loading and execution of the decrypted second computer program logic in the protected memory area.

2. The process of claim 1, wherein the encrypted computer program logic and the first executable computer program logic are stored in a single data file accessible through the operating system.

3. The process of claim 1, wherein the execution of the decrypted second computer program logic is performed as a second process having a second protected memory area defined by the operating system.

4. A digital information product including a computer readable medium having digital information stored thereon, the digital information including computer program logic defining first executable computer program logic, wherein the first executable computer program logic when executed performs the following steps:

storing the encrypted computer program logic in a data file accessible through an operating system of a computer, wherein the data file also includes first executable computer program logic;

through the operating system, reading, loading and executing the first executable computer program logic from the data file as a first process having a protected memory area;

Petitioner Apple Inc. - Exhibit 1012, p. 1606

the first process decrypting the encrypted computer program logic into second executable computer program logic and storing the second executable computer program logic in the protected memory area; and

the first process causing loading and execution of the decrypted second computer program logic in the protected memory area.

5. A computer system comprising:

a processor for executing computer program logic;

a main memory operatively connected to the processor for storing digital information including executable computer program logic at memory locations addressed by the processor; and

an operating system defined by executable computer program logic stored in the memory and executed by the processor and having a command which when executed by the processor defines means for creating a process in response to a request specifying a process identifier and a memory location in the main memory, wherein the process identifier indicates the process making the request and the memory location stores executable computer program logic which when executed defines the process.

6. A computer system having an operating system, for decrypting digital information, comprising:

means for storing the encrypted computer program logic in a data file accessible through the operating system, wherein the data file also includes first executable computer program logic;

means, invokable through the operating system, for reading, loading and executing the first executable computer program logic from the data file as a first process having a protected memory area;

the first process defining means for decrypting the encrypted computer program logic into second executable computer program logic and storing the second executable computer program logic in the protected memory area; and

the first process defining means for causing loading and execution of the decrypted second computer program logic in the protected memory area.

Petitioner Apple Inc. - Exhibit 1012, p. 1607

7. The computer system of claim 6, wherein the encrypted computer program logic and the first executable computer program logic are stored in a single data file accessible through the operating system.

8. The computer system of claim 6, wherein the execution of the decrypted second computer program logic is performed as a second process having a second protected memory area defined by the operating system.

9. A digital information product, including a computer readable medium with computer readable information stored thereon, wherein the computer readable information comprises:

a first portion of executable computer program logic; and

a second portion of encrypted digital information; and

wherein the first portion of executable program logic, when executed, defines means, operative in response to requests for digital information, for accessing the second portion of encrypted digital information, for decrypting the encrypted digital information, and for outputting the decrypted digital information.

10. The digital information product of claim 9, wherein the encrypted digital information is encrypted executable computer program logic.

11. A computer program product including a self-decrypting encrypted executable computer program, comprising:

a computer readable medium having computer program logic stored thereon, wherein the computer program logic defines:

a first module,

a second module,

wherein the first module, when executed by a computer, defines means for loading the second module into memory of the computer, and

a third module defining the encrypted executable computer program,

wherein the second module, when executed by a computer, defines means for communicating with an operating system of the computer to receive requests for program code from the encrypted executable computer program from the third module, and for processing the

Petitioner Apple Inc. - Exhibit 1012, p. 1608

requests to access and decrypt the encrypted executable computer program and for providing the decrypted executable code from the third module to the operating system.

12. A process for executing encrypted executable computer programs on a computer system having a processor, memory and operating system, comprising the steps of:

receiving computer program logic having a first module defining a start up routine, a second module, and a third module containing the encrypted executable computer program;

executing the first module of the received computer program logic using the processor,

wherein the step of executing causes the second module to be loaded into the memory of the computer system, and

generating requests from the operating system for data from the encrypted executable computer program which are received by the second module, and

accessing and decrypting the encrypted executable computer program and returning the decrypted executable computer program to the operating system.

Petitioner Apple Inc. - Exhibit 1012, p. 1609

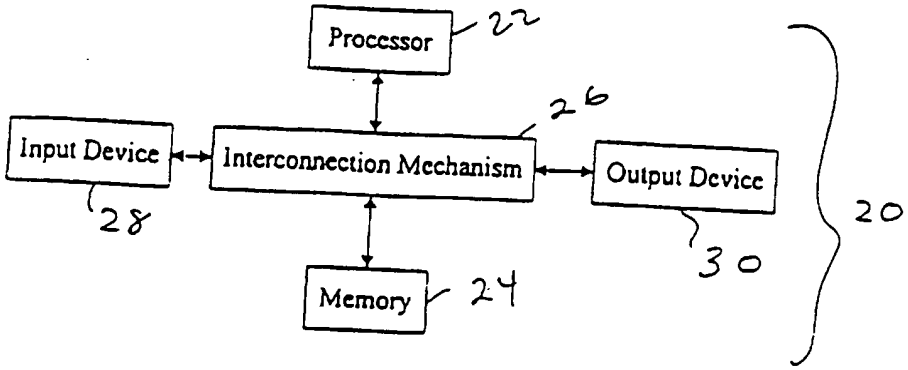


Fig. 1

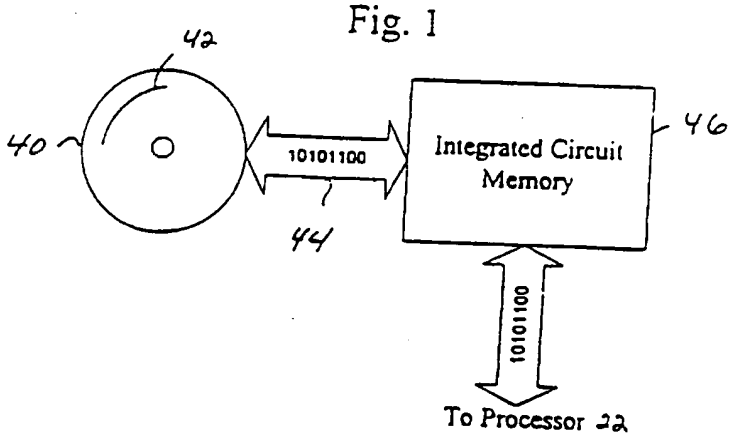


Fig. 2

Petitioner Apple Inc. - Exhibit 1012, p. 1610

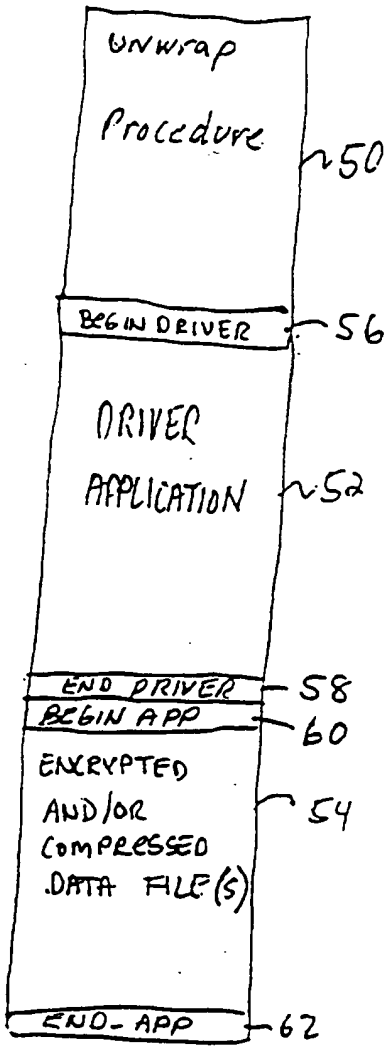


FIG. 3

Petitioner Apple Inc. - Exhibit 1012, p. 1611

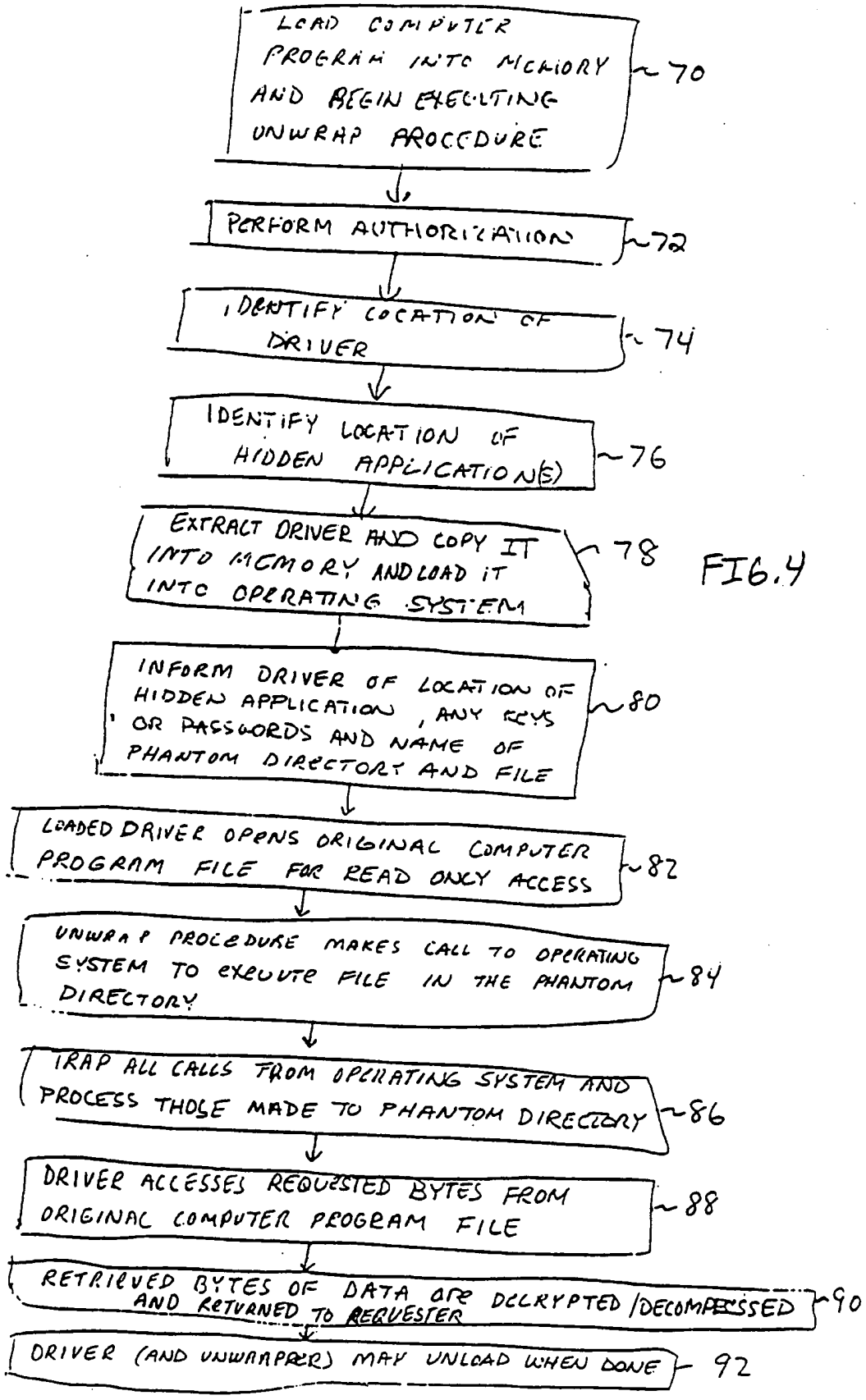


FIG. 4

Petitioner Apple Inc. - Exhibit 1012, p. 1612

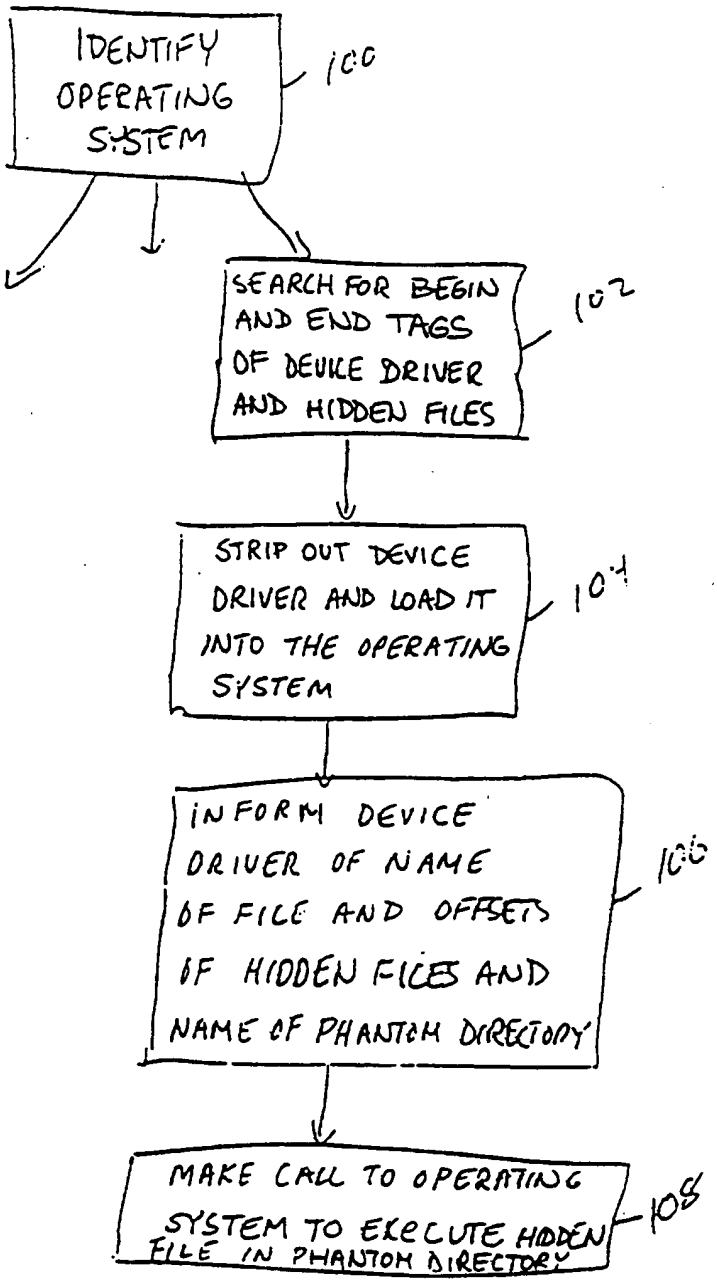


FIG. 5

BNSDOCID: <WO___9811690A1_I_>

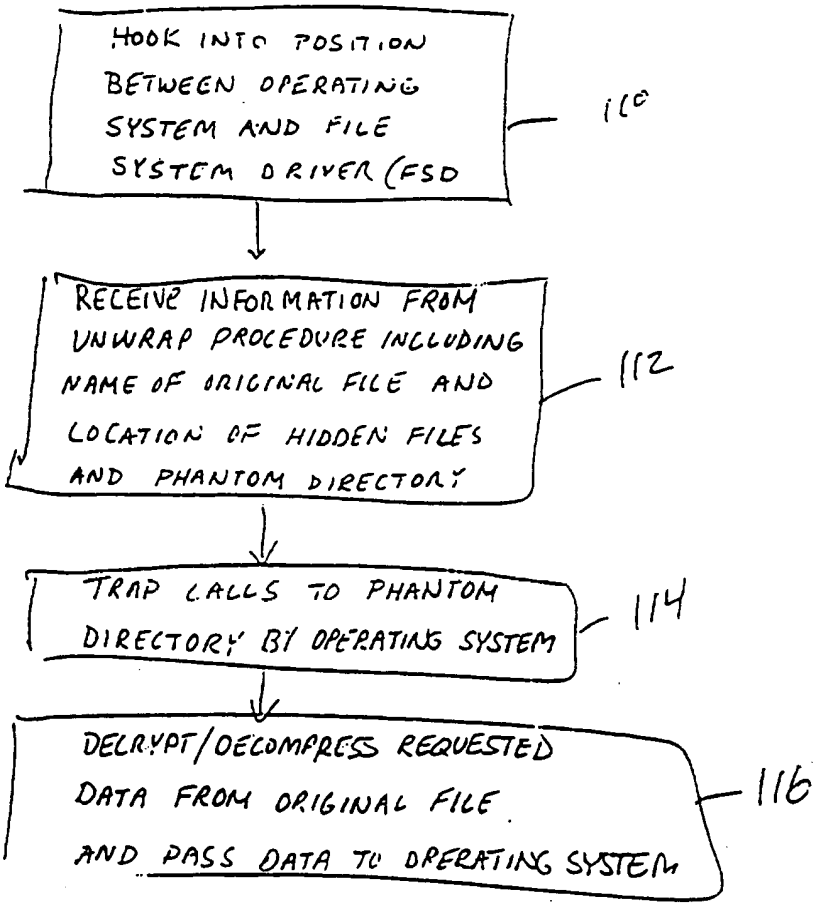


FIG. 6

Petitioner Apple Inc. - Exhibit 1012, p. 1614

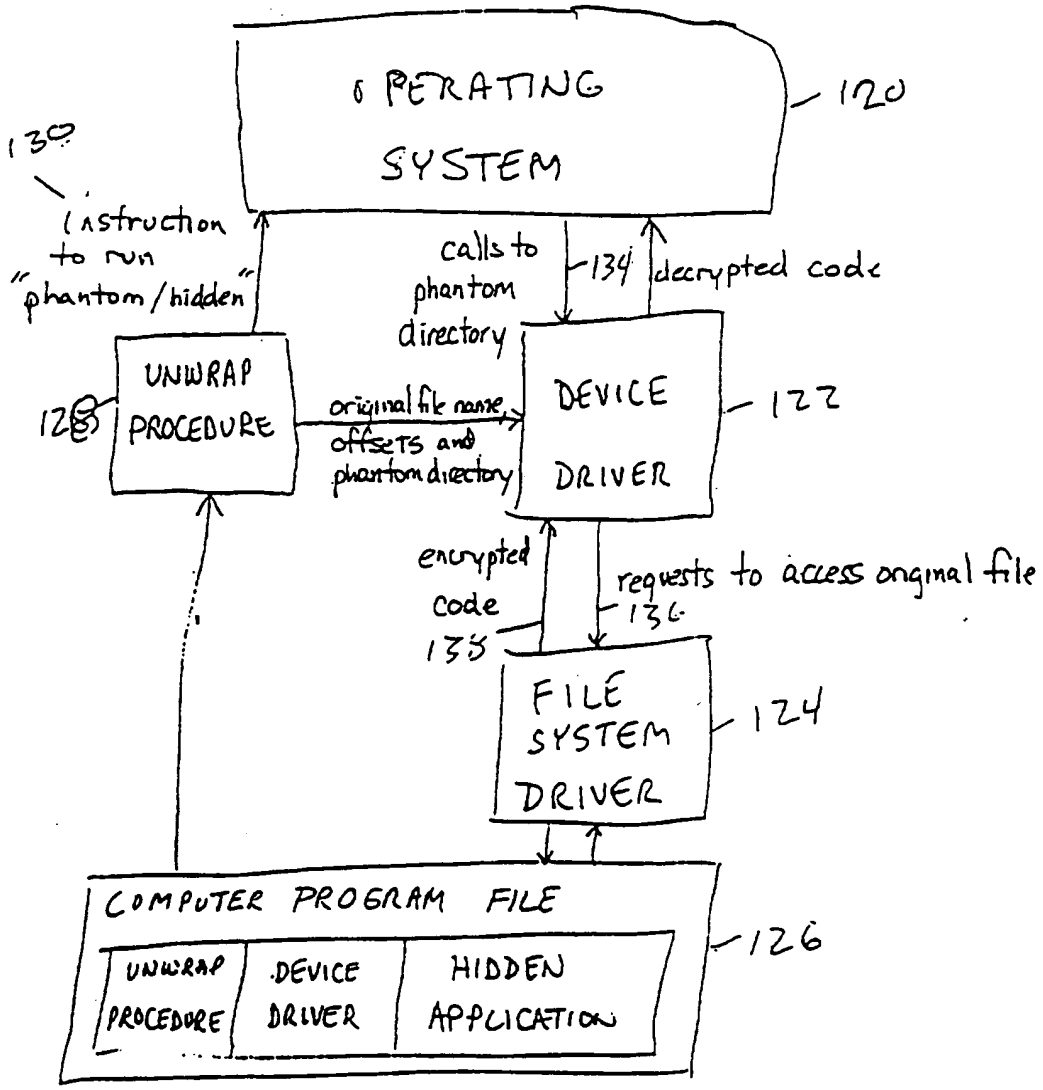

OPERATING SYSTEM
120
130
instruction to run "phantom/hidden"
calls to phantom directory
134
decrypted code
UNWRAP PROCEDURE
128
original file name, offsets and phantom directory
DEVICE DRIVER
122
encrypted code
135
requests to access original file
136
FILE SYSTEM DRIVER
124
COMPUTER PROGRAM FILE
UNWRAP PROCEDURE
DEVICE DRIVER
HIDDEN APPLICATION
126

FIG. 7

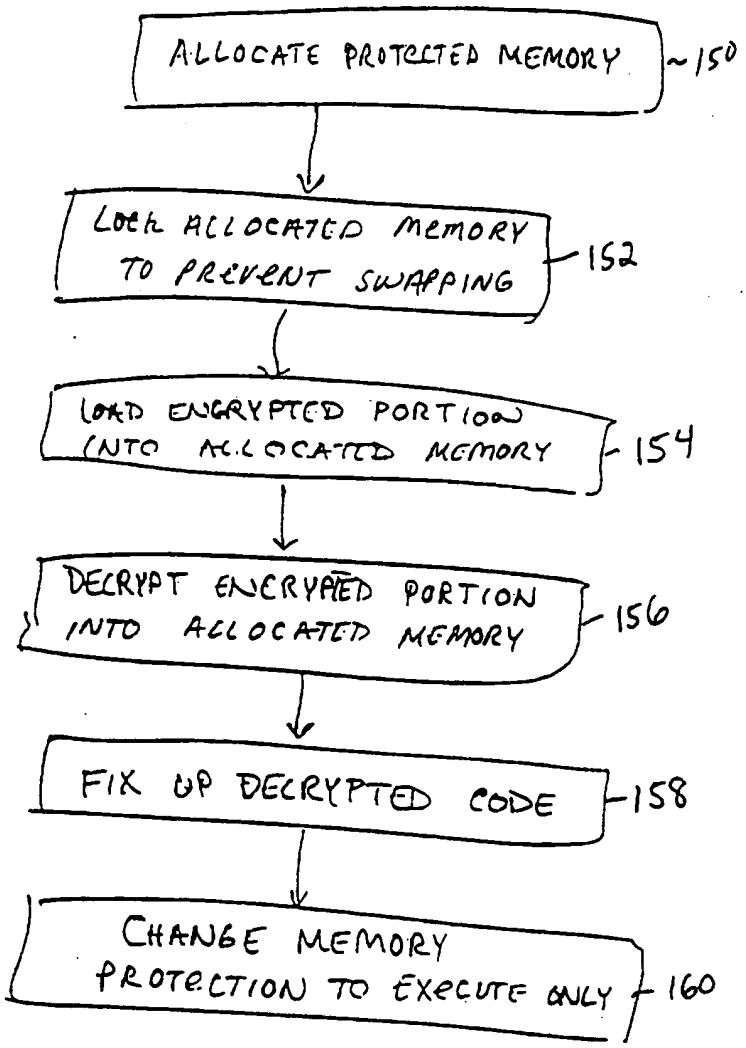


FIG. 8

Petitioner Apple Inc. - Exhibit 1012, p. 1616

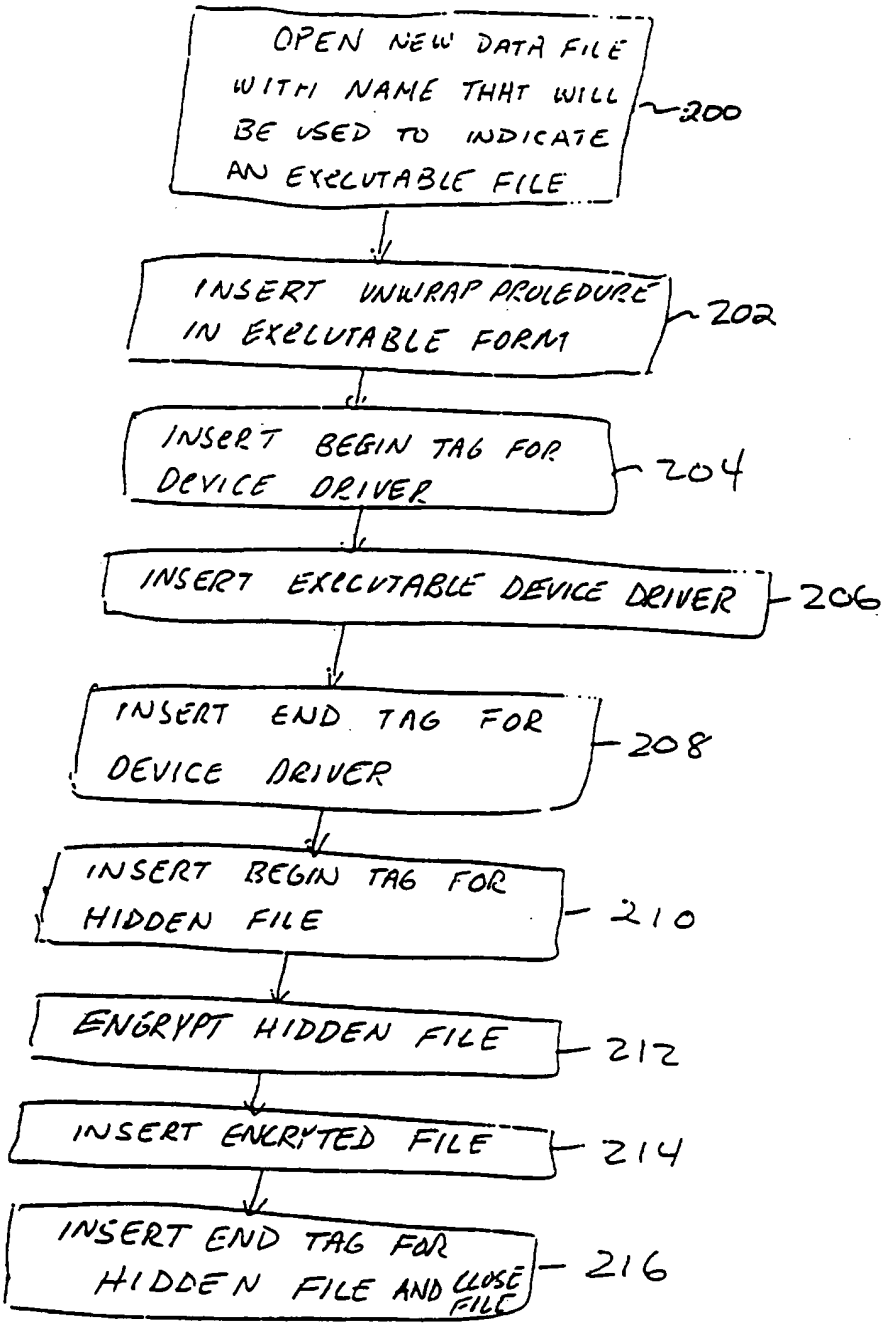


FIG. 9

BNSDOCID: <WO___9811690A1_I_>

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/16223

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL : 380/4

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/4,9,23,25,49,50,59

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4,937,861 A (CUMMINS) 26 June 1990, see Abstract.	1-12
A	US 5,007,082 A (CUMMINS) 09 April 1991, see Abstract.	1-12
A	US 5,144,659 A (JONES) 01 September 1992, see Abstract.	1-12
A	US 5,155,827 A (GHERING) 13 October 1992, see Abstract.	1-12
A	US 5,396,609 A (SCHMIDT et al) 07 March 1995, see Abstract.	1-12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
20 JANUARY 1998	18 FEB 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer BERNARR EARL GREGORY Telephone No. (703) 306-4153

Form PCT/ISA/210 (second sheet)(July 1992)*

BNSDOCID: <WO___9811690A1_I_>

CORRECTED VERSION*

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00	A1	(11) International Publication Number: WO 98/11690
		(43) International Publication Date: 19 March 1998 (19.03.98)

(21) International Application Number: PCT/US97/16223

(22) International Filing Date: 12 September 1997 (12.09.97)

(30) Priority Data:

60/025,991	12 September 1996 (12.09.96)	US
08/887,723	3 July 1997 (03.07.97)	US

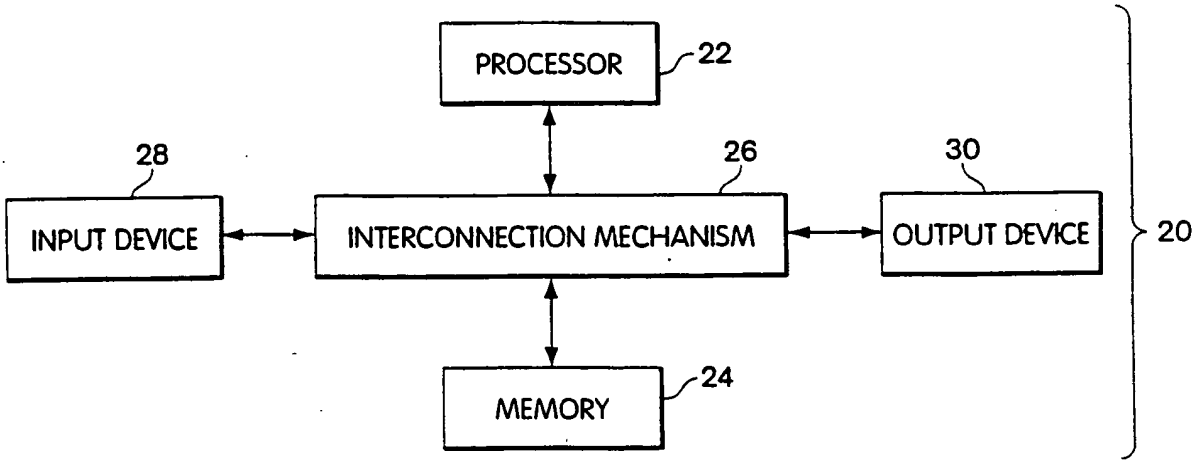
(71)(72) Applicant and Inventor: GLOVER, John, J. [US/US]; 26 Amaranth Avenue, Medford, MA 02155 (US).

(74) Agent: GORDON, Peter, J.; Wolf, Greenfield & Sacks, P.C., 600 Atlantic Avenue, Boston, MA 02210 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: SELF-DECRYPTING DIGITAL INFORMATION SYSTEM AND METHOD



(57) Abstract

The claimed data protection device (20) includes a processor (22) connected to a memory system (24) through an interconnection mechanism (26). An input device (28) is also connected to the processor (22) and memory system (24) through the interconnection mechanism (26). The interconnection mechanism (26) is typically a combination of one or more buses and one or more switches. The output device (30) may be a display, and the input device (28) may be a keyboard and/or mouse or other cursor control device.

*(Referred to in PCT Gazette No. 32/1998, Section II)

BNSDOCID: <WO___9811690A1_IA>

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

BNSDOCID: <WO___9811690A1_IA>

SELF-DECRYPTING DIGITAL INFORMATION SYSTEM AND METHOD

Field of the Invention

The present invention is related to mechanisms for protecting digital information from being copied. In particular, the present invention is related to mechanisms which permit authorized execution of computer program code or access to other digital information which is encrypted or otherwise encoded.

Background of the Invention

A serious problem which faces the electronic publishing and software industries is the ease with which digital information can be copied without authorization from the publisher. Digital information also may be used or modified without authorization. For example, computer software may be reverse engineered or attacked by computer viruses.

There are many mechanisms available which may be used to limit or prevent access to digital information. Such mechanisms often either restrict the ability of the user to make back-up copies or involve the use of special purpose hardware to limit access to the digital information. For example, some mechanisms restrict the use of digital information to a particular machine. See, for example, U.S. Patent 4,817,140. Other mechanisms require the digital information to be stored on a particular recording medium in order to be used. See, for example, U.S. Patent 5,412,718. Yet other mechanisms allow only a certain number of uses of the digital information. See for example, U.S. Patent 4,888,798. Many of these access control mechanisms cause distribution to be more costly.

Several other patents describe a variety of systems for encryption, compression, licensing and royalty control and software distribution such as: U.S. Pat. No. 4,405,829, U.S. Pat. No. 4,864,616, U.S. Pat. No. 4,888,800, U.S. Pat. No. 4,999,806, U.S. Pat. No. 5,021,997, U.S. Patent No. 5,027,396, U.S. Pat. No. 5,033,084, U.S. Pat. No. 5,081,675, U.S. Pat. No. 5,155,847, U.S. Pat. No. 5,166,886, U.S. Pat. No. 5,191,611, U.S. Pat. No. 5,220,606, U.S. Pat. No. 5,222,133, U.S. Pat. No. 5,272,755, U.S. Pat. No. 5,287,407, U.S. Pat. No. 5,313,521, U.S. Pat. No. 5,325,433, U.S. Pat. No. 5,327,563, U.S. Pat. No. 5,337,357, U.S. Pat. No. 5,351,293, U.S. Pat. No. 5,341,429, U.S. Pat. No. 5,351,297, U.S. Pat. No. 5,361,359, U.S. Pat. No. 5,379,433, U.S. Pat. No. 5,392,351, U.S. Pat. No. 5,394,469, U.S. Pat. No. 5,414,850, U.S. Pat. No. 5,473,687, U.S. Pat. No. 5,490,216, U.S. Pat. No. 5,497,423, U.S. Pat. No. 5,509,074, U.S.

Pat. No. 5,,511,123, U.S. Pat. No. 5,524,072, U.S. Pat. No. 5,532,920, U.S. Pat. No. 5,555,304, U.S. Pat. No. 5,557,346, U.S. Pat. No. 5,557,765, U.S. Pat. No. 5,592,549, U.S. Pat. No. 5,615,264, U.S. Pat. No. 5,625,692, and U.S. Pat. No. 5,638,445.

Computer programs or other digital information also may be encrypted in order to prevent an individual from making a useful copy of the information or from reverse engineering a program. Even with such encryption, however, a computer program must be decrypted in order for a computer to load and execute the program. Similarly, other digital information must be decrypted before it can be accessed and used. Generally, digital information is decrypted to disk, and not to main memory of the computer which is more protected by the operating system, because decryption to main memory results in a significant loss of memory resources. If the purpose for using encryption is to prevent users from copying the digital information, then decryption of the information to accessible memory for use defeats this purpose.

One way to protect digital information using encryption has been made available by International Business Machines (IBM) and is called a "CRYPTOLOPE" information container. This technology is believed to be related to U.S. Patent Nos. 5,563,946 and 5,598,470 (to Cooper et al.), and published European patent applications 0679977, 0679978, 0679979 and 0681233. The CRYPTOLOPE system requires a user to have a "helper application" and a key. The CRYPTOLOPE information container is generated by IBM. The content provider submits data to IBM, which in turn encrypts and packages the data in a CRYPTOLOPE information container. The helper application is a form of memory resident program, called a terminate and stay resident (TSR) program, which is a form of input/output (I/O) device driver installed in the operating system and which monitors requests from the operating system for files on specified drives and directories. Because the TSR program must know the directory, and/or file name to be accessed, that information also is available to other programs. Other programs could use that information to manipulate the operation of the TSR program in order to have access to decrypted contents of the information container. The encrypted information container includes an executable stub which is executed whenever the application is run without the installed TSR program or from a drive not monitored by the TSR program to prevent unpredictable activity from executing encrypted code. This stub may be used to install decryption and cause the application be executed a second time, or to communicate with the TSR program to instruct the TSR program to monitor the drive. It may be preferable from the point of view of the content provider however to maintain an encryption process and keys independently of any third party.

Multimedia content, such as a movie or hypertext presentation also may be stored on a digital versatile disk (DVD), sometimes called a digital video disk, compact disk read-only memory (CD-ROM), rewriteable compact disks (CD-RW) or other medium in an encrypted digital format for use with special-purpose devices. For example, concern about illegal copying of content from digital video disks or other digital media has resulted in a limited amount of content being available for such devices. This problem has caused representatives of both multimedia providers and digital video disk manufacturers to negotiate an agreement on an encryption format for information stored on DVDs. This copy protection scheme is licensed through an organization called the CSS Interim Licensing organization. However, in this arrangement, the content provider is limited to using the agreed upon encryption format and a device manufacturer is limited to using a predetermined decryption system.

Encryption has also been used to protect and hide computer viruses. Such viruses are typically polymorphic, i.e., they change every time they infect a new program, and are encrypted. The virus includes a decryption program that executes to decrypt the virus every time the infected program is run. Such viruses are described, for example, in "Computer Virus-Antivirus Coevolution" by Carey Nachenberg, Communications of the ACM, Vol. 40, No. 1, (Jan. 1997), p. 46 et seq. Such viruses include decryption keys within them since, clearly, their execution is not carried out by the user and a user would not be asked for authorization keys to permit execution of the viruses. Additionally, such viruses are typically only executed once at the start of execution of an infected program and permanently return control to the infected program after execution.

Summary of the Invention

Some of these problems with digital information protection systems may be overcome by providing a mechanism which allows a content provider to encrypt digital information without requiring either a hardware or platform manufacturer or a content consumer to provide support for the specific form of corresponding decryption. This mechanism can be provided in a manner which allows the digital information to be copied easily for back-up purposes and to be transferred easily for distribution, but which should not permit copying of the digital information in decrypted form. In particular, the encrypted digital information is stored as an executable computer program which includes a decryption program that decrypts the encrypted information

to provide the desired digital information, upon successful completion of an authorization procedure by the user.

In one embodiment, the decryption program is executed as a process within a given operating system and decrypts the digital information within the memory area assigned to that process. This memory area is protected by the operating system from copying or access by other processes. Even if access to the memory area could be obtained, for example through the operating system, when the digital information is a very large application program or a large data file, a copy of the entire decrypted digital information is not likely to exist in the memory area in complete form.

By encrypting information in this manner, a platform provider merely provides a computer system with an operating system that has adequate security to define a protected memory area for a process and adequate functionality to execute a decryption program. The content provider in turn may use any desired encryption program. In addition, by having a process decrypt information within a protected memory area provided by the operating system, the decrypted information does not pass through any device driver, memory resident program or other known logical entity in the computer system whose behavior may be controlled to provide unauthorized access to the data. The ability to reverse engineer or attack a computer program with a computer virus also may be reduced.

In another embodiment, the decryption program is part of a dynamically loaded device driver that responds to requests for data from the file containing the encrypted data. When the digital information product is first executed, this device driver is extracted from the file and is loaded into the operating system. The executed digital information product then informs the loaded device driver of the location of the hidden information in the file, any keys or other passwords, and the name of a phantom directory and file to be called that only the digital information product and the device driver know about. The name of this directory may be generated randomly. Each segment of hidden information in the digital information product may be assigned its own unique file name in the phantom directory. The digital information product then makes a call to the operating system to execute one of the files in the phantom directory. The loaded driver traps these calls to the operating system, accesses the original file, decrypts the desired information and outputs the desired information to the operating system.

In combination with other mechanisms that track distribution, enforce royalty payments and control access to decryption keys, the present invention provides an improved method for

Petitioner Apple Inc. - Exhibit 1012, p. 1624

identifying and detecting sources of unauthorized copies. Suitable authorization procedures also enable the digital information to be distributed for a limited number of uses and/or users, thus enabling per-use fees to be charged for the digital information.

Accordingly, one aspect of the invention is a digital information product including a computer-readable medium with digital information stored thereon. The digital information includes computer program logic having a first portion of executable computer program logic and a second portion of digital information. The first portion of executable program logic, when executed, defines a mechanism for responding to requests for digital information from an operating system of a computer. This mechanism, when used to access the second portion of the encrypted digital information, decrypts the encrypted digital information, and provides the encrypted digital information to the operating system.

In the foregoing aspect of the invention, the digital information may be executable computer program logic. Hence, one aspect of the invention is a computer program product, including a computer readable medium with computer program logic stored thereon. The computer program logic includes a first portion of executable computer program logic and a second portion of encrypted computer program logic. The first portion of executable computer program logic, when executed, defines a mechanism for responding to requests for computer program logic from an operating system of a computer. This mechanism accesses the second portion of encrypted computer program logic, decrypts the encrypted computer program logic, and provides the decrypted computer program logic to the operating system.

Another aspect of the present invention is a computer program product, a computer system and a process which produce a computer program or digital information product in accordance with other aspects of the invention, using executable program code for the first and second portions of the desired computer program product.

Another aspect of the present invention is a computer program product including a self-decrypting encrypted executable computer program. The product includes a computer readable medium having computer program logic stored thereon. The computer program logic defines first, second and third modules, wherein the third module defines the encrypted executable computer program. The first module, when executed by a computer, defines a mechanism for loading the second module into memory of the computer. The second module, when executed by a computer, defines a mechanism for communicating with an operating system of the computer to receive requests for program code from the encrypted executable computer program from the

Petitioner Apple Inc. - Exhibit 1012, p. 1625

third module, and for processing the requests to access and decrypt the encrypted executable computer program and for providing the decrypted executable code from the third module to the operating system.

Another aspect of the invention is a process for executing encrypted executable computer programs on a computer system having a processor, memory and operating system. The process involves receiving computer program logic having a first module defining a start up routine, a second module, and a third module containing the encrypted executable computer program. The first module of the received computer program logic is executed using the processor. When the first module is executed, the second module is caused to be loaded into the memory of the computer system. Requests are generated from the operating system for data from the encrypted executable computer program and are received by the second module. The second module accesses and decrypts the encrypted executable computer program in response to these requests and returns the decrypted executable computer program to the operating system.

These and other aspects, advantages and features of the present invention and its embodiments will be more apparent given the following detailed description.

Brief Description of the Drawing

In the drawing,

Fig. 1 is a block diagram of a typical computer system with which the present invention may be implemented;

Fig. 2 is a block diagram of a memory system in the computer system of Fig. 1;

Fig. 3 is a diagram of a computer program or digital information product which may be recorded on a computer readable and writable medium, such as a magnetic disc;

Fig. 4 is a flowchart describing how the computer program or digital information product of Fig. 3 is used;

Fig. 5 is a flowchart describing operation of an example unwrap procedure as shown in Fig. 3 in one embodiment of the invention;

Fig. 6 is a flowchart describing operation of an example device driver as shown in Fig. 3 in one embodiment of the invention;

Fig. 7 is a block diagram of a computer system in the process of executing a computer program product in accordance with one embodiment of the invention;

Fig. 8 is a flowchart describing operation of an example unwrap procedure in another embodiment of the invention; and

Fig. 9 is a flowchart describing how a computer program product such as shown in Fig. 3 is constructed.

Detailed Description

The present invention will be more completely understood through the following detailed description which should be read in conjunction with the attached drawing in which similar reference numbers indicate similar structures.

Embodiments of the present invention may be implemented using a general purpose digital computer or may be implemented for use with a digital computer or digital processing circuit. A typical computer system 20 is shown in Fig. 1, and includes a processor 22 connected to a memory system 24 via an interconnection mechanism 26. An input device 28 also is connected to the processor and memory system via the interconnection mechanism, as is an output device 30. The interconnection mechanism 26 is typically a combination of one or more buses and one or more switches. The output device 30 may be a display and the input device may be a keyboard and/or a mouse or other cursor control device.

It should be understood that one or more output devices 30 may be connected to the computer system. Example output devices include a cathode ray tube (CRT) display, liquid crystal display (LCD), television signal encoder for connection to a television or video tape recorder, printers, communication devices, such as a modem, and audio output. It also should be understood that one or more input devices 28 may be connected to the computer system. Example input devices include a keyboard, keypad, trackball, mouse, pen and tablet, communication device, audio or video input and scanner. It should be understood that the invention is not limited to the particular input or output devices used in combination with the computer system or to those described herein.

The computer system 20 may be a general purpose computer system, which is programmable using a high level computer programming language, such as "C++," "Pascal," "VisualBasic." The computer system also may be implemented using specially programmed, special purpose hardware. In a general purpose computer system, the processor is typically a commercially available processor, such as the Pentium processor from Intel Corporation. Many other processors are also available. Such a processor executes a program called an operating

system, such as Windows 95 or Windows NT 4.0, both available from Microsoft Corporation, which controls the execution of other computer programs and provides scheduling, debugging, input output control, accounting compilation, storage assignment, data management and memory management, and communication control and related services. Other examples of operating systems include: MacOS System 7 from Apple Computer, OS/2 from IBM, VMS from Digital Equipment Corporation, MS-DOS from Microsoft Corporation, UNIX from AT&T, and IRIX from Silicon Graphics, Inc.

The computer system 20 also may be a special purpose computer system such as a digital versatile disk or digital video disk (DVD) player. In a DVD player, there is typically a decoder controlled by some general processor which decodes an incoming stream of data from a DVD. In some instances, the DVD player includes a highly integrated DVD decoder engine. Such devices generally have a simple operating system which may be modified to include the capabilities described and used herein in connection with the typical operating systems in a general purpose computer. In particular, some operating systems are designed to be small enough for installation in an embedded system such as a DVD player, including the WindowsCE operating system from Microsoft Corporation and the JavaOS operating system from SunSoft Corporation. The operating system allows a content provider to provide its own programs that define some of the content, which is particularly useful for interactive multimedia. This capability also can be used to provide encryption and decryption, in accordance with the invention.

The processor and operating system define a computer platform for which application programs in a programming language such as an assembly language or a high level programming language are written. It should be understood that the invention is not limited to a particular computer platform, operating system, processor, or programming language. Additionally, the computer system 20 may be a multi-processor computer system or may include multiple computers connected over a computer network.

An example memory system 24 will now be described in more detail in connection with Fig. 2. A memory system typically includes a computer readable and writable non-volatile recording medium 40, of which a magnetic disk, a flash memory, rewriteable compact disk (CD-RW) and tape are examples. The recording medium 40 also may be a read only medium such as a compact disc-read only memory (CD-ROM) or DVD. A magnetic disk may be removable, such as a "floppy disk" or "optical disk," and/or permanent, such as a "hard drive." The disk,

which is shown in Fig. 2, has a number of tracks, as indicated at 42, in which signals are stored, in binary form, i.e., a form interpreted as a sequence of 1's and 0's, as shown at 44. Such signals may define an application program to be executed by the microprocessor, or information stored on the disk to be processed by the application program. Typically, in the operation of a general purpose computer, the processor 22 causes data to be read from the non-volatile recording medium 40 into an integrated circuit memory element 46, which is typically a volatile random access memory, such as a dynamic random access memory (DRAM) or static random access memory (SRAM). The integrated circuit memory element 46 allows for faster access to the information by the processor than disk 40, and is typically called the system or host memory. The processor generally causes the data to be manipulated within the integrated circuit memory 46 and may copy the data to the disk 40, if modified, when processing is completed. A variety of mechanisms are known for managing data movement between the disk 40 and the integrated circuit memory 46, and the invention is not limited thereto. It should also be understood that the invention is not limited to a particular memory system.

The file system of a computer generally is the mechanism by which an operating system manages manipulation of data between primary and secondary storage, using files. A file is a named logical construct which is defined and implemented by the operating system to map the name and a sequence of logical records of data to physical storage media. An operating system may specifically support various record types or may leave them undefined to be interpreted or controlled by application programs. A file is referred to by its name by application programs and is accessed through the operating system using commands defined by the operating system. An operating system provides basic file operations provided by for creating a file, opening a file, writing a file, reading a file and closing a file.

In order to create a file, the operating system first identifies space in the storage media which is controlled by the file system. An entry for the new file is then made in a directory which includes entries indicating the names of the available files and their locations in the file system. Creation of a file may include allocating certain available space to the file. Opening a file returns a handle to the application program which it uses to access the file. Closing a file invalidates the handle.

In order to write data to a file, an application program issues a command to the operating system which specifies both an indicator of the file, such as a file name, handle or other descriptor, and the information to be written to the file. Given the indicator of the file, the

operating system searches the directory to find the location of the file. The directory entry stores a pointer, called the write pointer, to the current end of the file. Using this pointer, the physical location of the next available block of storage is computed and the information is written to that block. The write pointer is updated in the directory to indicate the new end of the file.

In order to read data from a file, an application program issues a command to the operating system specifying the indicator of the file and the memory locations assigned to the application where the next block of data should be placed. The operating system searches its directory for the associated entry given the indicator of the file. The directory may provide a pointer to a next block of data to be read, or the application may program or specify some offset from the beginning of the file to be used.

A primary advantage of using a file system is that, for an application program, the file is a logical construct which can be created, opened, written to, read from and closed without any concern for the physical storage used by the operating system.

The operating system also allows for the definition of another logical construct called a process. A process is a program in execution. Each process, depending on the operating system, generally has a process identifier and is represented in an operating system by a data structure which includes information associated with the process, such as the state of the process, a program counter indicating the address of the next instruction to be executed for the process, other registers used by process and memory management information including base and bounds registers. Other information also may be provided. The base and bounds registers specified for a process contain values representing the largest and smallest addresses that can be generated and accessed by an individual program. Where an operating system is the sole entity able to modify these memory management registers, adequate protection from access to the memory locations of one process from another process is provided. As a result, this memory management information is used by the operating system to provide a protected memory area for the process. A process generally uses the file system of the operating system to access files.

The present invention involves storing encrypted digital information, such an audio, video, text or an executable computer program, on a computer readable medium such that it can be copied easily for back-up purposes and transferred easily for distribution, but also such that it cannot be copied readily in decrypted form during use. In particular, the digital information is stored as a computer program that decrypts itself while it is used to provide the digital information, e.g., to provide executable operation code to the operating system of a computer, as

the digital information is needed. Any kind of encryption or decryption may be used and also may include authorization mechanisms and data compression and decompression. In one embodiment of the present invention, decrypted digital information exists only in memory accessible to the operating system and processes authorized by the operating system. When the digital information is a large application program, a copy of the entire decrypted application program is not likely to exist in the main memory at any given time, further reducing the likelihood that a useful copy of decrypted code could be made. The decryption operation also is performed only if some predetermined authorization procedure is completed successfully.

One embodiment of the invention, in which the decryption program is a form of dynamically loaded device driver, will first be described. Fig. 3 illustrates the structure of digital information as stored in accordance with one embodiment of the present invention, which may be stored on a computer readable medium such as a magnetic disc or compact disc read only memory (CD-ROM) to form a computer program product. The digital information includes a first portion 50, herein called an unwrap procedure or application, which is generally unencrypted executable program code. The purpose of the unwrap procedure is to identify the locations of the other portions of the digital information, and may perform other operations such as verification. In particular, the unwrap procedure identifies and extracts a program which will communicate with the operating system, herein called a virtual device driver 52. The unwrap procedure may include decryption and decompression procedures to enable it to decrypt/decompress the driver, and/or other content of this file. The program 52 need not be a device driver. The virtual device driver 52 typically follows the unwrap procedure 50 in the file container, the digital information. The virtual device driver, when executed, decrypts and decodes the desired digital information such as an executable computer program code from hidden information 54, which may be either encrypted and/or encoded (compressed). It is the decrypted hidden information which is the desired digital information to be accessed. This hidden information may be any kind of digital data, such as audio, video, text, and computer program code including linked libraries or other device drivers.

In this embodiment of the computer program product, labels delineate the boundaries between the device driver and the hidden files. These labels may or may not be encrypted. A first label 56 indicates the beginning of the code for the virtual device driver 52. A second label 58 indicates the end of the virtual device driver code. Another label 60 indicates the beginning of the hidden information and a label 62 indicates the end of that application. There may be one

or more blocks of such hidden information, each of which can be given a different name. It may be advantageous to use the name of the block of information in its begin and end tags. This computer program product thus contains and is both executable computer program code and one or more blocks of digital information. A table of locations specifying the location of each portion of the product could be used instead of labels. Such a table could be stored in a predetermined location and also may be encrypted.

The overall process performed using this computer program product in one embodiment of the invention will now be described in connection with Fig. 4. This embodiment may be implemented for use with the Windows95 operating system and is described in more detail in connection with Figs. 5-7. An embodiment which may be implemented for use on the WindowsNT 4.0 operating system is described in more detail below in connection with Fig. 8. In both of these described embodiments, the digital information is an executable computer program which is read by the operating system as data from this file and is executed. The same principle of operation would apply if the data were merely audio, video, text or other information to be conveyed by a user. In the embodiment of Fig. 4, the computer program is first loaded into memory in step 70, and the unwrap procedure 50 is executed by the operating system, as any typical executable computer program is executed. The unwrap procedure may perform authorization, for example by checking for a required password or authentication code, and may receive any data needed for decryption or decompression, for example keys or passwords, in step 72. Suitable authorization procedures may provide the ability to distribute software for single use. The unwrap procedure locates the virtual device driver 52 within the computer program in step 74, and then locates the hidden application in step 76. The virtual device driver 52 is then extracted by the unwrap procedure from the computer program, copied to another memory location and loaded for use by the operating system in step 78. An advantage of an operating system like Windows95 is that it allows such device drivers to be loaded dynamically without restarting the computer.

The executed unwrap procedure 50, in step 80, informs the loaded virtual device driver 52 of the location of the hidden information in the file, any keys or other passwords, and a name of a phantom directory and file to be called that only the unwrap procedure and the virtual device driver know about. The name of this phantom directory may be generated randomly. Each segment information hidden in the digital information product may be assigned its own unique file name in the phantom directory.

After the loaded virtual device driver 52 receives all communications from the unwrap procedure, it opens the original application file for read only access in step 82. The unwrap procedure then makes a call to the operating system in step 84 to execute the file in the phantom directory for which the name was transmitted to the loaded virtual device driver. One function of the loaded virtual device driver 52 is to trap all calls from the operating system to access files in step 86. Any calls made by the operating system to access files in the phantom directory are processed by the virtual device driver, whereas calls to access files in other directories are allowed to proceed to their original destination. In response to each call from the operating system, the virtual device driver obtains the bytes of data requested by the operating system from the original computer program file in step 88. These bytes of data are then decrypted or decompressed in step 90 and returned to the operating system. When processing is complete, the phantom application is unloaded from the operating system in step 92, and may be deleted from the memory.

A more detailed description of the process of Fig. 4 will now be described in connection with Figs. 5-7. Fig. 5 is a flowchart describing the operation of one embodiment of the unwrap procedure in more detail. The first step performed by this procedure is identifying the operating system being used, in step 100. This step is useful because different methods may be used with different operating systems. All code that may be used to run in various operating systems may be placed in this unwrap procedure. This procedure also may contain the decompression/decryption code, for example or any other computer program code to be executed.

The executed application then opens the original executable file as a data file and searches for the begin and end tags of the device driver and hidden files in step 102. The device driver code is copied into memory and loaded into the operating system in step 104. The unwrap procedure then informs the device driver of the name of the original application file, offsets of the hidden files and the name of a phantom directory, which is typically randomly generated (step 106). This communication may be performed using a "DeviceIOControl" function call in the Windows95 operating system. The unwrap procedure then makes a call to the operating system to execute the hidden file in the phantom directory, in step 108.

The operation of one embodiment of a device driver will now be described in connection with Fig. 6. After the device driver is loaded into the operating system, it hooks into a position between the operating system and a file system driver (FSD), in step 110, to intercept

Petitioner Apple Inc. - Exhibit 1012, p. 1633

calls made by the operating system to the FSD for data from files in the phantom directory. The FSD is the code within the operating system that performs physical reading and writing of data to disk drives. The operating system makes requests to the FSD for data from files in directories on the disk drives. The driver then receives information from the unwrap procedure including the name of the original file, the location of hidden files within the original file, and the name of the phantom directory created by the unwrap procedure (step 112). The device driver opens the original file as a read only data file. The device driver now traps calls, in step 114, made from the operating system for files in the phantom directory. Calls to other directories are ignored and passed on to the original destination. The device driver then reads the data from the original data file, decrypts and decompresses it, and returns the decrypted/decompressed data to the operating system in step 116.

For example, if the offset for the hidden application in the original data file is 266,270 bytes and the operating system asks for 64 bytes starting at offset 0 of the hidden application in the phantom directory, the device driver reads 64 bytes from the original file starting at offset 266,270, decrypts/decompresses those 64 bytes, and returns the first 64 decrypted/decompressed bytes back to the operating system. From the point of view of the operating system, the 64 bytes appear to have come from the file in the phantom directory. Steps 114 and 116 are performed on demand in response to the operating system.

A block diagram of the computer system in this embodiment, with a device driver loaded and in operation, will now be described in more detail in connection with Fig. 7. Fig. 7 illustrates the operating system 120, the loaded device driver 122, a file system driver 124, the original executable file 126 as it may appear on disk and the unwrap procedure 128. The executable file may in fact be on a remote computer and accessed through a network by the device driver. The unwrap procedure causes the operating system to begin execution of the hidden file by issuing an instruction to execute the file in the phantom directory, as indicated at 130. This command is issued after the device driver 122 is informed of the file name of the original executable file 126, offsets of the hidden files within that file and the name of the phantom directory, as indicated at 132. The operating system then starts making calls to the phantom directory as indicated at 134. The device driver 122 traps these calls and turns them into requests 136 to the file system driver to access the original executable file 126. Such requests actually are made to the operating system 120, through the device driver 122 to the file system driver 124. The file system driver 124 returns encrypted code 138 to the device driver

Petitioner Apple Inc. - Exhibit 1012, p. 1634

122. The encrypted code 138 actually passes back through the device driver 122 to the operating system 120 which in turn provides the encrypted code 138 to the device driver 122 as the reply to the request 136 for the original file. The device driver 122 then decrypts the code to provide decrypted code 140 to the operating system 120.

Another embodiment of the invention will now be described in connection with Fig. 8. This embodiment may be implemented using the WindowsNT 4.0 operating system, for example. In this embodiment, the device driver portion 52 of the computer program product is not used. The unwrap procedure for this embodiment begins by identifying the operating system being used similar, which is step 100 in Fig. 5. If the operating system is Windows NT 4.0, for example, a different unwrap procedure for this embodiment is performed. Before describing this unwrap procedure, a brief description of some of the available operating system commands will be provided.

Currently, under all versions of the Window operating system or operating environment from Microsoft Corporation (such as Windows 3.1, Windows 95 and Windows NT 3.51 and 4.0) all executable files (.exe) or dynamic link library (.dll and .ocx) files, which are executable files with different header and loading requirements than .exe files, that are loaded into memory by the operating system must reside as a file either locally, e.g., on a disk drive or remotely, e.g., over a network or communications port. All further references herein to loading an executable will be using the Win32 function calls used in Windows 95 and NT 3.51 and 4.0 operating systems. The CreateProcess() function which loads files with an .exe extension takes ten parameters:

```
BOOL CreateProcess(// Prototype from Microsoft Visual C++ Help Documentation
  LPCTSTR lpApplicationName,                  // pointer to name of executable module
  LPTSTR lpCommandLine,                       // pointer to command line string
  LPSECURITY_ATTRIBUTES lpProcessAttributes,  // pointer to process security attributes
  LPSECURITY_ATTRIBUTES lpThreadAttributes,   // pointer to thread security attributes
  BOOL bInheritHandles,                       // handle inheritance flag
  DWORD dwCreationFlags,                      // creation flags
  LPVOID lpEnvironment,                       // pointer to new environment block
  LPCTSTR lpCurrentDirectory,                 // pointer to current directory name
  LPSTARTUPINFO lpStartupInfo,                // pointer to STARTUPINFO
  LPPROCESS_INFORMATION lpProcessInformation  // pointer to PROCESS_INFORMATION
  );
```

Three of these parameters are pointers to strings that contain an application file name, command line parameters, and the current directory. The other parameters are security, environmental, and process information. The LoadLibrary() function takes one parameter that is a pointer to a string that contains the application file name:

```
HINSTANCE LoadLibrary(// Prototype from Microsoft Visual C++ Help Documentation
  LPCTSTR lpLibFileName      // address of filename of executable module
);
```

The LoadLibraryEx() function takes three parameters the first being the same as LoadLibrary(), the second parameter must be null, and the third tells the operating system whether to load the file as an executable or as a data file in order to retrieve resources such as icons or string table data from it and not load it as an executable:

```
HINSTANCE LoadLibraryEx(// Prototype from Microsoft Visual C++ Help Documentation
  LPCTSTR lpLibFileName,     // points to name of executable module
  HANDLE hFile,              // reserved, must be NULL
  DWORD dwFlags              // entry-point execution flag
);
```

The CreateFile() function is used to create and open files and to load files such as device drivers. This function also requires a pointer to a string that contains the name of a physical file:

```
HANDLE CreateFile(// Prototype from Microsoft Visual C++ Help Documentation
  LPCTSTR lpFileName,                          // pointer to name of the file
  DWORD dwDesiredAccess,                       // access (read-write) mode
  DWORD dwShareMode,                           // share mode
  LPSECURITY_ATTRIBUTES lpSecurityAttributes,  // pointer to security descriptor
  DWORD dwCreationDistribution,                // how to create
  DWORD dwFlagsAndAttributes,                  // file attributes
  HANDLE hTemplateFile                         // handle to file with attributes to copy
);
```

There are other functions such as MapViewOfFile() and MapViewOfFileEx() that map areas of memory to an already opened physical file through a handle to that file. They have the following parameters:

```
LPVOID MapViewOfFile(// Prototype from Microsoft Visual C++ Help Documentation
  HANDLE hFileMappingObject,        // file-mapping object to map into address space
  DWORD dwDesiredAccess,            // access mode
  DWORD dwFileOffsetHigh,           // high-order 32 bits of file offset
  DWORD dwFileOffsetLow,            // low-order 32 bits of file offset
  DWORD dwNumberOfBytesToMap        // number of bytes to map
 );

LPVOID MapViewOfFileEx(// Prototype from Microsoft Visual C++ Help Documentation
  HANDLE hFileMappingObject,        // file-mapping object to map into address space
  DWORD dwDesiredAccess,            // access mode
  DWORD dwFileOffsetHigh,           // high-order 32 bits of file offset
  DWORD dwFileOffsetLow,            // low-order 32 bits of file offset
  DWORD dwNumberOfBytesToMap,       // number of bytes to map
  LPVOID lpBaseAddress              // suggested starting address for mapped view
 );
```

All of the foregoing functions directly use a pointer to a string that is a physical file. The only file functions that do not directly use a physical filename are functions like CreateNamedPipe(), which has the following parameters:

```
HANDLE CreateNamedPipe(// Prototype from Microsoft Visual C++ Help Documentation
  LPCTSTR lpName,                          // pointer to pipe name
  DWORD dwOpenMode,                        // pipe open mode
  DWORD dwPipeMode,                        // pipe-specific modes
  DWORD nMaxInstances,                     // maximum number of instances
  DWORD nOutBufferSize,                    // output buffer size, in bytes
  DWORD nInBufferSize,                     // input buffer size, in bytes
  DWORD nDefaultTimeOut,                   // time-out time, in milliseconds
  LPSECURITY_ATTRIBUTES lpSecurityAttributes  // pointer to security attributes structure
 );
```

The string to which CreateNamedPipe() points using the first parameter is a string that both an existing executable and the operating system know about and does not exist physically. Unfortunately both of the executables that "know" this private name could only be loaded using one of the other procedures that required a physical file. Currently it is not possible to load an executable using a "named pipe" name. Both of or any executables that use the name of the "named pipe" already must have been loaded into memory.

All of the foregoing functions require a physical file because all of them use "file mapping" processes. File mapping allows large executable files to appear to be loaded rapidly since they are rarely completely loaded into memory but rather are mapped into memory. The detriment to this mapping capability is that executable code must remain in physical memory in a file in unencrypted form in order to be loaded, unless there is a middle layer or file system driver that the operating system uses as a physical layer and that decrypts the executable code to the operating system on demand. The potential weakness here is that another file system driver can hook into the operating system to monitor traffic between the operating system and all file system drivers and capture decrypted executable code passing from the file system driver to the operating system. Some operating systems allow such monitoring more than others. Many anti-viral software packages use this technique to prevent computer virus attacks.

One method of loading and executing encrypted executable computer program code is to use a stub executable having two parts. The first part is the normal front end loader code that all executables have. In addition, the first part would perform any authorization which may include receiving a password from the user, then allocate enough memory to hold hidden encrypted code when it is decrypted, either in its entirety or a portion of it, copy the encrypted code into that area of protected (and preferably locked so no disk swapping occurs) memory, decrypt it once it is in memory and only in memory, and then have the operating system load the code only from memory therefore bypassing any file system drivers or TSRs so they have access to only encrypted code.

Some of the file functions listed above and similar functions on other operating systems could be modified easily by a programmer having access to source code for those operating systems, or a new operating system may be made to provide functions which allow direct loading of executable code from memory rather than physical files. For example, in the Win32 commands, a command similar to CreateProcess() command could be provided. The command should have a few extra parameters including the process identifier of the process that contains

the now decrypted executable code, the memory address of the start of the decrypted code, and the size of the decrypted code. The command could also contain a parameter specifying a "call back" function within the first process that would provide decrypted code on demand directly to the operating system through a protected buffer, therefore allowing only a portion of the encrypted code to be decrypted at any one time instead of in its entirety, for better protection and less memory use. The second parameter of the LoadLibraryEx() command that now needs to be NULL could be expanded to hold a structure that contained the same information. Both of these and other similar functions could be changed or created to allow loading executable code either as an .exe, .dll, or other extensions or identifiers, such as by using a "named pipe" name that only the operating system and process that holds decrypted code know about and having the operating system load from the named pipe.

Alternatively, without having such additional capabilities in the operating system, an application program can be divided into two parts. The first part is code that is common to all applications such as code for allocating memory off the heap and code that provides some interaction with the user. This kind of code is generally not code that the content provider is concerned about copying. The second part is the code that the content provider believes is valuable. Typically this valuable code is a business logic code or what would be considered a middle tier of a three-tier environment. A content provider would like to protect this second part of the code, at least much more that the first part of the code. The content provider would place all of the important code to be protected inside a dynamic link library and the code that is not that important would reside in the front end "stub" executable. Both of these would be combined into another executable containing the .dll in encrypted form only, along with any other files, data, information, and/or tables for holding, for example, hardware identifiers. This other executable is the final digital information product.

The first part of the digital information product, i.e., the executable stub, would load and execute normally like any other application. It then would perform any authorization procedures. Once the proper authorization or password was completed successfully, an unwrap procedure would be performed as will now be described in connection with Fig. 8, it would then allocate enough protected memory using a function like VirtualAlloc() as shown in step 150:

```
DWORD nFileSize = 0;
DWORD nPhantomFileSize = 0;
```

```
DWORD exeOffset = 0;
DWORD nPreferredLoadAddress = GetPreCompiledLoadAddress();
CString cCommandFile = UnwrapGetNTCommandFile();
exeOffset = UnwrapGetDllOffset(cCommandFile);
nFileSize = UnwrapGetDllSize(cCommandFile);
nPhantomFileSize = nFileSize + 0x3000; // add any needed extra space
// Increase buffer size to account for page size (currently Intel page size).
DWORD nPageSize = GetPageSize();
nPhantomFileSize += (nPageSize -(nPhantomFileSize % nPageSize));
// Allocate the memory to hold the decrypted executable.
LPVOID lpvBlock = VirtualAlloc((LPVOID) nPreferredLoadAddress,
                    nPhantomFileSize,
                        MEM_RESERVE | MEM_COMMIT, PAGE_READWRITE);
```

This function can request a particular address space. Preferably, this address space is the preferred load address space to which the .dll was linked in order to minimize any needed relocation and fix up code. The stub executable may lock that area of memory in step 152, for example by using VirtualLock() to prevent any memory writes to a swap file, depending on the operating system, as shown below:

```
BOOL bVLock = VirtualLock((LPVOID) nPreferredLoadAddress, nPhantomFileSize);
```

The memory area still should be secure even without this preventive step since the Windows 95 and NT operating systems do not allow any user access to swap files.

The encrypted code is then copied from the digital information product into the allocated protected memory in step 154, for example by using the following command:

```
UnwrapCopyHiddenExeToMem(cCommandFile, exeOffset, nFileSize, (char *) lpvBlock);
```

Once in memory, the stub would then decrypt the code to that same portion of memory in step 156, for example by using the following commands:

```
CwrapDecryptSeed(cPassword.GetBuffer(0), cPassword.GetLength());
CwrapDecrypt((unsigned char *) lpvBlock, 0, nFileSize);
```

Any "fix up and relocation" type services would then be performed in step 158, for example by using the following command:

```
UnwrapFixUpAndRelocateDll(lpvBlock);
```

Possibly, the memory protection may be changed to execute only in step 160, for example by using the VirtualProtect() command as follows:

```
DWORD lpflOldProtect; // variable to get old protection
BOOL bVProtect = VirtualProtect((LPVOID) nPreferredLoadAddress,
                                nPhantomFileSize,
                                PAGE_EXECUTE,
                                &lpflOldProtect);
```

Function calls then can be made into that area of memory that now contains the decrypted code:

```
UnwrapDoDllAlgorithms();
```

Some of the "fix up" operations to be performed above include placing the addresses of external or stub.exe functions into the address place holders of the decrypted .dll or internal code, by using commands similar to the following:

```
WriteAddress((char*) 0x0a406104, (DWORD) &CallBackFunction1);
WriteAddress((char*) 0x0a406100, (DWORD) &CallBackFunction2);
```

For instance a wrapper function could be created in the outer stub.exe that received a size parameter, allocated that amount of memory off of the heap, and passed back the starting address of that block of memory. Another example would be to have encrypted algorithms within the hidden, encrypted .dll which would be called at run time from the front end stub once decrypted

within protected memory. The dynamic link library would be compiled and linked to expect a pointer to a function that took that parameter and/or returned a value by including prototypes in the header file as follows:

```
void (*lpCallBackFunc1)();
void (*lpCallBackFunc2)(unsigned long);
```

Function calls to "external" functions also could be added as follows:

```
(*lpCallBackFunc1)();
unsigned long z = x * x;
(*lpCallBackFunc2)(z);
```

At run time the "fix up" code would take the run time address of that "wrapper function" and place it into the pointer address within the .dll block of code as follows:

```
WriteAddress((char*) 0x0a406104, (DWORD) &CallBackFunction1);
WriteAddress((char*) 0x0a406100, (DWORD) &CallBackFunction2);
```

This information is readily available using the .cod output files from the compiler, an example of which follows:

```
_TestSum PROC NEAR                                          ; COMDAT
; Line 8
 00000    56          push   esi
; Line 23
 00001    ff 15 00 00 00
          00          call   DWORD PTR_lpCallBackFunc1
; Line 24
 00007    8b 44 24 08 mov    eax, DWORD PTR_a$[esp]
 0000b    50          push   eax
 0000c e8 00 00 00 00 call   _TestSquare
```

```
00011      83 c4 04       add    esp, 4
00014      8b f0          mov    esi, eax
; Line 25
00016      8b 44 24 0c    mov    eax, DWORD PTR _b$[esp]
0001a      50             push   eax
0001b      e8 00 00 00 00 call   _TestSquare
00020      83 c4 04       add    esp, 4
00023      03 c6          add    eax, esi
; Line 28
00025      5e             pop    esi
00026      c3             ret    0
_TestSum ENDP
_TEXT      ENDS
;      COMDAT_TestSquare
_TEXT      SEGMENT
_x$ = 8
_TestSquare PROC NEAR                                    ; COMDAT
; Line 30
00000      56             push   esi
; Line 32
00001      8b 74 24 08    mov    esi, DWORD PTR _x$[esp]
00005      0f af f6       imul   esi, esi
; Line 34
00008      56             push   esi
00009      ff 15 00 00 00
           00             call   DWORD PTR _lpCallBackFunc2
0000f 83 c4 04            add    esp, 4
00012      8b c6          mov    eax, esi
; Line 36
00014      5e             pop    esi
00015      c3             ret    0
_TestSquare ENDP
```

Such information also is available from .map output files from the linker where the "f" between the address (i.e., 0a406100) and the object file (i.e. Algorithms.obj) means it is a "flat" address (i.e., hard coded by the linker) and the lack of an "f" means that it is an address pointer to be supplied at run time (load time) where the address that is contained in that address location is used and not the actual address location (i.e., the address that is contained at address location 0a406100 and not 0a406100 itself):

```
0001:00000000   _TestSum            0a401000 f Algorithms.obj
0001:00000030   _TestSquare         0a401030 f Algorithms.obj

0003:00001100   _lpCallBackFunc2    0a406100   Algorithms.obj
0003:00001104   _lpCallBackFunc1    0a406104   Algorithms.obj
```

When the code inside the .dll makes a "call" to a dereferenced pointer, it would jump to the correct function in the outer code and return the expected return value (if any). For example:

```
void CallBackFunction1(){
// This is the first function that exists in the Stub executable
// whose address has been placed at the appropriate location inside the "dll" code
// that has now been decrypted in a block of memory. The code inside the "dll"
// makes a function call to this function. In its encrypted state, the "dll" does not contain
// this address, but merely has a placeholder for the address. The “dll” has enough space
allocated to hold an
// address of this size. After the “dll” has been decrypted at run time, its address is
// placed in that location so the code inside the "dll" that references (or more
// appropriately dereferences) that address can jump (which is function call) to this
// address.
AfxMessageBox(
_T("This is the FIRST Stub.exe call back function being called from the dll."));
        return;
}
```

```
void CallBackFunction2(DWORD nNumber){
// See comment for CallBackFunction1 except this function receives a parameter off
// of the stack.  It could also return a value as well.
        CString
        cString(
T("This is the SECOND Stub.exe call back function being called from the dll"));

        har buffer[20];
        ltoa(nNumber, buffer, 10);

        cString += _T(" with a parameter of ");
        cString += buffer;
        cString += _T(".");
        AfxMessageBox(cString.GetBuffer(0));
        return;
}
```

The outer stub.exe would make the same kinds of jumps or function calls into the now protected decrypted code block as follows:

```
DWORD c;

// This command declares a function pointer.  This command is different for different function
// calls.  Here the called function takes two integer parameters and
// passes back a DWORD.
DWORD (*lpFunc)(DWORD,DWORD);

// The function pointer is then pointed to the starting address of the function in the
// block of memory that now holds the decrypted DLL.
lpFunc = (DWORD (*)(DWORD,DWORD)) UnwrapFixUpAndRelocateDll();

// Now call that "function" which is really like all function calls, i.e., a jump to
```

```
// the address where that function exists.  In this case, two
// variables are passed to that function and returning a value from that function.  This function
illustrates that the function call
// can be more complicated than merely a simple jump
// to an address.  Inline assembler code may be used to push the variables onto
// the stack frame and return the variable from the eax register, but this function enables
// the C++ compiler to do the same function.
c = (DWORD) (*lpFunc)(a, b);
```

This mechanism requires the unwrap procedure and the now decrypted code to have intimate knowledge about procedural interfaces of each other but no knowledge about each other's implementation. This is the way most executable .exe files and .dll files behave but with the addition of a series of "wrapper" functions on either side for communication. This method works under Windows 95 and Windows NT 4.0 operating systems and should work under Windows NT 3.51 and other operating systems.

Another modified version of this mechanism that works under the Windows NT 4.0 operating system because of functions specific to Windows NT 4.0 would be to have another hidden and/or encrypted executable within the digital information product. This executable would be copied to a physical disk in an unencrypted form, launched or loaded with the CreateProcess() command in its current form but called with a parameter to load the executable in suspended mode:

```
BOOL success = CreateProcess(cFrontEndExe.GetBuffer(0), 0, 0, 0, TRUE,
                    CREATE_NEW_CONSOLE | CREATE_SUSPENDED,
                0, 0, &startUpInfo, &processInfo);
```

Then the first process would copy the encrypted dll into its own process and decrypt it, allocate enough memory using VirtualAllocEx() in its current form in the second process that has just loaded the expendable front end executable in a suspended state as follows:

```
LPVOID lpvBlockEx = VirtualAllocEx(processInfo.hProcess,
```

```
(LPVOID) nPreferredLoadAddress, nPhantomFileSize,
MEM_RESERVE | MEM_COMMIT,
PAGE_READWRITE);
```

The decrypted code is copied from the first process to the second suspended process using WriteProcessMemory() in its current form:

```
BOOL bWriteProcessMemory = WriteProcessMemory((HANDLE) processInfo.hProcess,
(LPVOID) lpvBlockEx, (LPVOID) nPreferredAddress,
(DWORD) nPhantomFileSize, (LPDWORD) &nBytesWritten);
```

The primary thread of the previously launched second process is then resumed:

```
DWORD nResumed = ResumeThread(processInfo.hThread);
```

Any necessary function pointers are then placed in the correct locations by the second process, the area of memory is locked to prevent any writes to a swap file, and the memory protection is changed to execute only as follows:

```
WriteAddress((char*) 0x0a406104, (DWORD) &CallBackFunction1);
WriteAddress((char*) 0x0a406100, (DWORD) &CallBackFunction2);

BOOL bVLock = VirtualLock((LPVOID) nPreferredLoadAddress, nPhantomFileSize);
DWORD lpflOldProtect; // variable to get old protection
BOOL bVProtect = VirtualProtect((LPVOID) nPreferredLoadAddress,
nPhantomFileSize, PAGE_EXECUTE, &lpflOldProtect);
```

The program can continue running by making and receiving calls to and from the decrypted dynamic link library that now resides in the protected memory of its process using commands such as the following:

```
DWORD c;
```

```
DWORD (*lpFunc)(DWORD,DWORD);
lpFunc = (DWORD (*)(DWORD,DWORD)) ExpendableGetEntryAddress();
c = (DWORD) (*lpFunc)(a, b);
```

The first process can either close down or launch another instance of that same process.

In either of these implementations using the same process or launching into a second process, the hidden encrypted code never passes through a file system driver or memory resident program in decrypted form. Code can be split up among different dynamic link libraries so that no two would reside in memory at the same time in order to protect code further. Both of these systems can be implemented using the Win32 function calls. If additional functions, similar to a CreateProcess() command or a LoadLibrary() command but that take a process identifier and address location in memory to load in an executable instead of a physical file, are provided in an operating system then the entire executable and dynamic link library can be hidden, encrypted, and protected on the physical disk and then decrypted within protected memory and use the operating system loader to load it directly to the operating system from memory without residing in decrypted form on any physical medium.

Having described the operation and use of the computer program product in accordance with the invention, embodiments of which are described above in connection with Figs. 3-8, and the operation of the unwrap procedure and device driver it contains, the process of constructing such a computer program product will now be described in more detail. Referring now to Fig. 9, an embodiment of this process for creating a computer program product is shown. This process can be applied to any digital information including an arbitrary executable computer program, dynamic link libraries and related files of data. All digital information is treated as mere data by this process. Each separate data file is combined into a single file by this process, with an executable program for performing the unwrap procedure, and optionally executable program code for a virtual device driver, into the computer program product. Each file of hidden information has a unique location and is identified by its own begin and end markers as shown in Fig. 3. The first step of this process is opening a new data file for the computer program using a name that will be used to indicate an executable file (step 200). For example, an executable word processing program may be named "word_processor.exe" in the Windows95 operating system.

The three portions of the computer program product are then inserted into the open data file. First, the unwrap procedure is inserted at the beginning of the file in an executable format in step 202. The begin tag for the optional device driver is then inserted in step 204. The executable device driver program code is then inserted in step 206, followed by its corresponding end tag in step 208. For each hidden file to be inserted into this computer program product, steps 210 to 216 are performed. First, the begin tag is inserted in step 210. The begin tag also may include an indication of a unique name of the file which will be used as its name in the phantom directory created by the unwrap procedure. The hidden file is then encrypted and/or compressed in step 212 and inserted into the data file in step 214. The end tag for the hidden file is then inserted in step 216. The device driver and all of the tags may be encrypted also if the unwrap procedure has suitable decryption procedures. The computer program file is closed when the last hidden file is processed.

Using the present invention digital information, such as executable program code or various kinds of data, is loaded and unloaded as needed, and thus does not take up any more memory than is necessary. At no time does unencrypted digital information, such as computer program code, exist on disk in accessible and complete decrypted form. Because the original digital information is available as a read only file in one embodiment of the invention accessible only to the device driver, the digital information may be accessed over networks, from a CD-ROM or from a DVD, and can be made to have a limited number of uses. This mechanism is particularly useful for controlling distribution of computer programs, digitized movies or other information while reducing the cost of such distribution and control. For example, software may be distributed over a network on a single use basis, and charges may be levied on a per use basis. The ability to reverse engineer an application program also may be reduced.

One benefit with this system over some other systems for preventing unauthorized access to digital information is that the content provider maintains control of the encryption applied to the information how it may be decrypted. Any need for either a centralized facility or a predetermined decryption program is eliminated. An operating systems manufacturer or other platform vendor merely provides the capability for the information to be accessed and decrypted on the fly. Since the valuable information and any other tables of authorization codes, passwords, or hardware identifiers that the content provider may use to secure the information resides in one large encrypted file, it becomes difficult, if not impossible, for someone to determine just where any of this information exists.

A potential scenario with authorization procedure in which the present invention may be used is the following. A consumer purchases a DVD disk containing a movie. The user puts the disk into the player. This is the first time the disk is installed. The content provider's functions are loaded into the DVD chip, which looks in the encrypted table and sees that this is the first time this disk is being played. The player then displays on a screen a numeric identifier and toll free phone number. The consumer calls the toll free phone number and inputs the numeric identifier that was displayed on the screen. The content provider provides a numeric password based on the numeric identifier that the user inputs into the DVD. The content provider may develop a database of information about its consumers that also may be used to detect pirating of the digital information product. Now that this authorization has taken place, the software that the content provider wrote, and is now in the DVD chip, takes a hardware identifier from the DVD and encrypts it and puts it in the encrypted and buried table on the disk. Alteratively, the data may be decrypted in memory and re-encrypted back onto the disk using the hardware identifier as part of a key. Now that disk will run and show the movie and will only run on that DVD and no other. The content provider could allow for a table of hardware id's so they could limit the number of DVD's that disk would run on or a limited number of times it can be shown. It should be understood that many other authorization procedures may be used.

In the foregoing scenario, the movie is encrypted on the same disk inside of the encrypted file that contains the table and functions the content provider distributed. The movie is decrypted by the decryption functions contained in the file directly to the DVD chip. At no time does the movie reside anywhere in decrypted form. The content provider can protect the movie with any desired level of security (for both encryption and authorization).

In the present invention, the onus of protection of content does not reside with a hardware manufacturer or platform provider but in the hands of the content provider. The hardware manufacturer only provides the mechanism to protect the digital information through the operating system. The technique and implementation of protection resides in the hands of the content provider. This mechanism allows the content providers to change the level of security as needed without any modifications to the hardware. The security of the content is provided by the encryption/decryption algorithms, public/private keys, and authorization methods which are determined by the content provider. Even each individual product can have its own encryption/decryption algorithms and/or public/private keys. All of these can be changed and enhanced as the market demands.

The present invention also could be used for on-line or live use of digital information. For example, a movie could be retrieved on demand and recorded by a consumer. A set top box could receive the digital information, decrypt it, and then re-encrypt and store the information using, for example, a hardware identifier of the set top box. Since home movies digitally recorded would be encrypted using the hardware identifier of the device used in recording, that home movie could not be played on another or only on a limited number of other devices and/or for only a specified number of times depending on the wishes of the content provider. Since the algorithms are downloaded at the time of recording from a service provider, e.g., the cable company, the content provider (movie company) would provide the encrypted data to the service provider to present to their customers. The service provider need not be concerned with the encryption/decryption and authorization functions used by the content provider. Similar uses are possible with other data transmission systems including, but not limited to, telephone, cellular communications, audio transmission including communication and the like.

In another embodiment, the stub executable program is a first process that is implemented similar to a debugging tool such as the SoftIce debugger from NuMega Technologies or the WinDebug debugger from Microsoft Corporation for Ring 0 kernel level debugging for an Intel processor based architecture, or the CodeView debugger for ring 3 application level debugging. Such a debugger controls execution of a program to be debugged as a second process and steps through each program statement or opcode of the debugged program. The debugging tool could be modified to monitor each opcode that indicates a jump to a program fragment, such as each instruction or a block code. If the program fragment to be executed is not decrypted, the modified debugger decrypts the program fragment before the jump command is allowed to execute. Each program fragment may be re-encrypted after execution. Clearly, unnecessary debugging commands may be omitted from the modified debugger.

Having now described a few embodiments of the invention, it should be apparent to those skilled in the art that the foregoing is merely illustrative and not limiting, having been presented by way of example only. Numerous modifications and other embodiments are within the scope of one of ordinary skill in the art and are contemplated as falling within the scope of the invention as defined by the appended claims and equivalent thereto.

CLAIMS

1. A computer-implemented process for executing encrypted computer program logic while maintaining protection against copying of corresponding decrypted executable computer program logic, wherein the encrypted computer program logic is stored in association with first executable computer program logic, the process comprising the steps of:

through an operating system of a computer, reading, loading and executing the first executable computer program logic as a first process having a protected memory area defined by the operating system;

the first process decrypting the encrypted computer program logic into second executable computer program logic and storing the second executable computer program logic in the protected memory area; and

the first process causing loading and execution of the decrypted second computer program logic in the protected memory area.

2. The process of claim 1, wherein the encrypted computer program logic and the first executable computer program logic are stored in a single data file accessible through the operating system.

3. The process of claim 1, wherein the execution of the decrypted second computer program logic is performed as a second process having a second protected memory area defined by the operating system.

4. A digital information product including a computer readable medium having digital information stored thereon, the digital information including computer program logic defining first executable computer program logic, wherein the first executable computer program logic when executed performs the following steps:

storing the encrypted computer program logic in a data file accessible through an operating system of a computer, wherein the data file also includes first executable computer program logic;

through the operating system, reading, loading and executing the first executable computer program logic from the data file as a first process having a protected memory area;

the first process decrypting the encrypted computer program logic into second executable computer program logic and storing the second executable computer program logic in the protected memory area; and

the first process causing loading and execution of the decrypted second computer program logic in the protected memory area.

5. A computer system comprising:

a processor for executing computer program logic;

a main memory operatively connected to the processor for storing digital information including executable computer program logic at memory locations addressed by the processor; and

an operating system defined by executable computer program logic stored in the memory and executed by the processor and having a command which when executed by the processor defines means for creating a process in response to a request specifying a process identifier and a memory location in the main memory, wherein the process identifier indicates the process making the request and the memory location stores executable computer program logic which when executed defines the process.

6. A computer system having an operating system, for decrypting digital information, comprising:

means for storing the encrypted computer program logic in a data file accessible through the operating system, wherein the data file also includes first executable computer program logic;

means, invokable through the operating system, for reading, loading and executing the first executable computer program logic from the data file as a first process having a protected memory area;

the first process defining means for decrypting the encrypted computer program logic into second executable computer program logic and storing the second executable computer program logic in the protected memory area; and

the first process defining means for causing loading and execution of the decrypted second computer program logic in the protected memory area.

7. The computer system of claim 6, wherein the encrypted computer program logic and the first executable computer program logic are stored in a single data file accessible through the operating system.

8. The computer system of claim 6, wherein the execution of the decrypted second computer program logic is performed as a second process having a second protected memory area defined by the operating system.

9. A digital information product, including a computer readable medium with computer readable information stored thereon, wherein the computer readable information comprises:

a first portion of executable computer program logic; and

a second portion of encrypted digital information; and

wherein the first portion of executable program logic, when executed, defines means, operative in response to requests for digital information, for accessing the second portion of encrypted digital information, for decrypting the encrypted digital information, and for outputting the decrypted digital information.

10. The digital information product of claim 9, wherein the encrypted digital information is encrypted executable computer program logic.

11. A computer program product including a self-decrypting encrypted executable computer program, comprising:

a computer readable medium having computer program logic stored thereon, wherein the computer program logic defines:

a first module,

a second module,

wherein the first module, when executed by a computer, defines means for loading the second module into memory of the computer, and

a third module defining the encrypted executable computer program,

wherein the second module, when executed by a computer, defines means for communicating with an operating system of the computer to receive requests for program code from the encrypted executable computer program from the third module, and for processing the

requests to access and decrypt the encrypted executable computer program and for providing the decrypted executable code from the third module to the operating system.

12. A process for executing encrypted executable computer programs on a computer system having a processor, memory and operating system, comprising the steps of:

receiving computer program logic having a first module defining a start up routine, a second module, and a third module containing the encrypted executable computer program;

executing the first module of the received computer program logic using the processor,

wherein the step of executing causes the second module to be loaded into the memory of the computer system, and

generating requests from the operating system for data from the encrypted executable computer program which are received by the second module, and

accessing and decrypting the encrypted executable computer program and returning the decrypted executable computer program to the operating system.

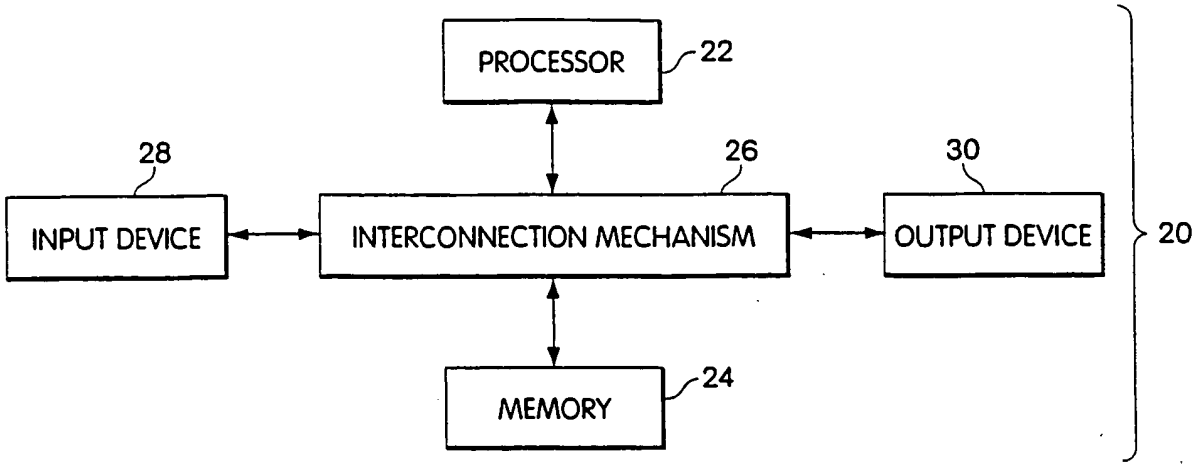


Fig. 1

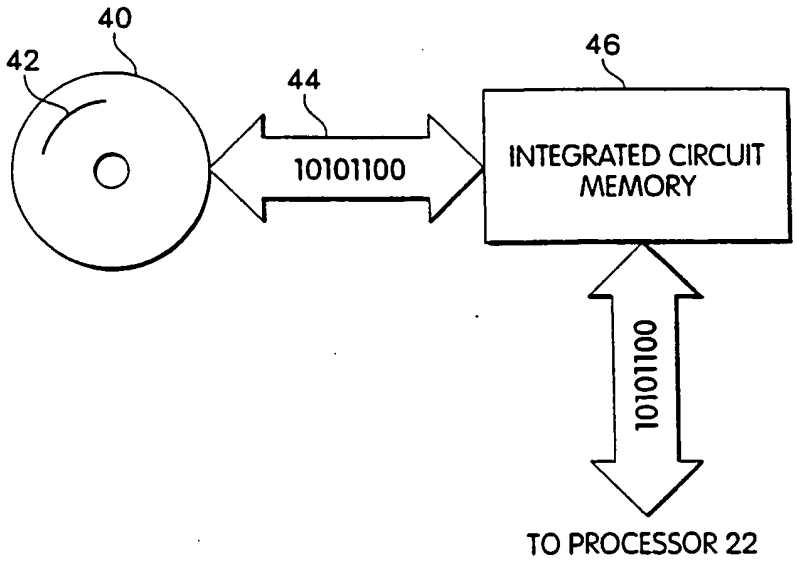


Fig. 2

BNSDOCID: <WO__9811690A1_IA>

Petitioner Apple Inc. - Exhibit 1012, p. 1656

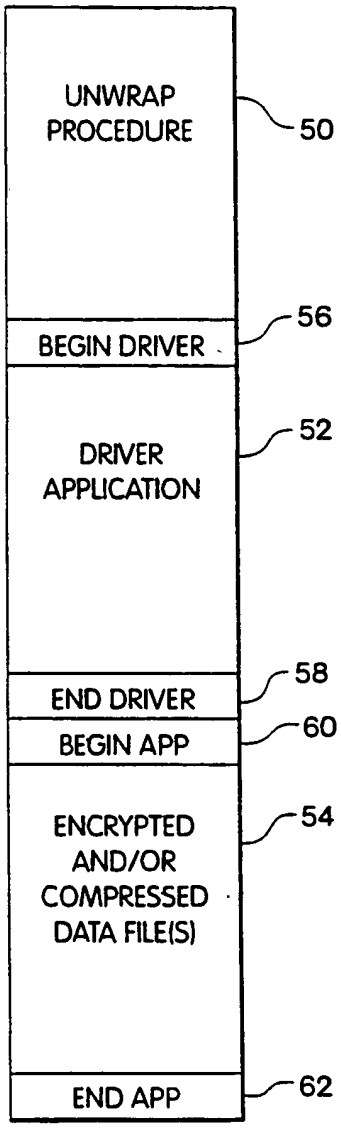


Fig. 3

BNSDOCID: <WO___9811690A1_IA>

Petitioner Apple Inc. - Exhibit 1012, p. 1657

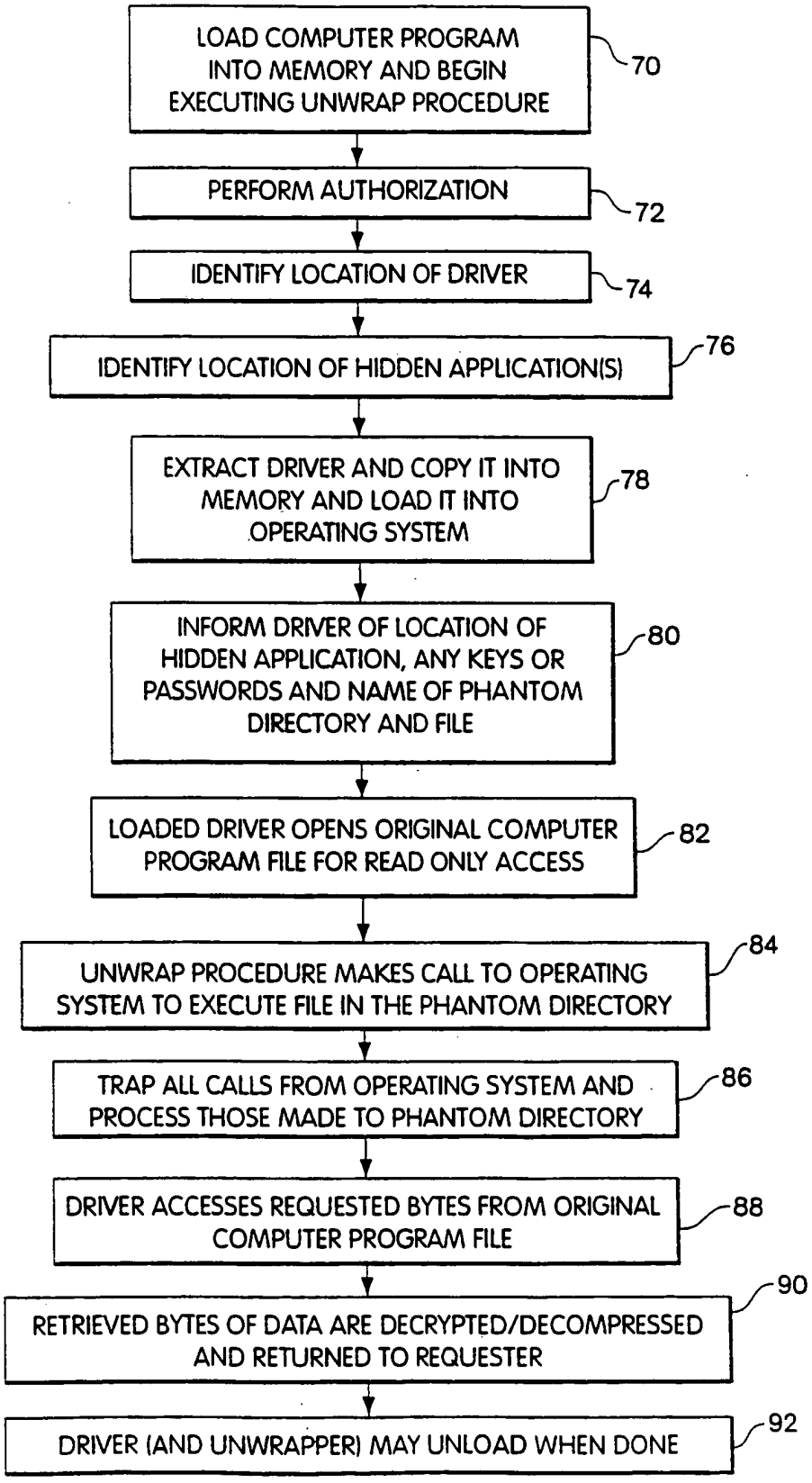


Fig.4

BNSDOCID: <WO___9811690A1_IA>

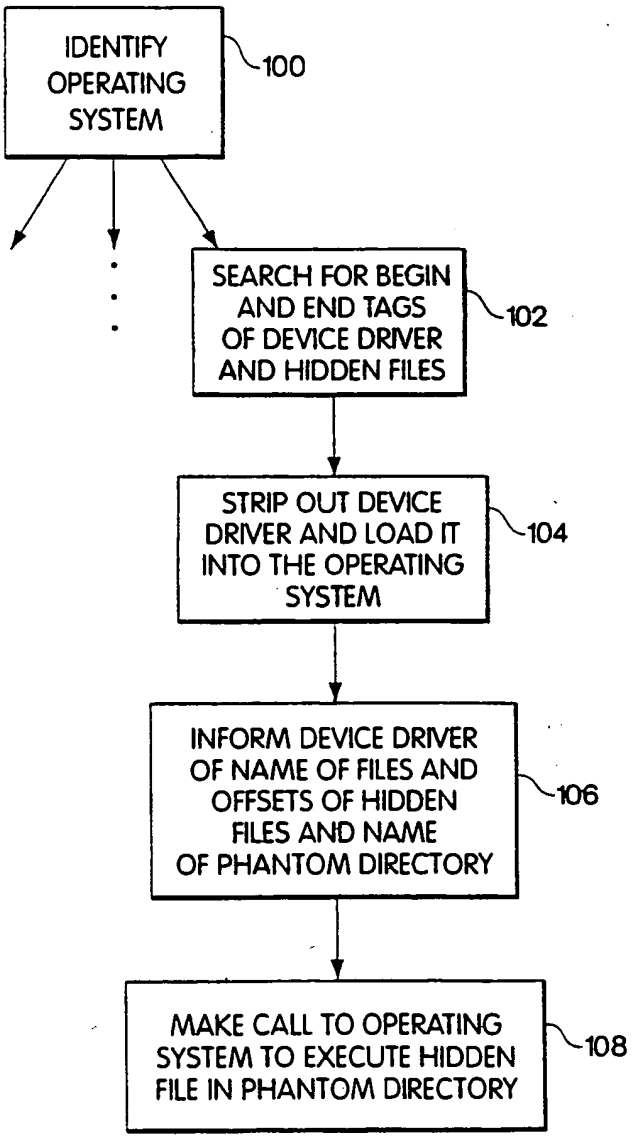


Fig. 5

BNSDOCID: <WO___9811690A1_IA>

Petitioner Apple Inc. - Exhibit 1012, p. 1659

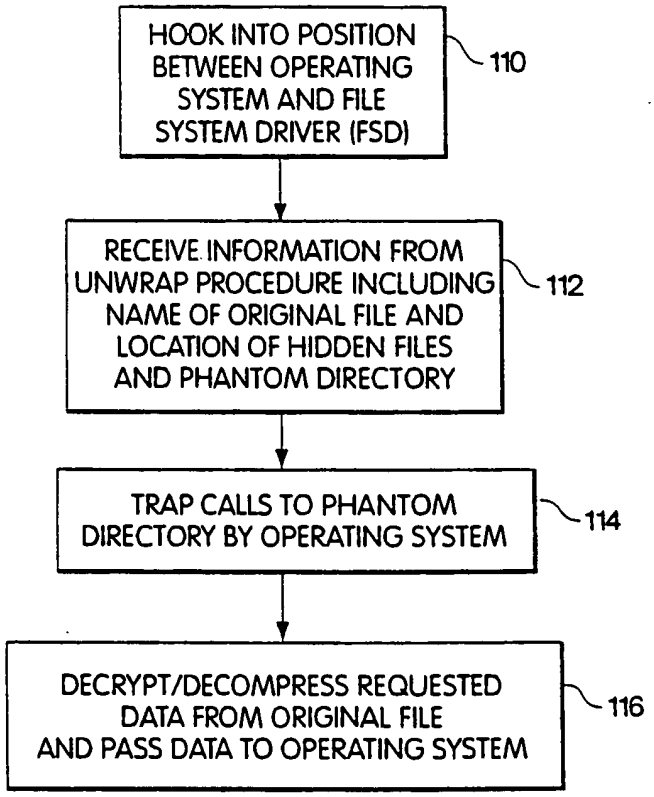


Fig. 6

BNSDOCID: <WO___9811690A1_IA>

Petitioner Apple Inc. - Exhibit 1012, p. 1660

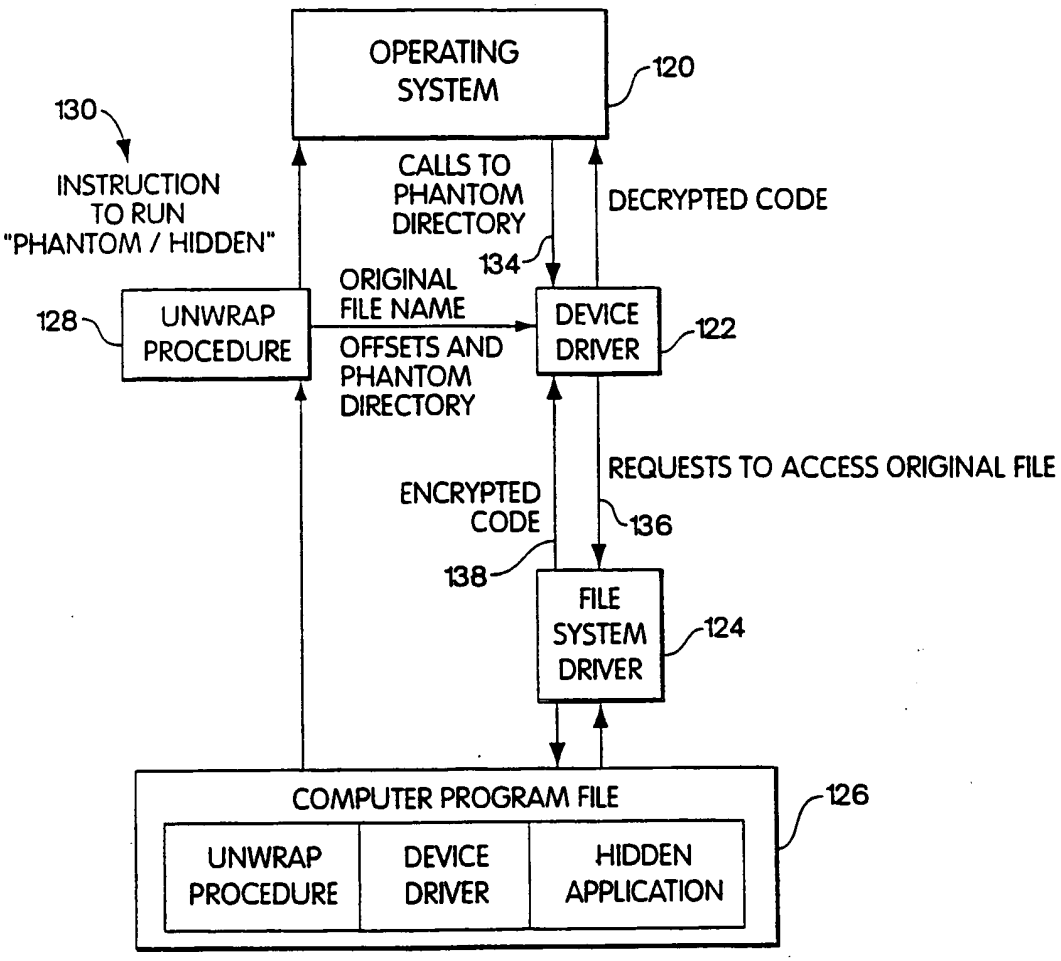


Fig. 7

BNSDOCID: <WO___9811690A1_IA>

Petitioner Apple Inc. - Exhibit 1012, p. 1661

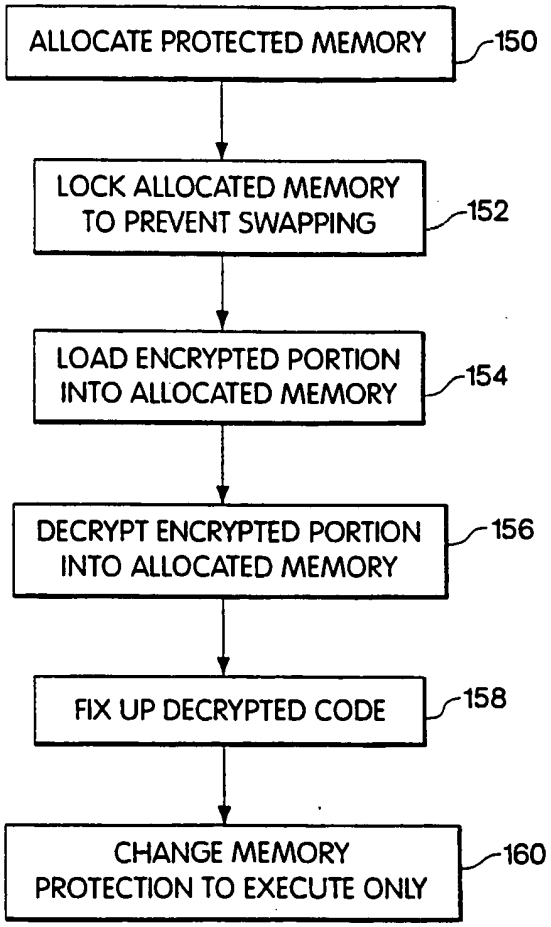


Fig. 8

BNSDOCID: <WO___9811690A1_IA>

Petitioner Apple Inc. - Exhibit 1012, p. 1662

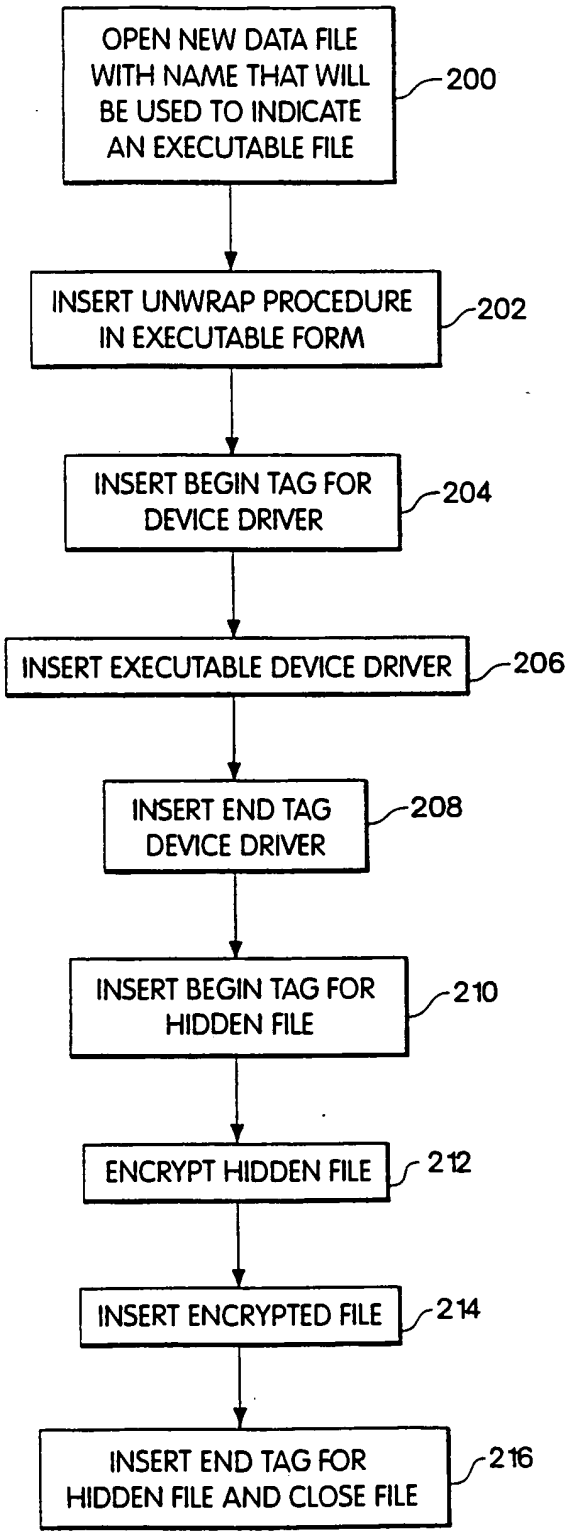


Fig. 9

BNSDOCID: <WO___9811690A1_IA>

Petitioner Apple Inc. - Exhibit 1012, p. 1663

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/16223

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/00
US CL : 380/4
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/4,9,23,25,49,50,59

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 4,937,861 A (CUMMINS) 26 June 1990, see Abstract.	1-12
A	US 5,007,082 A (CUMMINS) 09 April 1991, see Abstract.	1-12
A	US 5,144,659 A (JONES) 01 September 1992, see Abstract.	1-12
A	US 5,155,827 A (GHERING) 13 October 1992, see Abstract.	1-12
A	US 5,396,609 A (SCHMIDT et al) 07 March 1995, see Abstract.	1-12

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 20 JANUARY 1998	Date of mailing of the international search report 18 FEB 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer BERNARR EARL GREGORY Telephone No. (703) 306-4153

Form PCT/ISA/210 (second sheet)(July 1992)*

BNSDOCID: <WO___9811690A1_IA>

EP 715241 A2

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 715 241 A2

(12) EUROPEAN PATENT APPLICATION

(43) Date of publication:
05.06.1996 Bulletin 1996/23

(51) Int. Cl.[6]: **G06F 1/00**

(21) Application number: **95116615.6**

(22) Date of filing: **21.10.1995**

(84) Designated Contracting States:
DE FR GB

(30) Priority: **27.10.1994 JP 264200/94**
02.12.1994 JP 299835/94

(71) Applicant: **MITSUBISHI CORPORATION**
Chiyoda-ku Tokyo 100 (JP)

(72) Inventors:
- **Saito, Makoto**
  Tama-shi, Tokyo (JP)
- **Momiki, Shunichi**
  Higashimur-ayama-shi, Tokyo (JP)

(74) Representative: **Neidl-Stippler & Partner**
Rauchstrasse 2
81679 München (DE)

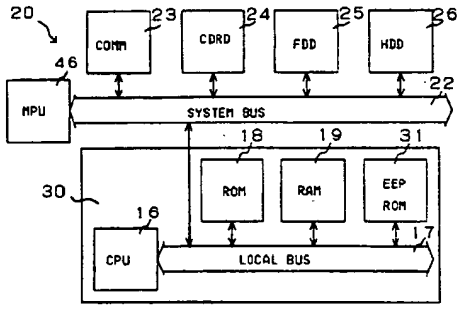
(54) Apparatus for data copyright management system

(57) A data copyright management apparatus is used with a user terminal and comprises a CPU, a CPU bus, ROM, EEPROM, and RAM.

The CPU, ROM, EPROM, and RAM are connected to the CPU bus, and a system bus of a device which utilizes the data can be connected to the CPU bus. A data copyright management system program, crypt algorithm, and user information are stored in the ROM, and a second private-key, a permit key, a second secret-key, and copyright information are stored in the EEPROM. A first public-key, a first private-key, a second public-key, and a first secret-key are transmitted to the RAM during the operation. The data copyright management apparatus may be configured in the form of a monolithic or hybrid IC, a thin IC card, PC card, and insertion board which have a unique terminal. If a copyright management program is supplied from the external, the it is stored in the EEPROM, otherwise it is stored in the ROM.

In addition to a microprocessor of user terminal which decrypts encrypted data for displaying and processing and re-encrypts the decrypted data for storing, copying, or transferring, at least one microprocessor, desirably two microprocessors, are added for decrypting and re-encrypting data which is encrypted and supplied. The microprocessors to be added may be connected to a system bus of the microprocessor of the user terminal, it is desirable that a multiprocessor configuration is implemented by using a SCSI bus, PCI bus, or SCI bus. Apparatus for decryption and re-encryption may be configured separately or as a unit. Device which is used to input and output encrypted data may be connected directly to the apparatus for decryption and re-encryption. The data copyright management apparatus may be implemented in the form of a monolithic IC, a hybrid IC, or a built-in subboard, and the apparatus in these forms is incorporated in a computer, television set, set-top box, digital video tape recorder, digital video disk recorder, digital audio tape apparatus, or personal digital assistants, and the like.

Fig. 3



Printed by Rank Xerox (UK) Business Services
2.11.9/3.4

BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1665

Description

Field of the Invention

The present invention relates to an apparatus for displaying, storing, copying, editing or transmitting digital data in using data, and intends to protect digital data copyrights.

Background of the Invention

In information-oriented society of today, a database system has been spread in which various data values having independently been stored in each computer so far are mutually used by connecting computers by communication lines.

The information having been handled by the database system is classical type coded information which can be processed by a computer and has a small amount of information or monochrome binary data like facsimile data at most. Therefore, the database system has not been able to handle data with an extremely large amount of information such as a natural picture and a motion picture.

However, while the digital processing technique for various electric signals develops, development of the digital processing art for a picture signal other than binary data having been handled only as an analog signal is progressed.

By digitizing the above picture signal, a picture signal such as a television signal can be handled by a computer. Therefore, a "multimedia system" for handling various data handled by a computer and picture data obtained by digitizing a picture signal at the same time is noticed as a future technique.

Because picture data includes an overwhelmingly large amount of information compared to character data and audio data, it is difficult to directly store or transmit the picture data or apply various processings to the picture data by a computer.

Therefore, it has been considered to compress or expand the picture data and several standards for compressing or expanding picture data have been prepared. Among those standards, the following standards have been prepared so far as common standards: JPEG (Joint Photographic image coding Experts Group) standard for a still picture, H.261 standard for a video conference MPEG1 (Moving Picture image coding Experts Group 1) standard for storing pictures, and MPEG2 corresponding to the present telecast and tire high-definition telecast.

Real-time processing of digital picture data has been realized by these techniques.

Because hitherto widely-spread analog data is deteriorated in quality whenever storing, copying, editing, or transmitting it, copyrights produced due to the above operation has not been a large problem. However, because digital data is not deteriorated in quality after repeatedly storing, copying, editing, or transmitting it, the control of copyrights produced due to the above operation is a large problem.

Because there is not hitherto any exact method for dealing with a copyright for digital data, the copyright is handled by the Copyright Act or relevant contracts. Even in the Copyright Act, compensation money for a digital-type sound- or picture-recorder is only systematized.

Use of a database includes not only referring to the contents of the database but also normally effectively using the database by storing, copying, or editing obtained data. Moreover, it is possible to transmit edited data to another person via on-line by a communication line or a proper recording medium.

Furthermore, it is possible to transmit the edited data to the database to enter it as new data.

In an existing database system, only character data is handled. In a multimedia system, however, audio data and picture data which are originally analog data are digitized and formed into a database in addition to the data such as characters which have been formed into a database so far.

Under the above situation, how to deal with a copyright of data formed into a database is a large problem. However, there has not been adequate copyright management means for solving the problem so far, particularly copyright management means completed for secondary utilization of the data such as copying, editing, or transmitting of the data.

Although data of "Software with advertisement" or "free software" is, generally, available free of fee, it is copyrighted and its use may be restricted by the copyright depending on the way of use.

The inventor of the present invention et al. proposed a system for managing a copyright by obtaining a permit key from a key control center via a public telephone line through Japanese Patent Laid-Open No. 46419/1994 and Japanese Patent Laid-Open No. 141004/1994 and moreover, proposed an apparatus for managing the copyright through Japanese Patent Laid-Open No. 132916/1994.

Furthermore, they proposed a system for managing a copyright of digital data through Japanese Patent Application No. 64889/1994 and Japanese Patent Application No. 237673/1994.

In these systems and apparatus, one who wants to view and listen encrypted programs requests to a control center for viewing by using communication device via a communications line, and the control center sends a permit key to the requester, performs charging and collects a fee.

After receiving the permit key, the requester sends the permit key to a receiver by using an on-line or off-line means, the receiver then decrypts the encrypted programs using the permit key.

Moreover, the system disclosed in Japanese Patent Application No. 64889/1994 uses a program and copyright information for managing the coyright in addition to the permit key so that the copyright in display (including process to sound), storage, copying, editing, or transmit-

BNSDOCID: <EP__0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1666

ting of the digital data in a database system including real-time transmission of a digital picture can be managed. The program for managing the copyright watches and manages to prevent users from using other than the conditions of user's request or permission.

The Japanese Patent Application No. 64889/1994 further discloses that data is supplied with encrypted from a database, decrypted by copyright management program when displayed or edited, and encrypted again when it is stored, copied or transmitted. Also the copyright management program itself being encrypted; decrypted by a permit key; the copyright management program thus decrypted performing encyption and decryption of copyright data; and when data is utilizedother than storage and displaying, copyright information including information of the person who has utilized, being stored as history in addition to original copyright information, are disclosed.

Though the present invention is described below, general description is made for cryptography at first.

The cryptography includes a secret-key cryptosystem and a public-key cryptosystem.

The secret-key cryptosystem is a cryptosystem using the same crypt key for encryption and decryption. While this cryptosystem requires only a short time for encryption or decryption, the secret-key is found, and thus, the cryption may be cryptanalized.

The public-key cryptosystem is a cryptosystem in which a key for encryption is open to the public as a public-key and a key for decryption is not open to the public. The key for encryption is referred to as a public-key and the key for decryption is referred to as a private-key. To use this cryptosystem, it is necessary that a party for transmitting information encrypts the information with a public-key of a party for receiving the information and the party for receiving the information decrypts the information with a private-key not open to the public. While this cryptosystem requires relatively a long time for encryption or decryption, the private-key can hardly be found and it is very difficult to cryptanalyze the cryption.

In the cryptography, a case of encrypting a plaintext M with a crypt key K to obtain a cryptogram C is expressed as

$$C = E(K, M)$$

and a case of decrypting the cryptogram C with the crypt key K to obtain the plaintext M is expressed as

$$M = D(K, C).$$

The cryptosystem used for the present invention uses a secret-key cryptosystem in which the same secret-key Ks is used for encryption and decryption, and a public-key cryptosystem in which a public-key Kb is used for encryption of a plaintext and a private-key Kv is used for decryption of a cryptogram.

Figure 1 shows a structure of the data copyright management system disclosed in the prior Japanese Patent Application No. 237673/1994 in which the apparatus for data copyright management system of the present invention is used.

In this system, encrypted data is two-way supplied in accordance with a request from the primary user 4.

This system rises the secret-key cryptosystem and the public-key cryptosystem as a cryptosystem.

It is matter of course that this system can be applied when using a satellite broadcast, ground wave broadcast, CATV broadcast or a recording medium other than a database as data supply means provided with advertisement requiring no charge or encryption.

In this system, reference numeral 1 represents a database, 4 represents a primary user terminal, 5 represents a secondary user terminal, 6 represents a tertiary user terminal, and 7 represents an n-order user terminal.

And 3 represents a copyright management center, 8, 9, and 10 represent a secondary copyright data, tertiary copyright data, and n-order copyright data stored at the copyright management center 3, and 2 represents a communication network such as a public telephone line offered by a communication enterprise or a CATV line offered by a cable television enterprise.

On the above arrangement, the database 1, primary user terminal 4, secondary user terminal 5, tertiary user terminal 6, n-order user terminal 7, and copyright management center 3 are connected to the communication network 2 and also they can be connected each other.

In this figure, a path shown by a broken line represents a path for encrypted data, a path shown by a solid line represents a path of requests from each user terminal, a path shown by a one-dot chain line represents a path through which authorization information corresponding to a utilization request in each data and a crypt key are transferred, and a path shown by a two-dot chain line represents a path through which copyright information is transferred from the database or from the data to a next-order data within copyright management center.

Each user who uses this system is previously entered in a database system and in this time, database utilization software is provided him. The database utilization software includes a program for decrypting an encrypted copyright management program in addition to normal communication software such as data communicating protocol.

To use the database 1, a primary user prepares primary-user authentication data Au1, a first public-key Kb1, a first private-key Kv1 corresponding to the first public-key Kb1, a second public-key Kb2, and a second private-key Kv2 corresponding to the second public-key Kb2, and accesses the database 1 from the primary user terminal 4 via the communication network 2.

The database 1 receiving the primary-user authentication data Au1, first public-key Kb1 and second public-key Kb2 from the primary user confirms the primary-user authentication data Au1 and transfers the confirmed primary-user authentication data Au1 to the secondary copyright management center 3 as the primary user information Iu1.

BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1667

The database 1 prepares two secret-keys, that is, first secret-key Ks1 and second secret-key Ks2.

In the prepared first secret-key Ks1 and second secret-key Ks2, the second secret-key Ks2 is also previously transferred to the copyright management center 3.

As the result of the above transfer, a permit key corresponding to primary utilization, the primary user information Iu1, original copyright information Ic0 and the second secret-key Ks2 are stored in the copyright management center 3. In this case, the original copyright information Ic0 is used for copyright royalties distribution.

When a primary user who desires data utilization accesses the database 1 from the primary user terminal 4, a data menu is transferred to him. In this case, information for charges may be displayed together with the data menu.

When the data menu is transferred, the primary user retrieves in the data menu to select the data M. In this case, the original copyright information Ic0 of the selected data M is transmitted to the copyright management center 3. The primary user selects permit key Kp1 corresponding to the required form of the usage such as viewing, storing, copying, editing and transmitting of data. Permit key Kp1 is also transmitted to the copyright management center 3.

Because viewing and storing of data are the minimum required forms of use for the primary user, these forms of use may be excluded from the choices as the minimum usage, and offering only copying, editing and transmitting as the choices.

The original data M0 is read out of the database 1 in accordance with a request of the primary user. The read original data M0 is encrypted by the first secret-key Ks1:

$$Cm0ks1 = E(Ks1, M0).$$

The encrypted data Cm0ks1 is provided with the uncrypted original copyright information Ic0.

The first secret-key Ks1 is encrypted by the first public-key Kb1 and the second secret-key Ks2 is encrypted by the second public-key kb2:

$$Cks1kb1 = E(Kb1, Ks1)$$

$$Cks2kb2 = E(Kb2, Ks2).$$

While the copyright management program P is also encrypted by the second secret-key Ks2

$$CpKs2 = E(Ks2, P),$$

the copyright management program P must not always be encrypted by the second secret-key Ks2 but it may be encrypted by any other proper crypt key.

The encrypted original data Cm0ks1, encrypted copyright management program Cpks2, and two encrypted secret-keys Cks1kb1 and Cks2kb2 are transferred to the primary riser terminal 4 via the communication network 2, and charged, if necessary.

It is possible to store the encrypted copyright management program Cpks2 such as in a ROM in the user terminal 4 instead of being supplied from the database 1.

The primary user receiving the encrypted original data Cm0ks1, two encrypted secret-keys Cks1kb1 and Cks2kb2, and encrypted copyright management program Cpks2 from the database 1 decrypts the encrypted first secret-key Cks1kb1 by the database utilization software using the first private-key Kv1 corresponding to the first public-key Kb1:

$$Ks1 = D(Kv1, Cks1kb1),$$

and decrypts the encrypted second secret-key Cks2kb2 using the second private-key Kv2 corresponding to the second public-key Kb2:

$$Ks2 = D(Kv2, Cks2kb2).$$

And the primary user decrypts the encrypted copyright management program Cpks2 using the decrypted second secret-key Ks2:

$$P = D(Ks2, Cpks2).$$

Finally, the primary user decrypts the encrypted data Cm0ks1 by the decrypted copyright management program P using the decrypted first secret-key Ks1:

$$M0 = D(Ks1, Cm0ks1)$$

and uses the decrypted original data M0 directly or data M1 as edited.

As described above, the first private-key Kv1 and second private-key Kv2 are crypt keys prepared by the primary user but not opened to others. Therefore, even if a third party obtains tire data M, it is impossible to use the encrypted data M by decrypting it.

Thereafter, to store, copy, or transmit the data M as the original data M0 or the edited data M1, it is encrypted and decrypted by the second secret-key Ks2:

$$Cmks2 = E(Ks2, M)$$

$$M = D(Ks2, Cmks2).$$

The decrypted second secret-key Ks2 is thereafter used as a crypt key for encrypting/decrypting data when storing, copying, or transmitting the data.

The first private-key Kv1 and second private-key Kv2, the first secret-key Ks1 and second secret-key Ks2, the data M, the copyright management program P, the original copyright information Ic, and also the original copyright information Ic0 and also copyright information Ic1 for information of the primary user and edited date and time when edited the data by the primary user are stored in the primary user terminal 4.

BNSDOCID: <EP__0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1668

Moreover, it is further protected by attaching the copyright information Ic1 to the data as copyright information label, and adding the digital signature.

The encrypted data Cmks2 is encrypted to be distributed. Since the copyright information label provides a clue to obtain the second secret-key Ks2 which is the key for decryption, the second secret key Ks2 cannot be obtained in the case where the copyright information label is removed from the encrypted data Cmks2.

When the encrypted data Cmks2 is stored in the primary user terminal 4, the second secret-key Ks2 is stored in the terminal 4. However, when the encrypted data Cmks2 is not stored in the primary user terminal 4 but is copied to the recording medium 11 or transmitted to the secondary user terminal 5 via the communication network 2, the second secret-key Ks2 is disused in order to disable subsequent utilization of the data in the primary user terminal 4.

In this case, it is possible to set a limitation for repetitions of copying or transmitting of the data so that the second secret-key Ks2 is not disused within limited repetions of copying and transmitting of the data.

The primary user who is going to copy the data M to the external recording medium 11 or transmit the data M via the communication network 2 must prepare the second secret-key Ks2 to encrypt the data M by this second secret-key Ks2 before copying or transmitting the data:

$$Cmks2 = E(Ks2, M).$$

The uncrypted original copyright information Ic0 and primary-user copyright information Ic1 are added to the encrypted data Cmks2.

Before using a database, a secondary user, similar to the primary user, prepares authentication data Au2 for authenticating the secondary user, a third public-key Kb3 and a third private-key Kv3 corresponding to the third public-key Kb3, a fourth public-key Kb4, and a fourth private-key Kv4 corresponding to the fourth public-key Kb4.

The secondary user who desires secondary utilization of the copied or transmitted encrypted data Cmks2 must designate original data name or number to the copyright management center 3 to request for secondary utilization to the center 3 from the secondary user terminal 5 via the communication network 2. In this time, the secondary user also transfers the third public-key Kb3 and the fourth public-key Kb4 as well as the secondary user authentication data Au2, original copyright information Ic0 and primary user copyright information Ic1.

The copyright management center 3 receiving the secondary utilization request from the secondary user confirms the secondary-user authentication data Au2, and transfers confirmed secondary-user authentication data Au2 to the tertiary copyright data 9 as secondary user information.

When the secondary copyright information Ic1 of the primary user is transferred, the secondary copyright information Ic1 is inquired to the secondary copyright data 8, and then, it recognizes the secondary copyright information Ic1 to be transferred to the tertiary copyright data 9.

The secondary user selects permit key Kp2 corresponding to the form of data usage such as viewing, storing, copying, editing and transmitting of data. Permit key Kp2 corresponding to the selected usage is sent to the tertiary copyright data 9.

Because viewing and storing of data are the minimum required forms of use for the secondary user, these forms of use may be excluded from the choices as the minimum usage, offering only copying, editing and transmitting as the choices.

The secondary copyright data 8 prepares a third secret-key Ks3.

The prepared third secret-key Ks3 is transferred to and stored in the tertiary copyright data 9.

As the result of the above transfer, the permit key Kp2, primary user copyright information Ic1, primary user information Iu1, original copyright information Ic0, secondary user information Iu2, and third secret-key Ks3 are stored in the tertiary copyright data 9. The permit key Kp2, primary user copyright information Ic1, and primary user information Iu1 are used for copyright royalties distribution.

Hereafter similarly, permit key Kpn corresponding to n-order usage, copyright information for secondary exploitation right Icn-1 of (n-1)-order user, primary user information Iu1, original copyright information Ic0, n-order user information Iun, and n-th secret-key Ksn are stored in n-order copyright data 10.

The permit key Kp2, primary user information Iu1, original copyright information Ic0 and second secret-key Ks2 are read out of the secondary copyright data 8. The original copyright information Ic0 is used for copyright royalties distribution.

The read second secret-key Ks2 and third secret-key Ks3 are encrypted by the third public-key Kb3 and fourth public-key Kb4 of the secondary user respectively:

$$Cks2kb3 = E(Kb3, Ks2)$$

$$Cks3kb4 = E(Kb4, Ks3).$$

The copyright management program P is encrypted by the third secret-key Ks3:

$$Cpks3 = E(Ks3, P).$$

The encrypted copyright management program Cpks3, encrypted second secret-key Cks2kb3, and encrypted third secret-key Cks3kb4 are transferred to the secondary user terminal 5 via the communication network 2. In this case, charging is performed, if necessary.

The secondary user receiving two encrypted secret-keys Cks2kb3 and Cks3kb4 and the encrypted copyright management program Cpks3 from the secondary copyright data 8 decrypts the encrypted second secret-key Cks2kb3 by the third private-key Kv3, and decrypts the

BNSDOCID: <EP__0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1669

encrypted third secret-key Cks3kb4 by the fourth private-key Kv4 corresponding to the fourth public-key Kb4, using the database utilization software:

$$Ks2 = D(Kv3, Cks2kb3)$$

$$Ks3 = D(Kv4, Cks3kb4).$$

The encrypted copyright management program Cpks3 is decrypted by the decrypted third secret-key Ks3:

$$P = D(Ks3, Cpks3).$$

Then, the encrypted data Cmks2 is decrypted to use it by the decrypted second secret-key Ks2 using decrypted copyright management program P:

$$M = D(Ks2, Cmks2).$$

As described above, the third private-key Kv3 and the fourth private-key Kv4 are prepared by the secondary user but not opened to others. Therefore, even if a third party obtains the encrypted data Cmks2, it is impossible to use the data by decrypting it.

Each user who uses above-mentioned system must previously be entered in a database system, and when entered in the system, software for database is supplied to the user.

Because the software includes not only normal communication software such as a data communication protocol but also a program for decrypting a copyright management program by a first crypt-key, it is necessary to be protected.

A first crypt-key K1, a second crypt-key K2, and a copyright management program P are transferred to each user in order to use data M, and each user keeps these keys and the program.

Further, the copyright information label, user information, the public-key and private-key in the public-key cryptosystem and the program containing algorithm for generating the secret-key are kept when needed.

For keeping them, it is the simplest means to use a flexible disk. However, the flexible disk is easy in disappearance or alteration of data.

Moreover, a hard disk drive is also unstable for disappearance or alteration of data though it is more stable than the flexible disk.

Recently, an IC card is spread in which an IC element is sealed in a card-like package. Particularly, standardization of a PC card with a microprocessor sealed in it is progressed as a PCMCIA card or JEIDA card.

The data copyright management apparatus proposed by the inventor of the present invention et al. in the prior Japanese Patent application No. 237673/1994 is described in Figure 2.

The data copyright management unit 15 is configured as a computer system, comprising a microprocessor (CPU) 16, a local bus 17 of CPU 16, read only memory (ROM) 18 connected to local bus 17, and write/read memory (RAM) 19, wherein the local bus 17 being connected to system bus 22 of the microprocessor 21 of the user terminal 20.

Moreover, a communication unit (COMM) 23 which receives data from an external database and transfer data to the external database, a CD-ROM drive (CDRD) 24 which reads data provided by CD-ROM, a flexible disk drive (FDD) 25 which copies received or edited data to a flexible disk drive to provide outside with such data, and a hard disc drive (HDD) 26 which stores data are connected to the system bus 22 in the user terminal 20.

As a matter of course, ROM and RAM or the like are connected to the system bus 22 of the user terminal, however, it is not shown in the figure.

Fixed information, such as software and user data, for utilizing the database is stored in ROM 18 of the data copyright management unit 15.

A crypt-key and the copyright management program provided from the key control center or copyright management center are stored in RAM 19.

The process of decryption and re-encryption are performed by the data copyright management unit 15, only of which results are transferred to the user terminal 20 via the local bus 17 and the system bus 21 of the user terminal.

The data copyright management unit 15 is implemented as monolithic IC, hybrid IC, an expansion board, an IC card, or a PC card.

Summary of the Invention

In the present application, apparatus for data copyright management system, resulted from further implementation of the apparatus used in the user terminal proposed in the prior Japanese patent application No. 237673/1994, is proposed.

The apparatus for data copyright management in the present invention is attached to the user terminal, which comprises central processing unit, central processing unit bus, read only semiconductor memory, electrically erasable programmable memory, and read/write memory.

Central processing unit, read only semiconductor memory, electrically erasable programmable memory, and read/write memory are connected to the central processing unit bus, and also system bus of a unit which utilizes the data can be connected to it. Data copyright management system program, a crypt algorithm, and user information are stored in the read only semiconductor memory, and a second private-key, permit key, second secret-key, and copyright information are stored in the electrically erasable programmable memory, wherein first public-key, first private-key, second public-key, and first secret-key being transferred to the read/write memory at the operation of the unit. If the copyright management program is provided from the outside, it is stored in the EEPROM. Otherwise, it is stored in ROM.

BNSDOCID: <EP__0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1670

As a form of the data copyright management apparatus, monolithic IC, hybrid IC, a thin IC card with special terminal, a PC card, and a board for insertion can be available.

In the data copyright management system described above as prior invention, while the obtained encrypted data is decrypted for utilization of displaying/editing, the obtained or edited data is re-encrypted to store/copy/transfer so that no unauthorized use of the data can be available.

Accordingly, in the apparatus used in the data copyright management system of the present invention, re-encryption of data, as well as decryption of data should be performed concurrently, however, those data copyright management apparatus described in the prior applications can perform only one process of either data decryption or data re-encryption.

Thus, in the present application, a data copyright management apparatus which, at the same time, can decrypt and re-encrypt data encrypted and supplied in order to manage copyright is proposed.

For the purpose of that, data which was encrypted and provided is decrypted and re-encrypted by adding at least one microprocessor, preferably 2 microprocessors, in addition to the microprocessor that controls the entire user terminal therein. When one microprocessor is added, one of the 2 microprocessors, one included in the user terminal or one added, will decrypt data and the other will re-encrypt data.

When 2 microprocessors are added, one of the added microprocessors will decrypt data, the other microprocessor will re-encrypt data, and the microprocessor of the user terminal will control the entire operation.

Although the added microprocessors may be connected to system bus of the microprocessor in the user terminal, this configuration may not allow a multiprocessor configuration to operate plural microprocessors concurrently.

Therefore, in the present application, a data copyright management apparatus as a multiprocessor configuration utilizing SCSI bus or PCI bus is proposed.

Other than character data, digital data includes graphic data, computer program, digital audio data, still picture data of JPEG standard, and motion-picture data of MPEG standard.

While the data works comprising these data are utilized by using various apparatus, it is necessary that these apparatus should also include the data copyright management function.

Thus, in the present application, it is proposed that, as a form of use, these data copyright management apparatus and the data copyright management apparatus described in the prior application are incorporated in various systems.

Brief Description of the Drawings

Figure 1 is a block diagram of the data copyright management system of the prior invention.

Figure 2 is a block diagram of the data copyright management apparatus of the prior invention.

Figure 3 is a block diagram of the data copyright management apparatus of embodiment 1 of the present invention.

Figure 4 is a specific block diagram of the data copyright management apparatus of the embodiment 1 of the present invention.

Figure 5 is a process flow chart of data copyright management system related to the present invention.

Figure 6 is a block diagram of the data copyright management system of the prior invention.

Figure 7 is a flow chart of a general edit process of digital data.

Figure 8 is a flow chart of encrypted data edit process of the present invention.

Figure 9 is a block diagram of the data copyright management apparatus of embodiment 2 of the present invention.

Figure 10 is a block diagram of the data copyright management apparatus of embodiment 3 of the present invention.

Figure 11 is a block diagram of the data copyright management apparatus of embodiment 4 of the present invention.

Figure 12 is a block diagram of the data copyright management apparatus of embodiment 5 of the present invention.

Figure 13 is a block diagram of the data copyright management apparatus of embodiment 6 of the present invention.

Figure 14 is a block diagram of the digital cash system as one example of use of the present invention.

Figure 15 is a block diagram of the video conference system as one example of use of the present invention.

Detailed Description of the Preferred Embodiments

The detailed embodiments of the present invention are described below with reference to the drawings.

The embodiment 1 of the data copyright management apparatus related to the present invention is shown in a block diagram of Figure 3.

The data copyright management unit 30 includes electrically erasable programmable memory (EEPROM) 31 in addition to the components of the data copyright management unit 15 described in the prior application No. 237673/1994.

The data copyright management unit 30 is a computer system having CPU 16, local bus 17 of CPU 16, ROM 18 connected to local bus 17, RAM 19, and EEPROM 31, wherein local bus 17 being connected to the system bus 22 of the microprocessor 21 in the user terminal 20.

BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1671

Moreover, communication unit (COMM) 23 which receives data from external database and transfers data outside, CD-ROM drive (CDRD) 24 which read data provided by CD-ROM, a flexible disc drive (FDD) 25 which copies data received or edited in order to supply to the outside, and hard disk drive (HDD) 26 which stores data are connected to the system bus 22 of the user terminal 20.

Further, ROM and RAM are connected to the system bus 22 of the user terminal, however, it is not shown in the figure.

Fixed information such as a data copyright management program, a cryptography program based on crypt algorithm, and user data are stored in ROM 18.

A crypt-key and copyright information are stored in EEPROM 31. Further, when data copyright management program and cryptography program are supplied from outside such as from database, they are stored in EEPROM 31, rather than in ROM 18.

The data copyright management unit 30 performs the process of decryption or re-encryption, only the result of which are transferred to the user terminal 20 via local bus 17 and system bus 22.

The data copyright management unit 30 is implemented as a monolithic IC, a hybrid IC, an expansion board, an IC card, or a PC card.

Fixed data such as a data copyright management program, a cryptography program based on crypt algorithm, and user data are stored in ROM 18 of the data copyright management unit 30 in the embodiment 1.

Further, a program for generating secret-keys based on secret-key algorithm of not secret, a decryption program, and a re-encryption program may be stored in ROM 18.

A crypt-key and copyright information are stored in EEPROM 31. Moreover, when the copyright management program and the encryption program are supplied from the outside such as database, they are stored in EEPROM 31, rather than ROM 18. Still more, the EEPROM is not necessarily required and may be omitted.

Either one of the first crypt-key or the second crypt-key supplied from the key control center or copyright management center, and data copyright management system program are stored in RAM 19.

On the other hand, information such as software and the user data required by MPU 46 in the user terminal 20 are supplied to the user terminal 20 by the software, and stored in RAM of the user terminal 20.

Besides, either one of the first crypt-key or the second crypt-key supplied from the key control center or the copyright management center, and the data copyright management system program are stored in RAM of the user terminal unit 20.

The process of decryption and re-encryption are shared by MPU 46 of the main body of the user terminal 20 and CPU 16 of the data copyright management unit 30; one encrypts data and the other decrypts data, and only the processed results of the data copyright management unit 30 are transferred to the user terminal.

The specific internal structure of the data copyright management unit 30 in Figure 3 is shown in Figure 4.

A microcomputer (CPU) 16, read only semiconductor memory (ROM) 18, write/read memory (RAM) 19, and electrically erasable programmable memory (EEPROM) 31 are enclosed in the data copyright management unit 30, and are connected to microcomputer bus 17 of the microcomputer 16, the microcomputer bus 17 being further connected to system bus 22 of the user terminal 20 main body.

The data copyright management system program, crypt algorithm, and the user information are stored in the read only semiconductor memory 18.

Inside of the electrically erasable programmable memory 31 is divided into three areas.

In the first area 35, the first public-key Kb1, the first private-key Kv1, the second public-key Kb2, and the second private-key Kv2 are stored.

In the second area 36, the copyright management program P, the first secret-key Ks1 as a permit key in the primary use such as view permit/store permit/copy permit/edit permit/transfer permit, and the second secret key Ks2 as a permit key in the secondary use such as view permit/store permit/copy permit/edit permit/transfer permit are stored.

Further, in some case where the copyright management program is not supplied form the outside, but preset in the user side, the copyright management program is stored in the read only memory 18, rather than in the second area 36 of the electrically erasable programmable memory 31.

In the third area 37, copyright information such as the original copyright information and the secondary copyright information, and air access control key are stored.

As in the case of the electrically erasable programmable memory 31, inside of the write/read memory 19 is divided into three areas.

In the first area 32, the first public-key Kb1, the first private-key Kv1, and the second public-key Kb2 are stored during operation.

In the second area 33, the first secret-key Ks1 as a permit key in the primary utilization such as view permit/store permit/copy permit/edit permit/transfer permit is stored during operation.

In the third area 34, an access control key is stored during operation.

The user terminal attached with the data copyright management apparatus is reliable since it performs all the process for utilizing data within the data copyright management unit related to the present invention, so that only the results are transferred to the user terminal for various utilization.

When picture data containing large amount of information is transmitted/received, original data is transmitted after being compressed in order to reduce the amount of data and the compressed data is expanded after reception to utilize it. In this case, data copyright may be managed by encryption.

BNSDOCID: <EP__0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1672

In Figure 5, an example of data copyright management flow when encrypted data is digital picture compressed in JPEG standard or MPEG standard. The flow is divided into transmitting side flow and receiving side flow with a transmit line in between, and the receiving side flow is further divided into display flow and storage flow.

The signal process in the transmitting side consists of process preparing digital picture and process processing the digital picture prepared. In this process, if an original picture is the digital picture 41, it proceeds to next process. If an original image is an analog picture 40, digitizing process 42 is performed.

The digital picture is compressed 43 first by given standard such as JPEG standard, or MPEG standard, then the compressed digital data is encrypted 44 using the first secret-key.

The picture data signal processed in transmitting side is transmitted through transmission line 45 such as satellite broadcasting wave, terrestrial broadcasting wave, CATV wave, or public telephone line/ISDN line.

Further, recording media such as a digital video tape, a digital video disk, or CD-ROM may be used as the transmission line.

Thus the picture data transmitted to the receiving side is decrypted 46 first using the first secret key, then the compressed picture data is expanded 47 to be displayed 49. When the display is a digital data display unit, it is directly displayed, however, when it is an analog data display unit, it is converted to analog data 48.

When data is stored in hard disk, flexible disk, optical magnetic disk, writable video disk or the like, it is stored after being re-encrypted 50 using the second secret key.

In displaying again the picture data re-encrypted and stored, it is re-decrypted 52 using the second secret key and displayed 49. If the display unit is a digital data display unit, it is directly displayed, however, if it is an analog data display unit, it is converted to analog data 48.

Moreover, for data compression/expansion means and transmission path, appropriate ones compatible with the data are used.

Figure 6 shows an example of the data copyright management system disclosed in the prior Japanese Patent Application No. 237673/1994. This system uses the secret-key system as a cryptosystem.

In the case of this system, reference numeral 1 represents a database in which text data, binary data serving as a computer graphic display or a computer program, digital audio data, and digital picture data are stored by being encrypted, 14 represents a space satellite such as a communications satellite or a broadcasting satellite, 15 represents a data recorder such as a CD-ROM or a flexible disk, 2 represents a communication network such as a public telephone line offered by a communication enterprise or a CATV line offered by a cable television enterprise, 4 represents a primary user terminal, and 16 represents a key control center for managing a secret-key, and 17 represents a copyright management center for managing a data copyright.

Reference numerals 5, 6, and 7 represent a secondary user terminal, a tertiary user terminal, and n-order user terminal respectively, and 11, 12, and 13 represent a secondary disk, tertiary disk, and n-order disk serving as a recording medium such as a flexible disk or CD-ROM respectively. The symbol "n" represents an optional integer. When "n" is larger than 4, a corresponding user terminal and a corresponding disk are arranged between the tertiary user terminal 6 and the n-order user terminal 7 and between the tertiary disk 12 and the n-order disk 13 respectively.

On the above arrangement, the database 1, key control center 16, copyright management center 17, primary user terminal 4, secondary user terminal 5, tertiary user terminal 6, and n-order user terminal 7 are connected to the communication network 2.

In this figure, the path shown by a broken line is a path of encrypted data, a path shown by a solid line is a path of requests from each user terminal, and a path shown by a one-dot chain line is a path through which authorization information corresponding to a utilization request and a secret-key are transferred.

Moreover, each user who uses this system is previously entered in the database system. When the user is entered in the system, a database utilization software is given to the user. The database utilization software includes not only normal communication software such as a data communication protocol but also a program for running a copyright management program.

Original data M0 of text data, binary data as a computer graphic display or computer program, digital audio data, or digital picture data stored in the database 1 or data recording medium 15 is one-way supplied to the primary user terminal 4 via the communication network 2, satellite 14 or recording medium 15.

In this case, the data is encrypted with a first secret-key Ks1:

$$Cm0ks1 = E(Ks1, M0).$$

Even if data provided with advertisement to be offered free of charge, it is necessary to be encrypted in order to protect the copyright.

It is disclosed in the Japanese Patent Application No. 64889/1994 which is the prior application that the data utilization includes not only displaying of data which is the most basic usage but also storing, editing, copying, and transmitting of the data, a use permit key is prepared which corresponds to one or several forms of usage, and its management is executed by the copyright management program.

Moreover, it is described there that data is encrypted again by the copyright management program for use such as storing, copying, editing and transmitting of the data other than displaying of the data and displaying for editing the data.

In other words, the data whose copyright is claimed is encrypted to be distributed, and only when the data is displayed or displayed for editing the data in a user ter-

BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1673

minal having a copyright treatment function, the data is decrypted to a plaintext.

This system disclosed in Japanese Patent Application No. 237673/1994 uses the method described in the prior application No. 64889/1994.

A primary user who desires primary utilization of the supplied encrypted data Cm0ks1 requests for primary utilization of the encrypted original data Cm0ks1 by designating the original data name or the original data number to the key control center 16 via the communication network 2 from the primary user terminal 4. In this case, the primary user must present information Iu1 for primary user to the key control center 16.

The key control center 16 receiving the primary utilization request from the primary user terminal 4 transfers first secret-key Ks1 for decrypting the encrypted original data Cm0ks1 obtained from the database 1 by the primary user and second secret-key Ks2 for re-encrypting the decrypted original data M0 or edited data M1 from the original data, together with a copyright management program P via the communication network 2 to the primary user terminal 4.

In the primary user terminal 4 receiving the first secret-key Ks1 as a decryption key and the second secret-key Ks2 as an encryption/decryption key, the encrypted original data Cm0ks1 is decrypted by the first secret-key Ks1 using the copyright management program P

$$M0 = D(Ks1, Cm0ks1)$$

to use the decrypted original data M0 directly or data M1 as edited.

When the data M which is the original data M0 or edited data M1 is stored in a memory or a built-in hard disk drive of the primary user terminal 4, only the primary user can use the data. However, when the data M is copied to the external recording medium 11 such as a flexible disk or transmitted to the secondary user terminal 5 via the communication network 2, a problem of a copyright due to secondary utilization occurs.

When the original data M0 obtained by the primary user is directly copied and supplied to a secondary user, the copyright of the primary user is not effected on the data M0 because the original data M0 is not modified at all. However, when the primary user produces new data M1 by editing the obtained data M0 or by using means such as combination with other data, the copyright of the primary user, i. e., secondary exploitation right occurred from secondarily utilizing original data, is effected on the data M1.

Similarly, when a secondary user produces new data M2 by editing the original data M0 or edited data M1 obtained from the primary user or by means such as combination of other data, the copyright of the secondary user; i. e., secondary exploitation right on the secondary user is also effected.

In this system, to correspond to the problem of the copyright, the data M is encrypted by the second secret-key Ks2 using the copyright management program P when the data M is stored, copied, or transmitted. Thereafter, in the primary user terminal 4, the data M is decrypted and encrypted by the second secret-key Ks2:

$$Cmks2 = E(Ks2, M)$$

$$M = D(Ks2, Cmks2).$$

It is free in principle that the primary user displays and edits data to obtain edited data. In this case, however, it is possible to limit the repetitions of the operation by the copyright management program.

When the data M is copied to the external recording medium 11 or transmitted via the communication network 2, the first secret-key Ks1 and the second secret-key Ks2 in the primary user terminal 4 are disused by the copyright management program P. Therefore, when reusing the data M the primary user requests for utilization of the data M to the key control center 16 to again obtain the second secret-key Ks2.

The fact that the user receives the regrant of the second secret-key Ks2 represents secondary utilization of data in which the data M has been copied to the external recording medium 11 or transmitted to the secondary user terminal 5 via the communication network 2. Therefore, the fact is entered in the copyright management center 17 from the key control center 16 and subsequent secondary utilization comes possible.

The data M is moved from the primary user terminal 4 to the secondary user terminal 5 by the external recording medium 11 or the communication network 2. When the data M is copied to the external recording medium 11 or transmitted via the communication network 2, it is encrypted by the second secret-key Ks2.

When the data M is copied to the external recording medium 11 or transmitted via the communication network 2, the first secret-key Ks1 and the second secret-key Ks2 in the primary user terminal 4 are disused. In this time, uncrypted primary user information Iu1 is added to the encrypted data Cmks2 stored in the primary user terminal 4 and when the encrypted data Cmks2 is transmitted to the secondary user, the primary user information Iu1 is also transferred.

A secondary user who desires secondary utilization of the encrypted data Cmks2 copied or transmitted from the primary user must designate original data name or data number to the copyright management center 17 via the communication network 2 by the secondary user terminal 5 and also present the secondary user information Iu2 to request for secondary utilization of the data Cmks2 to the center 17. In this time, the secondary user further presents the uncrypted primary user information Iu1 added to the encrypted data Cmks2 in order to clarify the relationship with the primary user.

The copyright management center 17 confirms that the primary user has received a regrant of the second secret-key Ks2 for secondary-utilizing the data, in accordance with the presented primary user information

BNSDOCID: <EP__0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1674

lu1 and then, transfers the second secret-key Ks2 serving as a decryption key and the third secret-key Ks3 serving as an encryption/decryption key to the secondary user terminal 5 via the communication network 2.

In the secondary user terminal 5 receiving the second secret-key Ks2 and the third secret-key Ks3, the encrypted data Cmks2 is decrypted using the second secret-key Ks2 by the copyright management program P

$$M = D(Ks2, Cmks2)$$

and is secondarily utilized such as being displayed or edited.

In this system, the key control center 16 processes a primary utilization requests and the copyright management center 17 processes a secondary utilization requests. While the data M supplied to a primary user is encrypted by the first secret-key Ks1, the data M supplied to a secondary user is encrypted by the second secret-key Ks2. Moreover, the first secret-key Ks1 and the second secret-key Ks2 are transferred to the primary user as crypt keys from the key control center 16.

Therefore, if the secondary user, instead of the primary user, falsely requests for primary utilization to the key control center 16, the first secret-key Ks1 for decryption and the second secret-key Ks2 for encryption/decryption are transferred to the secondary user. However, the secondary user cannot decrypt the encrypted data Cmks2 by using the first secret-key Ks1 transferred as a decryption key.

Therefore, it is impossible to falsely request for data utilization and resultingly, not only the original copyright of data but also the copyright of the primary user on the data are protected.

When storing, copying, or transmitting of the data M other than displaying and displaying for editing is performed in the secondary user terminal 5, the data M is encrypted using the third secret-key Ks3 by the copyright management program P and thereafter, the data is decrypted and encrypted by the third secret-key Ks3:

$$Cmks3 = E(Ks3, M)$$

$$M = D(Ks3, Cmks3).$$

Moreover, it is free in principle that the secondary user displays and edits data to obtain the edited data M2. In this case, it is possible to limit the repetitions of the operation by the copyright management program P.

When the data M is copied to the external recording medium 12 or transmitted via the communication network 2, the second secret-key Ks2 and the third secret-key Ks3 in the secondary user terminal 5 are disused by the copyright management program P. Therefore, when reusing the data M, the secondary user requests for the utilization of the data to the copyright management center 17 to again obtain the third secret-key Ks3.

The fact that the secondary user receives a regrant of the third secret-key Ks3 represents secondary utilization of data in which the data M has been copied to the external recording medium 12 or transmitted to the tertiary user terminal 6 via the communication network 2. Therefore, the fact is entered in the copyright management center 17 and allows subsequent data use.

The data M is moved from the secondary user terminal 5 to the tertiary user terminal 6 by the external recording medium 12 or by the communication network 2. When the data M is copied to the external recording medium 12 or transmitted via the communication network 2, it is encrypted by the third secret-key Ks3.

When the data M is copied to the external recording medium 12 or transmitted to the tertiary user terminal 6 via the communication network 2, the second secret-key Ks2 and the third secret-key Ks3 in the secondary user terminal 5 are disused. In this case, the uncrypted secondary user information lu2 is added to the encrypted data Cmks3 stored in the secondary user terminal 5, and when the encrypted data Cmks3 is transmitted to a tertiary user, the secondary user information lu2 is also transferred.

In adding each user information to data, there are two cases: a case in which every information is added to data whenever it is copied or transmitted; and another in which the history updated whenever the data is copied or transmitted is stored in the copyright management center.

A tertiary user who desires tertiary utilization of the encrypted data Cmks3 copied or transmitted from the secondary user must designate original data name or number to the copyright management center 17 from a tertiary user terminal 6 via the communication network 2 and also presents the tertiary user information lu3 to request for tertiary utilization of the data. In this time, the tertiary user further presents the uncrypted secondary user information lu2 added to the encrypted data Cmks3 in order to clarify the relationship with the secondary user.

The copyright management center 17 confirms that the secondary user has received a regrant of the third secret-key Ks3 for preparation of tertiary-utilizing the data, in accordance with the presented secondary user information lu2 and then, transfers the third secret-key Ks3 serving as a decryption key and fourth secret-keyKs4 serving as an encryption/decryption key to the tertiary user terminal 6 via the communication network 2.

In the tertiary user terminal 6 receiving the third secret-key Ks3 and the fourth secret-key Ks4, the encrypted data Cmks3 is decrypted using the third secret-key Ks3 by the copyright management program P

$$M = D(Ks3, Cmks3)$$

and is tertiarily utilized such as being displayed or edited.

In this system, the data M supplied to the primary user is encrypted by the first secret-key Ks1 and the data M supplied to the secondary user is encrypted by the second secret-key Ks2, and the data M supplied to the tertiary user is encrypted by the third secret-key Ks3.

BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1675

Therefore, if the tertiary user, instead of the primary user, falsely requests for primary utilization to the key control center 16, the first secret-key Ks1 for decryption and the second secret-key Ks2 for encryption/decryption are transferred to the tertiary user. However, it is impossible to decrypt the encrypted data Cmks3 by the first secret-key Ks1 transferred as a decryption key. Moreover, if the tertiary user, instead of the secondary user, falsely requests for secondary utilization to the copyright management center 17, the second secret-key Ks2 and the third secret-key Ks3 are transferred to the tertiary user as a decryption key and an encryption/decryption key respectively. However, it is impossible to decrypt the encrypted data CmKs3 by the second secret-key Ks2 transferred as a decryption key.

Therefore, it is impossible to falsely request for data utilization. As a result, not only the original copyright of the data but also the copyrights of the primary and secondary users on the data are protected.

The same procedure is applied to quaternary and subsequent utilization.

In the above described system, the database 1, key control center 16, and copyright management center 17 are separately arranged. However, it is not always necessary to arrange them separately. It is also possible to set all of or proper two of them integrally.

Moreover, it is also possible to request for a regrant of the secondary secret-key from the primary user not to the key control center 16 but to the copyright management center 17.

In Figures 7(a) and 7(b), signal process flow in data edit method of digital video or digital audio is shown. An edit flow generally processed is shown in 7(a) and an edit flow 7(b) which can avoid deterioration of signals.

In the edit flow shown in 7(a), signals supplied as digital signals 61 are converted to analog signals 62, the analog signals are then edited while being displayed 64, and the analog signals completed editing are re-digitized 65 to be stored, copied, and transferred 66.

Though this process may be simple, it can not avoid deterioration of signals since signal is edited in analog and re-digitized after completion of editing.

The edit flow shown in 7(b), digital signals 61 are converted to analog signals 62 to be displayed. While the analog signals 62 are used in editing 63, the analog signals are used only for displaying 64 rather than for storing, copying, transferring.

Signals for storage, copy, and transfer are edited 67, copied, and transferred 66 in the form of digital signals 61 correspond to signals displayed in analog.

In the case of this edit flow, there is no deterioration of signals since digital signals which are stored, copied, and transferred are never converted to analog signals.

Figures 8(a) and 8(b) illustrate flow examples when editing encrypted data to which signal process in data editing method of digital video or digital audio shown in Figure is applied. 8(a) shows a simplified signal processing flow and 8(b) shows a signal processing flow which allows sufficient copyright management.

In the signal processing flow shown in (a), the original data 71 Cm0ks1, encrypted using the first secret-key Ks1 and supplied is initially decrypted 72 using the first secret key Ks1:

$$M0=D\ (Ks1,\ Cm0ks1),$$

and the decrypted data M0 is then edited 73 while being displayed 74. The data M1 completed editing is re-encrypted 75 using the second secret key Ks2:

$$Cm1ks2=E\ (Ks2,\ M1)$$

and stored, copied, and transferred 76.

Though the process may be simple, copyright can not be properly managed since there is possibility that the decrypted data might be stored, copied, or transferred due to the data editing process in decrypted form.

On the other hand, in the signal processing flow shown in 8(b), the original data 71 Cm0ks1, encrypted using the first secret key Ks1 is decrypted 72 using the first secret-key Ks1:

$$M0=D\ (Ks1,\ Cm0ks1)$$

the decrypted data M0 is displayed 74.

While, the encrypted data Cm0ks1 is edited 73, lead by the decrypted data M0, and the original data M0 for storage or the edited data M1 are re-encrypted using the second secret-key:

$$Cm0ks2=E\ (Ks2,\ M0)$$

$$Cm1ks2=E\ (Ks2,\ M1)$$

the encrypted data Cm0ks2 or Cm1ks2 is stored, copied, and transferred 76.

Without being decrypted corresponding to the decrypted and displayed data, it is edited 77 in the encrypted form, and the edition program and the data still encrypted are used for store, copy, transfer 76.

In the case of this signal processing flow, the decrypted data are never stored, copied, or transferred since the data for storage, copy, transfer remains encrypted.

In the data copyright management system which applies the data copyright management apparatus of the present invention, while data is decrypted for utilization when the obtained encrypted data are displayed/edited, data copyright is managed by encrypting data when obtained or edited data is stored/copied/transferred.

However, the data copyright management unit 15 of the prior invention shown in Figure 2 and the data copyright management unit 30 of the present invention described in Figure 3 can perform only one process of decryption of encrypted data or encryption of decrypted data. When decrypted or edited data is stored/copied/transferred, therefore, it is necessary to store data in the user terminal or RAM of the data copyright manage-

BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1676

ment apparatus to re-encrypt the stored data afterwards. Thus, there is a possibility that decrypted or edited data might be lost due to accident or misoperation as well as posing limitation in volume to the data that can be processed.

With the exception of some high-class MPU, general MPU used in personal computers does not take into account the multiprocessor configuration which allows concurrent operation of plural microcomputers. Therefore, plural operations can not be performed at the same time, although accessory units are connected to the system bus of the personal computer.

Accordingly, to connect the data copyright management unit 15 shown in Figure 2 or the data copyright management unit 30 shown in Figure 3 to the system bus 22 of the user terminal 20 never provides multiprocessor function that enables concurrent operation of MPU 21 or 46 and CPU 16, and the processes of decryption of encrypted data and re-encryption of decrypted data are performed alternately, not concurrently. Thus, a large amount of data can not be processed since the data to be encrypted and decrypted is limited by the capacity of RAM. Further, it is impossible to increase the processing speed, even if the amount of data is not large.

On the other hand, in the data copyright management system described as the prior application, encrypted data obtained is decrypted to use for displaying or editing, and when the obtained or edited data is stored, copied, or transferred, it is re-encrypted in order to prevent unauthorized utilization of the data. Therefore, it is desirable that the apparatus in the data copyright management system of the present invention performs not only decryption but also re-encryption of data at the same time.

Recently, a PCI (Peripheral Component Interconnect) bus has attracted attention as means for implementing a multiprocessor configuration of typical personal computer.

The PCI bus is a bus for external connection connected to a system bus of personal computer via a PCI bridge, and allows to implement a multiprocessor configuration.

Figure 9 shows embodiment 2 of this invention, which is a configuration of data copyright management apparatus using a PCI bus and the same configuration of data copyright management unit 15 as shown in Figure 3, that is, a computer configuration having a CPU 16, a local bus 17 for the CPU 16, and ROM 18, RAM 19, and EEPROM 31 connected to the local bus 17.

In a user terminal 20, a PCI bus 81 is connected to a system bus 22 for a microprocessor 21 via a PCI bridge 82 and the local bus 17 for the CPU 16 of a data copyright management apparatus 80 is connected to the PCI bus 81. Also connected to the system bus 22 of the user terminal 20 are a communications device (COMM) 23 which receives data from external databases and transfers data to the external of tire terminal, a CD-ROM drive (CDRD) 24 which reads data supplied on CD-ROM a flexible disk drive (FDD) 25 which copies received or edited data to supply to the external of terminal, and hard disk drive (HDD) 26 used for storing data. COMM 23, CDRD 24, FDD 25, and HDD 26 may also be connected to the PCI bus 81.

While ROM, RAM etc., of course, are connected to the system bus 22 of the user terminal, these are not shown in Figure 9.

Configurations and operations of other parts are the same as embodiment 1 shown in Figure 3, and further explanation of them will be omitted.

A decryption task is performed by the MPU 21 of the user terminal 20 and an encryption task is performed by the CPU 16 of the data copyright management apparatus 80 at the same time, and vice versa. Since the configuration of the MPU 21 and CPU 16 in this embodiment is a multiprosessor configuration which performs parallel processing with a PCI bus, high processing speed can be achieved.

Other typical means for attaching external devices to a personal computer include SCSI (Small Computer System Interface), which is used for the connection of external storage medium such as hard disk drives and CD-ROM drives.

Up to eight devices, including the personal computer itself to which SCSI is attached, can be connected to SCSI, and a plurality of computers may be included in the eight devices. Each of these computers can play an equivalent role, in other words, SCSI function as not only an interface but also a multiprocessor bus.

Taking advantage of this function of SCSI, embodiment 3 connects a data copyright management apparatus 85 to the system bus 22 of a user terminal 20 via SCSI 86 (hereinafter called the "SCSI bus", for clear understanding) instead of the PCI bus 81 in embodiment 2.

Figure 10 shows a configuration block diagram of a data copyright management apparatus of embodiment 3 which uses and SCSI bus according to the present invention.

In embodiment 3, the configuration of the data copyright management apparatus 85 is the same as the data copyright management apparatus shown in Figure 3, that is, the apparatus has a CPU 16, a local bus 17 for the CPU 16, and ROM 18, RAM 19, and EEPROM 31 connected to the local bus 17.

On the other hand, an SCSI bus 86, which is controlled by an SCSI controller (SCSICONT) 87, is connected to a system bus 22 for a microprocessor 21 of a user terminal 20, and the local bus 17 for the CPU 16 of a data copyright management apparatus 85 is connected to this SCSI bus 86.

Also connected to the system bus 22 of the user terminal 20 are a communications device (COMM) 23 which receives data from external databases and transfers data to the external of the terminal, a CD-ROM drive (CDRD) 24 which reads data supplied on CD-ROM, a flexible disk drive (FDD) 25 which copies received or edited data to supply to the external of terminal, and hard disk drive (HDD) 26 used for storing data. COMM 23,

BNSDOCID: <EP__0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1677

CDRD 24, FDD 25, and HDD 26 may also be connected to the SCSI bus 86.

While ROM, RAM etc., of course, are connected to the system bus 22 of the user terminal, these are not shown in Figure 10.

Configurations and operations of other parts are the same as embodimnt 1 shown in Figure 3, and further explanation of them will be omitted.

A decryption task is performed by the MPU 21 of the user terminal 20 and a encryption task is performed by the CPU 16 of the data copyright management apparatus 85 at the same time, and vice versa. Since the configuration of the MPU 21 and CPU 16 in this embodiment is a multiprosessor configuration which performs parallel processing with an SISI bus 86, high processing speed can be achieved.

Other means for implementing a multiprocessor configuration, such as SCI (Scalable Coherent Interface), may be used, and, if possible, the microprocessors may be connected with each other without using a bus.

Data to be managed by the data copyright management apparatus of the present invention includes, in addition to text data, graphic data, computer programs, digital audio data, JPEG-based still picture data, and MPEG-based moving picture.

The above-mentioned multiprocessor configuration of the data copyright management apparatus 80 of embodiment 2 and the data copyright management apparatus 85 of embodiment 3 is implemented by connecting the apparatus to the system bus 22 of the microprocessor 21 in the user terminal 20 via a PCI bus or a SCSI bus. In such multiprocessor configuration, the MPU 21 of the user terminal 20 must also control the overall system. For relatively slow and small data such as text data and graphic data, data copyright management with encryption and re-encryption can be performed by the multiprocessor configuration using the MPU 21 and CPU 16, for JPEG-still-picture-based moving picture data and MPEG1 or MPEG2-based moving picture data, however, data copyright management by such configuration is considerably difficult to perform because the data is fast and large.

To deal with this problem, a multiprocessor system is configured by connection a first data copyright management apparatus 80 and a second data copyright management apparatus 90 to a PCI bus 81 in embodiment 4 shown in Figure 11.

The configuration of the second data copyright management apparatus 90 is the same as that of the first data copyright management apparatus 80, that is, the apparatus comprises a CPU 91, a local bus 94 for the CPU 91, and ROM 92, RAM 93, and EEPROM 95 connected to the local bus 94.

In this embodiment, the first data copyright management apparatus 80 decrypts encrypted data and the second data copyright management apparatus 90 re-encrypts decrypted data.

Fixed information, such as software for utilizing databases and user data, are stored in the ROM 18 of the first data copyright management apparatus 80 decrypting encrypted data. A first crypt-key and data copyright management system program supplied by a key control center or copyright management center are stored in the RAM 19.

Similarly, fixed information, such as software for utilizing databases and user data, are stored in the ROM 92 of the second data copyright management apparatus 90 re-encrypting decrypted data, and a second crypt-key and data copyright management system program supplied by a key control center or copyright management center are stored in the RAM 93.

In this multiprocessor configuration, SCSI or SCI may be used, and, if possible, the microprocessors may be connected with each other without using a bus.

In the prior application shown in Figure 2 and in embodiment 1 of the present invention described with reference to Figure 3, the communications device (COMM) 23 to which encrypted data is supplied and the CD-ROM drive (CDRD) 24 are connected to the system bus of the user terminal 20. In order to decrypt encrypted data, therefore, the encrypted data must be transmitted by way of the system bus of the user terminal 20 and the local bus of the data copyright management apparatus, and consequently, the processing speed can be slowed. This is true for a configuration in which those attached devices are connected to a PCI bus or SCSI bus.

In embodiment 5 shown in Figure 12, a communications device 23 to which encrypted data is supplied and a CD-ROM drive 24 are connected to a local bus 17 of a data copyright management apparatus 97 for decryption, in order to prevent processing speed from being slowed.

The data copyright management apparatus 97 of embodiment 5 shown in Figure 12 is a data copyright management apparatus for decryption and its configuration is essentially the same as that of the data copyright management apparatus 30 of embodiment 1 shown in Figure 3, that is, the computer system has a CPU 16, a local bus 17 for CPU 16, and ROM 18, RAM 19 and EEPROM 31 connected to the local bus 17, and a communication device COMM 23 and a CD-ROM drive CDRD 24 are connected to the local bus 17.

Fixed information, such as a copyright management program, cryptography program based on crypt algorithm, and user data, are stored in the ROM 18.

Copyright information is stored in the EEPROM 31. If the copyright management program and cryptography program are supplied from the external such as databases, those programs are stored in the EEPROM 31, rather than in the ROM 18.

A crypt-key for decryption and a data copyright management system program supplied from a key control center or copyright management center are stored in the RAM 19.

Encrypted data supplied from the COMM 23 or CDRD 24 is decrypted by the data copyright management apparatus 97 and transferred to a user terminal 95.

BNSDOCID: <EP__0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1678

While the above-mentioned data copyright management apparatus 80 and 90 of embodiment 4 are described as being configured separately, these apparatus, of course, can be configured as a unit.

Figure 13 shows a data copyright management apparatus of embodiment 6 which is extended from the data copyright management apparatus 97 of embodiment 5.

In the prior application shown in Figure 2 and the embodiment 1 described with reference to Figure 3, the storage medium, such as HDD 26, for storing re-encrypted data are connected to the system bus 22 of the user terminal 20. In order to store re-encrypted data, therefore, the encrypted data must be transmitted by way of the system bus 22 of the user terminal 20 and the local bus 17 of the data copyright management unit 15 or data copyright management unit 30, and consequently, processing speed can be slowed. This is true for a configuration in which those attached devices are connected to a PCI bus or SCSI bus.

In the data copyright management apparatus 100 of the embodiment 6 shown in Figure 13, in addition to the communications device COMM 23 and the CD-ROM drive CDRD 24 connected to the local bus 17 in the data copyright management apparatus 97 for decryption in the embodiment 5 shown in Figure 12, storage devices such as HDD 26 for storing re-encrypted data are connected to the local bus 94 of the data copyright management apparatus 101 for re-encryption.

The configuration of the data copyright management apparatus 101 for re-encryption in embodiment 6 is essentially the same as that of the data copyright management unit 30 shown in Figure 3, that is, the computer system has a CPU 91, a local bus 94 for the CPU 91, and ROM 92, RAM 93 and EEPROM 95 connected to the local bus 94, and HDD 26 is connected to the local bus 94.

Fixed information, such as a copyright management program, cryptography program based on crypt algorithm, and user data, are stored in the ROM 92.

Copyright information is stored in the EEPROM 95. If the copyright management program and cryptography program are supplied from the external such as databases, those programs are stored in the EEPROM 95 rather than the ROM 92.

A crypt-key for re-encryption and a data copyright management system program supplied from a key control center or copyright management center are stored in the RAM 93.

Data re-encrypted by the copyright management apparatus 101 for re-encryption is stored in HDD 26.

While the above-mentioned data copyright management apparatus 100 and 101 of embodiment 6 are described as being configured separately, these apparatus, of course, can be configured as a unit.

Digital data includes, in addition to text data, graphic data, computer programs, digital sound data, JPEG-based still picture data, and MPEG-based moving picture data.

A typical user terminal which utilizes copyrighted data is computer apparatus such as personal computers. Other apparatus which utilize such data are receivers such as television sets, set-top boxes used with those receivers, digital recording apparatus such as video tape recorders, digital video disk recorders, and digital audio tapes (DAT) which store digital data, and personal digital assistants (PDA).

The data copyright management apparatus shown in Figure 2 which is configured as an expansion board, IC card, or PC card and described in the prior patent application No. 237673/1994 or the data copyright management apparatus shown in Figure 6 may be used by attaching it to a user terminal which is a computer, receiver, set-top box, digital recording medium, or PDA. However, it is desirable that a data copyright management apparatus is factory-installed in the user terminal in order to eliminate labor and failure during the attachment of the apparatus.

To accomplish this, in each embodiment of the present invention, a data copyright management apparatus is implemented in the form of a monolithic IC, hybrid IC, or built-in subboard and is incorporated in a user terminal such as computer apparatus such as personal computers, receivers such as television sets, set-top boxes used with those receivers, digital recording medium such as digital video tape recorders, digital video disk recorders, and digital audio tape (DAT) which store digital signals, or personal digital assistants (PDA).

Further, the apparatus for managing data copyright described above can be applied not only to the data utilization but also to the handling of the digital cash and video conference systems.

The digital cash system which has been proposed so far is based on a secret-key cryptosystem. The encrypted digital cash data is transferred from a bank account or a cash service of a credit company, and is stored in the IC card so that a terminal device for input/output is used to make a payment. The digital cash system which uses this IC card as an electronic cash-box can be used at any place such as shops or the like as long as the input/ output terminal is installed. However, the system cannot be used at places such as homes or the like where no input/output terminal is installed.

Since the digital cash is an encrypted data, any device can be used as the electronic cash-box which stores digital cash data, in addition to the IC card, as long as the device can store encrypted data and transmit the data to the party to which the payment is made. As a terminal which can be specifically used as the electronic cash-box, there are personal computers, intelligent television sets, portable telephone sets such as personal information terminal, personal handyphone system (PHS), intelligent telephone sets, and PC cards or the like which has an input/ output function.

Trades in which such terminals are used as an electronic cash-box for a digital cash can be actualized by replacing in the constitution of the data copyright management system, the database with a customer's bank,

BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1679

a first user terminal with a customer, the second user terminal with a retailer, the copyright control center with a retailer's bank and a third user terminal with a wholesaler or a maker.

An example of the trading system will be explained in which the digital cash is transferred via a communication network by using Figure 14.

The example uses the constitution of the data copyright management system shown in Figure 1. In Figure 14, reference numeral 111 represents a customer, 112 a bank of the customer 111, 113 a retail shop, 114 a bank of the retail shop 113, 115 a maker, 116 a bank of the maker 115, 2 a communication network such as a public line provided by a communication enterprise or CATV line provided by a cable television enterprise. Customer 111, the customer's bank 112, the retail shop 113, the retail shop's bank 114, the maker 115, the maker's bank 116 can be mutually connected with the communication network 2. In this system, the customer 111 can use a credit company offering cashing service other than banks and he can also interpose appropriate number of wholesalers between the retail shop and the maker.

In addition, 117 and 118 are either IC cards or PC cards in which digital cash data is stored. The cards are used when the communication network is not used.

Incidentally, in Figure 14, what is represented by a broken line is a path of encrypted digital cash data, what is represented by the solid line is a path of requests from the customer, the retail shop or the maker, and what is represented by a one-dot chain line is a path of the secret-key from each bank.

In this example, first secret-key prepared by the customer's bank 112, the second secret-key generated by the customer, the third secret-key generated by the retail shop, and the fourth secret-key prepared by the maker are used as crypt keys.

Further, while the customer's bank 112, the retail shop's bank 114, and the maker's bank 116 are explained as separate entities, these can be considered as a financial system as a whole.

Digital cash management program P for encrypting and decrypting the digital cash data is preliminarily distributed to the customer 111 and is stored in the user terminal. Further, it is possible to transfer the digital cash management program P together with data every time trade with the bank is executed. Further, it is desirable to install the common digital cash management program P in all banks.

The customer 111 uses the user terminal to designate the amount of money via the communication network 2 to request drawing out from the account of the customer's bank 112 to the bank. At this time, the terminal presents customer information Ic of the customer 111.

The customer's bank 112 which receives the customer's request of drawing out from the account selects or generates the first secret-key Ks1 so that the digital cash data MO of the amount is encrypted by the first secret-key Ks1:

$$CmOks1=E(Ks1, MO)$$

and the encrypted digital cash data CmOks1 and the first secret-key Ks1 for a decrypting key are transferred to the customer 111, and the customer information Ic and the first secret-key Ks1 are stored.

In this case, the first secret-key Ks1 can be selected from what is preliminarily prepared by the customer's bank 112, and also may be generated by presentation of the customer information Ic at the time of drawing by the customer using the digital cash management program P on the basis of the customer information Ic:

$$Ks1=P(Ic).$$

Through this means, the first secret-key Ks1 can be private for the customer 111. At the same time, it is not necessary to transfer the first secret-key Ks1 to the customer 111 so that the safety of the system can be heightened.

Further, the first secret-key Ks1 can be generated on the basis of the bank information Ibs of the customer's bank 112 or on the basis of the bank information Ibs and the date of key generation.

The customer 111 to which the encrypted digital cash data CmOks1 and the first secret-key Ks1 are transferred generates second secret-key Ks2 according to any one or both of the customer information Ic and the first secret-key Ks1 using the digital cash management program P, for example:

$$Ks2=P(Ic)$$

and the generated second secret-key Ks2 is stored in the user terminal.

Further, the customer 111 uses the first secret-key Ks1 to decrypt the encrypted digital cash data CmOks1 with the digital cash management program P:

$$MO=D(Ks1, CmOks1)$$

and the content is confirmed. When the decrypted digital cash data MO whose content is confirmed is stored in the user terminal as a cash-box, it is encrypted by the generated second secret-key Ks2 using the digital cash management program P:

$$CmOKs2=E(Ks2, MO).$$

The first secret-key Ks1 is disused at this time.

The customer 111 who wishes to buy an article from the retail shop 113 decrypts the encrypted digital cash data CmOks2 which is stored in the user terminal as a cash-box by the digital cash management program P using the second secret-key Ks2:

$$MO=D(Ks2, CmOks2)$$

BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1680

and the digital cash data M1 which corresponds to the necessary amount of money is encrypted by the second secret-key ks2 using the digital cash management program P:

$$Cm1ks2=E(Ks2, M1)$$

and then, the payment is made by transmitting the encrypted digital cash data Cm1ks2 to the user terminal as a cash-box of retail shop 113 via the communication network 2.

At this time, the customer information Ic is also transmitted to the user terminal of the retail shop 113.

Further, the residual amount digital cash data M2 is encrypted by the second secret-key Ks2 using the digital cash management program P:

$$Cm2ks2=E(Ks2, M2)$$

and stored in the user terminal of the customer 111.

The retail shop 113 to which the encrypted digital cash data Cm1ks2 and the customer information Ic are transferred stores the transferred encrypted digital cash data Cm1ks2 and customer information Ic in the user terminal, and presents the customer information Ic to the retail shop's bank 114 via the communication network 2 for confirming the content to request the transmission of the second secret-key Ks2 for decription.

The retail shop's bank 114 which is requested by the retail shop 113 to transmit the second secret-key Ks2 transmits the request of the transmission of the second secret-key Ks2 and the customer information Ic to the customer's bank 112.

The customer's bank 112 which is requested to transmit the second secret-key Ks2 from the retail shop's bank 114 generates the second secret-key Ks2 according to the customer information Ic by the digital cash management program P in the case where the second secret-key Ks2 is based only on the customer information Ic, or generates the second secret-key Ks2 according to the customer information Ic and the first secret-key Ks1 by the digital cash management program P in the case where the second secret-key Ks2 is based on the customer information Ic and the first secret-key Ks1, and transmits the generated second secret-key Ks2 to the retail shop's bank 114.

The retail shop's bank 114 to which the second secret-key Ks2 is transmitted from the customer's bank 112 transmits the second secret-key Ks2 to the retail shop 113 via the communication network 2.

The retail shop 113 to which the second secret-key Ks2 is transferred decrypts the encrypted digital cash data Cm1ks2 by the second secret-key Ks2 using the digital cash management program P:

$$M1=D(Ks2, Cm1ks2)$$

and after confirming the amount of money, forwards the article to the customer 111.

Incidentally, in this case, the retail shop 111 can directly requests the transfer of the second secret-key Ks2 to the customer's bank 112 instead of the retail shop's bank 114.

In case where the digital cash received by the retail shop 113 is deposited in the account of the retail shop's bank 114, the customer information Ic is transferred to the retail shop's bank 114 together with the encrypted digital cash data Cm1ks2 via the communication network 2.

The retail shop's bank 114 to which the encrypted digital cash data Cm1ks2 and the customer information Ic are transferred requests the transfer of the second secret-key Ks2 to the customer's bank 112 by transmitting the customer information Ic.

The customer's bank 112, which is requested to transfer the second secret-key Ks2 from the retail shop's bank 114, generates the second secret-key Ks2 according to the customer's information Ic by the digital cash management program P when the second secret-key Ks2 is only based on the customer's information Ic, or generates the second secret-key Ks2 according to the customer's information Ic and the first secret-key Ks1 by the digital cash management program P when the second secret-key Ks2 is based on the customer's information Ic and the first secret-key Ks1, then the generated second secret-key Ks2 is transferred to the retail shop's bank 114.

The retail shop's bank 114, to which the second secret-key Ks2 is transferred from the customer's bank 112, decrypts the encrypted digital cash data Cm1ks2 by the second secret-key Ks2 using the digital cash management program P:

$$M1=D(Ks2, Cm1ks2)$$

and the decrypted digital cash data M1 is deposited in the bank account of the retail shop's bank 114.

In the general trade system, the retail shop 113 stocks products from the maker 115 or from the wholesaler which intervenes between the retail shop 113 and the maker 115. Then the retail shop 113 sells the products to the customer 111. Consequently, a trading form is present between the customer 111 and the retail shop 113 just as between the retail shop 113 and the maker 115.

The handling of the digital cash between the retail shop 113 and the maker 115 is not basically different from the handling of the digital cash which is carried out between the customer 111 and the retail shop 113. Therefore, the explanation there will be omitted for the sake of clarity.

In this digital cash system, the digital cash is handled through banks. As information such as the processed amount of the digital cash, date, and the secret-key demanding party information with respect to the handling of the digital cash is stored in the customer's bank, the residual amount of digital cash and usage history can be grasped.

BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1681

Even in the case where the user terminal which is an electronic cash-box storing the digital cash data cannot be used owing to the loss or the breakage, it is possible to reissue the digital cash on the basis of the residual amount, and usage history kept in the customer's bank.

It is desirable to add a digital signature to the digital cash data for heighten the safety of the digital cash.

In this example, digital cash is added by the customer's information which may be accompanied by digital signature. Therefore, the digital cash in the example can also have a function of settlement system for checques drawn by customers.

Also this system can be applicable to various systems in the international trading such as payment settlement of import/export by a negotiation by a draft using a letter of credit and a bill of lading which have been executed by documents.

In the video conference system, a television picture has been added to the conventional voice telephone set. Recently the video conference system is advanced in which a computer system is incorporated in the video conference system so that the quality of the voice and the picture are improved, and data can be handled at the same time as well as the voice and the picture.

Under these circumstances, security against the violation of the user's privacy and the data leakage due to eavesdropping by persons other than the participants of the conference are protected by the cryptosystem using a secret-key.

However, since the conference content obtained by the participants themselves are decrypted, in the case where participants themselves store the content of the conference and sometimes edit the content, and further, use for secondary usage such as distribution to the persons other than the participants of the conference, the privacy of other participants of the video conference and data security remains unprotected.

In particular, the compression technology of the transmission data is advanced while the volume of the data storage medium is advanced with the result that the possibility is getting more and more realistic that all the content of the video conference is copied to the data storage medium or is transmitted via a network.

In view of the circumstances, the example is intended, when video conference participants perform secondary use, to secure the privacy of other participants and data security by using the aforementioned constitution of the data copyright management system.

This video conference data management system can be actualized, for example, by replacing the database in the data copyright management system constitution shown in Figure 1 with a participant of the video conference, the first user terminal with another participant of the video conference, and the second user terminal with non-participant of the video conference.

An example when utilizing will be explained by using Figure 15.

Referring to Figure 15, reference numeral 121 represents a participant as a host of the video conference, 122 a participant of the video conference as a guest, 123 a non-participant of the video conference as a user, 124 a non-participant of the video conference as another user, 2 a communication network such as a public telephone line provided by the communication enterprise and a CA television line provided by the cable television enterprise or the like. The participant 121 of the video conference is connected to the participant 122 of the video conference via the communication network 2. Further, the participant 122 of the video conference can be connected to the non-participant 123 of the video conference, and the non-participant 123 of the video conference to the non-participant 124 of the video conference, via the communication network 2. Reference numeral 125 and 126 represent a data recording medium.

Referring to Figure 15, what is represented by the broken line is a path of the encrypted video conference content, represented by the solid line is a path requesting the crypt key from the non-participants of the video conference 123 and 124 to the participant of the television conference 121, and represented by the one-dot chain line is a path of crypt keys from the participant of the video conference 121 to the participant of the video conference 122 and the non-participants of the video conference 123 and 124.

In this example, a video conference data management system is described here only the protection for data security and privacy in case of the video conference participant 121 to simplify the explanation, however, it is of course, possible to protect for data security and privacy of the video conference participant 122.

A video conference data management program P for encryption/decryption of the video conference data of the participant 121 including audio and picture is previously distributed to the video conference participant 122 and the video conference non-participants 123 and 124, and is stored in each terminal. This video conference data management program P may be transferred whenever a crypt-key is transferred.

In this example, further, a first secret-key prepared by the video conference participant 121, a second secret-key prepared by the video conference participant 122, a third secret-key prepared by the video conference non-participant 123 and subsequent secret-keys prepared similarly are used as a crypt key.

The video conference participant 121 and the video conference participant 122 perform the video conference by transmitting audio, picture and data (referred to as video conference data on the whole) each other, using each terminal via communication network 2. Before the video conference, the video conference participant 121 generates or selects the first secret-key Ks1 to transfer to the video conference participant 122 prior to the start of the video conference.

The video conference participant 122 receiving the first secret-key Ks1 generates the second secret-key

BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1682

Ks2 by the first secret-key Ks1 using the video conference data management program P:

$$Ks2=P(Ks1).$$

The generated second secret-key Ks2 is stored in the terminal.

The video conference participant 121 encrypts the video conference data MO with the first secret-key Ks1, in the video conference through the communication network 2:

$$CmOks1=E(Ks1, MO)$$

and transfers the encrypted video conference data CmOks1 to the video conference participant 122.

The video conference participant 122 who receives the video conference data CmOks1 encrypted by the first secret-key Ks1 decrypts the video conference data CmOks1 by the first secret-key Ks1:

$$M0=D(ks1, CmOks1)$$

and uses decrypted video conference data MO.

Further, the second secret-key Ks2 is generated based on the first secret-key Ks1 with the video conference data management program P:

$$Ks2=P(Ks1).$$

In the case where the decrypted video conference data MO is stored in the terminal of the participant 122 of the video conference, copied to the data record medium 125, or transferred to the non-participant of the video conference via the communication network 2, the data M is encrypted by the second secret-key Ks2 using the video conference data management program P:

$$Cmks2=E(Ks2, M).$$

The encrypted data Cmks2 is copied to the record medium 125 or supplied to the non-participant of the video conference via the communication network 2, together with the video conference data name or the video conference data number.

The non-participant of the video conference 123 who obtains the encrypted data CmKs2 requests to the participant 121 for the secondary use of the video conference data M from the terminal by specifying the name or number of the video conference data.

The participant 121 of the video conference who receives the request for the second use of the data M finds out the first secret-key Ks1 according to the name or the number of the video conference data name or number to generate the second secret-key Ks2 based on the first secret-key Ks1:

$$Ks2=P(Ks1)$$

and supplies the generated second secret-key Ks2 to the non-participant of the video conference 123.

The non-participant of video conference 123 who receives the second secret-key Ks2 decrypts the encrypted data Cmks2 by the second secret-key Ks2 by using the television conference data management program P:

$$M=D(Ks2, Cmks2)$$

and then, uses decrypted video conference data M.

In the case where the video conference data M is stored in the terminal of the non-participant of the video conference 123, copied to the record medium 126, or transmitted to the non-participant of the video conference 124, the video conference data M is encrypted by the second secret-key Ks2 using the video conference data management program P:

$$Cmks2=E(Ks2, M).$$

Incidentally, the third secret-key Ks3 may be generated on the basis of the second secret-key Ks2 with the video conference data management program P:

$$Ks3=P(Ks2),$$

and the data M can be encrypted with the video conference data management program P by this generated third secret-key Ks3:

$$Cmks3=E(Ks3, M).$$

Claims

1. A data copyright management apparatus used with a user terminal for utilizing digital data,

   said digital copyright management apparatus comprising a central processing unit, a central processing unit bus, read-only semiconductor memory, electrically erasable programmable memory, and read/write memory;

   wherein,

   said central processing unit, said read-only semiconductor memory, said electrically erasable programmable memory, and read/write memory are connected to said central processing unit bus, and a system bus of said user terminal is able to be connected to said central processing unit bus;

   a data copyright management system program, a copyright management program, and user information are stored in said read-only semiconductor memory;

   a second private-key, a permit key, a second secret-key, a copyright management program, and copyright information are stored in said electrically erasable programmable memory; and

   a first public-key, a first private-key, a second

BNSDOCID: <EP__0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1683

public-key, and a first crypt-key are transmitted to said read/write memory during operation.

2. A data copyright management apparatus used with a user terminal for utilizing digital data,

said data copyright management apparatus comprising a central processing unit, a central processing unit bus, read-only semiconductor memory, electrically erasable programmable memory, and read/write memory;

wherein,

said central processing unit, said read-only semiconductor memory, said electrically erasable programmable memory, and said read/write memory are connected to said central processing unit bus, and a system bus of said user terminal is able to be connected to said central processing unit bus;

a data copyright management system program, a copyright management program, crypt algorithm, and user information are stored in said read-only semiconductor memory;

a second private-key, a permit key, a second secret-key, and copyright information are stored in said electrically erasable programmable memory; and

a first public-key, a first private-key, a second public-key, and a first crypt-key are transmitted to said read/write memory during operation.

3. The data copyright management apparatus according to Claim 1 or 2, which is configured in the form of air IC.

4. The data copyright management apparatus according to Claim 1 or 2, which is configured in the form of an IC card.

5. The data copyright management apparatus according to Claim 1 or 2, which is configured in the form of a PC card.

6. The data copyright management apparatus according to Claim 1 or 2, which is configured in the form of an insertion board.

7. A data copyright management apparatus used in a user terminal for decrypting encrypted data to display or edit said data and for re-encrypting decrypted data to store, copy, or transfer said data;

wherein, a computer comprising a microprocessor, a local bus connected to said microprocessor, read-only semiconductor memory and read/write memory connected to said local bus is configured;

whereby, one of the microprocessor of said user terminal and the microprocessor of said data copyright management apparatus performs decryption and the other performs re-encryption.

8. A data copyright management apparatus used in a user terminal for decrypting encrypted data to display or edit said data and for re-encrypting decrypted data to store, copy, or transfer said data;

said data copyright management apparatus comprising a first microprocessor and a second microprocessor;

wherein, a first computer comprising a first local bus connected to said first microprocessor, and first read-only semiconductor memory arid first read/write memory connected to said first local bus; and,

a second computer comprising a second local bus connected to said second microprocessor, and second read-only semiconductor memory and second read/write memory connected said second local bus are configured;

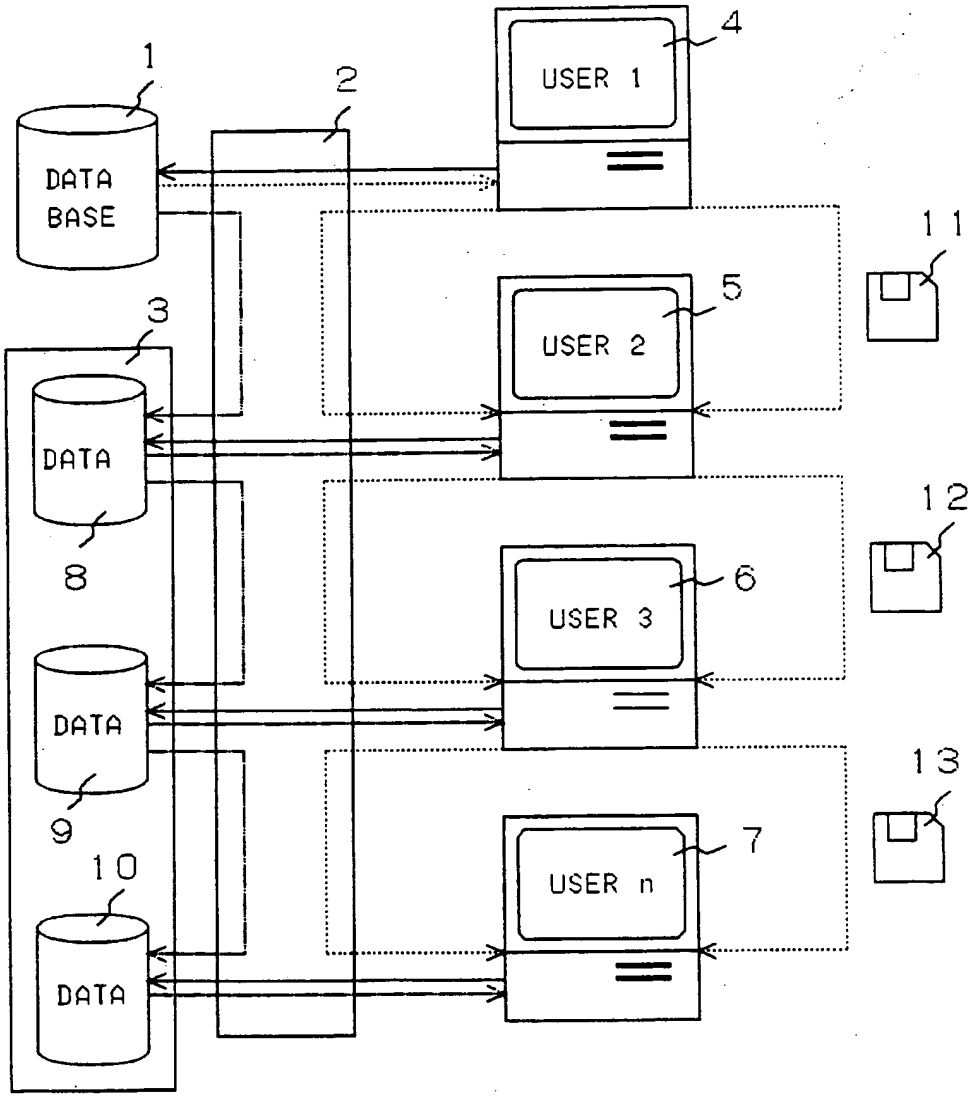
whereby, said first microprocessor decrypts encrypted data, and

said second microprocessor re-encrypts decrypted data.

BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1684

Fig. 1



BNSDOCID: <EP___0715241A2_I_>~

Petitioner Apple Inc. - Exhibit 1012, p. 1685

Fig. 2

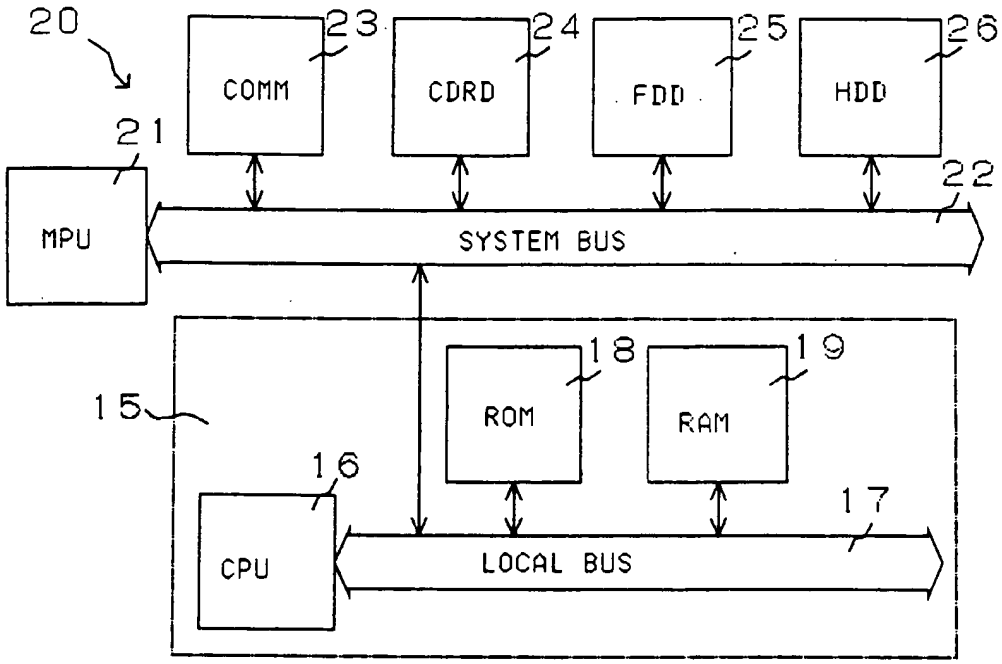
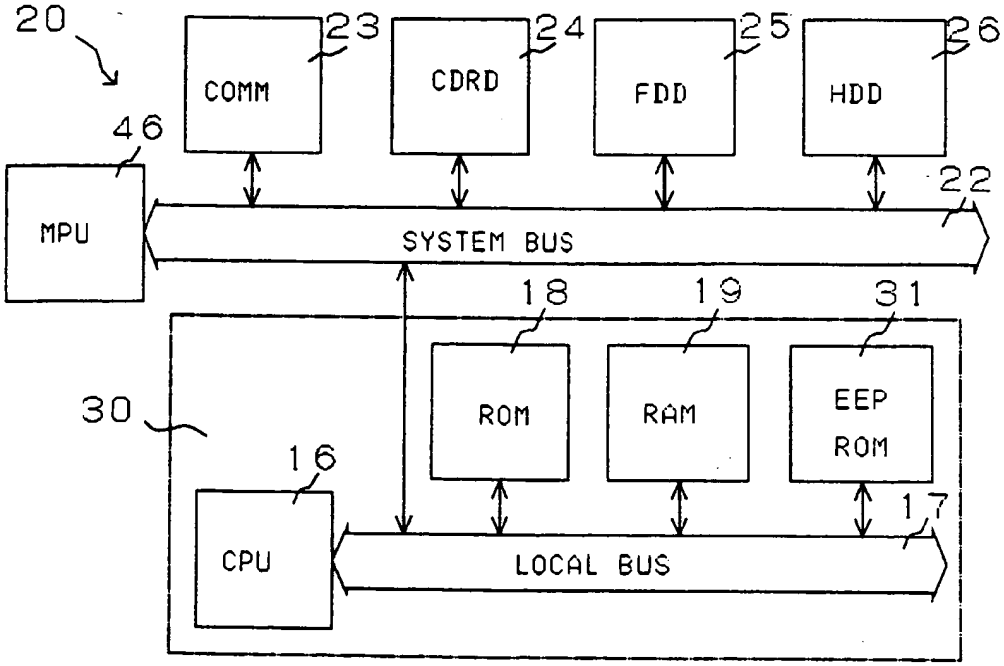


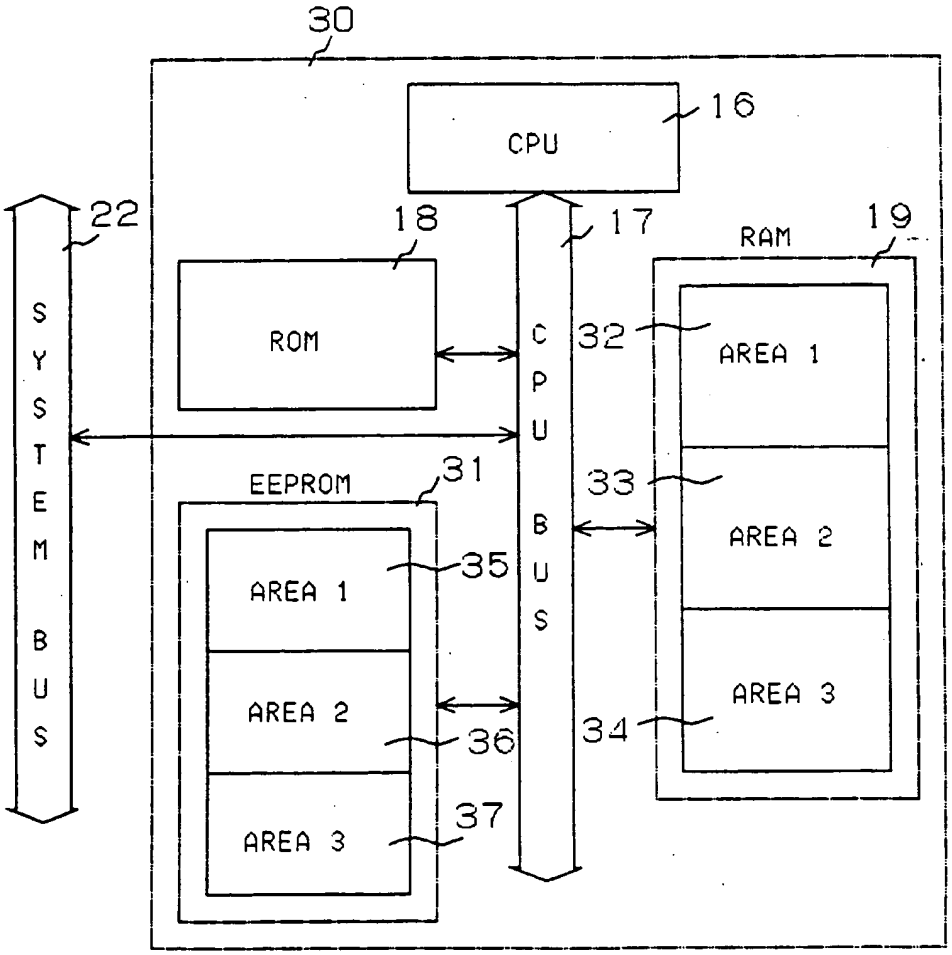
Fig. 3



BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1686

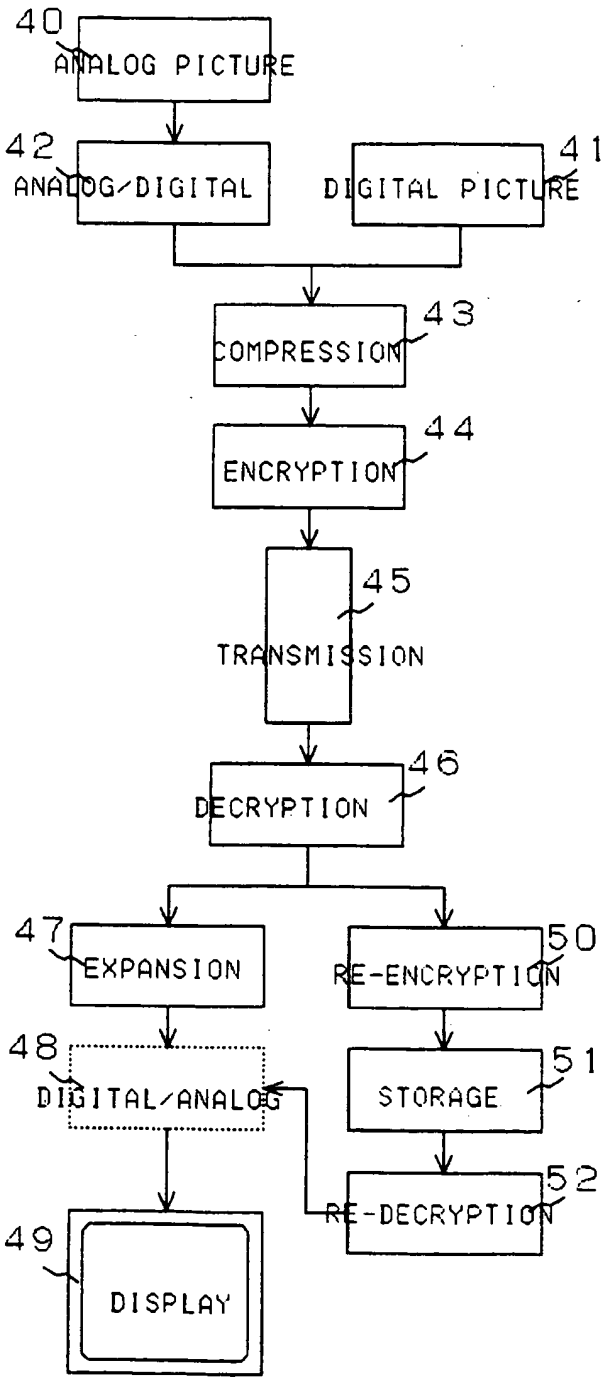
Fig. 4



BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1687

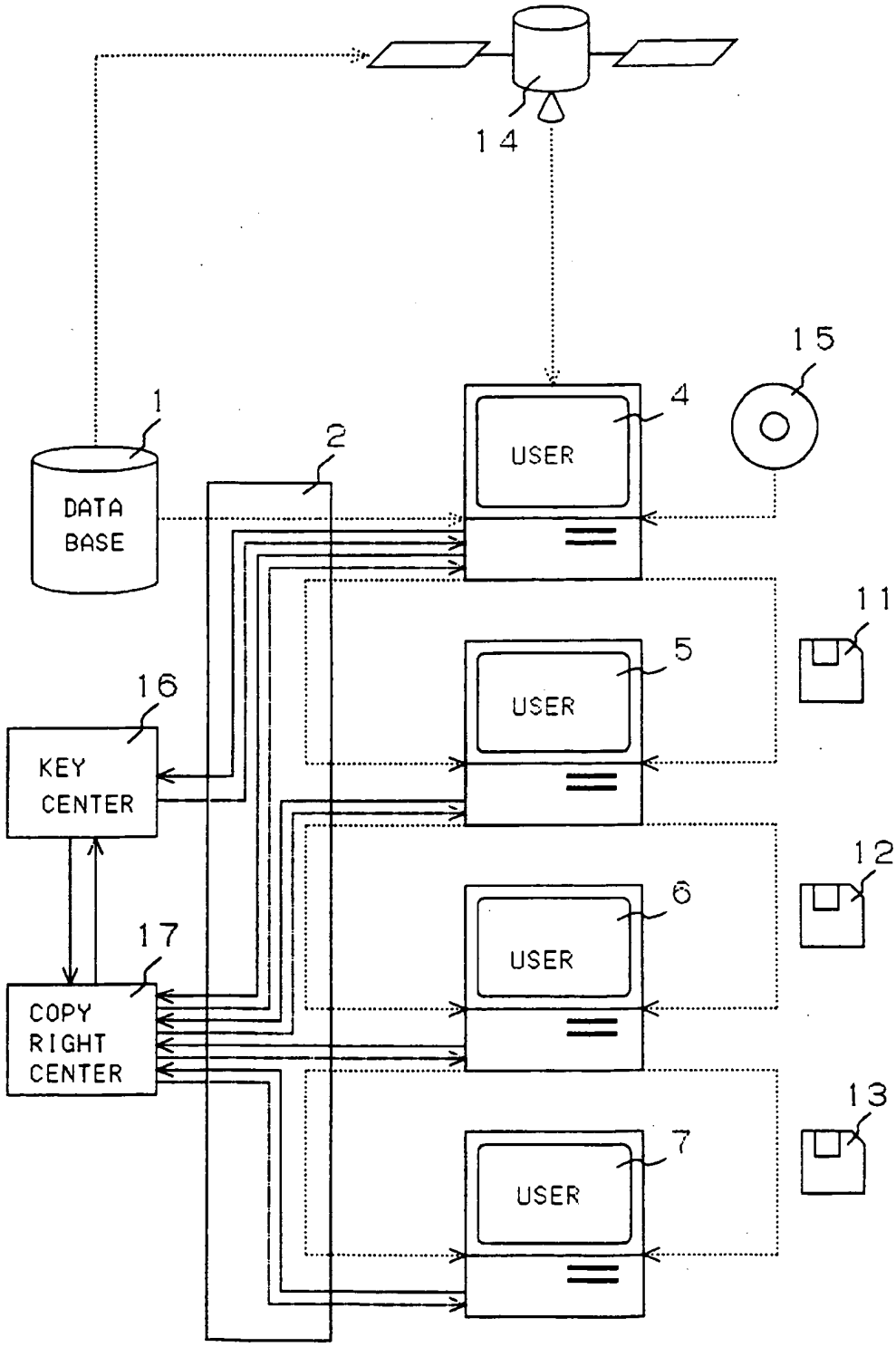
Fig. 5



BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1688

Fig. 6



BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1689

Fig. 7

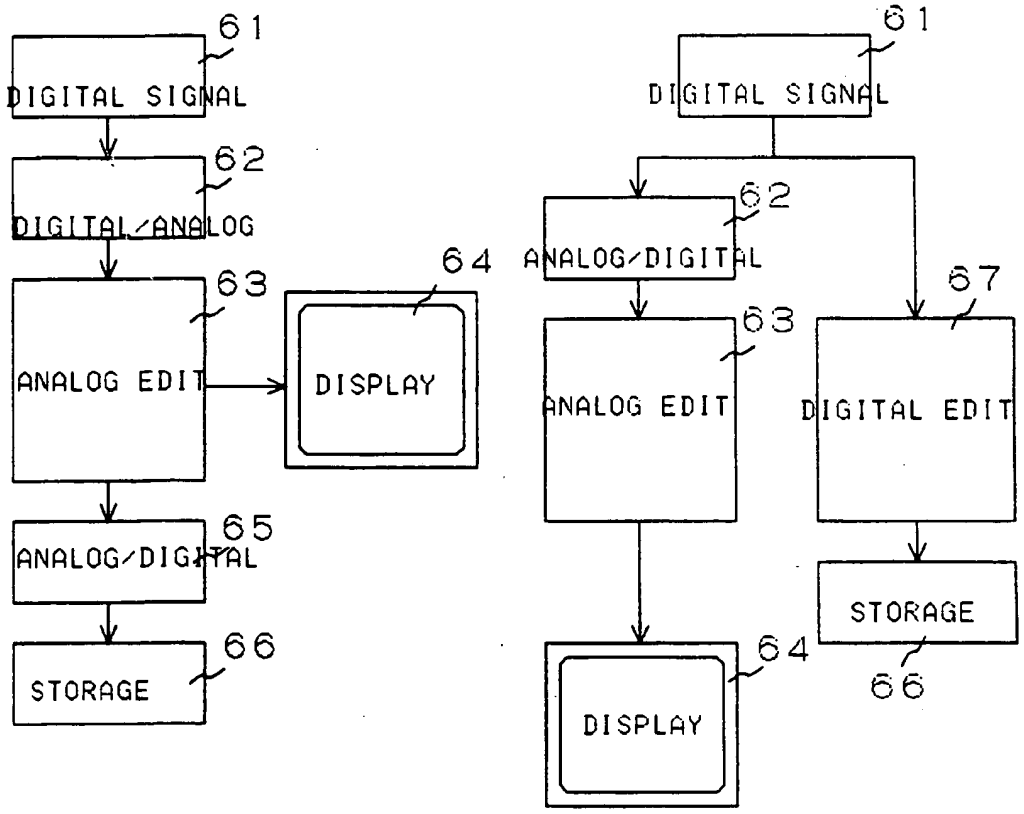


Fig. 7(a) Fig. 7(b)

BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1690

Fig. 8

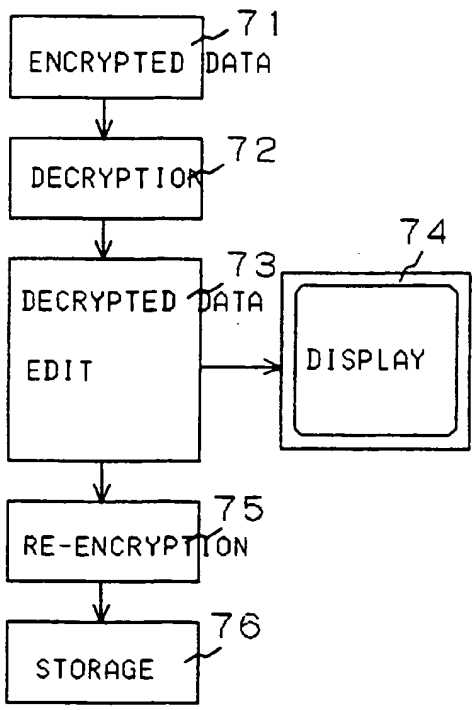


Fig. 8(a)

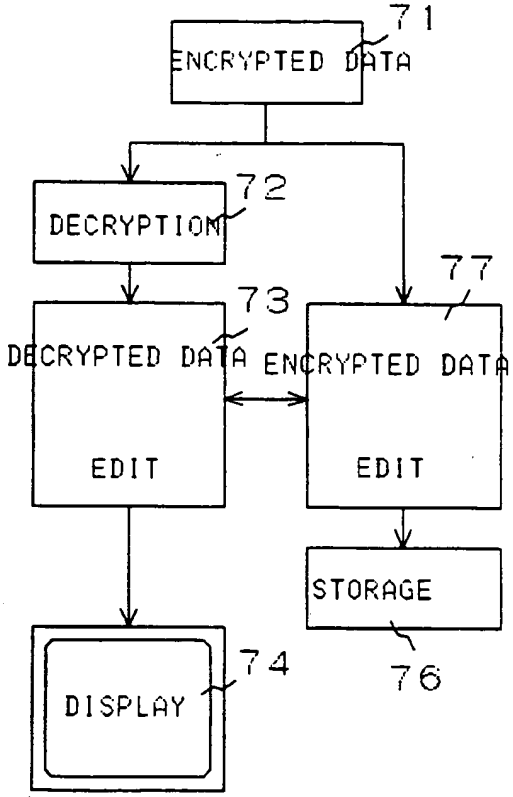
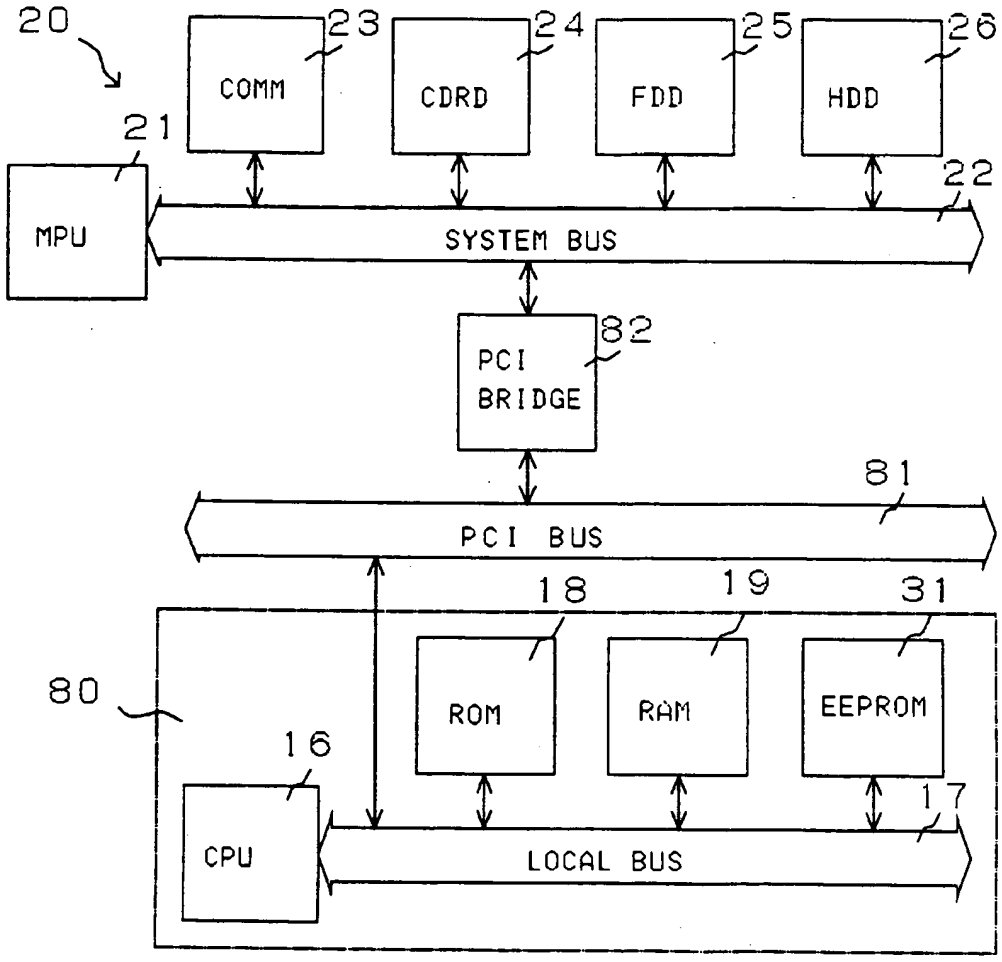


Fig. 8(b)

BNSDOCID: <EP__0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1691

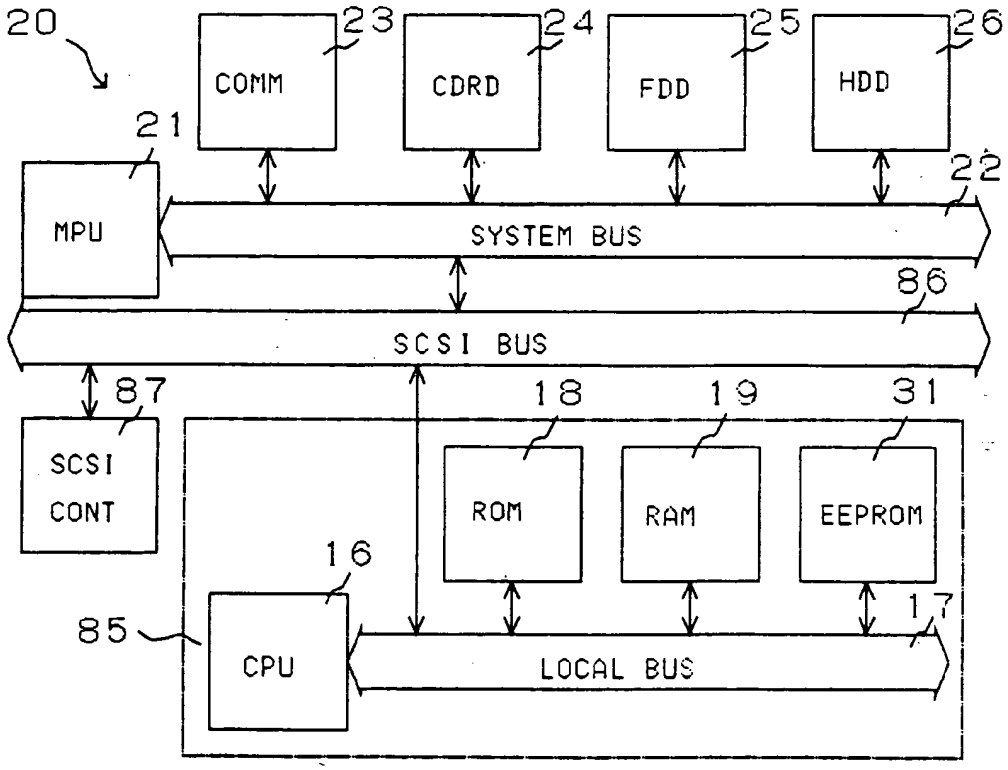
Fig. 9



BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1692

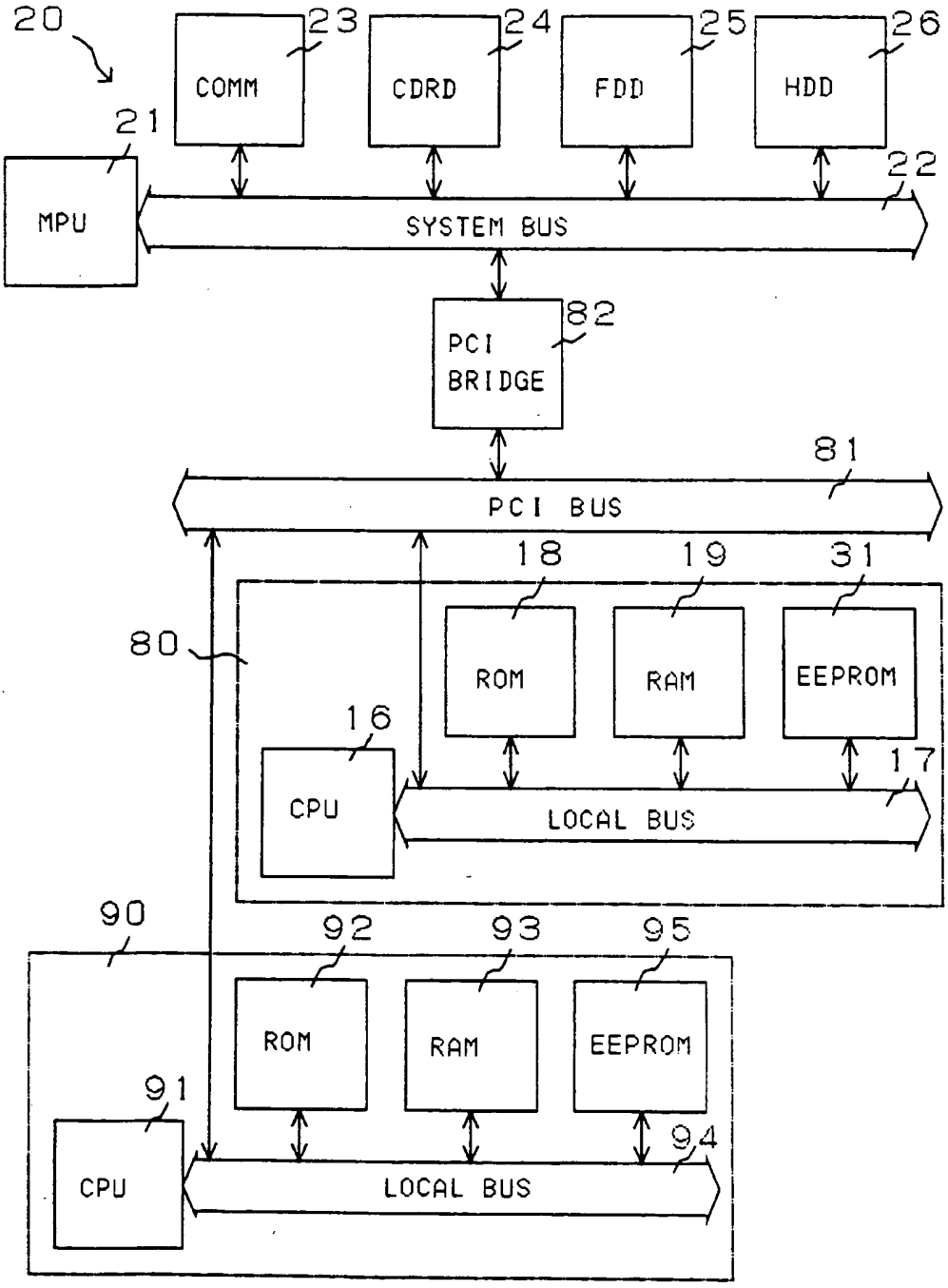
Fig. 10



BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1693

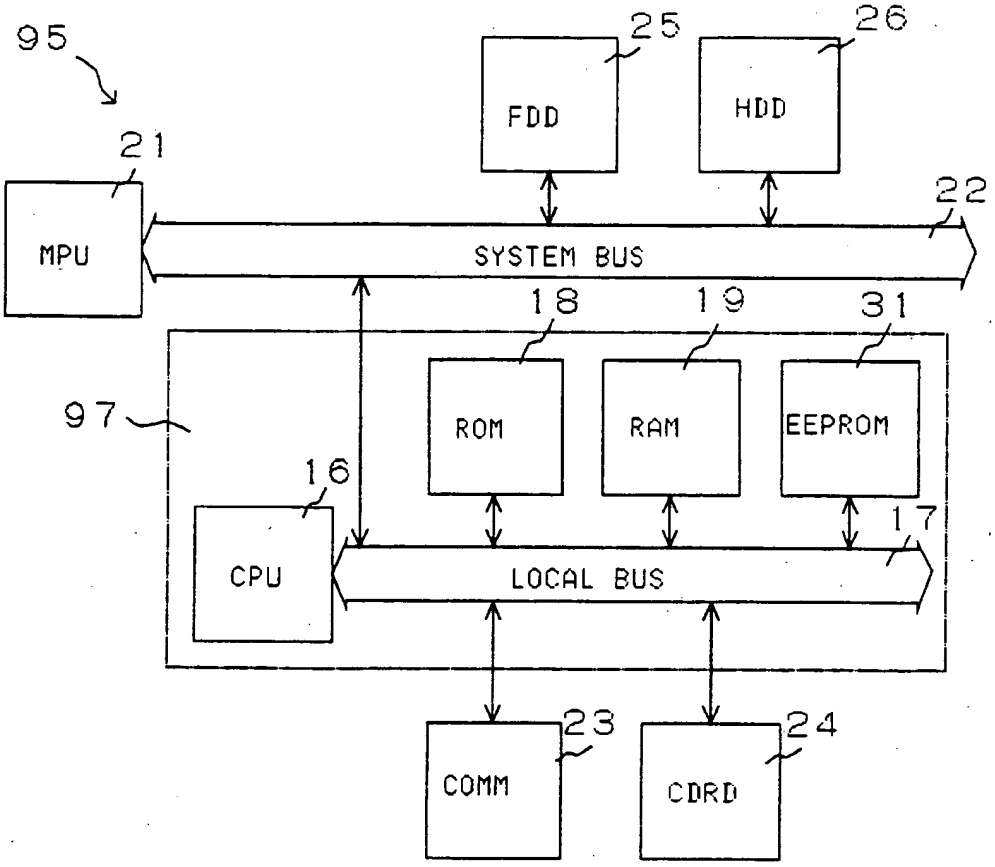
Fig. 11



BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1694

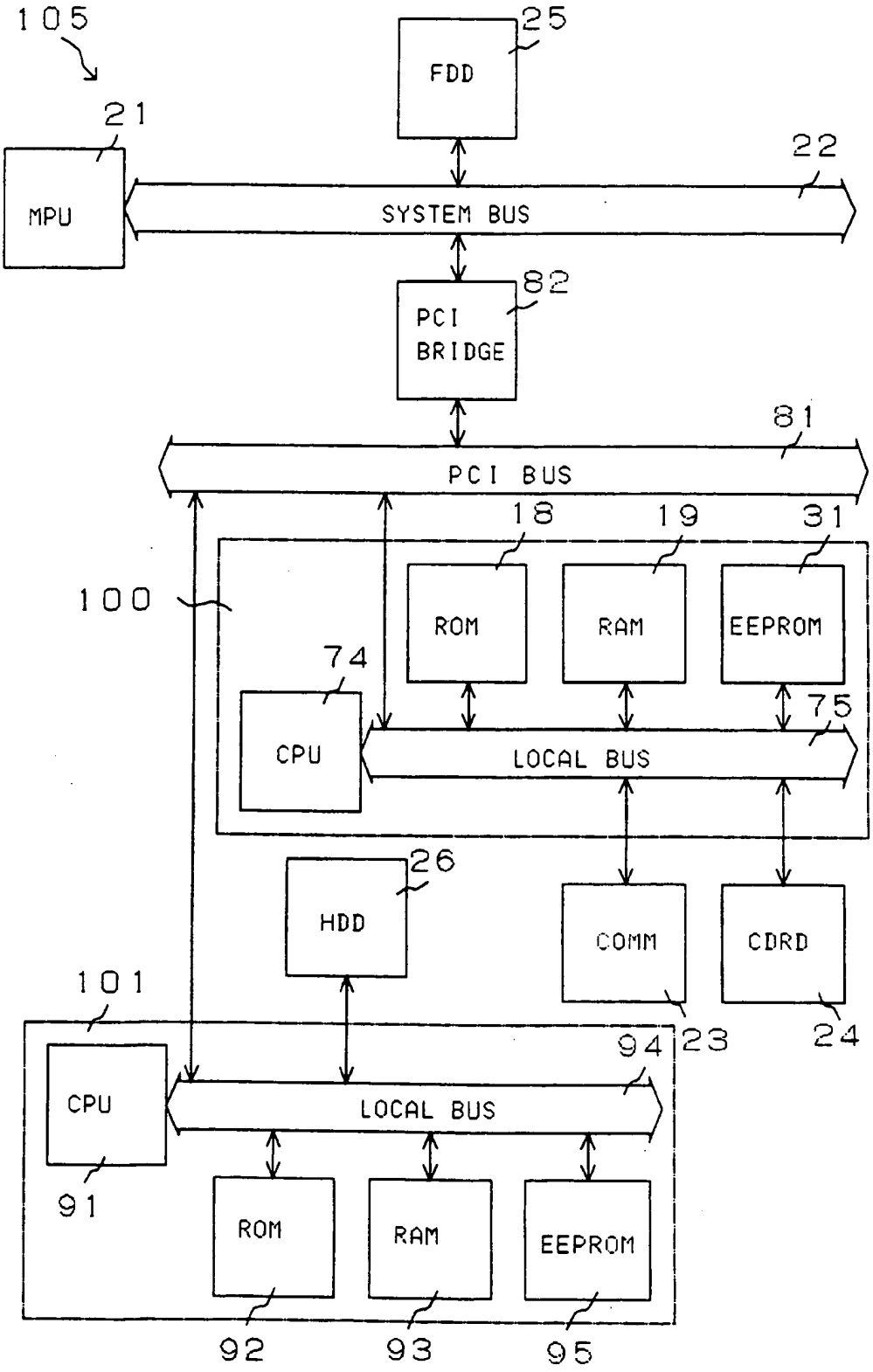
Fig. 12



BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1695

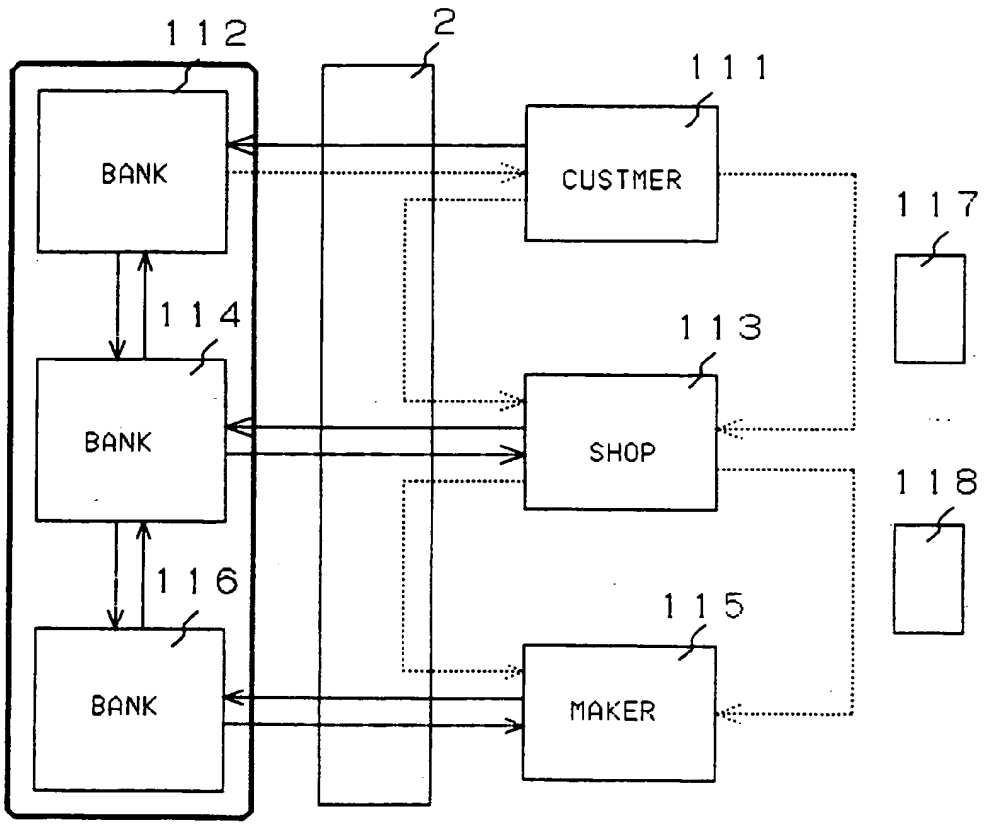
Fig. 13



BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1696

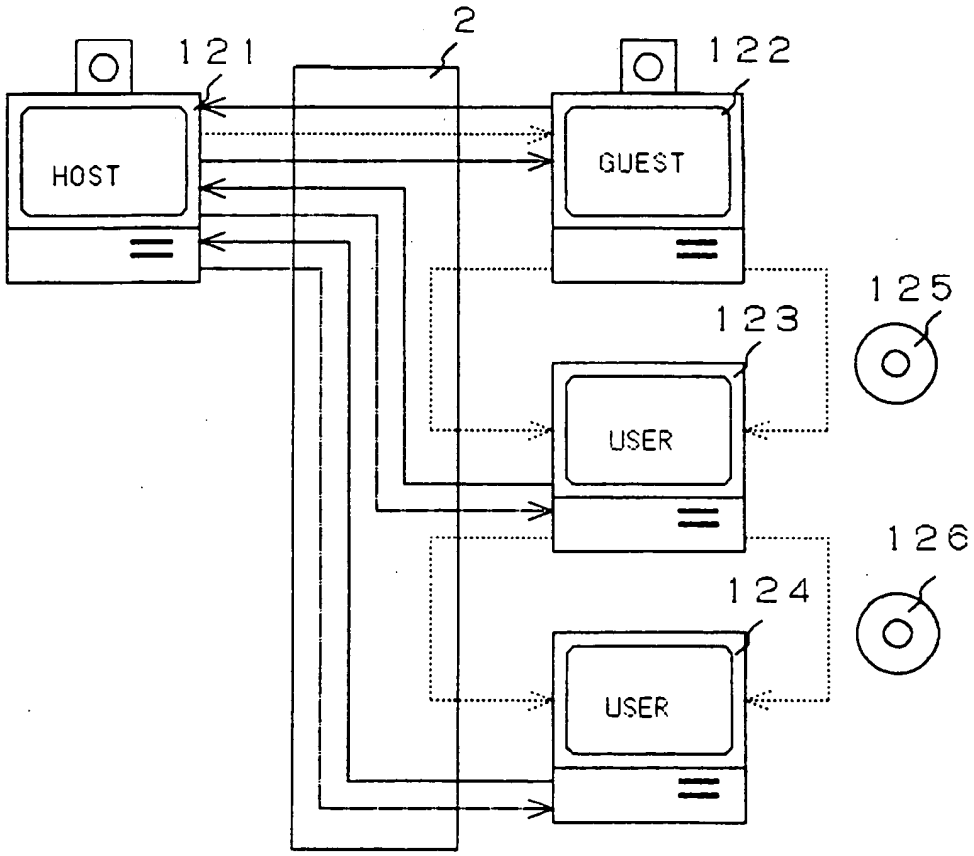
Fig. 14



BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1697

Fig. 15



BNSDOCID: <EP___0715241A2_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1698

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 715 241 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
03.02.1999 Bulletin 1999/05

(43) Date of publication A2:
05.06.1996 Bulletin 1996/23

(21) Application number: **95116615.6**

(22) Date of filing: **21.10.1995**

(51) Int. Cl.[6]: **G06F 1/00**, H04N 7/167

(84) Designated Contracting States:
DE FR GB

(30) Priority: **27.10.1994 JP 264200/94**
02.12.1994 JP 299835/94

(71) Applicant:
MITSUBISHI CORPORATION
Chiyoda-ku Tokyo 100 (JP)

(72) Inventors:
- **Saito, Makoto**
  Tama-shi, Tokyo (JP)
- **Momiki, Shunichi**
  Higashimur-ayama-shi, Tokyo (JP)

(74) Representative:
Neidl-Stippler & Partner
Rauchstrasse 2
81679 München (DE)

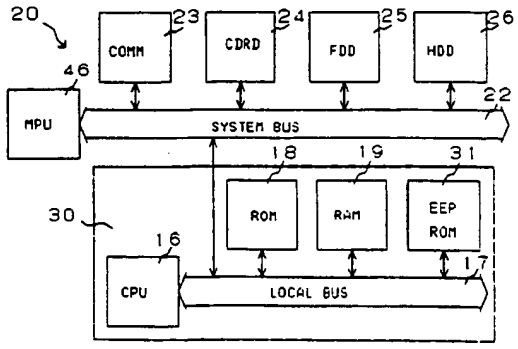
(54) Apparatus for data copyright management system

(57) A data copyright management apparatus is used with a user terminal and comprises a CPU, a CPU bus, ROM, EEPROM, and RAM.

The CPU, ROM, EPROM, and RAM are connected to the CPU bus, and a system bus of a device which utilizes the data can be connected to the CPU bus. A data copyright management system program, a crypt algorithm, and user information are stored in the ROM, and a second private-key, a permit key, a second secret-key, and copyright information are stored in the EEPROM. A first public-key, a first private-key, a second public-key, and a first secret-key are transmitted to the RAM during the operation. The data copyright management apparatus may be configured in the form of a monolithic or hybrid IC, a thin IC card, PC card, or an expansion board. If the copyright management program is provided from the outside, then it is stored in the EEPROM, otherwise it is stored in ROM.

In addition to a microprocessor in the user terminal which decrypts encrypted data for displaying and processing purposes and re-encrypts the decrypted data for storing, copying, or transferring purposes, at least one other microprocessor, desirably two other microprocessors, are added for decrypting and re-encrypting data. The microprocessors to be added may be connected to the system bus of the microprocessor of the user terminal. However, to allow concurrent microprocessor operation it is desirable that the multiprocessor configuration is implemented by using a SCSI bus, PCI bus, or SCI bus. The data copyright management apparatus may be implemented in the form of a monolithic IC, a hybrid IC, or a built-in subboard, and the apparatus in these forms is incorporated in a computer, television set, set-top box, digital video tape recorder, digital video disk recorder, digital audio tape apparatus, or personal digital assistants, and the like.

Fig. 3



EP 0 715 241 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 95 11 6615

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
A	EP 0 430 734 A (SCHLUMBERGER IND SA) 5 June 1991 * column 3, line 17 - line 37 * * column 4, line 4 - column 5, line 24; figures 1,2 *	1,2,4,7, 8	G06F1/00 H04N7/167
A	WO 90 02382 A (INDATA CORP) 8 March 1990 * page 35, paragraph 2 - page 38, paragraph 4; figures 10,12 *	1,2,7,8	
A	EP 0 121 853 A (BURROUGHS CORP) 17 October 1984 * page 3, line 30 - page 4, line 12; figure 1 *	1,2,7,8	
A	US 4 352 952 A (BOONE CHARLES A ET AL) 5 October 1982 * abstract; figures 1,2 *	7,8	

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

G06F
H04N

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	1 December 1998	Moens, R

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

BNSDOCID: <EP___0715241A3_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1700

EP 17424 (2)

PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00

A1

(11) International Publication Number: **WO 98/42098**

(43) International Publication Date: 24 September 1998 (24.09.98)

(21) International Application Number: PCT/US98/04658

(22) International Filing Date: 11 March 1998 (11.03.98)

(30) Priority Data:
08/818,132 14 March 1997 (14.03.97) US

(71) Applicant: CRYPTOWORKS, INC. [US/US]; 2084 Union Street, San Francisco, CA 94123 (US).

(72) Inventor: LeBOURGEOIS, John, H.; 193 San Carlos Way, Novato, CA 94945 (US).

(74) Agent: WOLFELD, Warren, S.; Fliesler, Dubb, Meyer and Lovejoy LLP, Suite 400, Four Embarcadero Center, San Francisco, CA 94111–4156 (US).

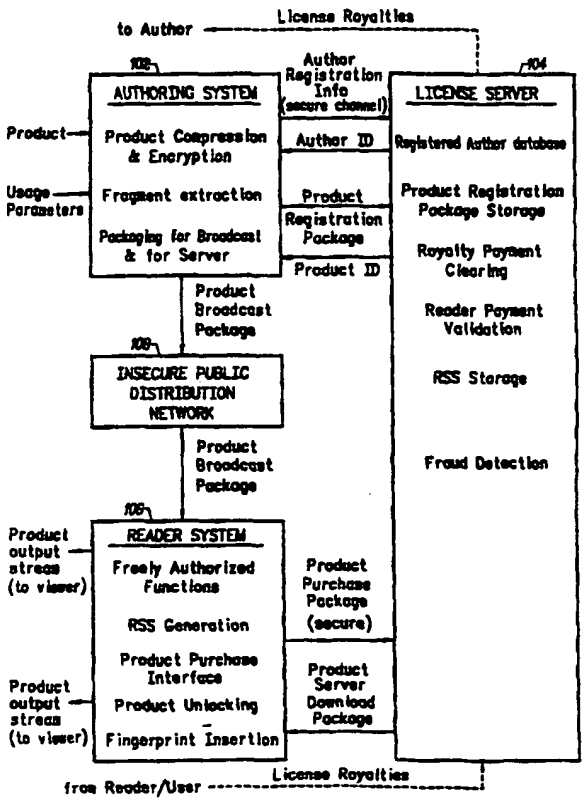
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: DIGITAL PRODUCT RIGHTS MANAGEMENT TECHNIQUE

(57) Abstract

A digital product is freely distributed through uncontrolled channels in encrypted form (108). Security fragment(s) of the encrypted product are withheld (102), and provided only upon communication with license server (104). The customer uses reader software (106) to purchase a license. Such software (106) examines components then present on the reader system to develop a reader system signature, which the license server (106) uses to encrypt the product decryption key and the security fragments before sending them to the reader system. When the customer wishes to use the product, a new reader system signature is generated and used to decrypt the product fragments.



Petitioner Apple Inc. - Exhibit 1012, p. 1701

FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	ES	Spain	LS	Lesotho	SI	Slovenia
AM	Armenia	FI	Finland	LT	Lithuania	SK	Slovakia
AT	Austria	FR	France	LU	Luxembourg	SN	Senegal
AU	Australia	GA	Gabon	LV	Latvia	SZ	Swaziland
AZ	Azerbaijan	GB	United Kingdom	MC	Monaco	TD	Chad
BA	Bosnia and Herzegovina	GE	Georgia	MD	Republic of Moldova	TG	Togo
BB	Barbados	GH	Ghana	MG	Madagascar	TJ	Tajikistan
BE	Belgium	GN	Guinea	MK	The former Yugoslav Republic of Macedonia	TM	Turkmenistan
BF	Burkina Faso	GR	Greece			TR	Turkey
BG	Bulgaria	HU	Hungary	ML	Mali	TT	Trinidad and Tobago
BJ	Benin	IE	Ireland	MN	Mongolia	UA	Ukraine
BR	Brazil	IL	Israel	MR	Mauritania	UG	Uganda
BY	Belarus	IS	Iceland	MW	Malawi	US	United States of America
CA	Canada	IT	Italy	MX	Mexico	UZ	Uzbekistan
CF	Central African Republic	JP	Japan	NE	Niger	VN	Viet Nam
CG	Congo	KE	Kenya	NL	Netherlands	YU	Yugoslavia
CH	Switzerland	KG	Kyrgyzstan	NO	Norway	ZW	Zimbabwe
CI	Côte d'Ivoire	KP	Democratic People's Republic of Korea	NZ	New Zealand		
CM	Cameroon			PL	Poland		
CN	China	KR	Republic of Korea	PT	Portugal		
CU	Cuba	KZ	Kazakstan	RO	Romania		
CZ	Czech Republic	LC	Saint Lucia	RU	Russian Federation		
DE	Germany	LI	Liechtenstein	SD	Sudan		
DK	Denmark	LK	Sri Lanka	SE	Sweden		
EE	Estonia	LR	Liberia	SG	Singapore		

BNSDOCID: <WO___9842098A1_I_>

DIGITAL PRODUCT RIGHTS MANAGEMENT TECHNIQUE

BACKGROUND

1. Field of the Invention

The invention relates to controlled distribution of digital products in a manner that tends to ensure that authors receive proper royalty payments for their work.

2. Description of Related Art

Digitally encoded products, such as software, music, images and video segments are extremely important in today's economy. However, the ease and economy with which perfect copies can be made of digitally encoded products has promoted the widespread unauthorized copying and distribution of such products through such channels as user-to-user copying and sharing, digital data networks such as the Internet, and CD-ROM publishing. These distribution channels have made it difficult for the creators and copyright holders of such products to regulate the use of their products or to receive payment and registration information from their users. Consequently, digital product producers often forfeit substantial revenues and valuable information about their customer base and potential markets, while businesses and universities find themselves subject to legal prosecution and intimidation for copyright infringement.

But the problem of unauthorized distribution of digital products is not limited to the simple loss of revenues which rightfully belong to the original developer of the product, although that problem can be substantial by itself. There is also the additional problem that developers will be less willing to spend

Petitioner Apple Inc. - Exhibit 1012, p. 1703

substantial time and money in developing new digital products if they cannot depend on a market which pays fair value for their products.

In the past, when copying and distribution of products was more expensive, time consuming and imperfect, the creators of digital products could depend in part on economic factors as well as legal protections to minimize unauthorized copying and distribution. Neither is effective today with digital products, easy and inexpensive channels of distribution, and huge numbers of people participating in the illicit trade.

One technique that has been developed to deter unauthorized copying of digital products involves copy protection mechanisms built into hardware or software. However, copy protection mechanisms sometimes can inconvenience users who have a legitimate need for making copies. Copy protection mechanisms also can prevent digital product developers from taking advantage of the new distribution channels, such as the Internet.

Another method for controlling the distribution of digital products is described in Commerce Direct International (CDI), "Electronic Commerce", World Wide Web URL http://www.cdi.net/electron/commerce.htm (visited March 23, 1996) and CDI, "CDI In Action", World Wide Web URL http://www.cdi.net/cdiactio/cdinactn.htm (visited March 23, 1996), both incorporated herein by reference. The mechanisms described in these documents call for a customer to review an on-line catalog of products and choose one to buy. The customer's software then sends encrypted credit card information to the product distributor, and the product distributor transmits the product to the customer in a strongly

Petitioner Apple Inc. - Exhibit 1012, p. 1704

encrypted form. The customer's software then uses a "secret key" to decrypt the product and use it. Secure direct modem connections may be used instead of Internet connections at various parts of the process in order to further ensure that no one else can use the encrypted product.

The CDI technique suffers from at least two problems. First, while the encryption of a data product during transmission may be very strong, it is still theoretically possible for an unauthorized third party to decipher it. Second, even if the product remains secure during transmission, once it is decrypted by the customer, CDI's strong encryption techniques no longer protect the product against further unauthorized distribution. The above-cited documents indicate that content as well as executables can be "locked" to a specific registered machine while still allowing for unrestricted distribution of the software in a crippled or time-dated mode, but the documents do not explain how this is to be accomplished.

In Schull U.S. Patent No. 5,509,070, incorporated by reference herein, Schull describes a technique for distributing digital products (specifically software) by selling a password to the user. The user uses the password to unlock advanced features of the product, but the password is usable only on one machine. Thus, the technique allows users to freely distribute software to other machines and other potential users, but does not allow other users to take advantage of advanced features of the software without obtaining a new password which is specific to the new machine. In the Schull method, the user generates a "passwordable-ID" either from the user's voice, by reading the serial

Petitioner Apple Inc. - Exhibit 1012, p. 1705

number of the machine's CPU, or by any of a number of other suggested methods. The passwordable-ID is transmitted to a licensing system which uses the passwordable-ID to generate an encrypting seed for the software advanced features. The encrypted encrypting seed is then transmitted back to the user as a key for unlocking the advanced features of the software.

One drawback of the Schull method is that the password ultimately provided by the licensing system to the user is stored on the user's machine. Without certain extraordinary copy protection mechanisms applied to the password, the password could simply be copied to a new machine, thereby allowing a different user to use the advanced features of a pirated version of the product without paying a fair licensing fee. The extraordinary methods suggested by Schull to protect the password as stored on the user's machine, reimposes many of the same problems that formed the basis for finding non-objectionable copy protection mechanisms in the first place.

Several other technologies for preventing unauthorized distribution of digital products are set forth in the following World Wide Web pages: Northeast Consulting Resources, Inc., "Digital Rights Management Technologies", Web page URL http://www.ncri.com/articles/rights_management/ (October 1995: visited November 19, 1996); Intertrust Technologies Corporation, Web pages http://www.intertrust.com/architecture/overview.html, http://www.intertrust.com/architecture/flow.html, http://www.intertrust.com/architecture/stc.html, http://www.intertrust.com/products/applications.html, http://www.intertrust.com/products/sdk.html, http://www.intertrust.com/about/whoweare.html, http://www.intertrust.com/about/vision.html (all

Petitioner Apple Inc. - Exhibit 1012, p. 1706

visited November 19, 1996, and all incorporated herein by reference). However, all of the technologies described in these references suffer from one or all of the problems mentioned above, as well as others.

Accordingly, there is a deeply felt need for a new technology which will control the distribution of digital products via the Internet and other uncontrolled distribution channels such that a fair return to the originator of the product can be ensured without unduly hampering wide and free distribution of sufficient information about the digital product to enable customers to decide whether to purchase a license.

SUMMARY OF THE INVENTION

According to the invention, roughly described, a digital product is freely distributed through uncontrolled channels in encrypted form. Unencrypted preview material may also be provided in order to help the customer decide whether to purchase a license. In an aspect of the invention, one or more fragments of the encrypted product are withheld from uncontrolled distribution, and provided only upon communication with a license server. Unlike prior art mechanisms, which rely on practical limitations of computing power in order to prevent unauthorized product decryption, the technique of the present invention renders it literally impossible for an eavesdropper to recover the complete decrypted product without contacting the licensor. The product is not merely encrypted; to the extent of the security fragments, it is not even there.

In a second aspect of the invention, again roughly described, the customer purchases a license through the use of reader software which examines the

Petitioner Apple Inc. - Exhibit 1012, p. 1707

components then present on the reader system to develop a reader system signature (RSS). The reader system signature is transmitted to a license server which uses it either to encrypt the product decryption key, or to further encrypt the security fragments, or both, before sending them to the reader system. The reader system signature is not stored on the reader system. Rather, at the time that the customer would like to use the digital product (view an image or movie, listen to a sound or execute software, for example), a new reader system signature is generated in the same manner as the original reader system signature. The new reader system signature is used to decrypt the product decryption key and/or the double-encrypted security fragments, only at the time of use. If the user is attempting to use the digital product on a different machine, such as would be the case in the event of unauthorized distribution, then the new reader system signature will not work properly and the unauthorized user will not be able to use the digital product.

The above second aspect of the invention could be problematical in the event that the user upgrades or modifies the reader system. A mechanism that regenerates the reader system signature each time a digital product is to be used could prevent a legitimate user from using the product after such an upgrade. Accordingly, in another aspect of the invention, the machine authorization of the reader system allows a certain amount of "upgrade drift" before it is deemed advisable to check for unauthorized use.

In an embodiment, the reader system signature is determined by examining various components (hardware and/or software) of the reader system, to determine individual signatures for each component. The

Petitioner Apple Inc. - Exhibit 1012, p. 1708

individual component signatures are then combined to form the overall reader system signature, for example by a weighted sum of the individual component signatures or by concatenating the individual component signatures together. If the reader system signature is determined on the basis of a weighted sum (or equivalently, a weighted average) of the individual component signatures, then the amount of permissible upgrade drift can be expressed as a percentage; that is, if the reader system signature generated upon usage of the digital product differs from the reader system signature generated at the time the product is purchased by no more than a predetermined percentage or fraction, then the usage is considered authorized. If the reader system signature is generated as a concatenation of the individual component signatures, then the number of components which differ at usage time relative to purchase time can be specified not to exceed a specific count.

In a situation where the reader system signature generated at the time of purchase is not stored on the reader system, it can instead be uploaded to a license server. If the reader system signature generated at usage time is found by the reader system not to properly decrypt either the product decryption key or the product itself, then in an embodiment, the reader system can automatically contact the license server for reauthorization. The reader system uploads the newly generated reader system signature, and the license server performs the upgrade drift test in comparison with the reader system signature that was stored on the license server at the time of purchase. If the license server determines that the newly generated reader system signature is within the permissible upgrade

Petitioner Apple Inc. - Exhibit 1012, p. 1709

drift parameter, then it transmits a new product decryption key and/or new product security fragments, back to the reader system, encrypted according to the new reader system signature. The reader system is then able to decrypt the digital product and play, view or otherwise use it in the desired manner. (In order to assist in evaluating the permissibility of an upgrade drift, one embodiment of the reader system also uploads the raw component signatures of the computer system. This allows customer support to determine which components have changed.)

In an embodiment of the invention, the reader system signature is generated in dependence upon a component whose individual component signature carries with it external assurances of substantial uniqueness among all computer systems which could reasonably pose as authorized reader systems. Such a component signature can be used by itself, or in conjunction with other component signatures, in order to generate the overall reader system signature. If used by itself, then upgrade drift is usually not permissible without manual re-validation.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will be described with respect to particular embodiments thereof, and reference will be made to the drawings, in which:

Fig. 1 is an overall symbolic diagram of a system according to the invention.

Fig. 2 is a block diagram illustrating the structure of a typical reader system of Fig. 1.

Fig. 3 illustrates the overall system flow for the authoring system of Fig. 1.

Petitioner Apple Inc. - Exhibit 1012, p. 1710

Fig. 4 is a flow chart illustrating the flow of a product registration segment of Fig. 3.

Fig. 5 is a flow chart illustrating the general operation of the reader system of Fig. 1.

Fig. 6 is a flow chart of the product purchase preparation step of Fig. 5.

Fig. 7 is a flow chart illustrating one technique for generating the reader system signature.

Figs. 8 and 9 together constitute a flow chart of steps which takes place in the license server 104 in response to receipt of a product purchase package.

Fig. 10 is a flow chart of the step in Fig. 8 in which the license server processes the customer's payment information.

Figs. 11-13 together constitute a flow chart of the step in Fig. 5 in which the reader system plays the digital product.

Fig. 14 is a flow chart illustrating the license server's operations in response to receipt of a re-validation package.

Figs. 15 and 16 are alternative details of the step in Fig. 14 in which the license server determines whether the difference between the two RSS's exceeds a threshold.

DETAILED DESCRIPTION

Fig. 1 is an overall symbolic diagram of a system according to the invention. The system has three primary components: an authoring system 102, a license server 104 and a reader system 106. In addition, the overall system is most useful when used with an uncontrolled distribution channel such as an insecure public distribution network 108 (e.g., the Internet). In general operation, the author or proprietor of one

Petitioner Apple Inc. - Exhibit 1012, p. 1711

or more digital products first uses the authoring system 102 to register with the license server 104 as an author. Author registration information is transmitted from the authoring system 102 to the license server 104, and an author ID is returned to the authoring system.

When the author has a digital product to market, the product is provided to the authoring system 102, together with certain usage parameters. The usage parameters include a set of free usage parameters and one or more sets of paid usage parameters. The authoring system compresses and encrypts the digital product (compression is optional), extracts one or more security fragments from the encrypted product and then packages the product for broadcast via the uncontrolled distribution network 108 and for upload to the license server 104. The authoring system then transmits the product registration package up to the license server 104 and receives a product ID in return. The authoring system also makes the product broadcast package available on the uncontrolled distribution network 108. Note that as used herein, a "product" can include one or more sub-products, all of which are considered herein to themselves be "products".

When a customer is interested in a particular digital product, he or she can download the product broadcast package from the uncontrolled distribution network 108. The customer utilizes the reading system 106 to perform those functions of the digital product which are freely authorized according to the free usage parameters that were previously specified by the author. Such functions can include, among other things, a preview of the digital product, and an indication of one or more licensing options which the

Petitioner Apple Inc. - Exhibit 1012, p. 1712

customer can purchase. If the customer chooses to purchase one of the license options, the reader system 106 examines certain components of the reader system and, in dependence thereon, generates a reader system signature (RSS). The reader system assembles a product purchase package including the RSS and payment information, and uploads it to the license server 104. The license server 104 processes the payment information and, if successful, transmits a product server download package back to the reader system. The reader system uses the product server download package to unlock the functions of the digital product which are authorized under the license option that the customer has purchased, and allows the user to use the product accordingly. In addition, the reader system 106 performs fingerprint and/or watermark insertion as described hereinafter.

The license server 104 performs a number of functions, including maintaining a database of registered authors and storing all of the product registration packages. The license server 104 also stores reader system signatures from customers, performs customer payment validation, as well as certain fraud detection functions as described below. The license server 104 also performs the functions of royalty payment clearing. Specifically, license royalties received from (or on behalf of) customers are properly accounted for and transferred to the proper authors after deduction of a commission.

In Fig. 1, the authoring system 102, the license server 104 and the reader system 106 are each illustrated as a respective individual block. Depending on the embodiment, each block might contain no more than a single computer, or in different

Petitioner Apple Inc. - Exhibit 1012, p. 1713

embodiments, different blocks can contain more than one computer. In one embodiment, one or more of the blocks 102, 104 and 106, for example the license server 104, contains a number of computers spread out over a great geographical area and interconnected by a network. The illustration of the authoring system 102, the license server 104, and the reader system 106 as single blocks is not intended to indicate that each must constitute only a single computer system or that each must be located at a respective single location.

Nor is there any requirement that computers used to form the authoring system 102, the license server 104, and the reader system 106 have any particular structure. Fig. 2 is a symbolic block diagram illustrating the structure of a typical computer system which may be used as an authoring system, a reader system or a license server. It comprises a CPU 202 and cache memory 204, both connected to a CPU bus 206. Interface circuitry 208 is also connected to the CPU bus 206. The interface circuitry 208 is further connected to a main memory 210, as well as to two I/O buses: PCI-bus 212 and ISA-bus 214. Connected to the PCI-bus 212 are sound and game controllers 216, a network adapter 232 and a display adapter 218, the last of which is further connected to a monitor 220. Connected to the ISA-bus 214 is a hard disk drive controller 222, a CD-ROM drive controller 224, a floppy disk drive controller 226, various I/O ports 228, and a boot PROM 230. Most of the peripheral components illustrated in Fig. 2 include on-board configuration data which can be read by the CPU 202. In addition, the boot PROM 230 includes a portion which is writeable by the CPU 202 to store configuration data. In general, the software to operate the authoring system

Petitioner Apple Inc. - Exhibit 1012, p. 1714

102, the license server 104 or the reader system 106 is stored on the disk drive controlled by the disk drive controller 222, and brought into main memory 210 as needed for execution. The computer system of Fig. 2 communicates with the other systems of Fig. 1, and with the distribution network 108, if appropriate, via the network adapter 232.

Fig. 3 illustrates the overall system flow for the authoring system 102. The authoring system flow is generally divided into two segments: an author registration segment 302 followed by one or more product registration segments 304. In the author registration segment 302, the author (or other proprietor) of one or more digital products enters his or her identification information. Such information can include, for example, the author's name, address, Social Security or other tax ID number, password or other challenge information (for confirmation of identity during customer service calls), e-mail address and/or telephone number (step 306). In a step 308, the authoring system uses this information to create an author registration package which is transmitted, in step 310, to the license server 104. The license server 104 adds the author and the author's identification information to its registered author database, and in step 312, the authoring system 102 receives and stores and author ID from the license server 104. The communication between the authoring system 102 and the license server 104 in the author registration segment 302 should take place via digital certificate and one-time secure channel, or by secure, signed electronic mail.

Fig. 4 is a flow chart illustrating the flow of a product registration segment 304 (Fig. 3). In a step

Petitioner Apple Inc. - Exhibit 1012, p. 1715

402, the author identifies one of possibly many digital products to the authoring system 102 and enters usage parameters. The digital product is identified, for example, by identifying a filename within which the digital product is stored. The usage parameters can include such parameters as the number of copies which will be permitted to be made on the reader system, whether the reader system will be authorized to save the digital product to a hard disk, whether printing will be enabled, whether preview is enabled, and the amount of RSS drift which will be permitted on a reader system before manual reauthorization will be required. The usage parameters may be specified as several options, including a set of free usage parameters (for which no payment is required) and one or more options of purchasable usage parameters (functions requiring a purchased license). In an embodiment, the author can also indicate at this point whether the product should be compressed.

In a step 404, if preview is to be enabled, the reader system extracts the appropriate preview material with the assistance of the author. The entire digital product is then encrypted in a step 406. In the product encryption step 406, the product is first compressed (step 408) by any known algorithm. For example, the product can be compressed using a Lempel-Ziv algorithm or by a Huffman encoding algorithm. The compression step 408 is considered part of the product encryption step 406 because compression is, in effect, a form of encryption; it is very difficult to recover the original uncompressed product unless the algorithm used for compression is known. Compression is optional because for certain kinds of products, the benefits to be gained by compression are outweighed by the

Petitioner Apple Inc. - Exhibit 1012, p. 1716

performance degradation that compression/decompression often entails.

In a step 410, a product encryption key is generated. The key can be generated in any known manner; for example, by a pseudo-random number generator using a seed derived from the time period between two successive user key strokes. In step 412, the compressed digital product is encrypted using the encryption key developed in step 410. Again, any known key-based symmetric encryption algorithm can be used (as long as the correct complementary algorithm is used for decryption on the reader system 106). One such well-known encryption algorithm is DES, described in National Institutes of Standards and Technology, "Data Encryption Standard," FIPS Publication No. 46-1 (January 1988), incorporated by reference herein. Another is Triple DES (also known as DES-3), and yet another is RC-5. RC-5 is described in R. W. Baldwin and R. Rivest, "The RC5, RC5-CBC, RC5-CBC-Pad, and RC5-CTS Algorithms", INTERNET-DRAFT (March 1996), available from ftp://ftp.nordu.net/internet-drafts/draft-baldwin-rc5-00.txt, visited March 4, 1997, incorporated herein by reference.

The result of product encryption step 406 is referred to herein as an encrypted "version" of the digital product. As used herein, a "version" of a digital product is still considered to be the digital product, because it continues to include all the information of the digital product. A native "version" of a product also is nevertheless "the product". A digital product can exist in several versions, each of which is a reversibly processed version of the native version.

Petitioner Apple Inc. - Exhibit 1012, p. 1717

After the product encryption step 406, in step 414, the authoring system 102 generates a digest of the encrypted product. Any suitable digesting algorithm can be used for this purpose including, for example, an error-correcting code (ECC) generator or the well-known SHA-1 algorithm. The SHA-1 digesting algorithm is described National Institute of Standards and Technology (NIST), FIPS Publication 180: Secure Hash Standard (SHS) (May 1993), as amended by National Institute of Standards and Technology (NIST) Announcement of Weakness in the Secure Hash Standard (May 1994), both incorporated herein by reference.

In a step 416, the authoring system 102 separates one or more "security fragments" in the encrypting product. The security fragments preferably constitute only a small portion of the overall digital products; for example, 1-5% of the byte count of the overall product not to exceed, for example, 30K bytes. The number and size of the security fragments can be predetermined and constant for all digital products, or it can be dynamically selected or optimized for different digital products. It is desirable to minimize the size of the security fragments while maximizing the effect that their absence would have in helping to prevent unauthorized usage of the digital products. One way of maximizing such effect is to include the beginning of the digital product in one of the security fragments. For many encryption algorithms, as well as data compression algorithms, it is much more difficult to decrypt (decompress) the portions that remain, if the beginning portion is missing. Also, if the digital product includes a header at the beginning, absence of the beginning portion of the product often makes it difficult to use any of the remaining portion

Petitioner Apple Inc. - Exhibit 1012, p. 1718

of the product even if such remaining portion can be decrypted.

In a step 418, the authoring system 102 generates a digest of the encrypted product less the security fragments. Again any digesting algorithm, such as SHA-1, can be used in this step. In step 420, the authoring system 102 creates a product registration package and transmits it to the license server in step 422. The license registration package can form part of a digital certificate in one embodiment. The license server stores the product registration package and returns a product ID to the authoring system 102 (step 424). The reason that the security fragments should be kept as small as possible is to minimize the storage capacity requirements of the license server. In a step 426, the authoring system 102 creates a product broadcast package for the digital product and makes it available (step 428) via any uncontrolled distribution network, such as the Internet.

The product registration package, which can also be digitally certified, includes the following items:

- author ID
- usage parameters (both the free usage parameters and the usage parameters at various purchasable options)
- the encrypted security fragments
- a product decryption key (complementary to the product encryption key of step 410)
- the digest of the encrypted product less security fragments
- digest of the full encrypted product

The product decryption key referred to above is whatever key is required to decrypt the results of the encryption process of step 412. For symmetric

Petitioner Apple Inc. - Exhibit 1012, p. 1719

encryption algorithms, such as for DES or RC-5, the product decryption key will be the same as the key used for product encryption in step 410; for asymmetric encryption algorithms (such as for public key encryption), the product decryption key might be different than the product encryption key (such as for RSA encryption). In both cases, the product decryption key is referred to herein as being "complementary" to the key used for product encryption in step 410.

The product decryption key is the only segment of the product registration package which should be transmitted to the license server securely. Other segments can be transmitted securely if desired or convenient, but this is not necessary. Security of the product decryption key can be ensured, for example, by public/private key encryption of the product decryption key itself, or by connecting to the license server 104 via a secure network.

The product broadcast package contains the following items. If more than one sub-product is included in the product broadcast package, then the package contains a set of these items for each sub-product.

- product ID
- preview material (unencrypted)
- free usage parameters
- purchasable usage parameter options
- Universal Resource Locator (URL) of license server 104
- copyright notice
- contact information for assistance or questions
- encrypted product less security fragments

Petitioner Apple Inc. - Exhibit 1012, p. 1720

As can be seen, whereas the great bulk of the product is transmitted via the uncontrolled distribution network 108, not only is it encrypted, but it is also incomplete so that even if it could be decrypted, for example by a powerful computer system, important fragments of the product simply are not there.

Fig. 5 is a flow chart illustrating the general operation of the reader system 106. When a user installs the reader software on the reader system 106, the reader software automatically generates an installation ID. The installation ID, which is stored on disk in the reader system 106, is a substantially unique identifier of the installation. The installation ID is stored in such a way that if the particular installation of the reader system software was to be copied to a different system, the installation ID would likely be copied as well.

In a step 502, the customer/user of the reader system 106 downloads the product broadcast package for a digital product that he or she wishes to examine. In a step 504, the customer performs one or more of the freely authorized functions, including a preview of the material in the digital product (if available). For example, if the digital product is a sound, the preview material might be a portion of that sound. If a digital product includes a movie, then the preview might be a portion of the movie, or a trailer. If the digital product is an image, then the preview material might include a thumb nail of the image. If the digital product is text, then the preview material might include an abstract.

In a step 506, the customer chooses to buy a license in accordance with one of the license options

Petitioner Apple Inc. - Exhibit 1012, p. 1721

made available in the usage parameters. In step 508, the customer enters his or her identification information, payment and contact information. The identification information can include the customer's name, address and phone, or optionally an arbitrary privacy ID. Such identification is desirable so that the licensing authority can identify the customer if and when the customer calls in for support. The payment information can include a credit card number and authorization and/or digital money information. Various forms of digital money are described in Daniel C. Lynch, "Digital Money" (John Wiley & Sons, 1996), incorporated herein by reference.

In a step 510, the reader system 106 prepares a product purchase package described hereinafter, and in a step 512, the reader system 106 uploads the product purchase package to the license server 104 at the URL identified in the product broadcast package. Note that multiple or bounce URLs may be available for this purpose. The product purchase package may be transmitted by secure channel and/or encrypted in a digital certificate. Assuming the product purchase package is in order, then in a step 514, the reader system receives the product server download package for the desired digital product. The product server download package need not be transmitted by secure channel. In a step 516, the reader system stores the product broadcast package on the reader system (or at least accessibly to the reader system) in conjunction with the product server download package. Either at that time or at a later time, at the customer's request, the reader system plays (or otherwise uses) the product (step 518). All further use of the product

Petitioner Apple Inc. - Exhibit 1012, p. 1722

by the customer occurs on the reader system 106 through the reader system software.

Fig. 6 is a flow chart of the step 510 (Fig. 5) in which the reader system 106 prepares the product purchase package. In a step 602, the reader system 106 generates a reader system signature (RSS) for the reading system 106. The manner in which the RSS is generated is described hereinafter. In a step 604, the reader system 106 retrieves the previously generated installation ID, and in a step 606, the reader system generates a digest of the encrypted product less the security fragments (as obtained from the product broadcast package). The digest performed in step 606 should be the same as that performed by the authoring system 102 in step 418 (Fig. 4).

In a step 608, the reader system 106 extracts the product ID from the product broadcast package and in a step 610, the reader system assembles the product purchase package.

The product purchase package includes the following items:

- product ID
- customer's installation ID
- customer's identification information (or privacy ID)
- customer's payment information
- customer's contact information (including information on where to send the product server download package)
- RSS of the reader system 106
- generated digest of the encrypted product less security fragments

Petitioner Apple Inc. - Exhibit 1012, p. 1723

The reader system signature can be generated in a number of different ways in different embodiments. In one embodiment, the system takes advantage of serial numbers or other identifying data which may be present in the reader computer system, and which carry external assurances of substantial uniqueness. That is, many computers when manufactured are assigned a serial number or other indicator which the manufacturer of the computer, or some other authority, guarantees to be unique. For example, Apple MacIntosh computers, when manufactured, are assigned an Ethernet address which is unique to that specific computer. Alternatively, the identifier can be assigned in software, such as in the operating system of the computer. It is not essential that whatever authority assigns the serial number guarantee uniqueness; it is sufficient only in that it be extremely unlikely that two computer systems which can act as reader systems 106 carry the same identifier. This is the case where, for example, the number carries external assurances of substantial uniqueness, such as in the case of Ethernet addresses.

In another embodiment, the reader system signature does not rely on a component having an identifier that carries external assurances of substantial uniqueness. Instead, a plurality of components (hardware or software) are examined to determine individual component signatures. The individual component signatures are then combined to form the overall reader system signature. In one embodiment, the individual component signatures are all concatenated together in a predetermined sequence to form the overall reader system signature. The individual component signatures may be digested prior to concatenation in order to limit their size to the

Petitioner Apple Inc. - Exhibit 1012, p. 1724

predefined field size. In another embodiment, optionally after digesting, the individual component signatures are averaged or summed together to form the overall reader system signature. The individual component signatures can be weighted prior to combination, in order to reduce the impact on the reader system signature that would result from changes in components that are more frequently subject to upgrade or replacement.

In one embodiment, the reader system 106 generates the reader system signature in dependence upon component signatures from the following components, to the extent present in the system. Except as indicated below, most of the component signatures set forth in this list are readable either from the CMOS or from a device manager driver. This is only an illustrative list; other embodiments can refer to other components not on this list.

Hard Disk Drive

- drive ID
- numbers of cylinders, sectors and heads
- drive defective sector map (obtained from sector 0)
- drive name
- drive manufacturer

Floppy Disk Controller

- I/O addresses and settings
- interrupt assignments
- manufacturer name

Petitioner Apple Inc. - Exhibit 1012, p. 1725

Monitor

- monitor name
- monitor type

Display Adaptor

- device name
- on-board memory

Mother Board

- CPU type
- CPU speed
- total memory present
- total cache present
- cache timings (measured empirically)

Ports

- I/O addresses and settings
- interrupt assignments

Sound, Video and Game Controllers

- device name
- driver name
- driver version

System Devices

- CMOS profile

In yet another embodiment, a combination of individual component signatures also includes one or more component signatures that carry external

Petitioner Apple Inc. - Exhibit 1012, p. 1726

assurances of substantial uniqueness, to the extent such a component exists in the machine.

Fig. 7 is a flow chart illustrating one technique for generating the reader system signature for reader system 106. In a step 704, it is determined whether the reader system 106 includes a component which has an ID that carries external assurances of substantial uniqueness. If so, then the reader system signature is given by the component ID of that component (step 706). If not, then in step 708, the reader system 106 obtains the data regarding the above-listed components to the extent present in the reader system 106. In a step 710, each of the individual component signatures is digested, and they are combined in step 712 to form the reader system signature.

Returning to Fig. 5, as previously mentioned, after the reader system prepares and uploads a product purchase package to the license server (step 512), the license server 104, if everything is in order, returns a product server download package to the reader system 106 (step 514). Fig. 8 is a flow chart of the steps which takes place in the license server 104 in response to receipt of a product purchase package. As used herein, steps which take place "in response to" a predecessor event, do so if the predecessor event influenced the performance of such steps. If there is an intervening time period, the performance of the steps can still be considered "responsive" to the predecessor event. If the performance of the steps depends on more than one predecessor event, then the steps are considered performed in response to *each* of the predecessor events.

In a step 802, the license server 104 compares the digest from the product purchase package with the

Petitioner Apple Inc. - Exhibit 1012, p. 1727

digest of the encrypted product less security fragments as stored on the server 104 with the product registration package for the product ID referred to in the newly received product purchase package. If the two digests do not match, then it is very likely that either the product broadcast package has been tampered with prior to generation of the digest on the reader system 106, or the customer is attempting to obtain the product server download package fraudulently. In this case, the license server 104 returns a package to the reader system 106 indicating that the attempt to purchase a license was unsuccessful (step 804).

If the two digests do match, then in step 806, the license server 104 processes the customer's payment information. If there is an error in this process, then again the license server returns an indication to the reader system 106 that the customer's attempt to purchase a license has been unsuccessful (step 804).

Assuming the customer's payment information was processed successfully, in step 808, the license server 104 stores the customer's RSS obtained from the product purchase package in conjunction with the customer's installation ID, also obtained from the product purchase package. This information need not be stored "on" the license server 104 itself, as long as it is stored in a manner in which it is "accessible" to the license server 104 at a future time.

In a step 810, the license server 104 performs certain fraud detection checks. This step is optional in different embodiments, as indicated by the dotted line surrounding the box in Fig. 8. If performed, the fraud detection step 810 can include a check of the installation ID from the product purchase package

Petitioner Apple Inc. - Exhibit 1012, p. 1728

against the installation IDs that have been stored previously on the license server for other product purchases. If a large number of purchases have been made using product purchase packages specifying the same installation ID, then it is likely that someone has altered an installation of the reader system software and is passing it around to different customers who are using it to purchase licenses. The same is true if the same license has been purchased several times from the same installation ID, or if several significantly varying reader system signatures have been stored in the license server's database in conjunction with the same installation ID. A number of other fraud detection mechanisms can also be employed. In any event, an investigation is warranted if step 810 suggests that an altered version of the reader system software might be being distributed.

The flow chart of Fig. 8 continues after step 810 with step 902 in Fig. 9, as indicated by the symbol "9" in both Figs. 8 and 9.

In Fig. 9, in step 902, the license server 104 further encrypts the already once-encrypted security fragments (from the product registration package) using the customer's RSS as a key. The key used in step 902 need not be the RSS exactly; it can be some other number which depends on the RSS. For example, it can be a digest reduction of the RSS from the customer's product purchase package. In any event, step 902 results in "double-encrypted" security fragments from the digital product.

In step 902, the product decryption key from the product registration package is also encrypted using the customer's RSS (or a number derived therefrom) as a key. Note that in a different embodiment, either

Petitioner Apple Inc. - Exhibit 1012, p. 1729

step 902 or step 904 can be omitted, although such an omission would likely reduce the security of the overall system.

In a step 906, the license server 104 assembles the product server download package, and in a step 908, it transmits the product server download package back to the reader system 106. Processing then resumes in the reader system 106 at step 514 (Fig. 5).

The product server download package includes the following items:

- product ID
- paid usage parameters
- payment confirmation information (such as a credit card payment confirmation)
- digest of full encrypted product (from the product registration package stored on the license server 104)
- encrypted product decryption key (product decryption key encrypted with the customer's RSS)
- double-encrypted security fragments (encrypted security fragments further encrypted with the customer's RSS)

Fig. 10 is a flow chart of the step 806 (Fig. 8), in which the license server 104 processes the customer's payment information. Fig. 10 illustrates the process where the customer is paying by credit card; a similar process would take place where the customer is paying with digital money or in some other payment form.

In step 1002, the license server 104 transmits the charge information to a credit card clearing house. The credit card clearing house returns either an approval code or an error. In step 1004, if an error was received, then the license server 104 returns an

Petitioner Apple Inc. - Exhibit 1012, p. 1730

error to step 806 (Fig. 8) (Step 1006). If an approval code was received, then in step 1008, the license server 104 credits the author's account with the amount of the approved purchase price less a commission. In step 1010, the license server 104 returns successfully to the step 806 (Fig. 8).

Returning to Fig. 5, as previously mentioned, each time the customer desires to use the digital product, he or she does so using the reader system software on the reader system 106. Fig. 11 is a flow chart of the step 518 in which the reader system plays the digital product. (The terms "play", "view" and "use" are used interchangeably herein as regards a digital product.) Referring to Fig. 11, in a step 1102, the reader system 106 regenerates the RSS for the reader system. This step takes place using the same algorithm that was used in step 602 (Fig. 6) when the RSS was generated for preparation of the product purchase package. In a step 804, the reader system 106 decrypts the double-encrypted security fragments using the new RSS as a key. As mentioned with respect to step 904 (Fig. 9), the key used in step 1104 need not be the RSS identically; another number which depends on the RSS can be used instead. However, whatever algorithm is used to derive the key from the RSS in step 1104 should be the same as that used in step 904.

In step 1106, the reader system 106 merges the encrypted security fragments into the encrypted product less the encrypted security fragments, thereby assembling a complete, but still encrypted, version of the digital product. In step 1108, the full encrypted digital product is digested using the same algorithm as was used originally by the authoring system 102 in step 414 (Fig. 4). In step 1110, the reader system 106

Petitioner Apple Inc. - Exhibit 1012, p. 1731

determines whether the newly calculated digest matches the digest which was provided by the license server 104 in the product server download package. If so, then usage of the product on the reader system 106 is authorized. Flow continues with the flowchart of Fig. 12 (as indicated by the number "12" in the small circles in both Figs. 11 and 12). If the two digests do not match in step 1110, then usage of the product on the reader system 106 is not immediately authorized. Flow continues with the flowchart of Fig. 13, as indicated by the number "13" in the small circles in both Figs. 11 and 13.

Referring to Fig. 12, since the two digests match in step 1110, the current reader system signature has been confirmed to be the same as that which was used when the reader system 106 first uploaded its product purchase package in step 512 (Fig. 5). It is also the same RSS that was used to encrypt the product decryption key as downloaded from the license server 104 to the reader system 106 in steps 908 and 514. Accordingly, in step 1202, the reader system 106 decrypts the product decryption key from the product server download package using the current RSS. Again, the actual key used to decrypt the product decryption key in step 1202 need not be identical to the current RSS, as long as it is dependent thereon, and as long as the algorithm to generate the key is the same as that which was used to generate the key with which the product decryption key was originally encrypted in step 904 (Fig. 9).

In step 1204, the reader system 106 decrypts the merged encrypted product using the product decryption key that was decrypted in step 1202. In step 1206, if the decrypted product was compressed, it is now

BNSDOCID: <WO__9842098A1_I_>

decompressed using an algorithm complementary to that used by the authoring system in step 408 (Fig. 4). The resulting decompressed digital product is transmitted in step 1210 to an appropriate viewer.

It will be appreciated that once the digital product is transmitted in step 1210 to a viewer, which may be any standard viewer appropriate to the content of the digital product, the output stream is no longer secured by the mechanisms built into the overall system as described herein. Accordingly, a step 1208 is optionally inserted between steps 1206 and 1210 of Fig. 12. In an embodiment which includes step 1208, a fingerprint and/or a watermark is (are) inserted into the digital output stream prior to or while it is being provided to the viewer. Watermarking is a technique using a visible identifier that will let the user know that he or she has been associated with this particular instance of the content. It acts primarily as a deterrent. Fingerprinting embeds and hides codes into the output stream itself that are retrievable only by the author or by the licensing authority. Such codes uniquely associate the particular copy of the digital product with the individual who purchased it. Fingerprinting is used primarily for criminal prosecution and court proceedings.

If fingerprinting is used, preferably the fingerprint is inserted in a manner which does not affect the resulting viewing experience. For example, if the output stream includes CD audio, then the fingerprint can be spread over a large number of the audio samples, either substituting for the low-order bit or modifying the low-order bit in an exclusive OR manner in each sample. Alternatively, to avoid differential cryptanalysis, the data stream can be

Petitioner Apple Inc. - Exhibit 1012, p. 1733

transformed into the frequency domain, modified in the frequency domain to insert the fingerprint codes, and then transformed back to the time domain. Also for images, steganographic techniques can be used to insert the fingerprint into the image. Steganography is described in Neil F. Johnson, "Steganography", available at http:// adams.patriot.net/ ~johnson/ html/ neil/ stegdoc/ stegdoc.html, visited March 4, 1997, incorporated by reference herein. The fingerprint to be inserted in the digital output stream should preferably be either the installation ID of the reader system 106, or the reader system signature that was generated at the time of product usage (step 1102). Optionally, the output stream can also be randomly seeded to further hamper differential cryptanalysis. In this manner, if pirated copies of a digital product do begin to appear, the author of the product or the licensing authority should be able to determine the original source of the pirated copies by examining the fingerprint.

Returning to Fig. 11, if the two digests do not match (step 1110), then the reader system 106 has determined that the newly generated reader system signature is not the same as that which was generated in step 602 (Fig. 6) at the time of product purchase. In an aspect of the invention, this determination does not immediately preclude usage of the product by the customer on the reader system 106. Instead, proceeding in Fig. 13, in a step 1302, the reader system 106 prepares a re-validation package. The re-validation package can be the same as set forth above with respect to the product purchase package, except that the customer's payment information can be omitted. In step 1304, the reader system 106 uploads the re-validation

Petitioner Apple Inc. - Exhibit 1012, p. 1734

package to the license server 104 at the URL identified in the product broadcast package. The license server's operations in response to receipt of a re-validation package are set forth in Fig. 14.

Referring to Fig. 14, in a step 1402, it is first determined whether the RSS in the re-validation package was based on a component in the reader system 106 having external assurances of substantial uniqueness. If so, then re-validation is considered unsuccessful (step 1404) and this result is returned to the reader system 106. If the RSS in the re-validation package was not based on a component having external assurances of substantial uniqueness, then in step 1406, the license server 104 compares the new RSS from the re-validation package to the RSS previously stored accessibly to the server for the same reader system 106 (as identified by the installation ID specified in the re-validation package). If the difference between the two RSS's exceeds the threshold that was specified by the author in the usage parameters stored on the server 104 for the product ID specified in the re-validation package (step 1408), then, again, re-validation is unsuccessful and such a result is returned to the reader system 106 (step 1404). In different embodiments, the threshold can be specified as a percentage of one or the other RSS, or as a number of component signatures which differ between the two RSS's, or by a number of other different specifications.

If the difference between the two RSS's does not exceed the designated threshold (step 1408), then the re-validation is considered successful. The license server 104 prepares a new product server download package using the same algorithms as set forth above

Petitioner Apple Inc. - Exhibit 1012, p. 1735

with respect to Fig. 9, but using the new RSS for encryption instead of the RSS that was used to download the original product server download package upon purchase. The new product server download package is then transmitted back to the reader system 106 with re-validation. Optionally, in order to assist investigation of any potential fraud, in step 1410, the license server 104 also stores the new RSS in conjunction with the installation ID specified in the re-validation package. A history of such ostensible reader system upgrades is maintained on the server 104.

Fig. 15 is a detail of step 1408 (Fig. 14) in which the license server 104 determines whether the difference between the two RSS's exceeds the threshold specified by the author in the usage parameters for the digital product. The flowchart set forth in Fig. 15 represents one embodiment, in which the threshold has been specified as a percentage. In a step 1502, the server 104 calculates the weighted sum of the RSS received in the product re-validation package. In a step 1504, the server 104 makes the same calculation with respect to the RSS previously stored on the server 104. In step 1506, the license server 106 determines whether the difference between the two calculated values exceeds the threshold specified by the author in the usage parameters. If so, then in step 1508, the routine returns to Fig. 14 affirmatively. If not, then in step 1510, the routine returns to Fig. 14 negatively.

Fig. 16 is a detail of step 1408 (Fig. 14) as performed in a second embodiment, in which the upgrade drift percentage is specified as a maximum number of components whose individual component signatures can differ between the two RSS's. In step 1602, the server

Petitioner Apple Inc. - Exhibit 1012, p. 1736

104 counts the number of components of the RSS in the re-validation package, which differ from the corresponding components of the RSS previously stored on the server 106 from the original product purchase package. If the count exceeds the predetermined drift threshold, then the routine returns affirmatively (step 1606). If not, then it returns negatively (step 1608).

Returning to the reader system flow as illustrated in Fig. 13, after the reader system 106 uploads the re-validation package to the license server 104, in a step 1306, the reader system 106 receives the re-validation result. If the re-validation was unsuccessful (step 1308), then the reader system displays an error message to the user and requests the customer to call customer service of the licensing authority (step 1310). In this situation, automatic re-validation has failed, and manual re-validation as in step 1310 is necessary. During the call, a customer service representative can determine whether the customer's license should be extended to cover the reader system 106 as it now stands. If automatic re-validation was successful (step 1308), then the reader system returns to step 514 (as indicated by the numeral "5" in the small circle in both Figs. 13 and 5) to store and process the new product server download package in the same manner as it processed the original product server download package received upon purchase.

It can be seen that a secure product distribution mechanism has been described which takes advantage of the benefits of an uncontrolled distribution network, while ensuring that authors and proprietors of digital products are paid an appropriate royalty for their efforts at creativity. In addition, the mechanism ensures that once a customer is licensed to use a

Petitioner Apple Inc. - Exhibit 1012, p. 1737

digital product on a particular reader system, that product cannot be used on any other reader system without re-validation. The mechanism allows for a certain amount of upgrade drift within which re-validation can be entirely automated.

The foregoing description of preferred embodiments of the present invention has been provided for the purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise forms disclosed. Obviously, many modifications and variations will be apparent to practitioners skilled in this art. For example, whereas the flowcharts described herein illustrate steps being performed in a particular sequence, it will be appreciated that in many instances the sequence of the steps can be reversed, or the steps can be performed in a pipelined, overlapping manner, or both, without departing from the scope of the invention. The embodiments herein were chosen and described in order to best explain the principles of the invention and its practical application, thereby enabling others skilled in the art to understand the invention for various embodiments and with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the following claims and their equivalents.

Petitioner Apple Inc. - Exhibit 1012, p. 1738

CLAIMS

1. A method for preparing a digital product for controlled distribution using a distribution network, comprising the steps of:

encrypting said product;

separating at least one encrypted fragment from said encrypted product;

transmitting said encrypted product less said at least one encrypted fragment onto said distribution network; and

withholding said at least one encrypted fragment from said distribution network.

2. A method according to claim 1, further comprising the step of transmitting said at least one encrypted fragment to a license server.

3. A method according to claim 2, further comprising the step of transmitting to said license server a decryption key that can be used to decrypt said product.

4. A method according to claim 1, wherein said encrypted product includes a header portion followed by a remainder portion,

and wherein said step of separating at least one encrypted fragment from said encrypted product comprises a step of separating from said encrypted product an encrypted fragment that includes at least part of said header portion.

Petitioner Apple Inc. - Exhibit 1012, p. 1739

5. A method according to claim 1, wherein said encrypted product consists of a starting byte followed at least logically by all remaining bytes,

and wherein said step of separating at least one encrypted fragment from said encrypted product comprises a step of separating from said encrypted product an encrypted fragment that includes said starting byte.

6. A method according to claim 1, wherein said encrypted product consists of a plurality of data bytes,

and wherein said at least one encrypted fragment consists of not more than five percent of said data bytes.

7. A method for controlling usage of a digital product, comprising the steps of:

storing accessibly to a server at least one fragment of an encrypted version of said digital product;

receiving product request information for acquisition by a user, of a usage license for said digital product; and

transmitting a version of said at least one fragment as stored accessibly to said server to said user in response to receipt of said product request information, transmissions of said at least one fragment to said user in response to receipt of said product request information being limited to less than all of said digital product.

Petitioner Apple Inc. - Exhibit 1012, p. 1740

8. A method according to claim 7, wherein less than all of said digital product is accessible to said server.

9. A method according to claim 7, wherein said product request information includes payment information,

further comprising a step of transmitting paid usage parameters to said user in response to said receipt of said product request information.

10. A method according to claim 7, wherein said product request information further includes a digest of a portion of a version of said digital product, said portion being non-co-extensive with said at least one fragment, further comprising the steps of:

storing a digest of said portion accessibly to said server prior to said step of receiving product request information; and

in response to receipt of said product request information, comparing said digest in said product request information with said digest stored accessibly to said server.

11. A method according to claim 7, wherein said product request information further includes a reader system signature of a particular reader system,

further comprising a step of encrypting at least one of said at least one fragment as stored accessibly to said server, in dependence upon said reader system signature, to form a further encrypted version of said at least one fragment as stored accessibly to said server,

Petitioner Apple Inc. - Exhibit 1012, p. 1741

the version transmitted to said user in said step of transmitting including said further encrypted version of said at least one fragment.

12. A method according to claim 7, wherein said product request information further includes a reader system signature of a particular reader system, further comprising the steps of:

storing a product decryption key accessibly to said server prior to said step of receiving product request information;

encrypting said product decryption key in dependence upon said reader system signature, to form an encrypted product decryption key; and

transmitting said encrypted product decryption key to said user in response to receipt of said product request information.

13. A method according to claim 7, wherein said product request information further includes a first reader system signature of a particular reader system,

further comprising the step of storing said reader system signature accessibly to said server, in response to receipt of said product request information;

and further comprising the steps of, subsequently to said step of transmitting:

receiving a product re-validation request identifying said particular reader system and including a second reader system signature;

determining whether differences between said first and second reader system signatures satisfy predetermined re-validation criteria.

Petitioner Apple Inc. - Exhibit 1012, p. 1742

14. A method according to claim 13, wherein said differences between said first and second reader system signatures satisfy said re-validation criteria, further comprising a step of encrypting at least one of said at least one fragment as stored accessibly to said server, in dependence upon said first reader system signature, to form a first further encrypted version of said at least one fragment,

the version transmitted to said user in said step of transmitting including said first further encrypted version of said at least one fragment;

said method further comprising the steps of:

encrypting said at least one of said at least one fragment as stored accessibly to said server, in dependence upon said second reader system signature, to form a second further encrypted version of said at least one fragment; and

transmitting said second further encrypted version of said at least one fragment to said user in response to said step of determining.

15. A method according to claim 13, wherein said differences between said first and second reader system signatures satisfy said re-validation criteria, further comprising the steps of:

storing a product decryption key accessibly to said server prior to said step of receiving product request information;

encrypting said product decryption key in dependence upon said first reader system signature, to form a first encrypted product decryption key; and

transmitting said first encrypted product decryption key to said user in response to receipt of said product request information,

Petitioner Apple Inc. - Exhibit 1012, p. 1743

said method further comprising the steps of:

encrypting said product decryption key in dependence upon said second reader system signature, to form a second encrypted product decryption key; and

transmitting said second encrypted product decryption key to said user in response to said step of determining.

16. A method for controlled usage of a digital product, comprising the steps of:

developing a first signature of a first reader system in dependence upon a first group of at least one component as present in said first reader system at a first time;

at a second time subsequent to said first time, developing a second signature of a second reader system in dependence upon a second group of at least one component present in said second reader system at said second time;

using a digital product at said second time if and only if said first and second signatures satisfy predetermined reader system drift criteria, said predetermined reader system drift criteria not requiring identity between said first and second signatures.

17. A method according to claim 16, wherein said digital product comprises a sound, and wherein said step of using said digital product comprises a step of playing said sound.

18. A method according to claim 16, wherein said digital product comprises software and wherein said

Petitioner Apple Inc. - Exhibit 1012, p. 1744

step of using said digital product comprises a step of executing said software.

19. A method according to claim 16, wherein said first and second signatures do not satisfy said predetermined reader system drift criteria, further comprising the steps of:

manually communicating with a licensing authority for re-authorization; and

using said digital product at a time subsequent to said second time in response to said re-authorization.

20. A method according to claim 16, wherein said second reader system is said first reader system.

21. A method according to claim 16, wherein said step of using said digital product at said second time if and only if said first and second signatures satisfy predetermined reader system drift criteria, comprises the steps of:

said second reader system making a determination that said first and second signatures match; and

using said digital product in response to said determination.

22. A method according to claim 21, further comprising the steps of:

storing accessibly to said second reader system a first digest of at least a covered portion of said digital product; and

storing, at said first time and accessibly to said second reader system, at least one fragment of said digital product encrypted in dependence upon said

Petitioner Apple Inc. - Exhibit 1012, p. 1745

first signature, said at least one fragment overlapping said covered portion of said digital product,

and wherein said step of said second reader system making a determination that said first and second signatures match, comprises the steps of:

decrypting said at least one fragment in dependence upon said second signature, to form at least one decrypted fragment;

digesting said covered portion of said digital product, using said at least one decrypted fragment, to form a second digest; and

comparing said second digest to said first digest.

23. A method according to claim 16, further comprising the step of storing said first signature accessibly to a server different from said second reader system,

and wherein said step of using said digital product at said second time if and only if said first and second signatures satisfy predetermined reader system drift criteria, comprises the steps of:

transmitting said second signature to said server; and

said server determining whether said first and second signatures satisfy said predetermined reader system drift criteria.

24. A method according to claim 16, wherein said reader system drift criteria are specified in conjunction with said digital product.

25. A method according to claim 16, wherein said first group includes more than one component, and

Petitioner Apple Inc. - Exhibit 1012, p. 1746

wherein said step of developing a first signature comprises the steps of:

developing a first component signature of each respective component in said first group as present in said first reader system at said first time; and

combining said first component signatures into a first combined signature.

26. A method according to claim 25, wherein said second group includes more than one component, and wherein said step of developing a second signature comprises the steps of:

developing a second component signature of each respective component in said second group as present in said second reader system at said second time; and

combining said second component signatures into a second combined signature,

wherein said first and second combined signatures constitute numerical combinations,

and wherein said step of using said digital product at said second time if and only if said first and second signatures satisfy predetermined reader system drift criteria, comprises the step of using said digital product at said second time if and only if said second combined signature differs from said first combined signature by no more than a predetermined maximum drift percentage.

27. A method according to claim 25, wherein said step of combining comprises a step of concatenating said first component signatures into said first combined signature,

wherein said second group includes more than one component,

Petitioner Apple Inc. - Exhibit 1012, p. 1747

and wherein said step of developing a second signature comprises the steps of:

developing a second component signature of each respective component in said second group as present in said second reader system at said second time; and

concatenating said second component signature into a second combined signature,

and wherein said step of using said digital product at said second time if and only if said first and second signatures satisfy predetermined reader system drift criteria, comprises the step of using said digital product at said second time if and only if a count of the number of said second component signatures in said second combined signature which differ from corresponding first component signatures in said first combined signature is no greater than a predetermined maximum drift number.

28. A method according to claim 16, further comprising the step of storing a version of said digital product accessibly to said second reader system, at least a portion of said version being encrypted in dependence upon said first signature.

29. A method according to claim 28, wherein said step of using said digital product at said second time if and only if said first and second signatures satisfy predetermined reader system drift criteria, comprises a step of decrypting said portion of said version in dependence upon said second signature.

30. A method according to claim 16, wherein said step of using said digital product comprises the steps of:

Petitioner Apple Inc. - Exhibit 1012, p. 1748

inserting into said digital product a fingerprint that substantially uniquely identifies said second reader system, said fingerprint being recoverable from said digital product; and

using said digital product with said fingerprint inserted.

31. A method according to claim 16, wherein said step of using said digital product comprises the steps of:

inserting into said digital product a watermark that substantially uniquely identifies said second reader system, said watermark being recoverable from said digital product; and

using said digital product with said watermark inserted.

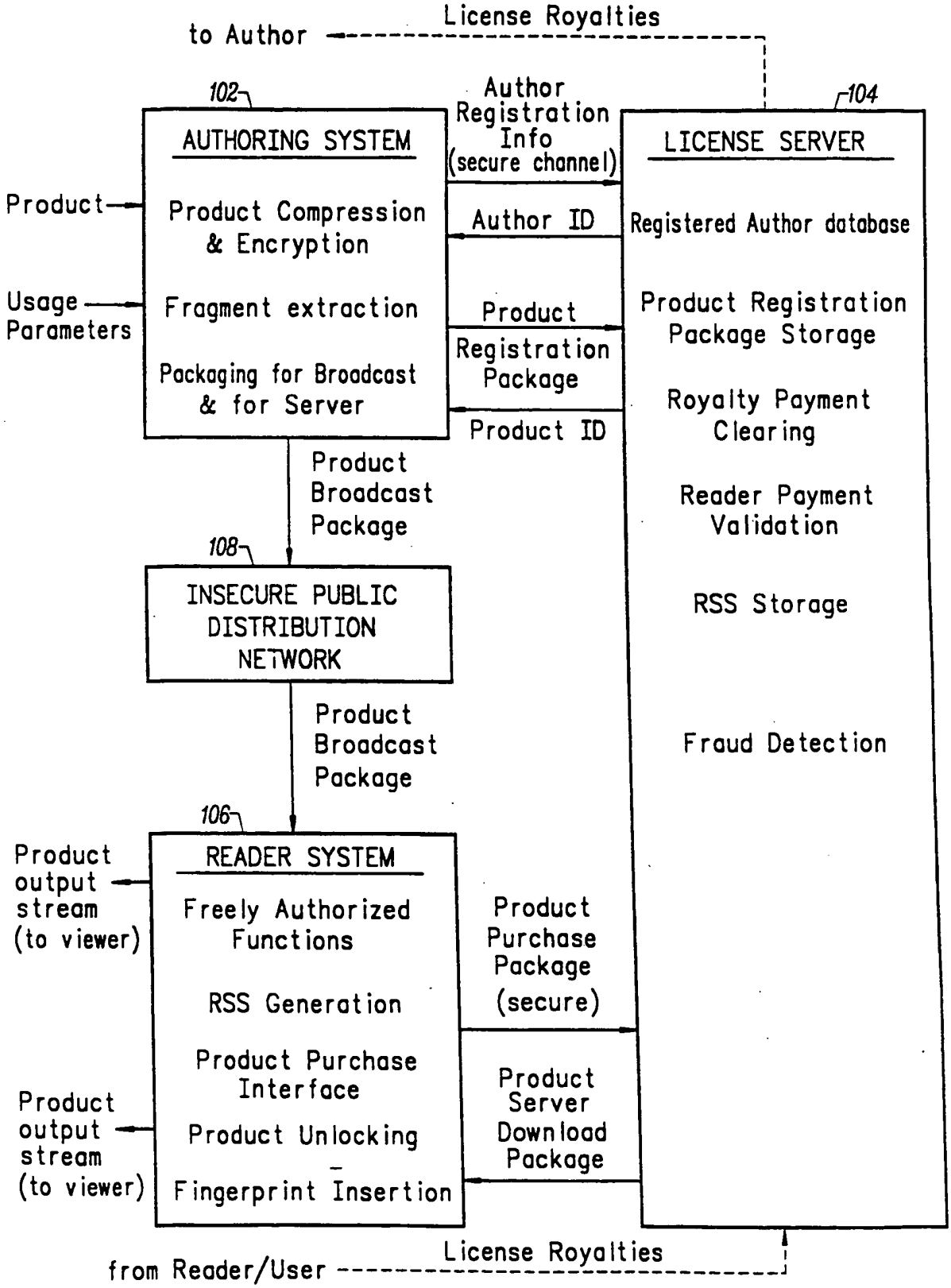


FIG. 1

BNSDOCID: <WO___9842098A1_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1750

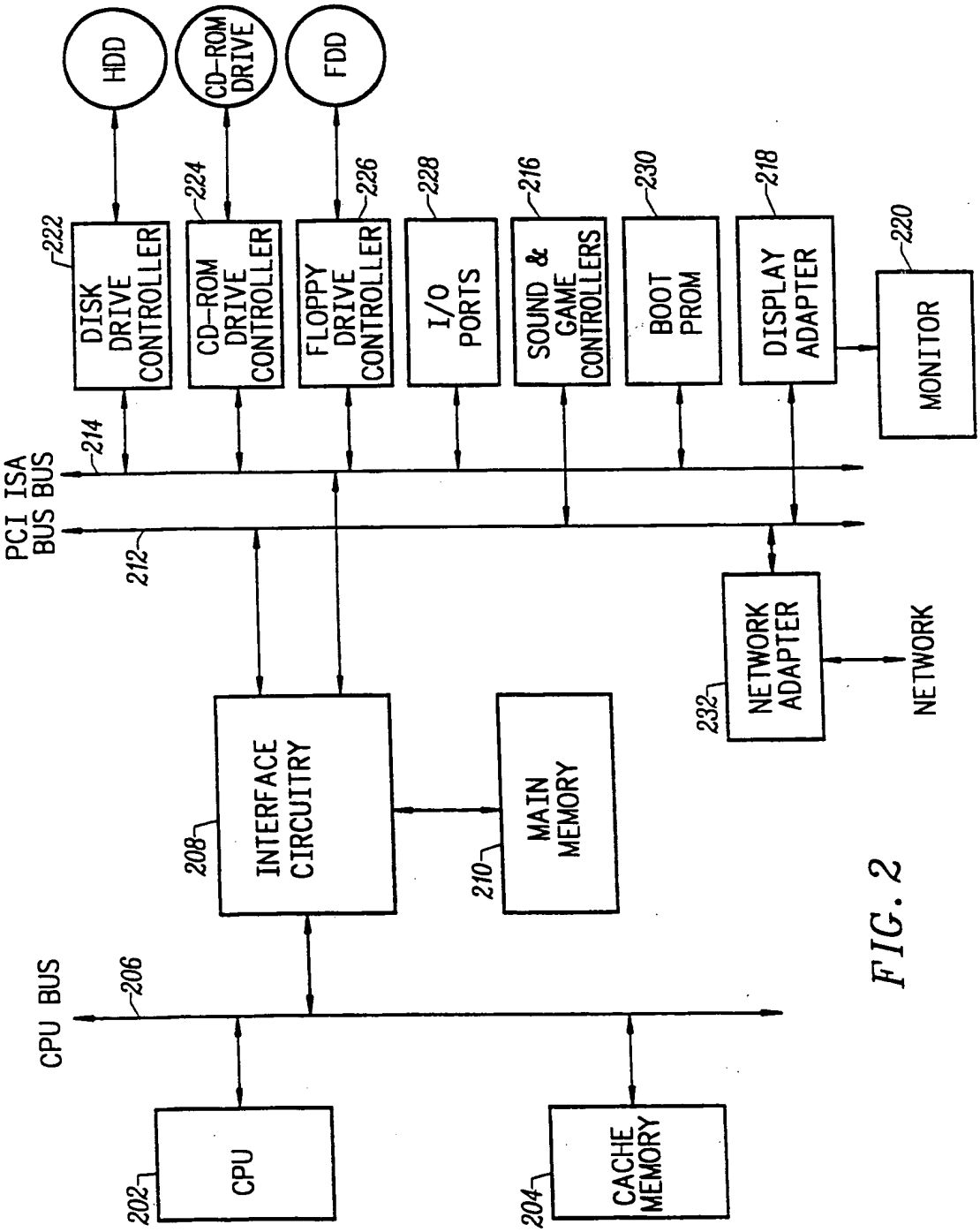


FIG. 2

BNSDOCID: <WO___9842098A1_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1751

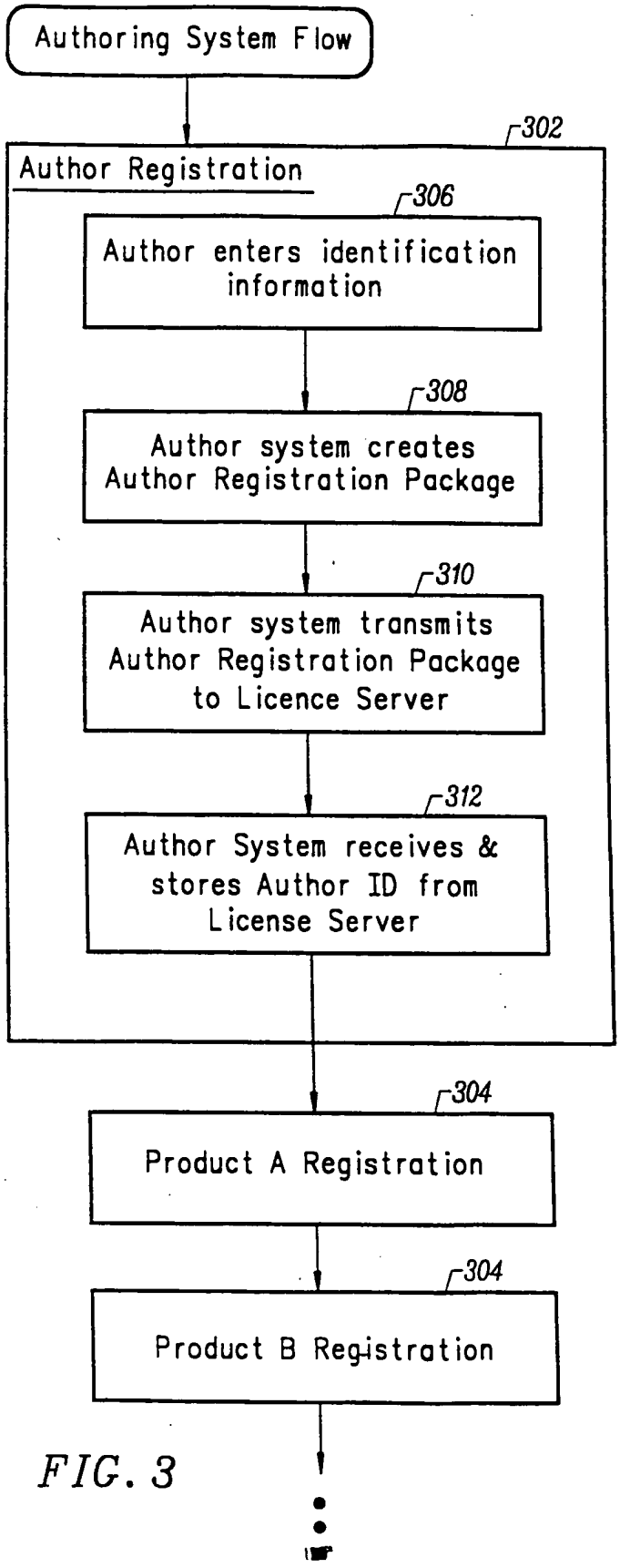


FIG. 3

BNSDOCID: <WO___9842098A1_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1752

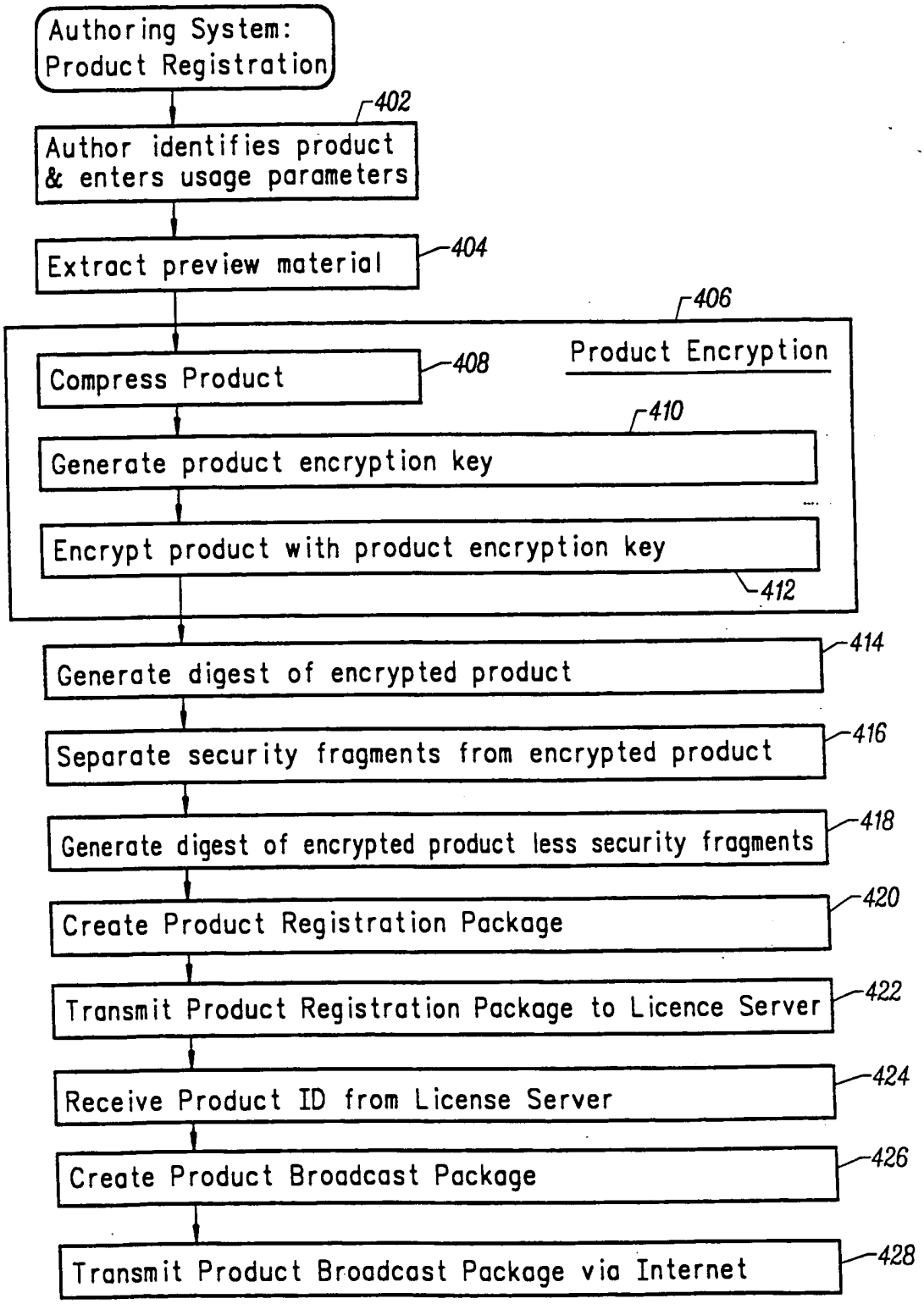


FIG. 4

BNSDOCID: <WO___9842098A1_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1753

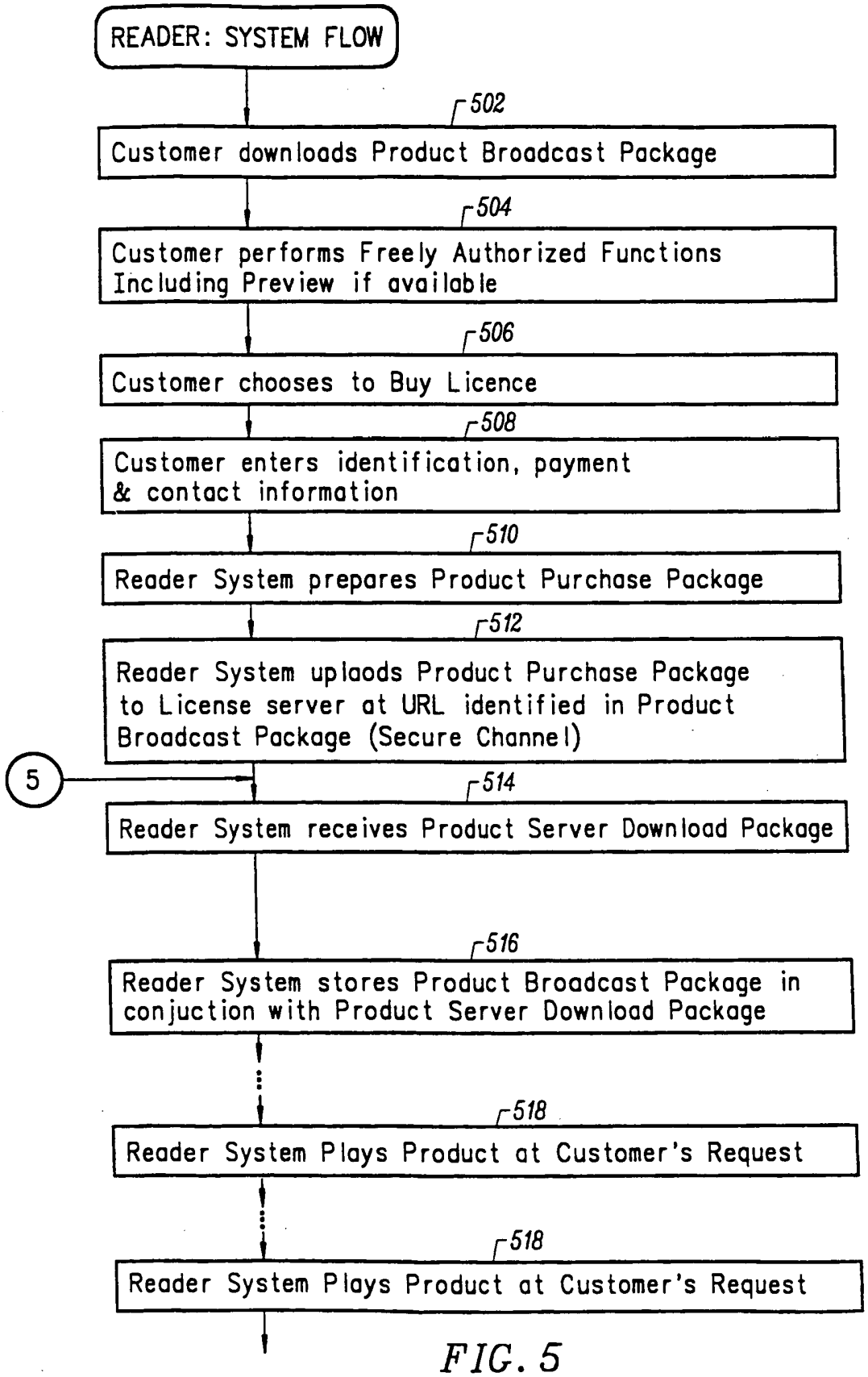


FIG. 5

BNSDOCID: <WO__9842098A1_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1754

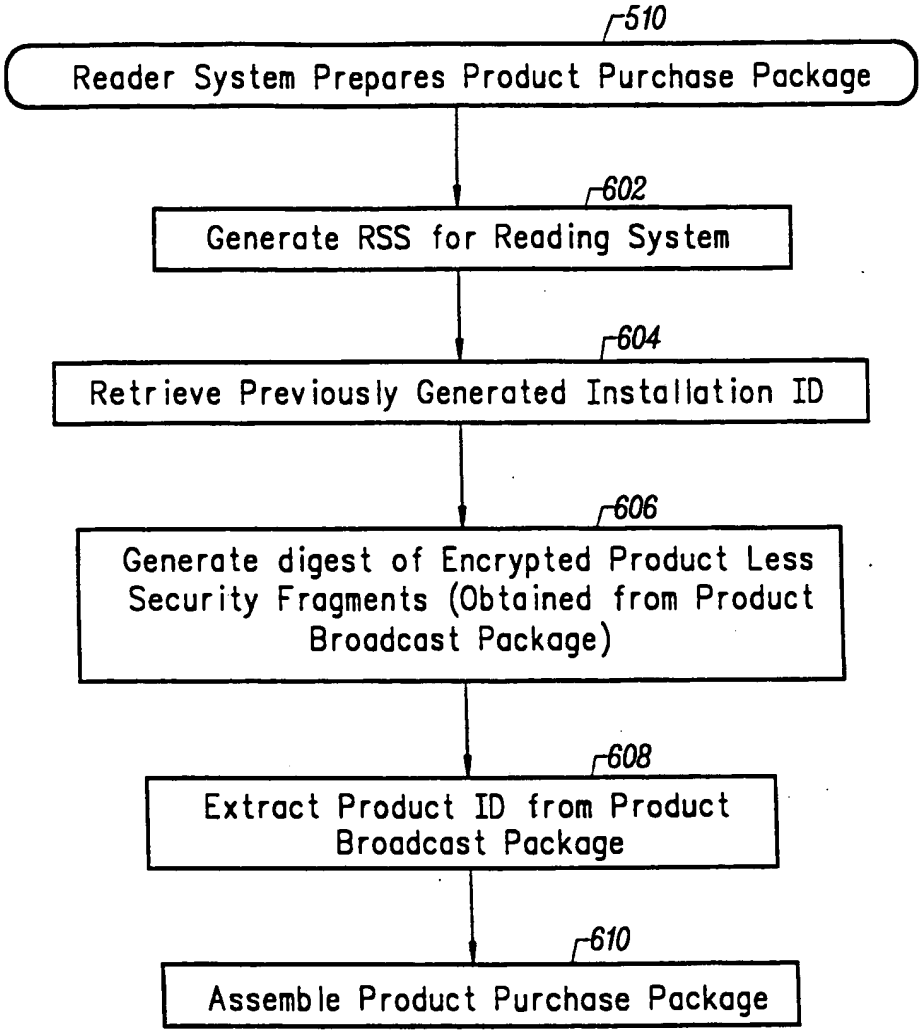


FIG. 6

BNSDOCID: <WO___9842098A1_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1755

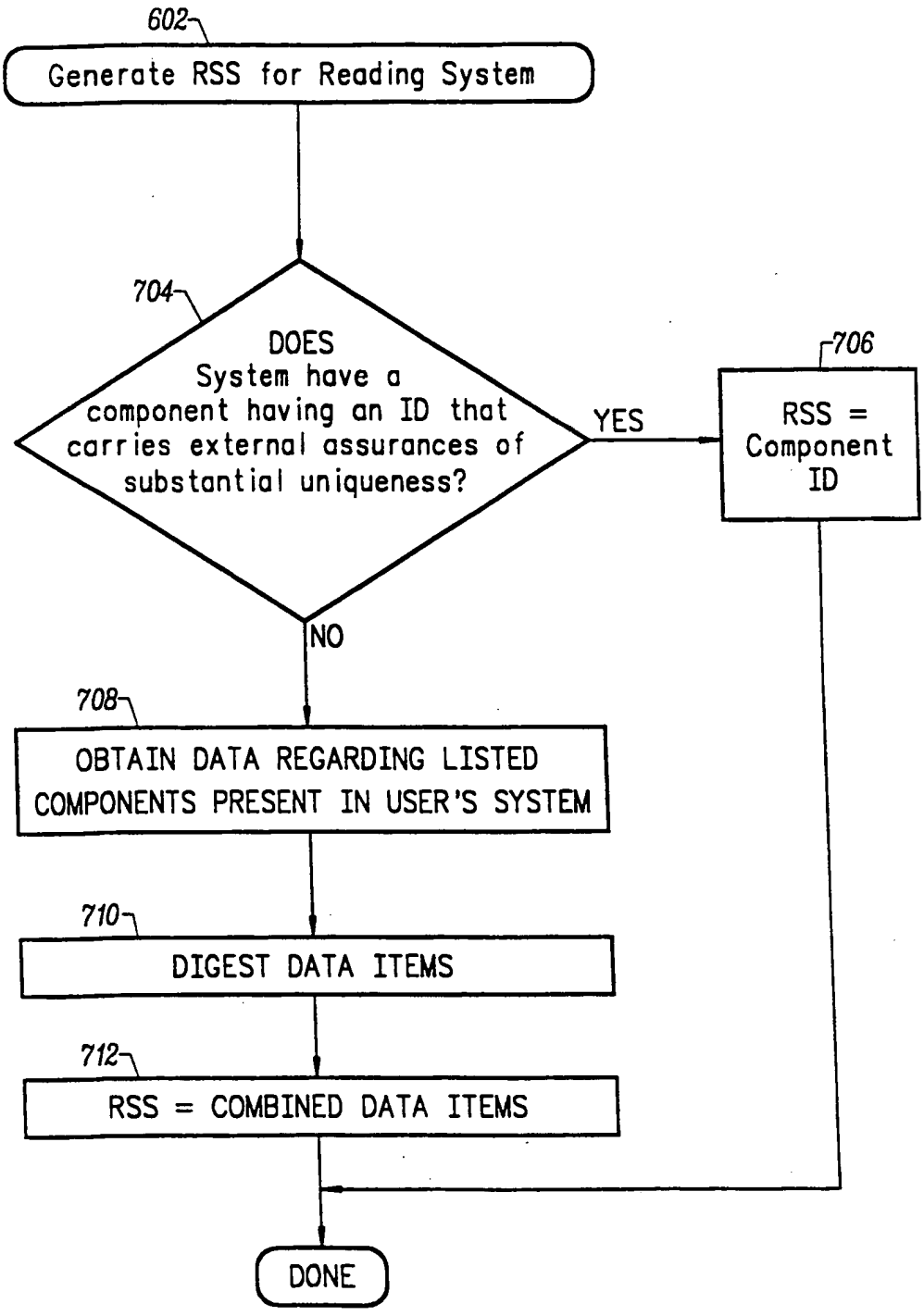


FIG. 7

BNSDOCID: <WO__9842098A1_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1756

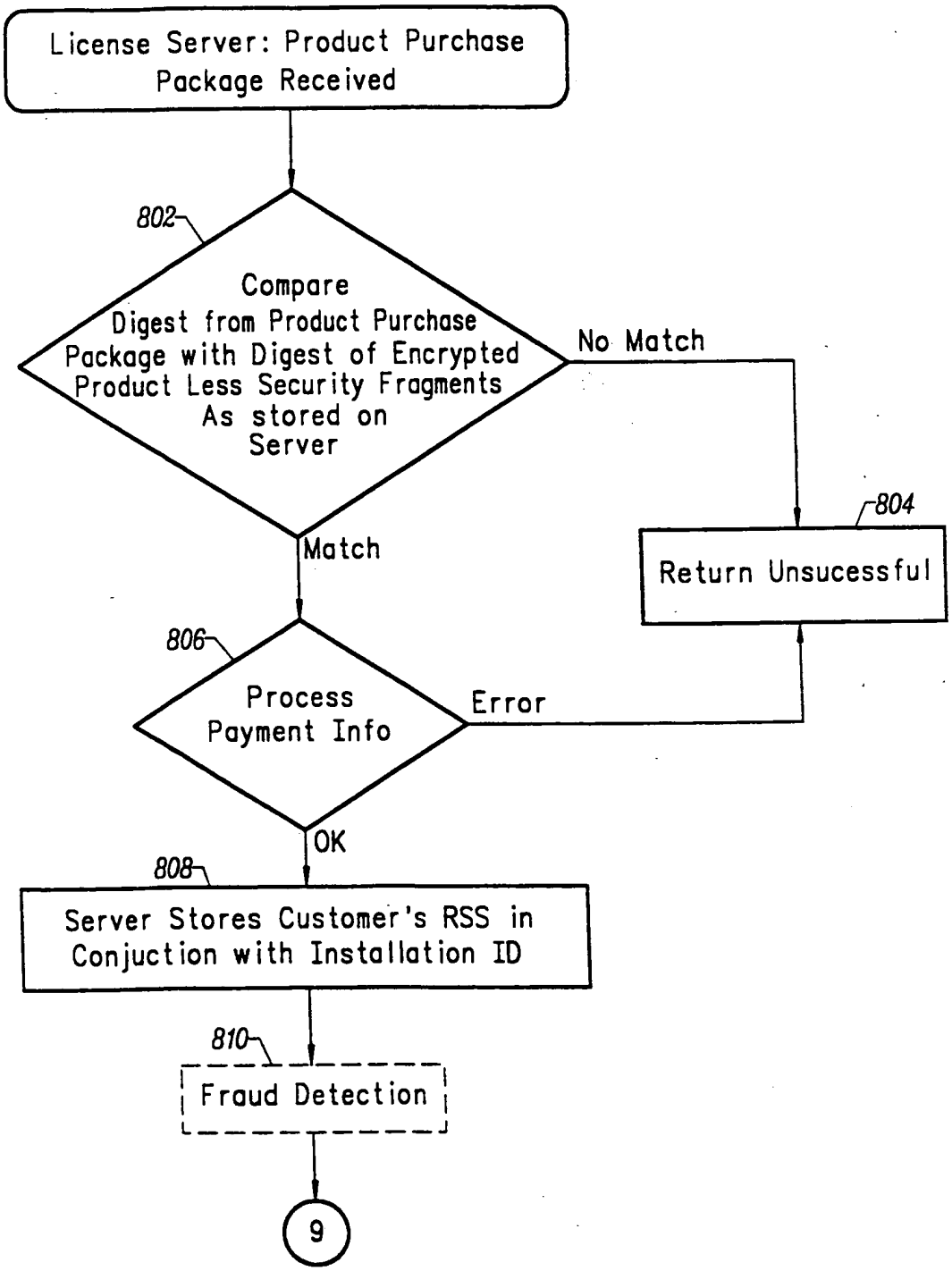


FIG. 8

BNSDOCID: <WO__9842098A1_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1757

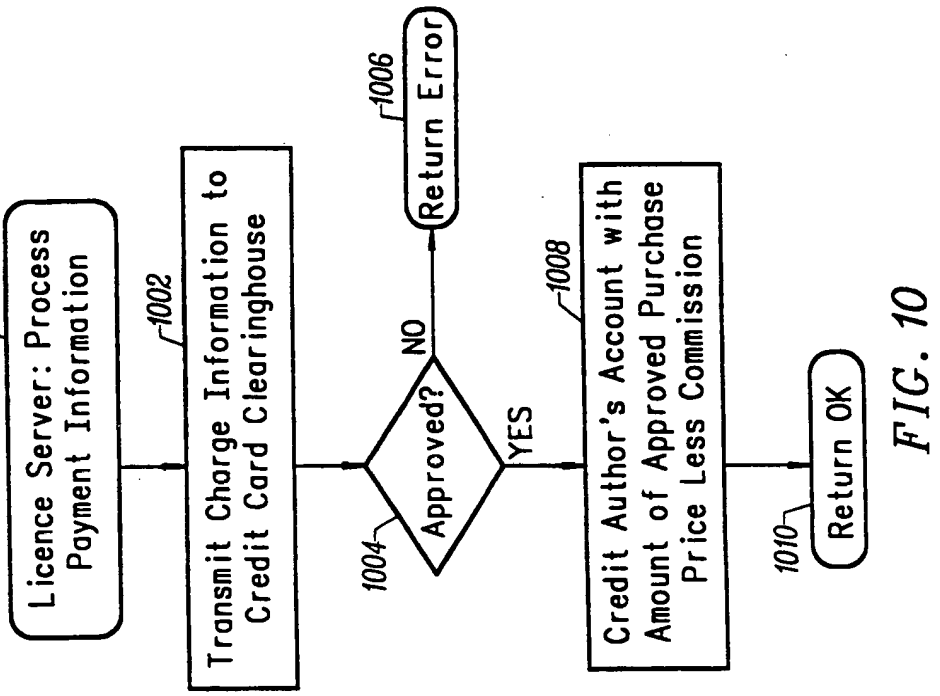


FIG. 10

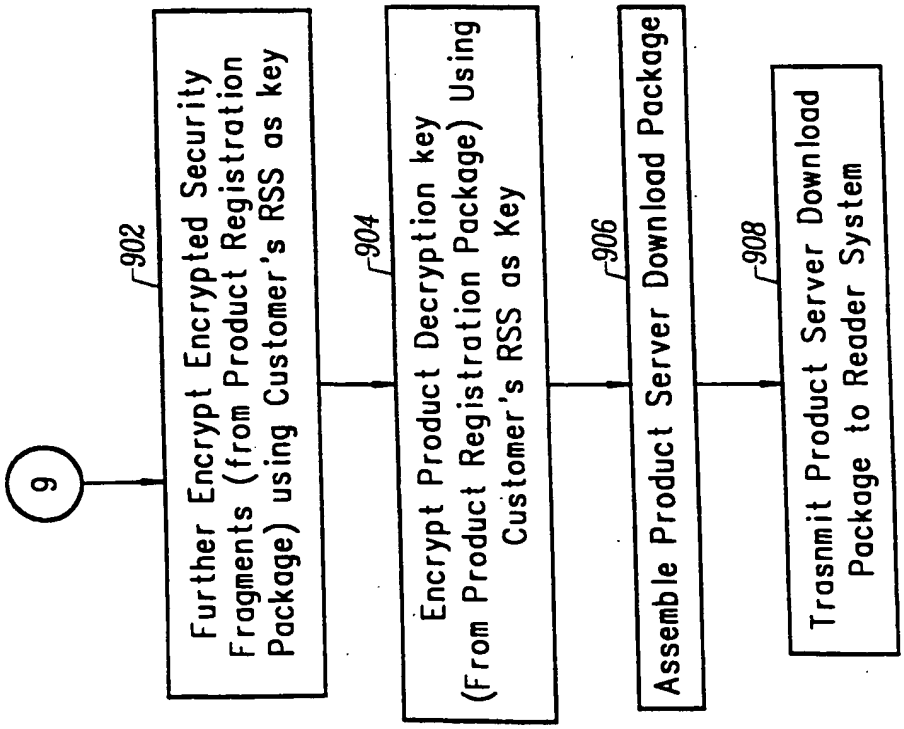


FIG. 9

BNSDOCID: <WO___9842098A1_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1758

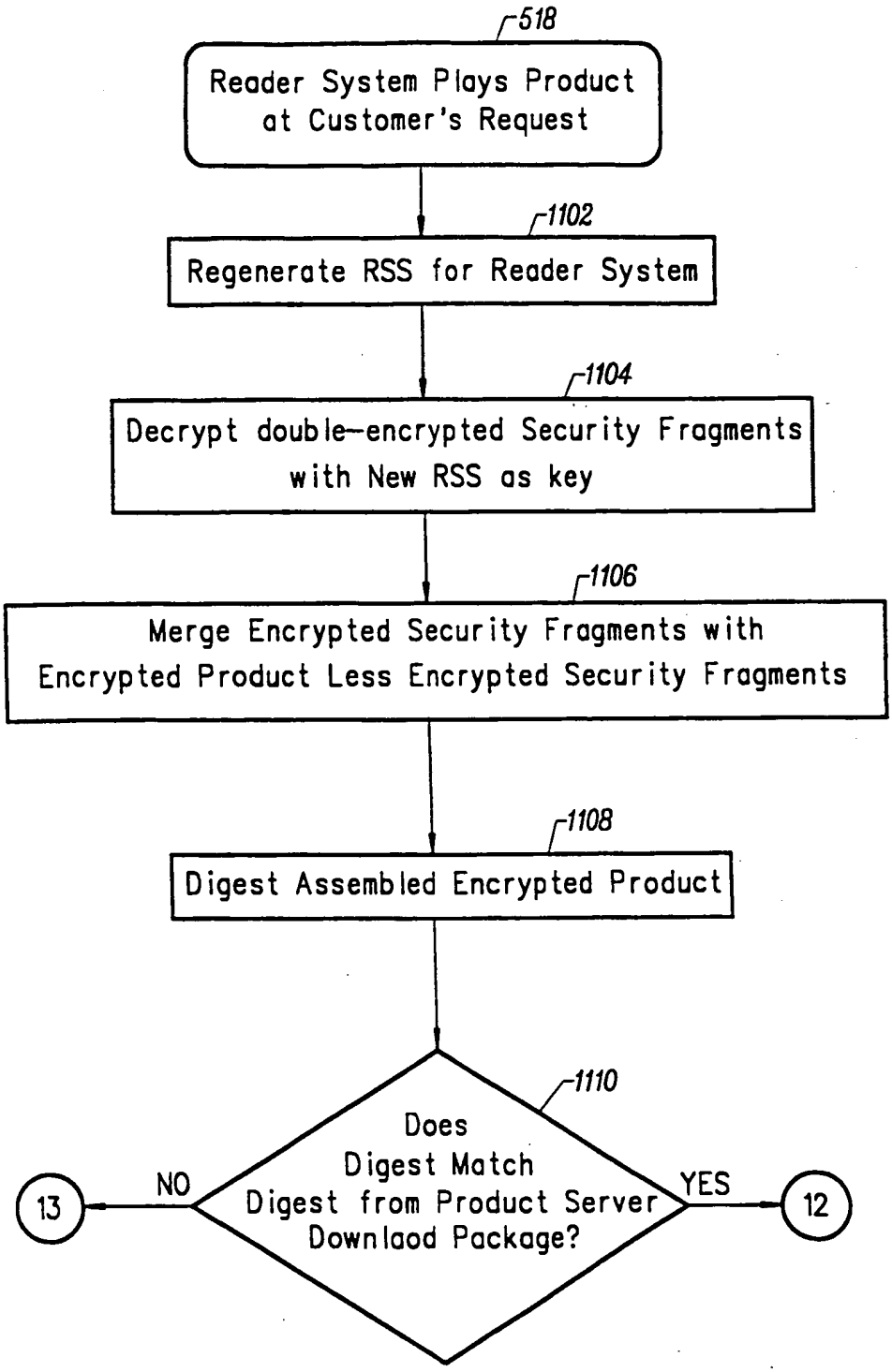


FIG. 11

BNSDOCID: <WO__9842098A1_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1759

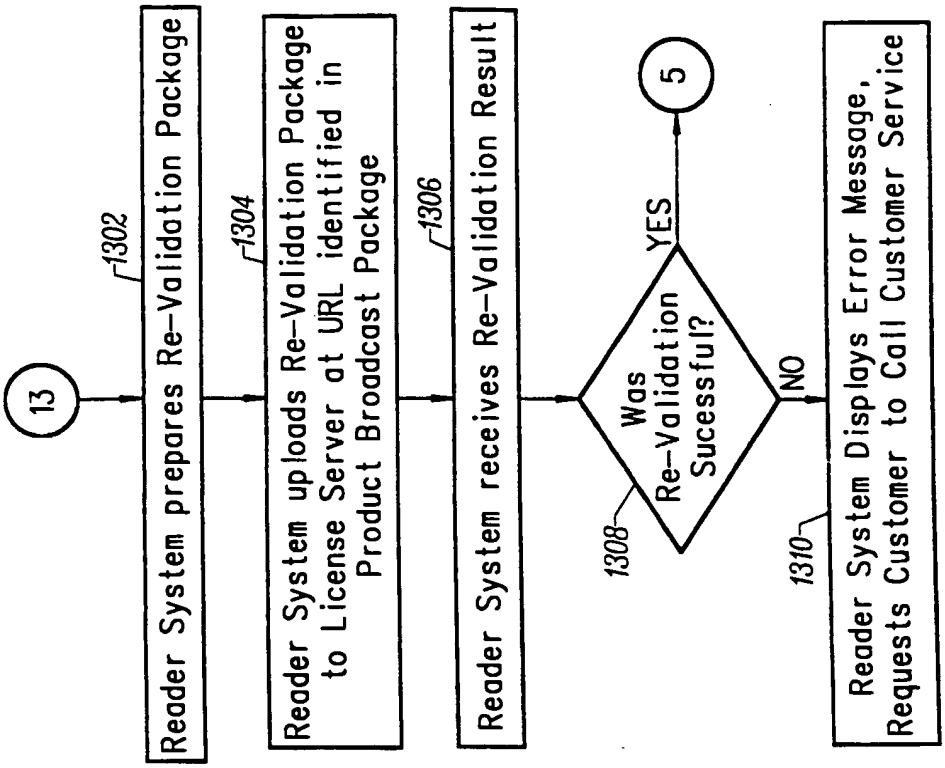


FIG. 13

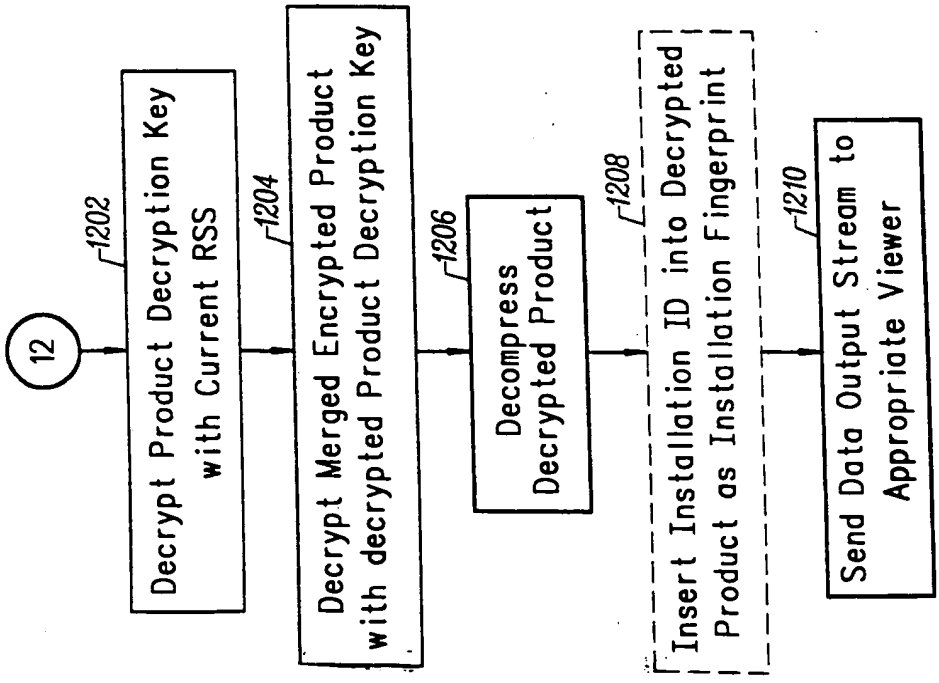


FIG. 12

BNSDOCID: <WO___9842098A1_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1760

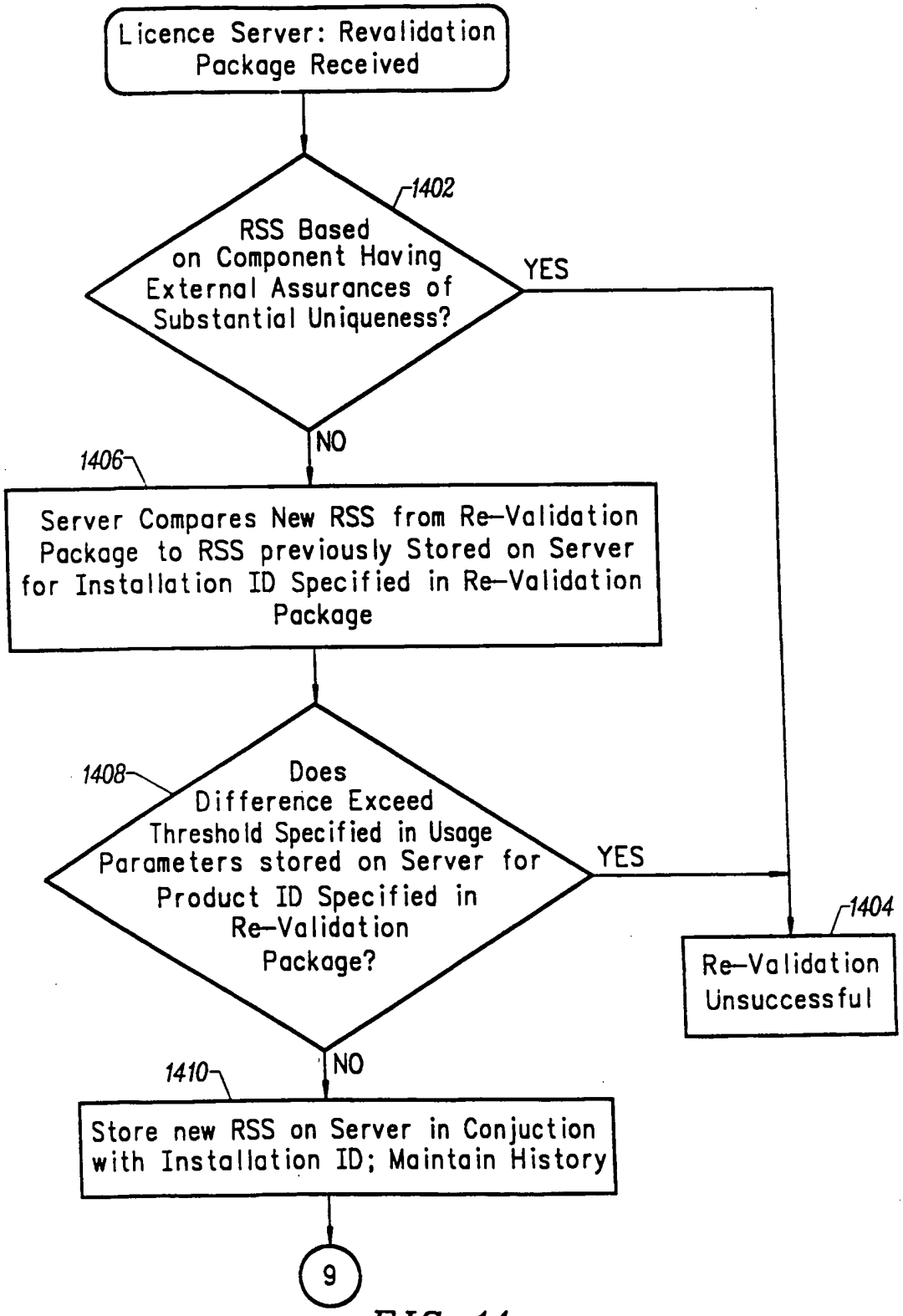


FIG. 14

BNSDOCID: <WO___9842098A1_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1761

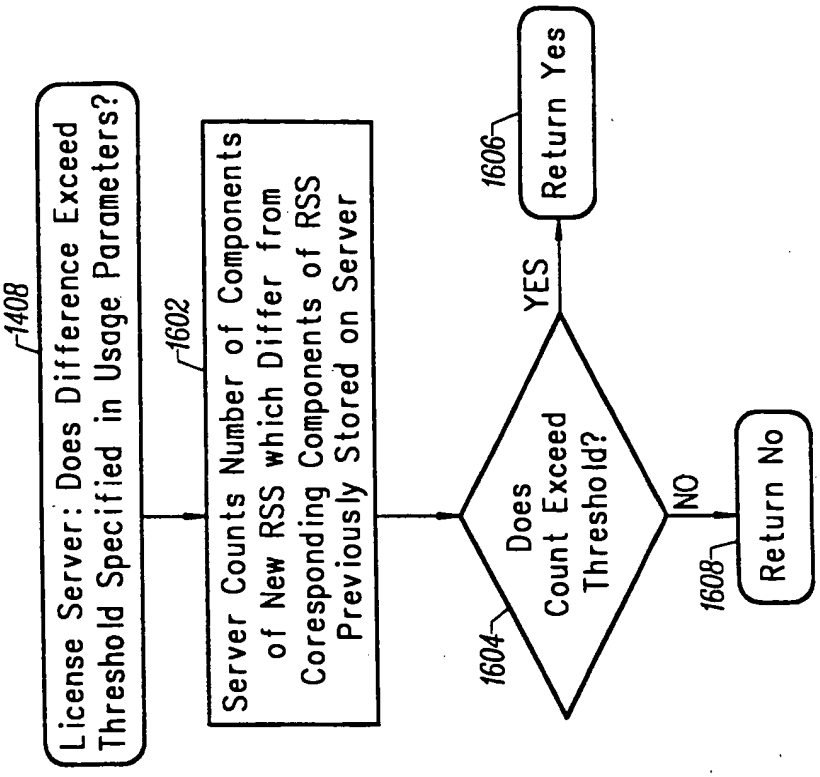


FIG. 16

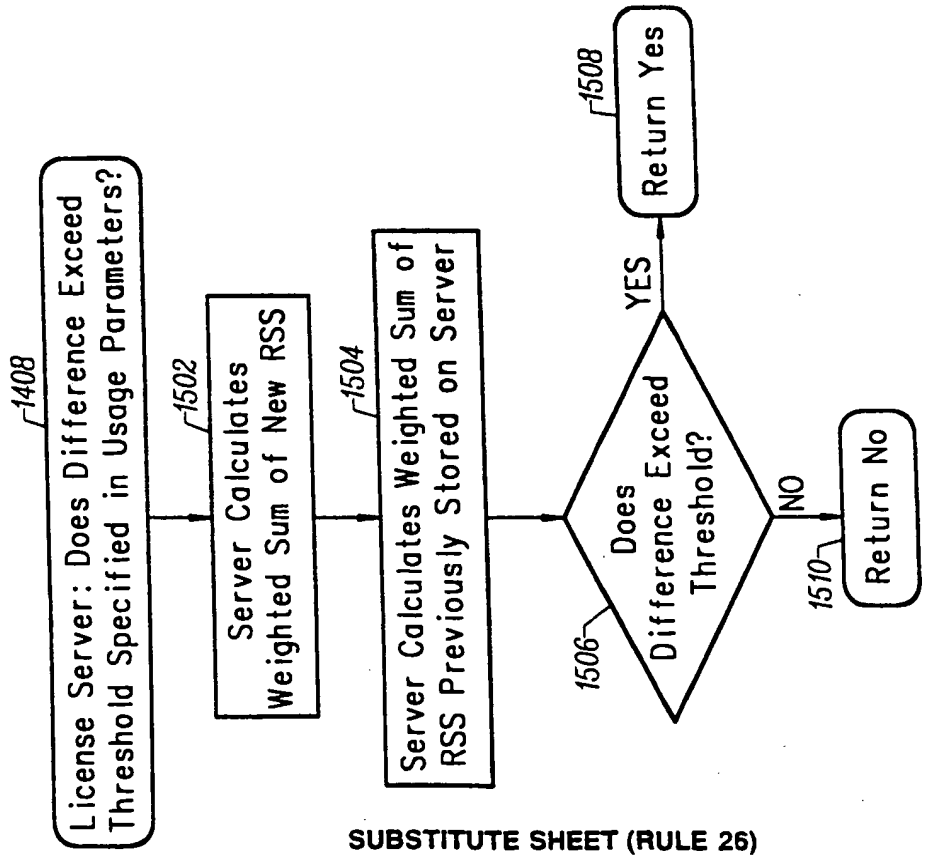


FIG. 15

BNSDOCID: <WO___9842098A1_I_>

Petitioner Apple Inc. - Exhibit 1012, p. 1762

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/04658

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :H04L 9/00
US CL :380/49
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/49, 4, 28, 30

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,530,757 A (KRAWCZYK) 25 June 1996, See Fig 3.	1-31
Y, P	US 5,613,004 A (COOPERMAN ET AL) 18 March 1997 See entire document.	1-31
Y	LITTMANN, M., Planet Graphics is aiming to orbit the Internet, Crain's chicago business 09 December 1996, page 18.	1-31
Y	FEDER, J., Applying Pay-per-View Idea to the Compact Disk Business, The New York Times, 30 September 1996, article.	1-31

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

*	Special categories of cited documents	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search 05 JUNE 1998	Date of mailing of the international search report 01 JUL 1998
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer SALVATORE CANGIALOSI Telephone No. (703) 305-1837

Form PCT/ISA/210 (second sheet)(July 1992)*

BNSDOCID: <WO___9842098A1_I_>

This Page Blank (uspto)

Refine Search

Search Results -

Terms	Documents
(copy adj control) and fee and @ay<1995	9

Database:
US Pre-Grant Publication Full-Text Database
US Patents Full-Text Database
US OCR Full-Text Database
EPO Abstracts Database
JPO Abstracts Database
Derwent World Patents Index
IBM Technical Disclosure Bulletins

Search: L7

Refine Search

Recall Text | Clear | Interrupt

Search History

DATE: Tuesday, July 20, 2004 Printable Copy Create Case

Set Name side by side	Query	Hit Count	Set Name result set
	DB=USPT; PLUR=YES; OP=OR		
L7	(copy adj control) and fee and @ay<1995	9	L7
L6	L5 and @ay<1995	33	L6
L5	(control with use with software) and copy and meter	58	L5
L4	(5673316 or 5825883).pn.	2	L4
L3	5499298.pn.	1	L3
L2	(5802518 or 5794217 or 4999806 or 5337357 or 5375240 or 5671412 or 5790664 or 5651064 or 4740890 or 5889860 or 5592549 or 5502766 or 5982390 or 5666411 or 5673316 or 5499298 or 5765152 or 5532920 or 5825883 or 4528643).pn. and @ay<1995	9	L2
L1	(5802518 or 5794217 or 4999806 or 5337357 or 5375240 or 5671412 or 5790664 or 5651064 or 4740890 or 5889860 or 5592549 or 5502766 or 5982390 or 5666411 or 5673316 or 5499298 or 5765152 or 5532920 or 5825883 or 4528643).pn. and @ay<1994	5	L1

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,951	12/17/2001	Mark J. Stefik	111325-88	5128

22204 7590 07/27/2004

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

EXAMINER	
HEWITT II, CALVIN L	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 07/27/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

Office Action Summary	Application No.	Applicant(s)
	10/015,951	STEFIK ET AL.
	Examiner	Art Unit
	Calvin L Hewitt II	3621

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *11 March 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

Status of Claims

1. Claims 1-34 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-3, 6, 9, 21, and 24 are rejected under 35 U.S.C. 102(e) as being clearly anticipated by Hartrick et al., U.S. Patent No. 5,532,920.

As per claims 1-3, 6, 9, 21, and 24, Hartick et al. teach a digital work distribution system comprising:

- digital content representing a portion of a digital work rendered on a rendering device (figure 1)
- usage rights associated with said digital content that indicate one or more ways said work can be used or distributed (figures 3A-7)

- usage rights that further specify status information indicating the status of the digital work and a fee (revenue) type and parameter (e.g. best price fee) (figures 10 and 11)
- storing content and rights on the same device (figure 1; column 4, lines 40-53)
- usage rights that include state information indicating the extent of the manner of use exercised by an authorized user (column 14, lines 15-50; column 15, lines 1-42)

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

5. Claims 4, 5, 7, 8, and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartrick et al., U.S. Patent No. 5,532,920 in view of Sprague et al., U.S. Patent No. 5,247,575.

As per claims 4, 5, 7, 8, and 26, Hartick et al. teach a digital content distribution system where users are charged fees for accessing content (figures 10 and 11). However, Hartick et al. do not specifically recite fees based on time.

Sprague et al. teach a digital content distribution system (abstract; column 24, lines 9-16) where users are charged based on the type or class of content, time or subscription (column 4, lines 8-56; column 13, lines 24-59). Sprague et al. also teach maintaining a database that stores user fee, account and other statistical information (e.g. usage) (column/line 19/63-20/18; column 23, lines 47-66), as well as fee tables, or schedules and authorized users (column 22, lines 59-66; column 23, lines 46-65). Regarding schedules, fee or tables are old and well known. Similarly, "mark-up" prices are old and well known to those of ordinary skill in retail. Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Hartrick et al. and Sprague et al. in order to allow users the opportunity to select an access method (e.g. rent, purchase, subscription) that best meets their needs.

6. Claims 10 and 25 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartrick et al., U.S. Patent No. 5,532,920.

As per claim 10, Hartick et al. teach that usage rights may be integrated within the text or in a separate file (column 4, lines 45-50; column/line 4/66-5/5). Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to store (e.g. floppy disk, CD-ROM) the rights on a separate disk if additional space was needed.

As per claim 25, Hartrick et al. teach storing book data such as author, title, copyright date and edition (figure 5). Therefore, it would have been obvious to store other bibliographic data such as publisher and publication date.

7. Claims 11-19, 23, and 27-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartrick et al., U.S. Patent No. 5,532,920 in view of Comerford et al. U.S. Patent No. 5,109,413.

As per claims 11-19, 23, and 27-33, Hartrick et al. teach a method and system of content distribution comprising:

- digital content representing a portion of a digital work rendered on a rendering device (figure 1)
- usage rights associated with said digital content that indicate one or more ways said work can be used or distributed (figures 3A-7)
- usage rights that further specify status information indicating the status of the digital work and a fee type and parameter (e.g. best price fee (figures 10 and 11)
- storing content and rights on the same device (figure 1; column 4, lines 40-53)

Regarding storing rights and content on different devices, Hartick et al. teach that usage rights may be integrated within the text or in a separate file (column 4, lines 45-50; column/line 4/66-5/5). Therefore, it would have been obvious to one

of ordinary skill at the time the invention was made to store (e.g. floppy disk, CD-ROM) the rights on a separate disk if additional space was needed. Hartrick et al. also teach storing book data such as author, title, copyright date and edition (figure 5). Therefore, it would have been obvious to stored other bibliographic data such as publisher and publication date. However, Hartrick et al. do not specifically recite distribution rights. Comerford et al. teach a software distribution system where a user can obtain rights to execute (e.g. no. of executions, period of time) and transfer software (abstract; figure 19; column/line 18/38-20/42; column 29, lines 17-47). Regarding schedules, fee or tables are old and well known. Similarly, "mark-up" prices are old and well known to those of ordinary skill in retail. Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Hartick et al. and Comerford et al. in order to provide publishers with a mechanism for allowing users to share content within the copy protection parameters set by the publisher ('413, column 2, lines 5-22).

8. Claim 22 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hartrick et al., U.S. Patent No. 5,532,920 in view of Wolfe, U.S. Patent No. 4,796,220.

As per claim 22, Hartrick et al. teach a digital distribution system of right protected content where users are charged fees for accessing content (figures 3A-7, 10 and 11). However, Hartrick et al. do not specifically recite indicating the

number of copies in use. Wolfe teaches a method for controlling the copying of software comprising indicating the number of copies (abstract; column 2, lines 32-52). Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Hartrick et al. and Wolfe et al. in order to allow publishers to track the number of copies in use and charge accordingly ('220, column 1, lines 40-46; column 4, lines 49-68).

9. Claim 34 is rejected under 35 U.S.C. 103(a) as being unpatentable over Hartrick et al., U.S. Patent No. 5,532,920 and Comerford et al. U.S. Patent No. 5,109,413 as applied to claim 27 above, and in further view of Sprague, U.S. Patent No. 5,247,575.

As per claim 34, Hartick et al. teach a digital content distribution system where users are charged fees for accessing content (figures 10 and 11). Comerford et al. teach a software distribution system where a user can obtain rights to execute (e.g. no. of executions, period of time) and transfer software (abstract; figure 19; column/line 18/38-20/42; column 29, lines 17-47). However, neither Hartrick et al. nor Comerford et al. specifically recite tracking the history of at least one of use and distribution of the digital work. Sprague et al. teach a digital distribution system that maintains at a user site a database that stores user fee, account and other statistical information (e.g. usage) (column/line 19/63-20/18; column 23, lines 47-66), as well as fee tables, or schedules and

authorized users (column 22, lines 59-66; column 23, lines 46-65). Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Hartrick et al., Comerford et al. and Sprague et al. in order to allow users the opportunity to select an access method (e.g. rent, purchase, subscription) that best meets their needs.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure:

- Narasimhalu et al. teach incorporating usage rights and history with content
- Grundy teaches content distribution
- McCarty teaches providing distribution rights to a user

11. Any inquiry concerning this communication or earlier communications from the Examiner should be directed to Calvin Loyd Hewitt II whose telephone number is (703) 308-8057. The Examiner can normally be reached on Monday-Friday from 8:30 AM-5:00 PM.

If attempts to reach the Examiner by telephone are unsuccessful, the Examiner's supervisor, James P. Trammell, can be reached at (703) 305-9768.

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

c/o Technology Center 2100

Washington, D.C. 20231

or faxed to:

(703) 305-7687 (for formal communications intended for entry and after-final communications),

or:

(703) 746-5532 (for informal or draft communications, please label "PROPOSED" or "DRAFT")

Hand-delivered responses should be brought to Crystal Park 5, 2451 Crystal Drive, 7th Floor Receptionist.

Any inquiry of a general nature or relating to the status of this application should be directed to the Group receptionist whose telephone number is (703) 308-1113.

Calvin Loyd Hewitt II

July 21, 2004

JAMES P. TRAMMELL
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

Search Notes

Application No.	Applicant(s)	
10/015,951	STEFIK ET AL.	
Examiner	**Art Unit**	
Calvin L Hewitt II	3621	

SEARCHED			
Class	Subclass	Date	Examiner
705	50-54	7/20/2004	CLH2

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
Used West in an attempt to locate prior and relevant art; text search independent of class/sub	7/20/2004	CLH2

Notice of References Cited	Application/Control No. 10/015,951	Applicant(s)/Patent Under Reexamination STEFIK ET AL.	
	Examiner Calvin L Hewitt II	Art Unit 3621	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-5,532,920 A	07-1996	Hartrick et al.	715/500
	B	US-5,109,413 A	04-1992	Comerford et al.	705/54
	C	US-4,796,220 A	01-1989	Wolfe, Everett W.	705/56
	D	US-5,247,575 A	09-1993	Sprague et al.	705/53
	E	US-5,499,298 A	03-1996	Narasimhalu et al.	705/54
	F	US-5,666,411 A	09-1997	McCarty, Johnnie C.	705/51
	G	US-5,375,240 A	12-1994	Grundy, Gregory	713/200
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Index of Claims

Application No.	Applicant(s)
10/015,951	STEFIK ET AL.
Examiner	**Art Unit**
Calvin L Hewitt II	3621

√	Rejected	–	(Through numeral) Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

Claim		Date
Final	Original	7/21/04
	1	√
	2	
	3	
	4	
	5	
	6	
	7	
	8	
	9	
	10	
	11	
	12	
	13	
	14	
	15	
	16	
	17	
	18	
	19	
	20	
	21	
	22	
	23	
	24	
	25	
	26	
	27	
	28	
	29	
	30	
	31	
	32	
	33	
	34	√
	35	
	36	
	37	
	38	
	39	
	40	
	41	
	42	
	43	
	44	
	45	
	46	
	47	
	48	
	49	
	50	

Claim		Date
Final	Original	
	51	
	52	
	53	
	54	
	55	
	56	
	57	
	58	
	59	
	60	
	61	
	62	
	63	
	64	
	65	
	66	
	67	
	68	
	69	
	70	
	71	
	72	
	73	
	74	
	75	
	76	
	77	
	78	
	79	
	80	
	81	
	82	
	83	
	84	
	85	
	86	
	87	
	88	
	89	
	90	
	91	
	92	
	93	
	94	
	95	
	96	
	97	
	98	
	99	
	100	

Claim		Date
Final	Original	
	101	
	102	
	103	
	104	
	105	
	106	
	107	
	108	
	109	
	110	
	111	
	112	
	113	
	114	
	115	
	116	
	117	
	118	
	119	
	120	
	121	
	122	
	123	
	124	
	125	
	126	
	127	
	128	
	129	
	130	
	131	
	132	
	133	
	134	
	135	
	136	
	137	
	138	
	139	
	140	
	141	
	142	
	143	
	144	
	145	
	146	
	147	
	148	
	149	
	150	

L Number	Hits	Search Text	DB	Time stamp
1	350	705/51.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:10
2	158	705/52.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:10
3	74	705/53.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:10
4	81	705/54.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:10
5	78	705/55.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:10
6	78	705/56.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:10
7	281	705/57.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:10
8	105	705/58.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:10
9	156	705/59.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:11
10	71	705/50.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:12
11	246	380/201.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:15
12	723	707/9.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:18
13	0	707/9.CCLS. AND DRM	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:16
15	2281	707/104.1.ccls.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:16
16	2	707/104.1.ccls. and "digital rights management"	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:17
17	220	713/182.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:18

Scanned Titles and Abstracts Read some

Petitioner Apple Inc. - Exhibit 1012, p. 1779

18	189	713/183.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:18
19	109	713/184.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:18
20	241	713/185.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:19
21	166	713/186.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:19
-	946	"digital rights management" or DRM	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 12:06
-	409	("digital rights management" or DRM) and (play or copy or save or transfer or crop or extract or embed or delete or render)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:13
-	207	(("digital rights management" or DRM) and (play or copy or save or transfer or crop or extract or embed or delete or render)) and distribut$	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:02
-	172	((("digital rights management" or DRM) and (play or copy or save or transfer or crop or extract or embed or delete or render)) and distribut$) and (NOT ginter)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 15:47
-	33	wyman WITH robert	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:34
-	5225	grammar	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:07
-	162	grammar and permission	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:06
-	203	grammar and (permission or privilege)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:06
-	1763	grammar and rights	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:06
-	127	(grammar and rights) and permission	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:06
-	1197	grammar and rule and (permission or priviliege or rights)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:08
-	109	grammar and rule and (permission or priviliege) and rights	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:10

Scanned Titles and Abstracts; Read Some

Scanned. Read Some, KWIC

KWIC Read

-	1034	(grammar or language) and rule and (permission or priviliege) and rights	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:10
-	107	(grammar and language) and rule and (permission or priviliege) and rights	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:11
-	106	((grammar and language) and rule and (permission or priviliege) and rights) and (play or copy or save or transfer or crop or extract or embed or delete or render)	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:13
-	73	embed$ WITH extract$ WITH digital and rights Scanned titles, KWIC Read	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:22
-	295	embed$ WITH extract$ WITH digital	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:30
-	438	embed$ WITH extract$ SAME digital	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:30
-	4	wyman WITH robert and fee	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 14:34
-	4	wyman WITH robert and fee and distribut$	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 15:39
-	4	(("5335346") or ("5295266")).PN.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 15:28
-	4	wyman WITH robert and fee and distribut$ AND PRINT Read, Scanned KWIC	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 15:39
-	6	((("digital rights management" or DRM) and (play or copy or save or transfer or crop or extract or embed or delete or render)) and distribut$) and (NOT ginter) and print and repository	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 15:48
-	28	((("digital rights management" or DRM) and (play or copy or save or transfer or crop or extract or embed or delete or render)) and distribut$) and (NOT ginter) and print	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 15:49
-	3250	repository and print$	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 15:55
-	1750	repository and print$ and "rights"	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 15:50
-	566	repository and print$ and "rights" and copyright	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 15:53
-	26	repository and print$ and "copy rights" Scanned Some	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 15:54

-	498	repository SAME print$	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/08/27 15:56
-	4	(("5295266") or ("5335346")).PN.	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 12:15
-	2	("5138712").PN. Read	USPAT; EPO; JPO; DERWENT; IBM_TDB	2004/10/18 14:09

Interview Summary	Application No.	Applicant(s)	
	10/015,951	STEFIK ET AL.	
	Examiner	Art Unit	
	Calvin L Hewitt II	3621	

All participants (applicant, applicant's representative, PTO personnel):

(1) *Calvin L Hewitt II*.

(2) James Trammell

(3) Bijan Tadayon

(4) Carlos Villamar

Date of Interview: 1/7/05

Type: a)☒ Telephonic b)☐ Video Conference
c)☑ Personal [copy given to: 1)☐ applicant 2)☑ applicant's representative]

Exhibit shown or demonstration conducted: d)☐ Yes e)☑ No.
If Yes, brief description: _____.

Claim(s) discussed: 1.

Identification of prior art discussed: Hertrick.

Agreement with respect to the claims f)☑ was reached. g)☐ was not reached. h)☐ N/A.

Substance of Interview including description of the general nature of what was agreed to if an agreement was reached, or any other comments: Language to emphasize Peer to Peer Aspects of Applicant's system.

(A fuller description, if necessary, and a copy of the amendments which the examiner agreed would render the claims allowable, if available, must be attached. Also, where no copy of the amendments that would render the claims allowable is available, a summary thereof must be attached.)

THE FORMAL WRITTEN REPLY TO THE LAST OFFICE ACTION MUST INCLUDE THE SUBSTANCE OF THE INTERVIEW. (See MPEP Section 713.04). If a reply to the last Office action has already been filed, APPLICANT IS GIVEN ONE MONTH FROM THIS INTERVIEW DATE, OR THE MAILING DATE OF THIS INTERVIEW SUMMARY FORM, WHICHEVER IS LATER, TO FILE A STATEMENT OF THE SUBSTANCE OF THE INTERVIEW. See Summary of Record of Interview requirements on reverse side or on attached sheet.

Examiner Note: You must sign this form unless it is an Attachment to a signed Office action.

Examiner's signature, if required

Petitioner Apple Inc. - Exhibit 1012, p. 1783

Summary of Record of Interview Requirements

Manual of Patent Examining Procedure (MPEP), Section 713.04, Substance of Interview Must be Made of Record
A complete written statement as to the substance of any face-to-face, video conference, or telephone interview with regard to an application must be made of record in the application whether or not an agreement with the examiner was reached at the interview.

Title 37 Code of Federal Regulations (CFR) § 1.133 Interviews
Paragraph (b)
In every instance where reconsideration is requested in view of an interview with an examiner, a complete written statement of the reasons presented at the interview as warranting favorable action must be filed by the applicant. An interview does not remove the necessity for reply to Office action as specified in §§ 1.111, 1.135. (35 U.S.C. 132)

37 CFR §1.2 Business to be transacted in writing.
All business with the Patent or Trademark Office should be transacted in writing. The personal attendance of applicants or their attorneys or agents at the Patent and Trademark Office is unnecessary. The action of the Patent and Trademark Office will be based exclusively on the written record in the Office. No attention will be paid to any alleged oral promise, stipulation, or understanding in relation to which there is disagreement or doubt.

The action of the Patent and Trademark Office cannot be based exclusively on the written record in the Office if that record is itself incomplete through the failure to record the substance of interviews.

It is the responsibility of the applicant or the attorney or agent to make the substance of an interview of record in the application file, unless the examiner indicates he or she will do so. It is the examiner's responsibility to see that such a record is made and to correct material inaccuracies which bear directly on the question of patentability.

Examiners must complete an Interview Summary Form for each interview held where a matter of substance has been discussed during the interview by checking the appropriate boxes and filling in the blanks.. Discussions regarding only procedural matters, directed solely to restriction requirements for which interview recordation is otherwise provided for in Section 812.01 of the Manual of Patent Examining Procedure, or pointing out typographical errors or unreadable script in Office actions or the like, are excluded from the interview recordation procedures below. Where the substance of an interview is completely recorded in an Examiners Amendment, no separate Interview Summary Record is required.

The Interview Summary Form shall be given an appropriate Paper No., placed in the right hand portion of the file, and listed on the "Contents" section of the file wrapper. In a personal interview, a duplicate of the Form is given to the applicant (or attorney or agent) at the conclusion of the interview. In the case of a telephone or video-conference interview, the copy is mailed to the applicant's correspondence address either with or prior to the next official communication. If additional correspondence from the examiner is not likely before an allowance or if other circumstances dictate, the Form should be mailed promptly after the interview rather than with the next official communication.

The Form provides for recordation of the following information:
- Application Number (Series Code and Serial Number)
- Name of applicant
- Name of examiner
- Date of interview
- Type of interview (telephonic, video-conference, or personal)
- Name of participant(s) (applicant, attorney or agent, examiner, other PTO personnel, etc.)
- An indication whether or not an exhibit was shown or a demonstration conducted
- An identification of the specific prior art discussed
- An indication whether an agreement was reached and if so, a description of the general nature of the agreement (may be by attachment of a copy of amendments or claims agreed as being allowable). Note: Agreement as to allowability is tentative and does not restrict further action by the examiner to the contrary.
- The signature of the examiner who conducted the interview (if Form is not an attachment to a signed Office action)

It is desirable that the examiner orally remind the applicant of his or her obligation to record the substance of the interview of each case. It should be noted, however, that the Interview Summary Form will not normally be considered a complete and proper recordation of the interview unless it includes, or is supplemented by the applicant or the examiner to include, all of the applicable items required below concerning the substance of the interview.

A complete and proper recordation of the substance of any interview should include at least the following applicable items:
1) A brief description of the nature of any exhibit shown or any demonstration conducted,
2) an identification of the claims discussed,
3) an identification of the specific prior art discussed,
4) an identification of the principal proposed amendments of a substantive nature discussed, unless these are already described on the Interview Summary Form completed by the Examiner,
5) a brief identification of the general thrust of the principal arguments presented to the examiner,
   (The identification of arguments need not be lengthy or elaborate. A verbatim or highly detailed description of the arguments is not required. The identification of the arguments is sufficient if the general nature or thrust of the principal arguments made to the examiner can be understood in the context of the application file. Of course, the applicant may desire to emphasize and fully describe those arguments which he or she feels were or might be persuasive to the examiner.)
6) a general indication of any other pertinent matters discussed, and
7) if appropriate, the general results or outcome of the interview unless already described in the Interview Summary Form completed by the examiner.

Examiners are expected to carefully review the applicant's record of the substance of an interview. If the record is not complete and accurate, the examiner will give the applicant an extendable one month time period to correct the record.

Examiner to Check for Accuracy

If the claims are allowable for other reasons of record, the examiner should send a letter setting forth the examiner's version of the statement attributed to him or her. If the record is complete and accurate, the examiner should place the indication, "Interview Record OK" on the paper recording the substance of the interview along with the date and the examiner's initials.

OIPE JC98 JAN 27 2005 PATENT & TRADEMARK OFFICE

Docket No. 111325-88 (020700)
Serial No. 10/015,951

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	
Mark J. **STEFIK,** *et al.*	)	Group Art Unit: 3621
Serial No. 10/015,951	)	Examiner: Hewitt II, Calvin L.
Filed: December 17, 2001	)	Confirmation No. 5128
For: DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME	))	

Commissioner of Patents
U.S. Patent and Trademark Office
Customer Window, Mail Stop Non-Fee Amendment
Randolph Building
Alexandria, VA 22314

RESPONSE

Sir:

In response to the non-final Office Action mailed **July 27, 2004**, the following amendments and remarks are submitted in connection with the above-identified application.

Petitioner Apple Inc. - Exhibit 1012, p. 1785

OIPE JC98 JAN 27 2005 PATENT & TRADEMARK OFFICE

1FW 3624

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. **STEFIK**, *et al.*
Group Art Unit	3621
Examiner Name	Calvin L. Hewitt, II
Total Number of Pages in This Submission	**Attorney Docket Number** 111325-88 (020700)
	Confirmation Number 5128

ENCLOSURES *(check all that apply)*

- ☒ Fee Transmittal Form
  - ☐ Fee Attached
- ☒ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☒ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Assignment Papers *(for an Application)*
- ☐ Drawing(s)
- ☐ Declaration and Power of Attorney
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance Communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Application Data Sheet
- ☐ Request for Corrected Filing Receipt with Enclosures
- ☐ A self-addressed prepaid postcard for acknowledging receipt
- ☐ Other Enclosure(s) (*please identify below*):

Remarks

☒ The Commissioner is hereby authorized to charge any additional fees required or credit any overpayments to Deposit Account No. 19-2380 for the above identified docket number.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm *or* Individual name	Carlos R. Villamar Registration No. 43,224 Nixon Peabody LLP 401 9th Street, N.W, Suite 900 Washington, D.C. 20004-2128
Signature	
Date	January 27, 2005

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

- ☐ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop _____, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450
- ☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) _____.

_____ Date

_____ Signature

_____ Typed or printed name

FEE TRANSMITTAL FOR FY 2005

Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT | **$1,020.00**

Complete if Known	
Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. STEFIK, et al.
Examiner Name	Calvin L. Hewitt, II
Art Unit	3621
Attorney Docket No.	111325-88 (020700)

OIPE JC98 JAN 27 2005 PATENT & TRADEMARK OFFICE

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit Card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 19-2380

Deposit Account Name: Nixon Peabody LLP

The Commissioner is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	300	2001	150	Utility filing fee	
1002	200	2002	100	Design filing fee	
1003	200	2003	100	Plant filing fee	
1004	300	2004	150	Reissue filing fee	
1005	200	2005	100	Provisional filing fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

		Extra Claims		Fee from below		Fee Paid
Total Claims	34	-34** = 0	X		=	0
Independent Claims	4	-4** = 0	X		=	0
Multiple Dependent			X		=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	50	2202	25	Claims in excess of 20
1201	200	2201	100	Independent claims in excess of 3
1203	360	2203	180	Multiple dependent claim, if not paid
1204	200	2204	100	** Reissue independent claims over original patent
1205	50	2205	25	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($)0.00

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	
1051	130	2051	65	Surcharge – late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1,020	2253	510	Extension for reply within third month	1,020.00
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1,080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	
1403	1,000	2403	500	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	500	2452	250	Petition to revive – unavoidable	
1453	1,500	2453	750	Petition to revive – unintentional	
1501	1,400	2501	700	Utility issue fee (or reissue)	
1502	800	2502	400	Design issue fee	
1503	1,100	2503	550	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	790	2809	395	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) **$1,020.00**

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

☐ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop _____, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450

☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) _____.

Date _____ Signature _____

Typed or printed name _____

SUBMITTED BY

Complete *(if applicable)*					
Name *(Print/Type)*	Carlos R. Villamar	Registration No. *(Attorney/Agent)*	43,224	Telephone	(202) 585-8204
Signature				Date	January 27, 2005

SEND TO: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

W632781.1

OIPE JC98 JAN 27 2005 PATENT & TRADEMARK OFFICE

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 111325-88 (020700)

CERTIFICATE OF MAILING OR TRANSMISSION
[37 CFR 1.8(a)]

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to Mail Stop _____, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, or being facsimile transmitted to the USPTO at _____, on _____.

Signature:_____

Name:_____

In re Application of
Mark J. **STEFIK**, *et al.*

Application Number: 10/015,951 | Filed: December 17, 2001

For: **DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME**

Group Art Unit: 3621 | Examiner: Calvin L. Hewitt, II

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and appropriate entity fee are as follows (check time period desired):

- ☐ One month (37 CFR 1.17(a)(1)) - ($60/$120) $_____
- ☐ Two months (37 CFR 1.17(a)(2)) - ($225/$450) $_____
- ☒ Three months (37 CFR 1.17(a)(3)) - ($510/$1020) $ 1,020.00
- ☐ Four months (37 CFR 1.17(a)(4)) - ($795/$1590) $_____
- ☐ Five months (37 CFR 1.17(a)(5)) - ($1080/$2160) $_____

☐ Applicant claims small entity status.

☐ A check to cover the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Commissioner has already been authorized to charge fees in this application to a Deposit Account.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 19-2380.
I have enclosed a duplicate copy of this sheet.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the ☐ applicant/inventor

☐ assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

☐ attorney or agent of record.

☒ attorney or agent under 37 CFR 1.34(a).
Registration number if acting under 37 CFR 1.34(a) 43,224.

_____ January 27, 2005
Signature Date

Carlos R. Villamar (202) 585-8204
Typed or printed name Telephone Number

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

☐ Total of _____ forms are submitted.

SEND TO: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

W632785.1

10051951
02/01/2005 SDENBOB1 00000013 192380
01 FC:1253 1020.00 DA

REMARKS

Claims 1-34 are pending in the present application, [[[with claims 1, 11, 21, 26, 27 and 34 amended without the introduction of new matter (see, e.g., Specification, ¶¶ **[0094]** and **[0097]**, and FIG. 15).

As a preliminary matter, Applicant requests consideration of the previously filed Information Disclosure Statements, for example, as filed on July 31, August 9 and 30, and September 27, 2002.

Referring now to the present Office Action, claims 1-3, 6, 9, 21, and 24 were rejected under 35 U.S.C. §102(e) based on *Hartrick et al.*, U.S. Patent No. 5,532,920; claims 4,5,7,8, and 26 were rejected under 35 U.S.C. §103(a) based on *Hartrick et al.* in view of *Sprague et al.*, U.S. Patent No. 5,247,575; claims 10, and 25 were rejected under 35 U.S.C. §103(a) based on *Hartrick et al.*; claims 11-19, 23, and 27-33 were rejected under 35 U.S.C, §103(a) based on *Hartrick et al.* in view of in view of *Comerford et al.*, U.S. Patent No. 5,109,413; claim 22 was rejected under 35 U.S.C. §103(a) based on *Hartrick et al.* in view of in view of *Wolfe*, U.S. Patent No. 4,796,220; and claim 34 was rejected under 35 U.S.C. §103(a) based on *Hartrick et al.* and *Comerford et al.* in view of *Sprague et al.*

The rejection of claims 1-34 is respectfully overcome because *Hartrick et al.*, *Comerford et al.*, *Sprague et al.*, and *Wolfe,* taken alone or in combination, fail to disclose, teach or suggest all of the features recited in the amended claims. For example, independent claims 1, 11, 21, and 27, as amended, recite "usage rights expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use indicating one or more stated purposes for which the digital work can be used and distributed by an authorized party."

By contrast, *Hartrick et al.* discloses a data processing system and method to enforce payment of royalties when copying softcopy books, wherein a publisher of a softcopy book includes royalty payment information either within the structured document text of the book or in a royalty payment information file which accompanies the book, and to read the book from the storage disk, the user applies a special softcopy book reading program. *Hartrick et al.* further discloses employing a structured document having tags for indicating royalty payment information for collecting fees for copying the softcopy

Petitioner Apple Inc. - Exhibit 1012, p. 1789

books (Figs. 3A-3C, and cols. 7-8). However, *Hartrick et al.* fails to disclose such tags being employed for "specifying a manner of use indicating one or more stated purposes for which the digital work can be used and distributed by an authorized party," as recited in independent claims 1, 11, 21, and 27.

Comerford et al. discloses manipulating rights-to-execute in connection with a software copy protection mechanism, wherein a software asset protection mechanism segregates the right to execute software from the software itself, and the rights to execute, when installed on a composite computing system, are stored in a coprocessor element of the composite computing system. *Comerford et al.* further discloses transfer of the execution rights based on a token or a disk and token pair (col. 4, line 41 to col. 5, line 9). However, *Comerford et al.* fails to disclose "usage rights expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols," as recited in independent claims 1, 11, 21, and 27.

Sprague et al. discloses an information distribution system that provides information to a user, when the information corresponds to criteria individually selected by the user, and then charges the user only for the selected information thus provided, wherein encrypted information packages (IP's) are provided at the user site, via high and/or low density storage media and/or by broadcast transmission. However, *Sprague et al.* fails to disclose "usage rights expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use indicating one or more stated purposes for which the digital work can be used and distributed by an authorized party," as recited in independent claims 1, 11, 21, and 27.

Wolfe discloses method of controlling the copying of software, wherein an authorized user of a program is allowed to make any number of backup copies of a computer program and to execute each such backup copy on the same authorized machine, but is inhibited from executing either the original or any copy thereof on any other machine, by including a control program with the application program to be copy controlled, and which control program causes an interaction and registration of the program during initialization of the program with a central computer. However, *Wolfe* fails to disclose "usage rights expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use

Petitioner Apple Inc. - Exhibit 1012, p. 1790

indicating one or more stated purposes for which the digital work can be used and distributed by an authorized party," as recited in independent claims 1, 11, 21, and 27.

Advantageously, employing "usage rights expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use indicating one or more stated purposes for which the digital work can be used and distributed by an authorized party," as recited in independent claims 1, 11, 21, and 27," enables the support of a wide variety of distribution and fee schemes (see, e.g., Specification, p. 25, ¶ **[0095]**). By contrast, *Hartrick et al.*, *Comerford et al.*, *Sprague et al.*, and *Wolfe*, taken alone or in combination, fail to disclose, teach or suggest "usage rights expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use indicating one or more stated purposes for which the digital work can be at least one of used and distributed by an authorized party," as recited in independent claims 1, 11, 21, and 27, nor the advantages thereof.

Dependent claims 2-10, 12-26, and 28-34 are allowable over *Hartrick et al.*, *Comerford et al.*, *Sprague et al.*, and *Wolfe,* taken alone or in combination, on their on merits and for at least the reasons as argued above with respect to independent claims 1, 11, 21, and 27.

The prior art that has been cited, but not applied by the Examiner, has been taken into consideration during formulation of this response. However, since this art was not considered by the Examiner to be of sufficient relevance to apply against any of the claims, no detailed comments thereon are believed to be warranted at this time.

Petitioner Apple Inc. - Exhibit 1012, p. 1791

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. If, however, the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

Respectfully submitted,

NIXON PEABODY, LLP

Carlos R. Villamar
Reg. No. 43,224

Date: **January 27, 2005**

NIXON PEABODY LLP
CUSTOMER NO.: 22204
401 9th Street, N.W., Suite 900
Washington, DC 20004
Tel: 202-585-8000
Fax: 202-585-8080

Petitioner Apple Inc. - Exhibit 1012, p. 1792

Amendments to the Claims:

1. (Currently amended) A digital work adapted to be distributed within a system for controlling ~~at least one of~~ the distribution and use of digital works, said digital work comprising:

digital content representing a portion of a digital work suitable for being rendered by a rendering device; and

usage rights associated with said digital content, said usage rights expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use indicating one or more stated purposes for which the digital work can be ~~at least one of~~ used and distributed by an authorized party.

2. (Original) The digital work as recited in claim 1, wherein said usage rights further specify status information indicating the status of the digital work.

3. (Original) The digital work as recited in claim 1, wherein said usage rights further specify a usage fee associated with exercise of the manner of use, said usage fee comprising a fee type and fee parameters.

4. (Original) The digital work as recited in claim 3 wherein said fee type is a metered use fee and said fee parameters comprise a fee unit and a time unit.

5. (Original) The digital work as recited in claim 3 wherein said fee type is a per use fee and said fee parameter comprises a fee unit.

6. (Original) The digital work as recited in claim 3 wherein said fee type is a best price fee and said fee parameters comprise an identifier to identify said best price.

7. (Original) The digital work as recited in claim 3 wherein said fee type is a scheduled fee and said fee parameters comprise time units and fee units.

Petitioner Apple Inc. - Exhibit 1012, p. 1793

8. (Original) The digital work as recited in claim 3 wherein said fee type is a mark-up fee and said fee parameters comprise a mark-up percentage.

9. (Original) The digital work as recited in claim 1 wherein said digital content and said usage rights are stored on the same physical device.

10. (Original) The digital work as recited in claim 1, wherein said digital content and said usage rights are stored on different physical devices.

11. (Currently amended) A method for creating a digital work to be used in a system for reporting fees associated with ~~at least one of~~ distribution and use of the digital work, said method comprising:

a) obtaining digital content representing a portion of a digital work suitable for being rendered by a rendering device;

b) associating usage rights with the digital content, the usage rights expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use indicating one or more stated purposes for which the digital work can be ~~at least one of~~ used and distributed by an authorized party; and

c) storing the digital content and the usage rights as the digital work.

12. (Original) A method as recited in claim 11, wherein said storing step comprises storing the digital content and the usage rights on the same physical device.

13. (Original) A method as recited in claim 11, wherein said storing step comprises storing the digital content and the usage rights on different physical devices.

14. (Original) A method as recited in claim 11, wherein said usage rights further specify a usage fee associated with exercise of the manner of use.

15. (Original) The method as recited in claim 14, wherein said usage fee comprises usage fee information including a fee type and fee parameters.

Petitioner Apple Inc. - Exhibit 1012, p. 1794

16. (Original) The method as recited in claim 15 wherein said fee type is a metered use fee and said fee parameters comprise a fee unit and a time unit.

17. (Original) The method as recited in claim 15 wherein said fee type is a per use fee and said fee parameters comprise a fee unit.

18. (Original) The method as recited in claim 15 wherein said fee type is a best price fee and said fee parameters comprise an identifier to identify the best price.

19. (Original) The method as recited in claim 15 wherein said fee type is a scheduled fee and said fee parameters comprise time units and fee units.

20. (Original) The method as recited in claim 17 wherein said fee type is a mark-up fee and said fee parameters comprise a mark-up percentage.

21. (Currently amended) A digital work adapted to be distributed within a system for controlling ~~at least one of~~ the distribution and use of digital works, said system having a mechanism for reporting status information relating to digital works, said digital work comprising:

digital content representing a portion of a digital work suitable for being rendered by a rendering device; and

usage rights associated with said digital content, said usage rights expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use indicating one or more stated purposes for which the digital work can be ~~at least one of~~ used and distributed by an authorized party, said usage rights also including state information indicating the extent of the manner of use exercised by ~~an~~ the authorized ~~user~~ party.

22. (Original) A digital work as recited in claim 21, wherein the state information comprises information indicating the number of copies of the digital work that are in use.

Petitioner Apple Inc. - Exhibit 1012, p. 1795

23. (Original) A digital work as recited in claim 21, wherein the state information comprises information indicating the number of time units for which the digital work can be used.

24. (Original) A digital work as recited in claim 21, wherein the state information comprises information indicating the revenue owner of the digital work.

25. (Original) A digital work as recited in claim 21, wherein the state information comprises information indicating the publication date of the digital work.

26. (Currently amended) A digital work as recited in claim 21, wherein the state information comprises information indicating the history of ~~at least one of~~ the use and distribution of the digital work.

27. (Currently amended) A method for creating a digital work to be used in a system for reporting fees associated with ~~at least one of~~ distribution and use of the digital work, said method comprising:

a) obtaining digital content representing a portion of a digital work suitable for being rendered by a rendering device;

b) associating usage rights with the digital content, the usage rights expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use indicating one or more stated purposes for which the digital work can be ~~at least one of~~ used and distributed by an authorized party, said usage rights also including state information indicating the extent of the manner of use exercised by ~~an~~ the authorized ~~user~~ party; and

c) storing the digital content and the usage rights as the digital work.

28. (Original) A method as recited in claim 27, wherein said storing step comprises storing the digital content and the usage rights on the same physical device.

Petitioner Apple Inc. - Exhibit 1012, p. 1796

29. (Original) A method as recited in claim 27, wherein said storing step comprises storing the digital content and the usage rights on different physical devices.

30. (Original) A method as recited in claim 27, wherein the state information comprises information indicating the number of copies of the digital work that are in use.

31. (Original) A method as recited in claim 27, wherein the state information comprises information indicating the number of time units for which the digital work can be used.

32. (Original) A method as recited in claim 27, wherein the state information comprises information indicating the revenue owner of the digital work.

33. (Original) A method as recited in claim 27, wherein the state information comprises information indicating the publication date of the digital work.

34. (Currently amended) A method as recited in claim 27, wherein the state information comprises information indicating the history of ~~at least one of~~ the use and distribution of the digital work.

Petitioner Apple Inc. - Exhibit 1012, p. 1797

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2001

Application or Docket Number: 10.015951

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	34	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	34 minus 20=	* 14
INDEPENDENT CLAIMS	4 minus 3 =	* 1
MULTIPLE DEPENDENT CLAIM PRESENT		☐

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY TYPE ☐		OR	OTHER THAN SMALL ENTITY	
RATE	FEE		RATE	FEE
BASIC FEE	370.00	OR	BASIC FEE	740.00
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL		OR	TOTAL	

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 34	Minus	** 34	=
Independent	* 4	Minus	*** 4	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Best Available Copy

EP 18527 IX (5)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 538 216 A1**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **92850205.3**

(51) Int. Cl.[5] : **H04M 1/68, H04L 9/32**

(22) Date of filing : **02.09.92**

(30) Priority : **12.09.91 SE 9102641**

(43) Date of publication of application :
21.04.93 Bulletin 93/16

(84) Designated Contracting States :
BE DE ES FR GB LU NL

(71) Applicant : **TELEVERKET**
S-123 86 Farsta (SE)

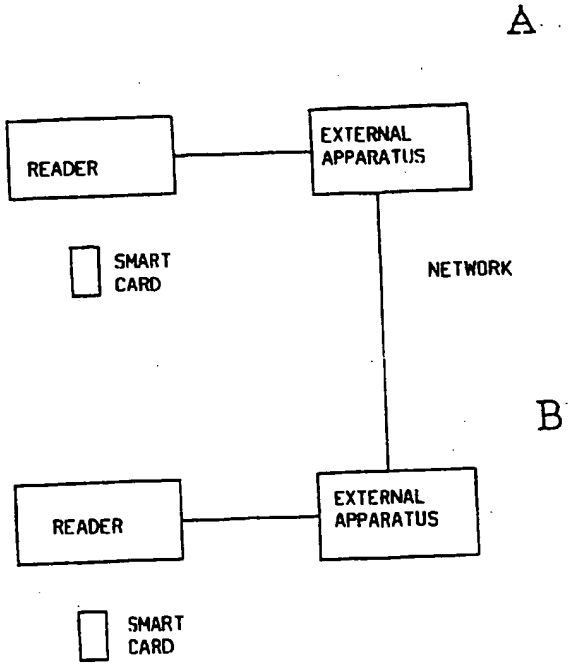
(72) Inventor : **Anvret, Lena**
STT AB, P.O: Box 1001
S-123 24 Farsta (SE)
Inventor : Mersich, Laszlo
STT AB, P.O: Box 1001
S-123 24 Farsta (SE)

(74) Representative : **Akerman, Marten Lennart et al**
c/o Lars Holmqvist Patentbyra AB P.O. Box 4289
S-203 14 Malmö 4 (SE)

BEST AVAILABLE COPY

(54) Means for identification and exchange of encryption keys.

(57) The invention relates to a means for identification and exchange of encryption keys between communicating apparatuses for encrypted transmissions. The means comprises a card reader for smart cards connected to the communication apparatus which may be a telecommunication apparatus, e.g. of telephone or facsimile type. The reader can communicate with another reader at a called telecommunication apparatus. For identification and exchange of encryption keys the required calculations are performed by the reader or the smart card using data stored on the smart card in a protected field with limited access. The means enable intercommunication between products of different makes owing to a standard identification procedure and exchange of encryption keys.



FIG

EP 0 538 216 A1

FIELD OF THE INVENTION

The present invention relates to means for identification and exchange of encryption keys between two communicating apparatuses for encrypted transmissions, comprising readers connected to the communication apparatuses. Each reader contains a reader unit which together with software is capable of handling smart cards. The reader can communicate with another reader in the other communication apparatus. The means includes a built-in keyboard for inputting of data.

STATE OF THE ART

Existing products for encryption, facsimile apparatuses, telephone, etc., often follow standards with respect to communication and algorithms, but exclude intercommunication between two products of different makes. A cheap accessory for these and new products would enable different makes to intercommunicate through a standard identification procedure and exchange of encryption keys. In addition, modern smart cards may be used in the procedures enabling strong algorithms and enhanced security.

SUMMARY OF THE INVENTION

The present invention provides a means for identification and exchange of encryption keys between two communicating apparatuses for encrypted transmissions. According to the invention a reader for smart cards is connected to each communication apparatus. The required calculations are performed by the reader or the smart card using data stored on the smart card in a proctected field with limited access.

Preferably the communication apparatus is a facsimile apparatus or a telephone.

Further embodiments of the invention are set forth in detail in the accompanying claims.

BRIEF DESCRIPTION OF THE DRAWINGS

The invention will now be described in detail with reference to the accompanying drawings in which the figure is a block diagram of the means according to the invention connected in a network.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENTS OF THE INVENTION

In the figure the means according to the invention is shown connected in a network, e.g. a telecommunication system. Between the external apparatuses exist encrypted traffic. The external apparatuses may be telephone or facsimile apparatuses. For identification and exchange of encryption keys two card readers are used communicating with each other. As a basis for the identification two smart cards are used which means that the identification is performed by the card (and its owner) and that the reader as such does not contain anything confidential.

The reader may be connected in parallell with a telephone to an ordinary telephone jack via a standard intermediate plug (not shown). The reader contains a reader unit that, together with software functions, is capable of handling smart cards. The reader can communicate through dual-tone multifrequency (DTMF) signalling or using a modem. In addition, it has a built-in keyboard for data input. The control of the reader is performed through anyone of the two communication channels available, using DTMF signalling or modem.

It is also possible to intergrate the telecommunication apparatus and the card reader into a unit. In this case the unit has a single keyboard and a slot for inserting the smart card.

The reader is controlled by a central unit. It is an eight bit central processing unit built for maximal integration of the function of the card reader directly in the central unit. The central unit is made with CMOS technology warranting a low current consumption. Internally there is random excess memory RAM having 256 bytes which is sufficient for the functions to be performed by the reader. The machine code may be stored in a programmable read-only memory PROM or mask programmed directly in the central unit to minimize the current consumption and the price.

The card reader is equipped with a built-in keyboard containing 12 keys: the digits 0-9 and the characters * and #. The appearance corresponds to keyboards of ordinary telephones. The keyboard is connected directly to the central unit eliminating the risk of leakage of input information.

The reader unit as such is intended for mounting directly on the circuit board which is important to minimize the overall size and price of the construction. The reader unit is adapted for handling all smart cards in the market. The reader unit is totally passive and is only a link between the card and the central unit. Via the reader unit the central unit can communicate with the card and assist with current supply and clock. Various supply voltages and clock frequencies are supplied to the card in dependence of which card is connected.

The basic communication is achieved using DTMF signalling. The reader is provided with both DTMF transmitter and receiver. The transfer rate is normally 10 characters (10 x 4 bits) per second. The DTMF receiver is connected in parallel with the ordinary telecommunication traffic which means that it can receive data both from the user's telephone and from the telecommunication network.

Since DTMF signalling sets large limitations in the amount of data which can be transferred the reader is also equipped with a built-in modem. The modem

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1800

can handle communication according to CCITT V.21 and V.23, resulting in a transfer rate ranging to 1200 bps. This provides a greater flexibility with respect to the functions to be performed by the reader.

The reader is also fitted with a number of light-emitting diodes (LED) in various colours, the functions of which will be described below.

The reader is constructed from low current consumption components but the most current consuming component is the smart card. Since various cards will be used no exact current consumption can be calculated. Additionally, the cards consume more current when they are written so that the current consumption varies with time. The current supply is provided by a battery or a battery eliminator. With a 9 V alkaline battery a continuous operation of the reader of approximately 3-4 hours is achieved. One of the above-mentioned light-emitting diodes indicates low battery voltage and need for change of battery.

When a card is inserted into the reading unit of the reader the reader is started automatically. When the card is pulled out the reader is switched off. Since smart cards are depedent of current supply from the reader they will return to idle position when pulled out of the reader unit. When the reader is started by inserting a card in the reader unit a yellow light-emitting diode is lighted. The reader tests the card to identify the type of smart card being used. If a card is accepted the yellow LED is switched off and the reader is ready for use. This means that the reader proceeds to listen for DTMF signals sent from the called system. If the reader does not recognize the card as anyone of the accepted types the card is of an unknown type or turned the wrong way. Then a red LED is lighted and the reader waits for the card to being pulled out. All calls to the reader will then only give an error message as response.

Using the keyboard the user can input data locally to the reader. The inputted information may then be used as data for a command to the card. The most common type of inputted information is a personal code which is to be tested in the card, but can also be another type of data, e.g. information to be encrypted. None of the operations on the keyboard will be sent in clear text on the telephone line. The reader accepts input from the keyboard after a command from the called system. When this is about to happen a green LED is lighted to indicate that the data is to be input. The input is terminated with "#" and the green LED is switched off. When the LED is switched off no manipulations on the keyboard will either be stored or sent on the line.

In a connected mode the reader listens continuously on the data in the form of DTMF signals or via the modem being sent from the called system. When a start character is detected the reader perceives this as a start of a command. The telecommunication apparatus is then disconnected from the line and the reader goes to a command mode. The reader now collects all data through the signal "#" indicating end of command. If there is a delay of more than one second between the various character the command is considered lost and the reader returns to search for the start character. When the whole command is received it will be decoded and performed. After the command is performed the reader always sends back a response. Thereafter the telephone is again connected to the line and the reader returns to listening. However, when the modem is connected the user will always be disconnected from the line. From the moment the reader has detected the start character until the reader has sent the whole response the yellow LED will be lighted.

The reader always begins in DTMF mode, i.e. it listens for DTMF signals from the called system. By means of a command it is possible to change communication channel and instead connect the modem. Thus, there is a number of various operation modes: DTMF signalling and signalling with a modem with various transfer rates. The operation mode of the modem can be changed during ongoing modem traffic by means of a new command on the modem line. This enables e.g. a change between 1200/75 bps as transmission rate. The response to the command will always be issued on the communication channel on which the command was sent, DTMF or modem. The change of communication channel or operation mode of the modem will not occur until after the response has been transmitted.

By sending a command the reader can be requested to accept data from the user via the keyboard. The green LED is lighted to indicate that input is to be performed on the key-board. The input is terminated by the user depressing the character #. The green LED is switched off when the input is terminated. The user has maximally 30 seconds to input data. If the input is not terminated within this time period instead an error code is returned. This command is normally used to accept the personal code which is to be used for opening the card connected.

A command may be sent directly to the card connected. The reader awaits a response from the card and then returns it. The reader waits maximally 30 seconds for a response. After this time period instead an error code is returned. The reader only investigates the length of the command as a controll that sufficient data has been transmitted. Besides this no check of the command is performed. It is the task of the calling system to see to it that the command follows the specification of the connected card.

If data has been inputted from the keyboard this may be sent to the connected card using a special command. The input data is stored in a buffer of the keyboard and is transmitted together with the command to the card. Also in this case only the length of the data is checked in the keyboard buffer. The soft-

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1801

ware of the card reader is designed so that two readers can communicate with each other, and the reader is provided with a serial port. This serial port is used to deliver the result of the identification and the exchange of encryption keys to the external unit. In other words, the reader is not used to perform the encryption as such but only for the exchange of keys.

The means should be capable of performing identification of both parties in a communication and should additionally genereate encryption keys exchanged between the systems. Identities and encryption keys are then delivered to the external apparatus for use. The external apparatus communicates with the card reader via an ordinary asynchronous serial port. The card reader is controlled via this interface to perform identification. The identity and the encryption key are also delivered here. The identity of the user (the apparatus) is stored in smart card. This card is protected by a password which is declared using the keyboard of the card reader. The card is also used in calculating and testing the identity.

Every user gets a pair of keys, one open and one secret key in accordance with RSA (Rivest-Shamir-Adleman). These keys are then used for identification and exchange of keys. According to RSA the keys are preferably chosen in the manner below.

Every user selects himself two large prime numbers p and q and calculates n=pq. From the range [max(p,q) + 1,n - 1] a new number d is chosen and thereafter the number e is calculated. These two new numbers are to be used together with n in encryption and decryption. d should be a prime number and is selected according to certain criteria, wherein the selection has an importance for the strength of the algorithm. e is calculated as $e=inv(d,\varnothing(n)\dagger)$ (†=totient function). d and e then gives the two functions $M=C^d \bmod n$ and $C=M^e \bmod n$, where M is a plain message and C is the encrypted correspondence thereof. Together this means $M = C^d \bmod n = (M^e \bmod n)^d \bmod n = M^{ed} \bmod n = ... = M$, i.e. the two functions are inverses of each other. This means that one key (function) for encryption and another for decryption are used. This is usually called asymmetric encryption.

The above two functions may be denoted as C=E(M) and M=D(C), where E and D are the individual users encryption and decryption transformations, respectively (or vice versa). E may be handed out, while D must be kept secret. Both these transformations (keys) are stored in the smart card of the user. Additionally, D is stored in a way which excludes copying.

In addition, two system constants, a and q, are stored on the smart card. a is a random number and q is a strong prime number ($q = 2p + 1$, where p is a prime number). These two constants are used in calculating the key of the secondary encryption (see below).

Every user has a card reader certificate, a digital identification. This certificate consists of four text fields, separated by semicolons. The entire certificate is stored on the user's smart card. The four fields are:

Identity: A string of any length consisting of alpha-numeric characters.

Public RSA key: This is in turn two fields, e and n (as mentioned above). These two fields are stored as long hexadecimal numbers, separated by a comma.

Validity date of certificate: This is a text field with the form yyyy-mm-dd.

A signature of the above: A hexadecimal number calculated as shown below.

A user's certificate is signed at a certification authority possessing two own transformations D_s and E_s, as shown above. E_s is generally known and resides in our case in the user's smart card. D_s is extremely secret, since D_s is used to generate signatures for all cards. If someone other than the authority would use D_s the whole reliability of the identification is lost. Therefore, D_s is stored in a special smart card and is protected by a password. D_s can never be read, but can only be used by the proprietor of the password. This protection is today the best allowed by technology.

A user, e.g. A, registers with the authority and receives a signature $S_A=D_s$ (MD(the user's certificate)). MD is a "Message Digest" function compressing the field in the certificate (excluding the signature field) to a short number. This function is used to limit the calculation need of long (heavy) numbers. The signature received can then be verified by everybody knowing E_s and is a proof of authentlcity for the user's identity and public key. The signature is stored in the user's smart card together with the rest of the certificate.

When the user A contacts user B they start with exchanging the respective identities, public keys as well as their signatures (certificates). Then A tests whether B and E_B belong together by testing the signature S_B, i.e. if ES (S_B)=MD (B's certificate). B does the same thing. In this way it is possible to learn if the claimed identity and the public key belong together.

A and B then select a random number each which is transmitted in plain text. The opposite party encrypts this using its secret key, i.e. X=D(R), where R is the random number and X is the result. The result of the encryption is then re-transmitted, and the respective reader decrypts this with the public key of the other reader which was in the transmitted certificate. If the random number reappears after the decryption, one of the readers knows that the other reader is the proprietor of the public key, which was in the certificate. Since the certificate has been proven to belong to the alleged identity also the identity has now been verified.

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1802

The last step is exchanging the encryption keys. Each user generates a random number X and calculates $Y=a^x$ mode q. a and q are two system constants and they are stored on the smart card. These Ys are exchanged between the readers, and reader A now calculates $K=Y_B{}^X A \bmod q=(a^xB)^XA \bmod q=a^xB^XA \bmod q$. If B treats Y_A in the corresponding way both A and B will now share the common key K. This key is then used for encryption in a secondary encryption. Since both parties have been involved in generating the key a disclosure of the keys of one party will not disclose K. In addition, by varying X for each session, two sessions will never have the same key.

The various public keys should be readily available to all needing, e.g. to test a signature e.g. in a directory.

A problem with directories is the protection of the contents of the directory. If someone is able to manipulate the public key and mislead those who utilize the directory to use the wrong key, this someone can act as if he was someone else, e.g. mask himself. It is possible to protect the directory from this by the directory being physically and logically protected against manipulation. A secure communication channel directory then provides an adequate protection against most invaders.

However, a more elegant way is that the information in the directory in turn is signed by means of a digital signature. This is achieved by the individual records being signed by a certification authority, which can be viewed in the same way as the authorities issuing ordinary identifications who in fact warrant the authenticity of the identification. This authority should be responsible for the security of the system.

The above description of the directory function works excellently e.g. in a computer network or in other environments where the communication is readily established. However, in many situations this is not possible. If e.g. two facsimile apparatuses are about to identify each other they must have direct access to the public keys of each other. One way to solve this is that the various systems have the key directories stored locally in a safe manner (e.g. in a smart card). The requirements on storage capacity may however be too large, but above all a problem arises when a new system comes into existence or when some system changes key/identity. Then every local directory has to be updated which can be a time-consuming procedure. In addition, there can be an interest in two systems being able to communicate with each other without previous contact. It should be sufficient that both are approved by a common certification authority for communication with each other.

The easiest way to solve this is letting the system exchanging their respective identities and the public keys with each other, signed by the common authority. Using this signature the various systems can check the authenticity of the identity of the others and the public key, without either previous or immediate contact with a third party. The important thing here is the possibility of a safe identification. As no third party is involved in the identification moment the identification procedure must be able to establish the identity with a 100 percent certainty of both parties. Every "masquerade" attempt should be made impossible.

All types of smart cards offer the possibility of protecting data fields using a personal code. These data fields may only be used by the proper user, the smart card not allowing access to these fields without the user having presented the right code. By protecting the key of the user's secret transformation in a public key system in such a data field, it is possible to presume with high reliability the authenticity of messages calculated using this transformation.

The problems associated with the above are mainly two. Partly, the equipment reading the key from the card or later handling it should not be able to be manipulated. In addition, this equipment must have the calculation capacity required for calculate exponents and divisions (modulo) of long numbers in an acceptable time. The first problem can be handled by the equipment being made secure or at least protected by the user in the same way as he/she protects his/her card. As the personal codes of the card often are handled in clear text inside this equipment this is another problem which has to be addressed. The calculation capacity may however be an even bigger problem, since the protection of the equipment only can be guaranteed relatively close to the card (in the card reader), where the calculation capacity often is limited.

One way to solve both problems simultaneously is to let the card as such take care of both the protection of the key and the calculations. This is increasingly more common and today exists in at least two types of smart cards. However, dependent on the choice of identification method, other requirements may be put on the smart card.

To perform an identification and exchange of keys at least five calculations of the type $a^x \bmod p$ are required. All five calculations are of the same type. In addition, this algorithm is built-in in at least two different commercially available smart cards. However, the cards differ as to the ability of calculating with generally selected a, x and p. The most common RSA calculation is the one with the secret key (D), in which case a is d and p is n. In our case, this is only one of the five calculations. In the other cases both x and b are totally different numbers.

Since the card reader is programmed to accept certain cards it is able to choose different methods of securing the identification.

In the most preferred embodiment of the invention the smart card calculates everything. In this type of card the secret part of the RSA key (e) is stored

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1803

safely. In addition, the modulo variable n is stored permanently on the card, so that the card efficiently can perform a^e mode n ($E_i()$ as mentioned above). Additionally, the card can be supplied with general arguments for the RSA algorithm. Since the card is especially designed for calculating with RSA this is the fastest method seen overall. One can assume that one calculation takes maximally one second and, thus, the whole phase of identification and exchange of encryption keys (overhead excluded) will take maximally five seconds.

If the card is not capable of calculating using general arguments for the RSA algorithm the reader has to use its built-in algorithm for calculating everything else than $E_i()$. This means no deterioration to the security, since precisely $E_i()$ is the only thing critical from the security point of view. However, this means a reduced efficiency. An RSA calculation in the card reader takes approximately ten seconds. Since three of the five calculations in this case has to be performed by the reader the whole procedure will take approximately 35 seconds.

If the card is not capable of calculating with RSA at all the reader must take care of all the calculations. The variables (n and p) normally stored permanently in the card are read as data stored on the card in this method. The reader reads these variables from the card in calculating $E_i()$. This means a substantial deterioration of the security, since the identity of the card can be manipulated in this way. The card and the data thereof are however still protected by the password of the card. This is also the least efficient method. The total procedure for identification and exchange of encryption key takes approximately 50 seconds, which is experienced as annoyingly slow. The advantage is that any smart card can be used in this method.

For the reader to be able to be used it has to be activated by inserting one's smart card in the reader. Using the keyboard the password is then inputted to the card, which is opened. Thereafter the reader is ready to receive commands through the serial port or as DTMF signals on the telephone line. If a command enters through the serial port the reader will take the initiative for identification of the other reader. A command from the telephone line is the result of an initiative of the other reader.

The card reader is provided with a serial port. This serial port may be very simple and is capable of transmitting and receiving data in 9600 bps asynchronously, 8 data bits, no parity.

The apparatus controls the reader to perform identification and generation of encryption keys. Since both operations occur simultaneously there is only one command for the apparatus to the reader. The reader transmits a status message to the apparatus simultaneously with the communication with the opposite reader and, after the identification and generation of encryption key, also the result

Between the two readers communication is accomplished by means of DTMF signalling and modem transmission. The DTMF signalling is used to generate the initial contact. The reader that takes the initiative transmits the DTMF sequence "A66#". The other reader responds with the sequence "B66#", whereupon both readers are switched over to modem communication. In modem mode the identification and exchange of encryption keys will be performed. The reader who took the first initiative begins with transmitting in modem mode. Thereafter, the readers are communicating alternatively with each other, until the entire procedure is performed.

Claims

1. Means for identification and exchange of encryption keys between two communicating apparatuses for encrypted transmissions, characterized in that a reader for smart cards is connected to each communication apparatus, the required calculations being performed by the reader or the smart card using data stored on the smart card in a protected field with limited access.

2. Means according to claim 1, **characterized** in that all the calculations are performed by the smart card.

3. Means according to claim 1 or 2, **characterized** in that the reader is connected to the communication apparatus via an asynchronous serial port.

4. Means according to claim 3, **characterized** in that the communication apparatus is a facsimile apparatus or a telephone set.

5. Means according to any one of the preceding claims, **characterized** in that the communication between the readers is achieved by means of dual-tone multifrequency signalling and/or modem communication.

6. Means according to any one of the preceding claims, **characterized** in that the card reader is connected to the telecommunication system in parallel with the telephone set, preferably by means of an intermediate plug.

7. Means according to any one of the preceding claims, **characterized** in that the card reader is integrated with the telephone set provided with a slot for inserting the card.

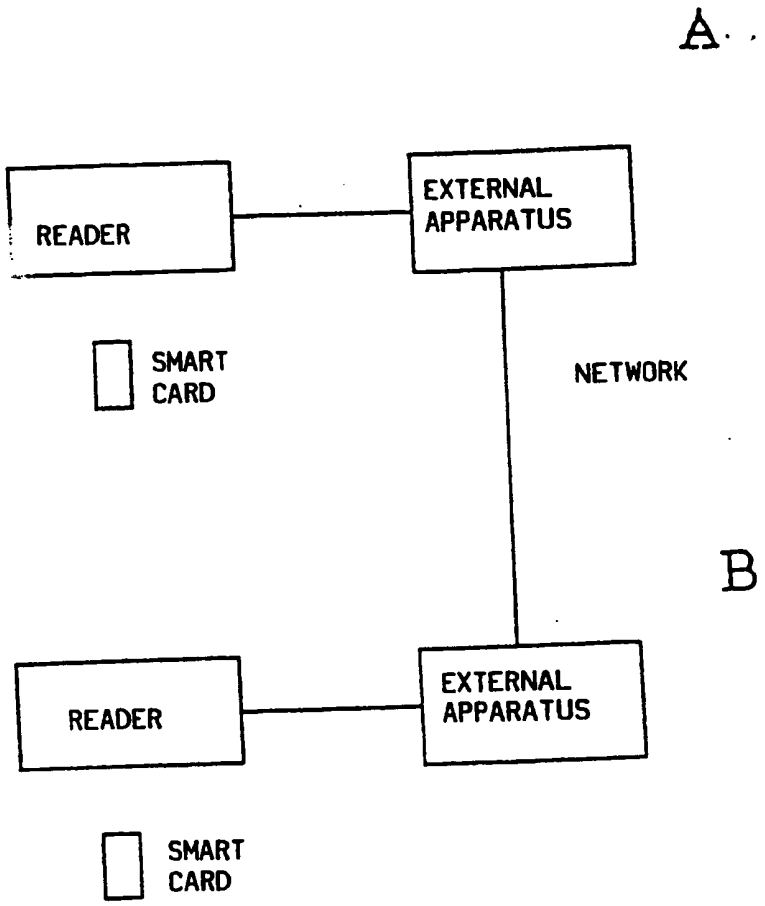
8. Means according to any one of the preceding claims, **characterized** in that bidirectional com-

BEST AVAILABLE COPY

munication in several steps occurs between the communication apparatuses.

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1805



FIG

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1806

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 92 85 0205

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int. Cl.5)
X	EP-A-0 266 044 (COMPUTREX CENTRES) * page 2, line 1 - page 6, line 49 * * page 12 - page 15; figures 1-8 *	1,2,4-6,8 3	H04M1/68 H04L9/32
X	SPEECH TECHNOLOGY vol. 5, no. 2, 1990, NEW YORK pages 66 - 69 , XP149383 MONOT ET AL 'THE FRENCH SECURE TELEPHONE UNIT' * the whole document *	1,4,7,8	
X	PATENT ABSTRACTS OF JAPAN vol. 12, no. 407 (E-675)27 October 1988 & JP-A-63 146 631 (NEC) * abstract *	1,2,4,6-8	
X	PATENT ABSTRACTS OF JAPAN vol. 13, no. 570 (P-977)18 December 1989 & JP-A-12 37 750 (HITACHI) * abstract *	1,8	
A	PATENT ABSTRACTS OF JAPAN vol. 13, no. 558 (E-858)12 December 1989 & JP-A-12 31 451 (IWATSU ELECTRIC) * abstract *	1,3,5-8	TECHNICAL FIELDS SEARCHED (Int. Cl.5) H04M H04L
A	US-A-4 694 492 (WIRSTROM ET AL) * column 6, line 18 - column 9, line 28; figures 1,2 *	1,3,5-8	

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	25 JANUARY 1993	DELANGUE P.C.J.

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P0601)

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1807

THIS PAGE BLANK (USPTO)

THIS PAGE BLANK (USPTO)

XP-002233403

P.D. 30 XII-1993
P. 1-22
22

perh2.txt

Knowbots, Permissions Headers and Contract Law

paper for the conference on

Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment

April 2-3, 1993 with revisions of 4/30/93

Copyright 1993
Henry H. Perritt, Jr.
Professor of Law
Villanova Law School
Villanova, PA 19085
(215) 645-7078
FAX (215) 645-7033, (215) 896-1723
Internet: perritt@ucis.vill.edu

BEST AVAILABLE COPY

Introduction

One of the ways to protect intellectual property on the NREN is through a digital library concept. Under this concept, a work would have attached to it a "permissions header," defining the terms under which the copyright owner makes the work available. The digital library infrastructure, implemented on the NREN, would match request messages from users with the permissions headers. If the request message and the permissions header match, the user would obtain access to the work. This concept encompasses major aspects of electronic contracting, which is already in wide use employing Electronic Data Interchange ("EDI") standards developed by ANSI Committee X12.1

This paper explains the relationship between the digital library concept and EDI practice, synthesizing appropriate solutions for contract law, evidence, and agency issues that arise in electronic contracting. The question of how electronic signatures should work to be legally effective is an important part of this inquiry. The paper also defines particular types of service identifiers, header descriptors, and other forms of labeling and tagging appropriate to allow copyright owners to give different levels of permission, including outright transfer of the copyright interest, use permission, copying permission, distribution permission, display permission, and permission to prepare derivative works.The paper considers how payment authorization procedures should work in conjunction with a permissions header and digital library concept in order to integrate the proposed copyright licensing procedures with existing and anticipated electronic payment authorization systems. The paper necessarily considers whether existing standards approaches related to SGML and X12 are sufficient or whether some new standards development efforts will be necessary for implementation of the concepts. The paper considers the relationship between technology and law in enforcing intellectual property, and emphasizes that the traditional adaptation of legal requirements to levels of risk is appropriate as the law is applied to new technologies.

There are certain common issues between the intellectual property question and other applications of wide area

Petitioner Apple Inc. - Exhibit 1012, p. 1809

digital network technology. The question of signatures and writings to reflect the establishment of duties and permissions and the transfer of rights is common to the intellectual property inquiry and to electronic commerce using EDI techniques. There also are common questions involving rights to use certain information channels: First Amendment privileges, and tort liability. These are common not only to technological means of protecting intellectual property but to all forms of wide area networking.

The problem

The law recognizes intellectual property because information technology permits one person to get a free ride on another person's investment in creating information value. Creative activity involving information usually is addressed by copyright, although patent has a role to play in protecting innovative means of processing information.2

Intellectual property arose in the context of letterpress printing technology. Newer technologies like xerography and more recently small computer technology and associated word processing and networking have increased the potential for free rides and accordingly increased the pressure on intellectual property.

The concern about free ride potential is especially great when people envision putting creative works on electronic publishing servers connected to wide area networks intending to permit consumers of information products to access these objects, frequently combining them and generally facilitating "publishing on demand" rather than the well known publishing just in case, typified by guessing how many copies of a work will sell, printing those in advance, and then putting them in inventory until someone wants them.

The concern is that it will be too easy to copy an entire work without detection and without paying for it. Worse, it will be easy to copy an entire work and resell it either by itself or as a part of a new derivative work or collection.

But technology is capable of protecting investment in new ways as well as gaining a free ride. Computer networks make it possible to restrict access and to determine when access occurs. Depending on how new networks are designed, they may actually reduce the potential for a free ride. The digital library is one way of realizing that potential. Professor Pamela Samuelson has observed that the digital library model replaces intellectual property with a system of technological controls.3

Digital Library Concepts

Basic Concepts

A digital library is a set of information resources ("information objects") distributed throughout an electronic network. The objects reside on servers (computers with associated disk drives connected to the network). They can be retrieved remotely by users using "client" workstations.

Origin of Concepts

The phrase "digital library" and the basic concept was first articulated in a 1989 report growing out of a workshop sponsored by the Corporation for National Research Initiatives.4 From its inception, the digital library concept envisioned retrieval of complete information

Petitioner Apple Inc. - Exhibit 1012, p. 1810

resources and not merely bibliographic information.5

The technologies of remote retrieval of complete information objects using electronic technologies is in wide use through the WESTLAW, Dialog, LEXIS, NEXIS, and National Library of Medicine databases. These remotely accessible databases, however, unlike the digital library involved a single host on which most of the data resides. The digital library concept envisions a multiplicity of hosts (servers).

Recent Developments

The remotely accessible database host concept is converging with the digital library concept as more of the electronic database vendors provide gateways to information objects actually residing on other computers. This now is commonplace with WESTLAW access to Dialog, and Dialog's gateways to other information providers.

The most explicit implementation of the digital library concept is the Wide Area Information Service ("WAIS"), which implements ANSI standard Z.39.6 WAIS permits a remote user to formulate a query that is applied to a multiplicity of WAIS servers each of which may contain information responsive to the query. The WAIS architecture permits search engines of varying degrees of sophistication, resident on WAIS information servers to apply the query against their own information objects, reporting matches back to the user.7 Future implementations of WAIS permit automatic refinement of searches according to statistical matching techniques.

The Corporation for National Research Initiatives has proposed a test bed for an electronic copyright management system.8 The proposed system would include four major elements: automated copyright recording and registration, automated, on line clearance of rights, private electronic mail and digital signatures to provide security. It would include three subsystems: a Registration and Recording System (RRS), a Digital Library System (DLS), and a Rights Management System (RMS). The RRS would provide the functions enumerated above and would be operated by the Library of Congress. It would provide "change of title" information.9 The RMS would be an interactive distributed system capable of granting rights on line and permitting the use of copyrighted material in the Digital Library System. The test bed architecture would involve computers connected to the Internet performing the RRS and RMS functions.

Digital signatures would link an electronic bibliographic record with the contents of the work, ensuring against alteration after deposit.10 Multiple RMS servers would be attached to the Internet. A user wishing to obtain rights to an electronically published work would interact electronically with the appropriate RMS. When copyright ownership is transferred, a message could be sent from the RMS to the RRS11 - creating an electronic marketplace for copyrighted material.

The EBR submitted with a new work would "identify the rights holder and any terms and conditions on the use of the document or a pointer to a designated contact for rights and permissions."12 The EBR, thus, is apparently equivalent to the permissions header discussed in this paper. Security in the transfer of rights would be provided by digital signatures using public key encryption, discussed further, infra in the section on encryption.

Basic Architectural Concepts

Petitioner Apple Inc. - Exhibit 1012, p. 1811

The digital library concept in general contemplates three basic architectural elements: a query, also called a "knowbot" in some descriptions; a permissions header attached to each information object; and a procedure for matching the query with the permissions header.

Two kinds of information are involved in all three architectural elements: information about the content of information objects desired and existing, and information about the economic terms on which an information object is made available. For example, a query desiring court opinions involving the enforcement of foreign judgments evidencing a desire to download the full text of such judicial opinions and to pay up to $1.00 per minute of search and downloading time would require that the knowbot appropriately represent the subject matter "enforcement of foreign judgments." It also requires that the knowbot appropriately represent the terms on which the user is willing to deal: downloading and the maximum price. The permissions header similarly must express the same two kinds of information. If the information object to which the permissions header is attached is a short story rather than a judicial opinion, the permissions header must so indicate. Or, if the information object is a judicial opinion and it is about enforcement of foreign judgments, the permission header may indicate that only a summary is available for downloading at a price of $10.00 per minute. The searching, matching, and retrieval procedure in the digital library system must be capable of determining whether there is a match on both subject matter and economic terms, also copying and transmitting the information object if there is a match.

Comparison to EDI

Electronic Data Interchange ("EDI") is a practice involving computer-to-computer commercial dealing without human intervention. In the most widespread implementations, computers are programmed to issue purchase orders to trading partners, and the receiving computer is programmed to evaluate the terms of the purchase order and to take appropriate action, either accepting it and causing goods to be manufactured or shipped or rejecting it and sending an appropriate message. EDI is in wide use in American and foreign commerce, using industry-specific standards for discrete commercial documents like purchase orders, invoices, and payment orders, developed through the American National Standards Institute.

There obviously are similarities between the three architectural elements of the digital library concept and EDI. There is a structured way of expressing an offer or instruction, and a process for determining whether there is a match between what the recipient is willing to do and what the sender requests.

There is also, however, an important difference. In the digital library concept, a match results in actual delivery of the desired goods and services in electronic form. In EDI practice, the performance of the contractual arrangement usually involves physical goods or performance of nonelectronic services.

Nevertheless, the digital library and EDI architectures are sufficiently similar and, it turns out the legal issues associated with both are sufficiently similar to make analogies appropriate.

Elements of Data Structure

For purposes of this paper, the interesting parts of the data structure are those elements that pertain to permission, more than those elements that pertain to content of the information object to which the header is attached. Accordingly, this section will focus on only permissions-related elements, after noting in passing that the content part of the header well might be a pointer to an inverted file to permit full text searching and matching.

The starting point conceptually for identifying the elements of the permissions header are the rights exclusively reserved to the copyright owner by 106 of the copyright statute. But these exclusive rights need not be tracked directly because the owner of an information object free to impose contractual restrictions as well as to enjoy rights granted by the Copyright Act. Accordingly, it seems that the following kinds of privileges in the requester should be addressed in the permissions header:

outright transfer of all rights

use privilege, either unrestricted or subject to restrictions

copying, either unlimited or subject to restrictions like quantitative limits

distribution, either unlimited or subject to restrictions, like geographic ones or limits on the markets to which distribution can occur

preparation of derivative works

Display and presentation rights, separately identified in 106 would be subsumed into the use element, because they are particular uses.

The simplest implementation would allow only binary values for each of these elements. But a binary approach does not permit the permissions header to express restrictions, like those suggested in the enumerated list. Elements could be defined to accept the most common kinds of restrictions on use, and quantitative limits on copying, but it would be much more difficult to define in advance the kinds of geographic or market-definition restrictions that an owner might wish to impose with respect to distribution.

In addition to these discrete privileges, the permissions header must express pricing information. The most sensible way of doing this is to have a price associated with each type of privilege. In the event that different levels of use, copying, or distribution privilege are identified, the data structure should allow a price to be associated with each level.

A complicating factor in defining elements for price is the likelihood that different suppliers would want to price differently. For example, some would prefer to impose a flat fee for the grant of a particular privilege. Others might wish to impose a volume-based fee, and still others might wish to impose a usage or connect-time based fee. The data structure for pricing terms must be flexible enough to accommodate at least these three different approaches to pricing.

Finally, the data structure must allow for a specification of acceptable payment terms and have some kind of trigger for a payment approval procedure. For example,

Petitioner Apple Inc. - Exhibit 1012, p. 1813

the permissions header might require presentation of a credit card number and then trigger a process that would communicate with the appropriate credit card database to obtain authorization. Only if the authorization was obtained would the knowbot and the permissions header "match."

There is a relationship between the data structures and legal concepts. The knowbot is a solicitation of offers. The permissions header is an offer. The matching of the two constitutes an acceptance. Mr. Linn's "envelope" could be the "contract."

There are certain aspects of the data structure design that are not obvious. One is how to link price with specific levels of permission. Another is how to describe particular levels of permission. This representation problem may benefit from the use of some deontic logic, possibly in the form of a grammar developed for intellectual property permissions. Finally, it is not clear what the acceptance should look like. Conceptually, the acceptance occurs when the knowbot matches with a permissions header, but it is unclear how this legally significant event should be represented.

Role of Encryption

The CNRI test bed proposal envisions the use of public key encryption to ensure the integrity of digital signatures and to ensure the authenticity of information objects. Public key encryption permits a person to encrypt a message - like a signature using a secret key, one known only to the sender, while permitting anyone with access to a public key to decrypt it. Use of public key cryptography in this fashion permits any user to authenticate a message, ensuring that it came from the purported sender.13 A related technology called "hashing" permits an encrypted digital signature to be linked to the content of a message. The message can be sent in plain text (unencrypted) form, but if any part of it is changed, it will not match the digital signature. The digital signature and hashing technologies thus permit not only the origin but also the content integrity of a message of arbitrary length to be authenticated without necessitating encryption of the content of the message. This technology has the advantage, among others, that it is usable by someone lacking technological access to public key encryption. An unsophisticated user not wishing to incur the costs of signature verification nevertheless can use the content of the signed information object.

It is well recognized that encryption provides higher levels of security than other approaches. But security through encryption comes at a price. Private key encryption systems require preestablished relationships and exchange of private keys in advance of any encrypted communication. The burdens of this approach have led most proponents of electronic commerce to explore public key encryption instead. But public key systems require the establishment and policing of a new set of institutions. An important infrastructure requirement for practicable public key cryptography is the establishment and maintenance of certifying entities that maintain the public keys and ensure that they are genuine ones rather than bogus ones inserted by forgers. A rough analogy can be drawn between the public key certifying entities and notaries public. Both kinds of institutions verify the authenticity of signature. Both kinds require some level of licensing by governmental entities. Otherwise the word of the "electronic notary"

Petitioner Apple Inc. - Exhibit 1012, p. 1814

(certifying entity) is no better than an uncertified, unencrypted signature. In a political and legal environment in which the limitations of regulatory programs have been recognized and have led to deregulation of major industries, it is not clear that a major new regulatory arrangement for public key encryption is practicable. Nevertheless, experimentation with the concept in support of digital library demonstration programs can help generate more empirical data as to the cost and benefits of public key encryption to reinforce electronic signatures.

On the other hand, it is not desirable to pursue approaches requiring encryption of content. No need to encrypt the contents is apparent in a network environment. Database access controls are sufficient to prevent access to the content if the permissions header terms are not matched by the knowbot. On the other hand, if the electronic publishing is effected through CDROMs or other physical media possessed by a user, then encryption might be appropriate to prevent the user from avoiding the permissions header and going directly to the content.

While encrypted content affords greater security to the owner of copyrighted material. Someone who has not paid the price to the copyright owner must incur much higher cost to steal the material. But the problem is everyone must pay a higher price to use the material. One of the dramatic lessons of the desktop computer revolution was the clear rejection of copyright protection in personal computer software. The reasons that copy protection did not survive in the market place militate against embracing encryption for content. Encryption interferes with realization of electronic markets, because producer and consumer must have the same encryption and description protocols. Encryption burdens processing of electronic information objects because it adds another layer. Some specific implementations have encryption require additional hardware at appreciable costs.

Digital libraries cannot become a reality until consumers perceive that the benefits of electronic formats outweigh the costs, compared to paper formats. Encryption interferes with electronic formats' traditional advantages of density, reusability, editability, and computer search ability and also, by impairing open architectures may perpetuate some of papers' advantages with respect with browsibility.14

The need for encryption of any kind depends upon whether security is available without it. That depends, in turn, on the kinds of free rides that may be obtainable and the legal status of various kinds of electronics transactions in the digital library system.

Legal Issues

Copyright: What legal effect is intended?

The design of the permissions header and the values in the elements of the header must be unambiguous as to whether an outright transfer of a copyright interest is intended or whether only a license is intended. If an outright transfer15 is intended, then the present copyright statute requires a writing signed by the owner of the rights conveyed.16 Recordation of the transfer with the Copyright office is not required, but provides advantages in enforcing transferee rights.17 On the other hand, non exclusive licenses need not be in writing nor registered. If the electronic transaction transfers the copyright in its entirety, then the rights of the transferor are extinguished, and the rights of the

Petitioner Apple Inc. - Exhibit 1012, p. 1815

transferee are determined by the copyright statute. The only significant legal question is whether the conveyance was effective.

On the other hand, when the copyright is not transferred outright but only certain permissions are granted or certain rights conveyed, the legal questions become more varied. Then, the rights of the transferor and the obligations of the transferee are matters of contract law. It is important to understand the degree to which the contract is enforceable and how it is to be interpreted in the event of subsequent disputes. The following sections consider briefly the first sale doctrine as a potential public policy obstacle to enforcing contractual restrictions different from those imposed by the copyright statute and then explore in greater depth whether electronic techniques satisfy the formalities traditionally required for making a contract, whether they adequately ensure against repudiation, and whether they provide sufficient information to permit predictable interpretation of contractual obligations and privileges.

First Sale Doctrine

The first sale doctrine may invalidate restrictions on use. It is impermissible for the holder of a patent to impose restrictions on the use of a patented product after the product has been sold. Restrictions may be imposed, however, on persons who merely license the product.18 The rationale for this limit on the power of the owner of the intellectual property interest is that to allow limitations on use of the product would interfere with competition beyond what the Congress - and arguably the drafters of the Constitution - intended in setting up the patent system.

The first sale doctrine applies to copyright owners.19 Indeed, because of the First Amendment's protection of informational activity, the argument against restrictions after the first sale may be even stronger in the copyright arena then in the patent arena.

The first sale doctrine is potentially important because it may invalidate restrictions imposed on the use of information beyond what is authorized by the Copyright Act and by common law trade secret. Thus, there may be serious questions about the legal efficacy of use restrictions suggested in ___, although such restrictions are common in remote database service agreements. The vendors could argue that the limitations pertain to the contractual terms for delivery of a service rather than use of information as such. The characterization avoids the overlap with copyright and thus may also avoid the conflict between federal policy and contract enforcement.20

Contract Formation Issues

The law does not enforce every promise. Instead, it focuses its power only on promises surrounded with certain formalities to make it likely that the person making the promise (the "promisor") and the person receiving the promise (the "promisee") understood that their communication had legal consequences. A threshold question for the digital library system is whether the traditional formalities for making a contract are present when the contract is made through electronic means. The digital library system considered in this paper clearly contemplates that a contract is formed when the knowbot and the permissions header achieve a match. In this respect, the digital library concept converges with EDI where trading parties contemplate that a contract to perform services or deliver goods is

Petitioner Apple Inc. - Exhibit 1012, p. 1816

formed when a match occurs either upon the receipt of a purchase order or upon the transmission of a purchase order acknowledgment.

It is not altogether clear, however, whether the match between values and computer data structures meets contract formation requirements, particularly those expressed in various statutes of frauds. Statutes of frauds require "writings" and "signatures" for certain kinds of contracts - basically those contemplating performance extending beyond a period of one year.21

In many instances, the digital library contract will be fully performed almost instantaneously upon delivery of the information object after the knowbot and the permissions header match. In such a case, the statute of frauds is not a problem and its requirements need not be satisfied. In other cases, however, as when the intent of the owner of the information object is to grant a license to do things that will extend beyond one year, the statute of frauds writing and signature requirements must be met.

Historical application of Statutes Of Frauds by the courts clearly indicates that there is flexibility in the meaning of "writing" and "signature." A signature is any mark made with the intent that it be a signature.22 Thus an illiterate person signs by making an "X," and the signature is legally effective. Another person may sign a document by using a signature stamp. Someone else may authorize an agent to sign his name or to use the signature stamp. In all three cases the signature is legally effective. There may of course be arguments about who made the X, or whether the person applying the signature stamp was the signer or his authorized agent, but these are evidentiary and agency questions, not arguments about hard and fast contract-law requirements.

Under the generally accepted legal definition of a signature, there is no legal reason why the "mark" may not be made by a computer printer, or for that matter by the write head on a computer disk drive or the data bus in a computer random access memory. The authorization to the computer agent to make the mark may be given by entering a PIN ("Personal Identification Number") on a keyboard. To extend the logic, there is no conceptual reason to doubt the legal efficacy of authority to make a mark if the signer writes a computer program authorizing the application of a PIN upon the existence of certain conditions that can be tested by the program. The resulting authority is analogous to a signature pen that can be operated only with a mechanical key attached to somebody's key ring, coupled with instructions to the possessor of the key.

Which of these various methods should be selected for particular types of transactions must depend, not on what the law requires, because the law permits any of these methods. Rather, it must depend on the underlying purposes of the legal requirement and which method best serves those purposes.

The real issue is how to prove that a particular party made the mark. In other words, the contingency to be concerned about is repudiation, not absence of formalities. Repudiation should be dealt with through usual evidentiary and fact finding processes rather than artificial distinctions between signed and unsigned documents.

Authority is skimpier on how flexible the "writing"

Petitioner Apple Inc. - Exhibit 1012, p. 1817

requirement is. The best approach is to borrow the fixation idea from the copyright statute and conclude that a writing is "embodiment in a copy . . . sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for more a period of more than transitory duration."23

The most important thing conceptually is to understand the purpose of the writing and signature requirements. They have two purposes: awareness or formality and reliability of evidence. Signature requirements, like requirements for writings and for original documents have an essentially evidentiary purpose. If there is a dispute later, they specify what kind of evidence is probative of certain disputed issues, like "who made this statement and for what purpose?" The legal requirements set a threshold of probativeness. Surely the values in a knowbot as well as the values in a permissions header constitute and "mark," and someone who knowingly sets up potential transactions in a digital library scheme can have the intent that the mark be a signature.

When a contract is made through a signed writing, it is more likely that the parties to the contract understand what they are doing. They are aware of the legal affect of their conduct because the writing in the signature involve a greater degree of formality than a simple conversation.

The awareness/formality purpose can be served by computerized contracting systems. This is so not so much because the computers are "aware" of the affect of their "conduct." Rather, it is true because the computers are agents of human principals. The programming of the computer to accept certain contract terms is the granting of authority to the computer agent to enter into a contract. The fact that a principal acts through an agent engaging in conduct at a later point and time never has been thought to defeat contract formation in the traditional evolution of agency and contract law. Nor should it when the agent is a computer.

Fulfillment of the evidentiary purpose depends on the reliability of the information retained by the computer systems making up the digital library. Such systems must be designed to permit the proponent of contract formation to establish the following propositions if the other party to the purported contract attempts to repudiate it.

1.It came from computer X

2.It accurately represents what is in computer X24 now25

3.What is in computer X now is what was in computer X at the time of the transaction

4.What was in computer X at the time of the transaction is what was received from the telecommunications channel26

5.What was received from the telecommunications channel is what was (a) sent, (b) by computer Y.

Two other questions relate to matters other than the authenticity of the message:

6 Computer Y was the agent of B

7 The message content expresses the content of the

Petitioner Apple Inc. - Exhibit 1012, p. 1818

contract (or more narrowly, the offer or the acceptance).27

Factual propositions 1-4 can be established by testimony as to how information is written to and from telecommunications channel processors, primary storage, and secondary storage. Factual proposition 5 requires testimony as to the accuracy of the telecommunications channel and characteristics of the message that associate it with computer Y. Only the last proposition (number 5) relates to signatures, because signature requirements associate the message with its source.28 The other propositions necessitate testimony as to how the basic message and database management system works. It is instructive to compare these propositions with the kinds of propositions that must be established under the business records exception to the hearsay rule when it is applied to computer information.

Those propositions may be supported with non technical evidence, presented by non programmers. A witness can lay a foundation for admission of computer records simply by testifying that the records are generated automatically and routinely in the ordinary course of business. The more inflexible the routine, and the less human intervention in the details of the computer's management of the database the better the evidence.29

The ultimate question is trustworthiness, and if the computer methods are apparently reliable, the information should be admitted unless the opponent of admissibility can raise some reasonable factual question undercutting trustworthiness.30

Contract Interpretation Issues

Assuming that the permissions header and knowbot constitute sufficient writings to permit a contract to be formed and that the signature requirement also is met, through digital signature technology or otherwise, there still are difficult contract interpretation questions. Contract interpretation questions arise not only after contractual relationships are formed, but also in connection with deciding whether there has been offer and acceptance, the prerequisites to contract formation.31 Contract interpretation always seeks to draw inferences about what the parties intended. When contract interpretation issues arise at the contract formation stage, the questions are what the offeror intended the content of the offer to be and what the offeree intended the content of the purported acceptance to be. The proposed Digital Library System envisions extremely cryptic expressions of offer and acceptance - by means of codes. The codes have no intrinsic meaning. Rather, extrinsic reference must be made to some kind of table, standard, or convention associating particular codes with the concepts they represent. Extrinsic evidence is available to resolve contract interpretation questions when the language of the contract itself is ambiguous, and perhaps at other times as well.32 The codes in the permissions header and knowbots certainly are ambiguous and become unambiguous only when extrinsic evidence is considered. So there is no problem in getting a standard or cable into evidence. The problem is whether the parties meant to assent to this standard.

In current EDI practice, this question is resolved by having parties who expect to have EDI transactions with each other to sign a paper trading partner agreement, in which the meaning of values or codes in the transaction sets is established.33 But requiring each pair of suppliers and users

Petitioner Apple Inc. - Exhibit 1012, p. 1819

of information in a digital library to have written contracts with each other in advance would defeat much of the utility of the digital library. Thus the challenge is to establish some ground rules for the meaning of permissions header and knowbot values that all participants are bound by. There are analogous situations. One is a standard credit card agreement that establishes contractual terms among credit card issuer, credit card subscriber, and merchant who accepts the credit card. The intermediary - the credit card company - unilaterally establishes contract terms to which the trading partners assent by using and accepting the credit card.34 Also, it is widely recognized that members of a private association can, through their constitution and bylaws establish contractual relationships that bind all of the members in dealing with each other.35 In the Digital Library System, similar legal arrangements can establish the standards by which electronic transactions between permissions header and knowbots will bind transferor and transferee of information.

Third Party Liability

It is not enough merely to ensure that the licensee is contractually bound. Trading partners also must ensure that the participants in funds transfers have enforceable obligations. For example, if the digital library system envisions that the information object would not be released to the purchaser without simultaneous release of a payment order, the supplier may be interested in enforcing the obligations of financial intermediaries who handle the payment order. This implicates the federal Electronic Funds Transfer Act, and Article 4A of the Uniform Commercial Code, regulating wire transfers.

Solutions

Satisfy the Business Records Exception to the Hearsay Rule

The discussion of contract formalities earlier in this paper concluded that legally enforceable contracts can be formed through electronic means and that the significant legal questions relate to reliability of proof and intent of the parties to be bound by using the electronic techniques. This section considers the reliability of proof further. Traditional evidence law permits computer records to be introduced in evidence when they satisfy the requirements of the business records exception: basically that they are made in the ordinary course of business, that they are relied on for the performance of regular business activities, and that there is no independent reason for questioning their reliability.36

The business records exception shares with the authentication concept statute of frauds and the parol evidence rule a common concern with reliability.37 The same procedural guarantees and established practices that ensure reliability for hearsay purposes also ensure reliability for the other purposes. Under the business records exception, the proponent must identify the source of a record, through testimony by one familiar with a signature on the record, or circumstantially.38 The steps in qualifying a business record under the common law, which since have been relaxed,39 were:

Proving that the record is an original entry made in the routine course of business

Proving that the entries were made upon the personal knowledge of the proponent/witness or someone reporting to him

Petitioner Apple Inc. - Exhibit 1012, p. 1820

Proving that the entries were made at or near the time of the transaction

Proving that the recorder and his informant are unavailable.40

These specific requirements are easier to understand and to adapt to electronic permissions and obligations formed in a digital library system by understanding the rationale for the business records exception. The hearsay rule excludes out of court statements because they are inherently unreliable, primarily because the maker of the statement's demeanor cannot be observed by the jury and because the maker of the statement is not subject to cross examine. On the other hand, there are some out of court statements that have other guarantees of reliability. Business records are one example. If a continuing enterprise finds the records sufficiently reliable to use them in the ordinary course of business, they should be reliable enough for a court. The criteria for the business records exception all aim at ensuring that the records really are relied upon the business to conduct its ordinary affairs.

The Manual for Multidistrict Litigation suggests steps for qualifying computer information under the business records exception:

1.The document is a business record

2.The document has probative value

3.The computer equipment used is reliable

4.Reliable data processing techniques were used41

The key in adapting the business records exception to electronic permissions in a digital library system are points 3 and 4. Establishing these propositions and the propositions set forth in section ___ of this paper requires expert testimony. Any designer of a digital library system must consult with counsel and understand what testimony an expert would give to establish these propositions. Going through that exercise will influence system design.

Reinforce the Evidentiary Reliability by Using Trusted Third Parties

The evidentiary purpose of contract formation requirements can be satisfied by using a trusted third party as an intermediary, when the third party maintains archival records of the transactions. The third party lacks any incentive for tampering with the records and when the third parties archiving system is properly designed, it can provide evidence sufficient to establish all of the propositions identified in ___.

This third party intermediary concept is somewhat different from the concept for a certifying agent in digital signature systems. To be sure, the custodian of transaction records envisioned by this section could be the same as the certifying entity for public and key encryption, but the custodian role can be played in the absence of any encryption. Indeed, the digital library itself is a good candidate for the custodian role. The library has no incentive to manipulate its records in favor of either of the producers of information value or the consumers. In order to carry out its affairs, it must use these transactional records in the ordinary course of business,

Petitioner Apple Inc. - Exhibit 1012, p. 1821

thereby making it likely that digital library records would qualify under the business records exception.

Standardization

Obviously, the digital library concept depends upon the possibility of an automated comparison between the knowbot and the permissions header. This means that potential requesters of information and suppliers of information must know in advance the data structures for representing the elements of the permissions header and the knowbot. This requires compatibility. Compatibility requires standardization. Standardization does not, however, necessarily require "Standard" in the sense that they are developed by some bureaucratic body like ANSI. It may simply imply market acceptance of a particular vendor's approach. Indeed, each digital library might use different data structures. All that is necessary is that the structure of the knowbot and the structure of the permissions header be compatible within any one digital library system. Also, as demands emerge for separate digital libraries to communicate with each other, there can be proprietary translation to assure compatibility between systems much as common word processing programs translate to and from other common formats and much as printers and word processing software communicate with each other through appropriate printer drivers. In neither of these cases has any independent standards organization developed a standard that is at all relevant in the marketplace.

Standardizing the elements of Knowbot and permissions headers involves content standardization, which generally is more challenging than format standardization.42 A permissions header/Knowbot standard is a system for representing legal concepts and for defining legal relations. As such, the standard is basically a grammar for a rule based substantive system in a very narrow domain.43 The data elements must correspond to legally meaningful relational attributes. The allowable values must correspond to legally allowable rights, obligations, privileges and powers. In other words, the standard setter must meet many of the challenges that a legal expert system designer working with Hohfeldian frameworks must meet.44 This adds a constraint to the standards setting process. Unlike setting format standards, where the participants are free to agree on an arbitrary way of expressing format attributes, participants in setting a content standard must remain within the universe of permissible content. The set of permissible values is determined by the law rather than being determined only by the imagination of format creators.

Enforcement and Bottlenecks

One of the many profound observations by Ithiel de Sola Pool was that copyright always has depended upon technological bottlenecks for its enforceability. The printing press was the original enforcement bottleneck. Now, a combination of the printing press and the practical need to inventory physical artifacts representing the work constitute the enforcement bottlenecks. As technologies change, old bottlenecks disappear and enforceability requires a search for new bottlenecks. When there are single hosts, like Westlaw, Dialog, Lexis, and CompuServe, access to that host is the bottleneck. The problem with distributed publishing on an open architecture internet is that there is no bottleneck in the middle of the distribution chain corresponding to the printer, the warehouse or the single host.

Petitioner Apple Inc. - Exhibit 1012, p. 1822

If new bottlenecks are to be found, they almost surely will be found at the origin and at the point of consumption. Encryption and decryption techniques discussed elsewhere in this volume concentrate on those bottlenecks as points of control. It also is possible that rendering software could become the new bottleneck as Mr. Linn suggests.

Even with those approaches, however, a serious problem remains in that the new technologies make it difficult or impossible to distinguish between mere use and copying. Thus the seller cannot distinguish between an end user45 and a potential competitor. On the other hand, the new technologies permit a much better audit trail, potentially producing better evidence for enforcement adjudication.

If network architectures for electronic publishing evolve in the way that Ted Nelson suggests with his Xanadu concept, the real value will be in the network and the pointers, not in the raw content. Thus, the creative and productive effort that the law should reward is the creation and productive effort that the law should reward is the creation and production and delivery of pointers, presentation, distribution, and duplication value. If this is so, then technological means will be particularly important, foreclosing access by those lacking passwords and other keys and limiting through contract what a consumer may do with the information.

In such an architecture, the law either will be relatively unimportant because technology can be counted on to prevent free riding or, the law will need to focus not on prohibiting copying or use without permission, but on preventing circumvention of the technological protections. Thus, legal approaches like that used to prevent the sale of decryption devices for television broadcasts and legal issues associated with contract enforcement may be more important than traditional intellectual property categories.

Weighing Risks and Costs

The law generally imposes sensible levels of transaction costs. Usually, transaction costs are proportional to the risk. Figure 1 shows a continuum of risk and transaction cost in traditional and new technologies. A real estate closing involves significant risks if there is some dispute later about the transaction. Therefore, the law affords much protection, including a constitutional officer called a registrar of deeds who is the custodian of records associated with the transaction. The risk level analogous to this in electronic publishing might be access to an entire library including access software as well as contents. Next, is a transaction involving a will or power of attorney. There, the risk is substantial because the maker of the instrument is not around to help interpret it. The law requires relatively high levels of assurance here, though not as great as those for real estate transactions. The law requires witnesses and attestation by a commissioned minor official called a notary public. The electronic publishing analogy of this level of risk might be the contents of an entire CDROM.

Next, in level of risk is the purchase of a large consumer durable like an automobile. The law requires somewhat less, but still significant protections for this kind of transaction: providing for the filing and enforcement of financing statements under the Uniform Commercial Code. The electronic publishing analogy might be the transfer of copyright to a complete work. Next, down

Petitioner Apple Inc. - Exhibit 1012, p. 1823

the risk continuum, is the purchase of a smaller consumer durable like a television set. Here, the law typically is reflected in written agreements of sale, but no special third party custodial mechanisms. The electronic publishing analogy might be use permission for a complete work.

Finally, is the purchase of a relatively small consumer item, say a box of diskettes. Neither the law or commercial practice involves much more than the exchange of the product for payment, with no written agreement or anything else to perform channeling, cautionary, evidentiary, or protective functions [make sure these function and the citation appears earlier]. The electronic publishing analogy might be use permission for part of a work.

Cost effectiveness = risk-proportional security

traditional transaction equivalent	institutions	electronic
real estate closing software and	registrar of deeds	entire library - contents
will/power of attorney CDROM	witnesses, notary public	contents of entire
auto purchase transfer of	UCC financing statement	complete work - copyright
television set purchase permission	written sale agreement	complete work - use
box of diskettes	-	part of a work - use permission

An encrypted object combined with rendering software is probably inconsistent with an open architecture. Because of the difficulty of setting standards for such technologies, this approach to intellectual property protection probably would be effectuated by proprietary approaches thus frustrating the vision of an open market for electronic publishing.

Conclusion

Realization of the digital library vision requires a method for collecting money and granting permission to use works protected by intellectual property. The concept of a knowbot and a permissions header attached to the work is the right way to think about such a billing and collection system. Standards for the data structures involved must be agreed to, and systems must be designed to satisfy legal formalities aimed at ensuring awareness of the legal significance of transactions and reliable proof of the terms of the transactions.

In the long run, not only must these technological issues be resolved, with appropriate attention to levels of risk and protections available under traditional legal doctrines, but also further conceptual development must be undertaken. Proponents of electronic publishing over wide area networks need to think about the appropriate metaphors: whether it is a library or a bookstore, if a library whether with or without xerox machines, if a bookstore whether it is a retail bookstore, or a mail order operation. Then,

Petitioner Apple Inc. - Exhibit 1012, p. 1824

thought must be given to how standards will be set. Finally, and most important, much more needs to be understood about the need for third party institutions. There is a good deal of enthusiasm for public key encryption. Yet the vulnerability of public key encryption systems is in the integrity of the key authority. In traditional legal protections, the third party custodians or authenticating agents like notary public and registrars of deeds receive state sanction and approval, and in the case of registrars of deeds, public funding. We must be clearer as to whether a similar infrastructure must be developed to protect against substantial risks and the use of EDI and electronic publishing technologies.

Finally, and perhaps most importantly, we must be thoughtful about what legal obligations, imposed on whom, are appropriate? The suggested 102(e) and (f) in the High Performance Computing Act looks very much like King James I's licensing of printing presses. It also looks like the FBI's proposal to prohibit the introduction of new technologies until certain conformity with past legal concepts is assured. Such approaches make the law a hurdle to new technology -- an uncomfortable position for both law and technology.

---

1 The use of EDI techniques to meter usage and determine charges for use of intellectual property is an example of billing and collection value in a typology of different types of value that can be produced in electronic marketplaces for information. See Henry H. Perritt, Jr., Market Structures for Electronic Publishing and Electronic Contracting in Brian Kahin, ed., Building Information Infrastructure: Issues in the Development of the National Research and Education Network (Harvard University and McGraw-Hill 1992) (developing typology for different types of value and explaining how market structures differ for the different types); Henry H. Perritt, Jr., Tort Liability, the First Amendment, and Equal Access to Electronic Networks, 5 Harv.J.Law & Tech. 65 (1992) (using typology of ten types of value to analyze access by competing producers of value).

2 See, e.g.U.S.Pat. No. 5,016,009, Data compression apparatus and method (May 14, 1991); U.S. Pat. No. 4,996,690, Write operator with gating capability (Feb. 26, 1991);U.S. Pat. No. 4,701,745, Data compression system (Oct. 20, 1987); Multi Tech Systems, Inc. v. Hayes Microcomputer Products, Inc., 800 F. Supp. 825 (D. Minn. 1992) (denying summary judgment on claim that patent for modem escape sequence is invalid)..

3 Comments on the 8\21 draft of "Knowbots in the Real World" from the intellectual property workshop participants at page 6 (author unknown, source unknown). Professor Samuelson also observed that the workshop, despite its title, actually did not focus much on intellectual property issues.

4 Corporation for National Research Initiatives, Workshop On The Protection Of Intellectual Property Rights In A Digital Library System: Knowbots in the Real World-May 18-19, 1989 (describing digital library system).

5 See generally Clifford A. Lynch, Visions of Electronic Libraries (libraries of future can follow acquisition-on-demand model rather than acquiring an advance of use; Z39.50 protocol will facilitate realization of that possibility, citing Robert E. Kahn & Vinton G. Serf, An Open Architecture

Petitioner Apple Inc. - Exhibit 1012, p. 1825

for a Digital Library System and a Plan for Its Development. The Digital Library Project, volume 1: The World of Knowbots (draft) (Washington D.C.: Corporation for National Research Initiatives; 1988)).

6 Clifford A. Lynch, The Z39.50 Information Retrieval Protocol: An Overview and Status Report, ACM Sigcomm Computer Communication Review at 58 (describing Z39.50 as an OSI application layer protocol that relieves clients from having to known the structure of data objects to be queried, and specifies a framework for transmitting and managing queries and results and syntax for formulating queries).

7 Brewster Kahle, Wide Area Information Server Concepts (Nov. 3, 1989 working copy; updates available from Brewster @THINK. (describing WAIS as "open protocol for connecting user interfaces on workstations and server computers") (describing information servers as including bulletin board services, shared databases, text searching and automatic indexing and computers containing current newspapers and periodicals, movie and television schedules with reviews, bulletin boards and chat lines, library catalogues, Usenet articles).

8 Robert E. Kahn, Deposit, Registration, Recordation in an Electronic Copyright Management System (August 1992) (Corporation for National Research Initiatives, Reston, Virginia).

9 Kahn 1992 at 4.

10 Kahn 1992 at 6.

11 Kahn 1992 at 10.

12 Kahn 1992 at 12.

13 Kahn 1992 at 15.

14 Browsability through techniques like the collapsible outliner function in Microsoft Word for Windows and competing products require more chunking and tagging value in the form of style and text element codes. Handling this additional formatting information through encryption and description processes is problematic.

15 " A 'transfer of copyright ownership' is an assignment, mortgage, exclusive license, or any other conveyance, alienation, or hypothecation of a copyright or of any of the exclusive rights comprised in a copyright, whether or not it is limited in time or place of effect, but not including a non-exclusive license " 17 U.S.C. 101 (1988).

16 17 U.S.C. 204(a) (1988); Valente-Kritzer Video v. Pinckney, 881 F.2d 772, 774 (9th Cir. 1989) (affirming summary judgment for author; oral agreement unenforceable under Copyright Act); Library Publications, Inc. v. Medical Economics Co., 548 F. Supp. 1231, 1233 (E.D. Pa. 1982) (granting summary judgment against trade book publisher who sought enforcement of oral exclusive distribution agreement; transfer of exclusive rights, no matter how narrow, must be in writing), aff'd mem., 714 F.2d 123 (3d Cir. 1983).

17 17 U.S.C. 205 (1988) provides constructive notice of the contents of the recorded document, determining priority as between conflicting transfers, and determines priority as between recorded transfer and non-exclusive license. The

Petitioner Apple Inc. - Exhibit 1012, p. 1826

former requirement for transfers to be recorded in order for the transferee to maintain an infringement, 17 U.S.C. 205(d), was repealed by the Berne Act Amendments 5.

18 under Adams v. Burke, 84 U.S. (17 Wall.) 453 (1873), a patentee must not attempt to exert control past the first sale. In general, use restrictions may be placed only on licensees, consistent with General Talking Pictures v. Western Elec., 304 U.S. 175 (1938). See generally Baldwin-Lima-Hamilton Corp. v. Tatnall, 169 F. Supp. 1 (E.D. Pa.1958) (applying no control after purchase rule).

19 See Red-Baron-Franklin Park, Inc. v. Taito Corp., 883 F.2d 275, 278 (4th Cir. 1989) (purchase of video game circuit boards did not create privilege to perform video game under first sale doctrine); United States v. Moore, 604 F.2d 1228, 1232 (9th Cir. 1979) (pirated sound recording not within first sale doctrine in criminal copyright infringement prosecution). But see Mirage Editions, Inc. v. Albuquerque A.R.T. Co., 856 F.2d 1341, 1344 (9th Cir. 1988) (first sale doctrine did not create privilege to prepare derivative work by transferring art in book to ceramic tiles).

20 The way in which the first sale doctrine would impact the electronically imposed use restrictions is by frustrating a breach-of-contract lawsuit by the licensor against a licensee who exceeds the use restrictions. The licensee exceeding the use restrictions would argue that it violates public policy to enforce the restrictions and therefore that state contract law may not impose liability for their violation. See generally Restatement (second) of Contracts 178 (1981) (stating general rule for determining when contract term in unenforceable on grounds of public policy).

21 In addition, as ___ of this paper notes, the Copyright Act itself requires signed writings for transfers of copyright interests. 17 U.S.C. 204(a). (1988).

22 Michael S. Baum & Henry H. Perritt, Jr., Electronic Contracting, Publishing and EDI Law ch. 6 (1991) (contract, evidence and agency issues) [hereinafter "Baum & Perritt"]. Accord, Signature Requirements Under EDGAR, Memorandum from D. Goelzer, Office of the General Counsel, SEC to Kenneth A. Fogash, Deputy Executive Director, SEC (Jan. 13, 1986) (statutory and non-statutory requirements for "signatures" may be satisfied by means other than manual writing on paper in the hand of the signatory . . . "In fact, the electronic transmission of an individual's name may legally serve as that person's signature, providing it is transmitted with the present intention to authenticate.").

23 17 U.S.C. 101 (1988). For copyright purposes, a work is created, and therefore capable of protection, when it is fixed for the first time. 17 U.S.C. 101 (1988). "[I]t makes no difference what the form, manner, or medium of fixation may be - whether it is in words, numbers, notes, sounds, pictures, or any other graphic or symbolic indicia, whether embodied in a physical object in written, printed, photographic, sculptural, punched, magnetic, or any other stable form, and whether it is capable of perception directly or by means of any machine or device 'now known or later developed.'" 1976 U.S. Code Cong. & Admin. News 5659, 5665. The legislative history further says that, "the definition of `fixation' would exclude from the concepts purely of an evanescent or transitory nature -- reproductions such as those projected briefly on a screen

Petitioner Apple Inc. - Exhibit 1012, p. 1827

shown electronically on a television or other video display or captured momentarily in the 'memory' of a computer." 17 U.S.C. 102 note (excerpting from House Report 94-1476).

24 Or, more likely, what is on computer medium read by computer x, such as a magnetic cartridge used for archival records. Further references in the textual discussion to "what is in computer x now" should be understood to include such computer readable media.

25 Cf. Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 NW.U.L.Rev. 956, 980 (1986) (proof that a printout accurately reflects what is in the computer is too limited a basis for authentication of computer records).

26 In some cases, the electronic transaction will be accomplished by means of a physical transfer of computer readable media. In such a case, this step in the proof would involve proving what was received physically.

27 See generally Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 NW.U.L.Rev. 956, 979 (1986) (citing as examples of authentication Ford Motor Credit Co. v. Swarens, 447 S.W.2d 53 (Ky. 1969) (authentication by establishing relationship between computer-generated monthly summary of account activity and the customer reported on); Ed Guth Realty, Inc. v. Gingold, 34 N.Y.2d 440, 315 N.E.2d 441, 358 N.Y.S.2d 367 (1974) (authentication of summary of taxpayer liability and the taxpayer)).

28 Of course, a paper document signed at the end also is probative of the fact that no alternations have been made. In this sense, a signature requirement telescopes several steps in the inquiry outlined in the text.

29 United States v. Linn, 880 F.2d 209, 216 (9th Cir. 1989) (computer printout showing time of hotel room telephone call admissible in narcotics prosecution). See also United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) (computer generated toll and billing records in price-fixing prosecution based on testimony by billing supervisor although he had no technical knowledge of system which operated from another office; no need for programmer to testify; sufficient because witness testified that he was familiar with the methods by which the computer system records information).

30 See United States v. Hutson, 821 F.2d 1015, 1020 (5th Cir. 1987) (remanding embezzlement conviction, although computer records were admissible under business records exception, despite trustworthiness challenged based on fact that defendant embezzled by altering computer files; access to files offered in evidence was restricted by special code).

31 Restatement (Second) of Contracts ___ (1981).

32 Cite for when extrinsic evidence is admissible.

33 See Baum & Perritt 2.6; The Electronic Messaging Services Task Force, The Commercial Use of Electronic Data Interchange--A Report and Model Trading Partner Agreement, 45 Bus.Law. 1645 (1990); Jeffrey B. Ritter, Scope of the Uniform Commercial Code: Computer Contracting Cases and Electronic Commercial Practices, 45 Bus.Law. 2533 (1990); Note, Legal Responses to Commercial Transactions Employing

Petitioner Apple Inc. - Exhibit 1012, p. 1828

Novel Communications Media, 90 Mich.L.Rev. 1145 (1992)

34 Garber v. Harris Trust & Savings Bank, 432 N.E.2d 1309, 1311-1312 (Ill. App. 1982) ("each use of the credit card constitutes a separate contract between the parties;" citing cases).

It is not quite this simple, because both merchant and credit card customer have separate written contracts with the credit card issuer. But there is no reason that a supplier of information to a Digital Library System and all customers of that system might not have their own contracts with the Digital Library System in the same fashion.

35 Rowland v. Union Hills Country Club, 757 P.2d 105 (Ariz. 1988) (reversing summary judgment for country club officers because of factual question whether club followed bylaws in expelling members); Straub v. American Bowling Congress, 353 N.W.2d 11 (Neb. 1984) (rule of judicial deference to private associations, and compliance with association requirements, counseled affirmance of summary judgment against member of bowling league who complained his achievements were not recognized). But see Wells v. Mobile County Board of Realtors, Inc., 387 So.2d 140 (Ala. 1980) (claim of expulsion of realtor from private association was justiciable and bylaws, rules and regulations requiring arbitration were void as against public policy; reversing declaratory judgment for defendant association).

36 F.R.E. 803(6) (excluding business records from inadmissibility as hearsay); 28 U.S.C. 1732 ("Business Records Act" permitting destruction of paper copies of government information reliably recorded by any means and allowing admission of remaining reliable record).

37 See Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 978-80, 984-85 (1986) (noting body of commentator opinion saying that business records exception and authentication are parallel ways of establishing reliability).

38 See F.R.E. 901(b)(4) (appearance, contents, substance, internal patterns, as examples of allowable authentication techniques).

39 Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 963-64 (1986) (identifying steps and trend resulting in F.R.E.).

40 Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 963 (1986).

41 Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 974 (1986) (reporting four requirements of Manual, and endorsing their use generally).

42 See Henry H. Perritt, Jr., ___, ___ Jurimetrics ___ (1993) (distinguishing between format and content standardization).

43 See Marc Lauritsen, ___ (explaining relationship between substantive legal systems and the field of artificial intelligence).

Petitioner Apple Inc. - Exhibit 1012, p. 1829

44 See Thorne, McCarty; Kevin Ashley; and Gardner.

45 It may not be particularly important to limit competition by consumers, because the consumers will never have the pointers and the rest of the network infrastructure.

Petitioner Apple Inc. - Exhibit 1012, p. 1830

OIPE JC174 JUN 07 2005 PATENT & TRADEMARK OFFICE

CFD 3621 $

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. STEFIK, *et al.*
Group Art Unit	3621
Examiner Name	Calvin L. Hewitt, II
Total Number of Pages in This Submission	
Attorney Docket Number	111325-88 (020700)
Confirmation Number	5128

ENCLOSURES *(check all that apply)*

- ☒ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☒ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Assignment Papers *(for an Application)*.
- ☐ Drawing(s)
- ☐ Declaration and Power of Attorney
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance Communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Application Data Sheet
- ☐ Request for Corrected Filing Receipt with Enclosures
- ☐ A self-addressed prepaid postcard for acknowledging receipt
- ☐ Other Enclosure(s) (*please identify below*):

Remarks

☒ The Commissioner is hereby authorized to charge any additional fees required or credit any overpayments to Deposit Account No. 19-2380 for the above identified docket number.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm *or* Individual name	Marc S. Kaufman Registration No. 35, 212 **Nixon Peabody LLP** 401 9th Street, N.W., Suite 900 Washington, D.C. 20004-2128
Signature	
Date	6-7-05

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

- ☐ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop _____, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450
- ☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) _____.

_____ Date

_____ Signature

_____ Typed or printed name

FEE TRANSMITTAL FOR FY 2005

Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT | **$180.00**

Complete if Known	
Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. STEFIK, *et al.*
Examiner Name	Calvin L. Hewitt, II
Art Unit	3621
Attorney Docket No.	111325-88 (020700)

OIPE JC14 JUN 07 2005 U.S. PATENT & TRADEMARK OFFICE

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit Card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 19-2380

Deposit Account Name: Nixon Peabody LLP

The Commissioner is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	300	2001	150	Utility filing fee	
1002	200	2002	100	Design filing fee	
1003	200	2003	100	Plant filing fee	
1004	300	2004	150	Reissue filing fee	
1005	200	2005	100	Provisional filing fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

	Extra Claims		Fee from below		Fee Paid
Total Claims		-20** =		X =	0
Independent Claims		-3** =		X =	0
Multiple Dependent				X =	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	50	2202	25	Claims in excess of 20
1201	200	2201	100	Independent claims in excess of 3
1203	360	2203	180	Multiple dependent claim, if not paid
1204	200	2204	100	** Reissue independent claims over original patent
1205	50	2205	25	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	
1051	130	2051	65	Surcharge – late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1,020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1,080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	
1403	1,000	2403	500	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	500	2452	250	Petition to revive – unavoidable	
1453	1,500	2453	750	Petition to revive – unintentional	
1501	1,400	2501	700	Utility issue fee (or reissue)	
1502	800	2502	400	Design issue fee	
1503	1,100	2503	550	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	180.00
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	790	2809	395	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) **$180.00**

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

☐ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop _____, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450

☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) _____.

Date _____ Signature _____

Typed or printed name _____

SUBMITTED BY				Complete *(if applicable)*	
Name *(Print/Type)*	Marc S. Kaufman	Registration No. *(Attorney/Agent)*	35,212	Telephone	(202) 585-8000
Signature				Date	6-7-05

SEND TO: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

W658338.1

OIPE
JUN 07 2005
PATENT & TRADEMARK OFFICE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	1	of	1

Complete if Known	
Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. **STEFIK**, *et al.*
Art Unit	3621
Examiner Name	Calvin L. Hewitt, II
Attorney Docket Number	111325-88 (020700)

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number - Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,882,752	November 21, 1989	Richard P. Lindman, *et al*	
		US-5,224,163	June 29, 1993	Morrie Gasser, *et al.*	
		US-5,299,263	March 29, 1994	Michael J. Beller, *et al.*	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Application of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
		EP 0 538 216 A	April 21, 1993	TELEVERKET		

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		HENRY H. PERRITT, JR., "Knowbots, Permissions Headers and Contract Law"; Papers for the conference on Technological Strategies For Protecting Intellectual Property In The Networked Multimedia Environment, April 2, 1993; pages 1-22, XP-002233403	
		European Search Report; mailed September 8, 2004 (European Application No. 03 01 5128).	
		European Search Report; mailed September 13,2004 (European Application No. 03 01 5127).	

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

JUN 07 2005
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: Mark J. **STEFIK**, *et al.*	)	Examiner: Calvin L. Hewitt, II
Application No.: 10/015,951	)	Group Art Unit: 3621
Filed: December 17, 2001	)	
For: **DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME**	)	Confirmation No.: 5128

U.S. Patent and Trademark Office
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. § 1.97 (b)

In accordance with the duty of disclosure as set forth in 37 C.F.R. §1.56, Applicants hereby submit the following information in conformance with 37 C.F.R. §§ 1.97 and 1.98. Pursuant to 37 C.F.R. § 1.98, copies of the listed documents are attached.

These listed documents were cited in two communications from the European Patent Office in a counterpart foreign applications. The European Search Reports were mailed on September 8, 2004 and September 13, 2004.

The Commissioner is hereby authorized to charge the Deposit Account No. 19-2380 in the amount of $180 to comply with the provisions of 37 C.F.R. § 1.97(c).

06/09/2005 SZEWDIE1 00000015 192380 10015951
01 FC:1806 180.00 DA

Petitioner Apple Inc. - Exhibit 1012, p. 1834

It is requested that the accompanying PTO-1449 be considered and made of record in the above-identified application. To assist the Examiner, the documents are listed on the attached form PTO-1449. It is respectfully requested that an Examiner initial a copy of this form be returned to the undersigned.

The Commissioner is hereby authorized to charge any fees connected with this filing which may be required now, or credit any overpayment to Deposit Account No. 19-2380 (111325-88/020700).

Respectfully submitted,

NIXON PEABODY, LLP

By: _____

Marc S. Kaufman
Registration No. 35,212

Date: 6-7-05

NIXON PEABODY LLP
CUSTOMER NO. 22204
401 9th Street, N.W., Suite 900
Washington, DC 20004-2128
Telephone: (202) 585-8000

Petitioner Apple Inc. - Exhibit 1012, p. 1835

P.B.5818 – Patentlaan 2
2280 HV Rijswijk (ZH)
☎ +31 70 340 2040
TX 31651 epo nl
FAX +31 70 340 3016

Europäisches Patentamt
Zweigstelle in Den Haag Recherchen-abteilung

European Patent Office
Branch at The Hague Search division

Office européen des brevets
Département à La Haye Division de la recherche

Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
80538 München
ALLEMAGNE

GRÜNECKER, KINKELDEY, STOCKMAIR & SCHWANHÄUSSER ANWALTSSOZIETÄT
14. Sep. 2004
FRIST
TERM
EINGANG - RECEIVED

Datum/Date
13.09.04

Zeichen/Ref./Réf.	Anmeldung Nr./Application No./Demande n°./Patent Nr./Patent No./Brevet n°.
EP18327XIII-034	03015127.8-1245-

Anmelder/Applicant/Demandeur/Patentinhaber/Proprietor/Titulaire
ContentGuard Holdings, Inc.

COMMUNICATION

The European Patent Office herewith transmits as an enclosure the European search report for the above-mentioned European patent application.

If applicable, copies of the documents cited in the European search report are attached.

☐ Additional set(s) of copies of the documents cited in the European search report is (are) enclosed as well.

The following specifications given by the applicant have been approved by the Search Division:

☒ abstract ☒ title

☐ The abstract was modified by the Search Division and the definitive text is attached to this communication.

The following figure will be published together with the abstract: 1

BEST AVAILABLE COPY

REFUND OF THE SEARCH FEE

If applicable under Article 10 Rules relating to fees, a separate communication from the Receiving Section on the refund of the search fee will be sent later.

Europäisches Patentamt · European Patent Office · Office européen des brevets

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 01 5127

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 224 163 A (KAUFMAN CHARLES W ET AL) 29 June 1993 (1993-06-29) * column 5, line 41 - column 6, line 31 * * column 7, line 29 - line 35 * * column 8, line 19 - line 51 * * column 14, line 51 - column 15, line 39 *	1-6, 25-30	G06F1/00
Y		7-9, 12-22, 31-33, 36-46	
X	US 5 299 263 A (BELLER MICHAEL J ET AL) 29 March 1994 (1994-03-29) * column 2, line 26 - line 35 * * column 2, line 45 - line 54 * * column 10, line 14 - column 11, line 10 *	1,25	
Y	PERRITT H H: "Knowbots, Permissions Headers and Contract Law" 2 April 1993 (1993-04-02), PROCEEDINGS TECHNOLOGICAL STRATEGIES FOR PROTECTING INTELLECTUAL PROPERTY IN THE NETWORKED MULTIMEDIA ENVIRONMENT, XX, XX, PAGE(S) 39-50 , XP002233403 * page 1, paragraphs 1,2 * * page 2, paragraph 7 * * page 4, line 1 - page 6, line 23 *	7-9, 12-18, 20-22, 31-33, 36-42, 44-46	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G06F H04L G07F
A		10,11, 23,24, 34,35, 47,48	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	7 September 2004	Sigolo, A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding

FORM 1503 03.82 (P04C01)

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1837

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 01 5127

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	US 5 260 999 A (WYMAN ROBERT M) 9 November 1993 (1993-11-09) * column 7, line 3 - line 40 * * column 11, line 3 - column 12, line 53 * * column 15, line 18 - line 64 *	17-19, 41-43	
A		10,11, 23,24, 34,35, 47,48	

TECHNICAL FIELDS SEARCHED (Int.Cl.7)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	7 September 2004	Sigolo, A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding

FORM 1503 03.82 (P04C01)

BEST AVAILABLE COPY

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 03 01 5127

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

07-09-2004

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5224163	A	29-06-1993	NONE		
US 5299263	A	29-03-1994	CA	2157011 A1	15-09-1994
			DE	69426416 D1	18-01-2001
			DE	69426416 T2	26-07-2001
			EP	0691055 A1	10-01-1996
			JP	8507619 T	13-08-1996
			WO	9421067 A1	15-09-1994
			US	5406628 A	11-04-1995
US 5260999	A	09-11-1993	AU	659652 B2	25-05-1995
			AU	2015892 A	21-12-1992
			DE	69228350 D1	18-03-1999
			DE	69228350 T2	23-09-1999
			EP	0538453 A1	28-04-1993
			IE	922107 A1	30-12-1992
			IL	102114 A	14-05-1996
			IL	116271 A	12-03-1999
			NZ	243277 A	26-10-1995
			WO	9220022 A1	12-11-1992

BEST AVAILABLE COPY

P.B.5818 – Patentlaan 2
2280 HV Rijswijk (ZH)
☎ +31 70 340 2040
TX 31651 epo nl
FAX +31 70 340 3016

Europäisches Patentamt
Zweigstelle in Den Haag Recherchenabteilung

European Patent Office
Branch at The Hague Search division

Office européen des brevets
Département à La Haye Division de la recherche

Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
80538 München
ALLEMAGNE

GRÜNECKER, KINKELDEY, STOCKMAIR & SCHWANHÄUSSER ANWALTSSOZIETÄT
08. Sep. 2004
FRIST TERM
EINGANG - RECEIVED

Datum/Date
08.09.04

Zeichen/Ref./Réf.	Anmeldung Nr./Application No./Demande n°./Patent Nr./Patent No./Brevet n°.
EP18327-IX-034	03015128.6-1245-

Anmelder/Applicant/Demandeur/Patentinhaber/Proprietor/Titulaire
ContentGuard Holdings, Inc.

COMMUNICATION

The European Patent Office herewith transmits as an enclosure the European search report for the above-mentioned European patent application.

If applicable, copies of the documents cited in the European search report are attached.

☐ Additional set(s) of copies of the documents cited in the European search report is (are) enclosed as well.

The following specifications given by the applicant have been approved by the Search Division:

☒ abstract ☒ title

☐ The abstract was modified by the Search Division and the definitive text is attached to this communication.

The following figure will be published together with the abstract: 1

BEST AVAILABLE COPY

REFUND OF THE SEARCH FEE

If applicable under Article 10 Rules relating to fees, a separate communication from the Receiving Section on the refund of the search fee will be sent later.

Europäisches Patentamt • European Patent Office • Office européen des brevets

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 01 5128

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	US 5 260 999 A (WYMAN ROBERT M) 9 November 1993 (1993-11-09) * column 2, line 35 - line 46 * * column 5, line 28 - line 50 * * column 6, line 49 - column 7, line 33 * * column 8, line 4 - line 15 * * column 9, line 54 - line 60 * * column 11, line 3 - line 30 * * column 12, line 12 - line 53 * * column 14, line 62 - column 15, line 4 * * column 17, line 36 - line 46 * * column 21, line 62 - column 22, line 4 * * column 30, line 1 - line 48 * * column 32, line 37 - line 38 * * figures 2-4,8,17,18 *	1-5, 8-11, 17-27, 29,30, 33, 35-53, 59-72, 74,76-78	G06F1/00
Y		7,31,32	TECHNICAL FIELDS SEARCHED (Int.Cl.7) G06F
X	PERRITT H H: "Knowbots, Permissions Headers and Contract Law" PROCEEDINGS TECHNOLOGICAL STRATEGIES FOR PROTECTING INTELLECTUAL PROPERTY IN THE NETWORKED MULTIMEDIA ENVIRONMENT, XX, XX, 2 April 1993 (1993-04-02), pages 39-50, XP002233403 * page 1, paragraphs 1,2 * * page 2, paragraph 7 * * page 4, line 1 - page 7, line 20 *	1-3,8,9, 15-17, 19-28, 30,34, 37, 39-45, 48,49, 57-67, 70-73, 75,76	
Y		12-14, 54-56	

-/--

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	1 September 2004	Sigolo, A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

3

BEST AVAILABLE COPY

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 03 01 5128

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
Y	EP 0 538 216 A (TELEVERKET) 21 April 1993 (1993-04-21) * column 6, line 1 - column 7, line 16 *	12-14, 54-56	
Y	US 4 882 752 A (LINDMAN RICHARD P ET AL) 21 November 1989 (1989-11-21) * column 4, line 32 - line 41 *	7,31,32	
			TECHNICAL FIELDS SEARCHED (Int.Cl.7)

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	1 September 2004	Sigolo, A

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

3

BEST AVAILABLE COPY

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO. EP 03 01 5128

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report. The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

01-09-2004

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5260999 A	09-11-1993	AU 659652 B2	25-05-1995
		AU 2015892 A	21-12-1992
		DE 69228350 D1	18-03-1999
		DE 69228350 T2	23-09-1999
		EP 0538453 A1	28-04-1993
		IE 922107 A1	30-12-1992
		IL 102114 A	14-05-1996
		IL 116271 A	12-03-1999
		NZ 243277 A	26-10-1995
		WO 9220022 A1	12-11-1992
EP 0538216 A	21-04-1993	SE 470001 B	18-10-1993
		DE 69218335 D1	24-04-1997
		DE 69218335 T2	09-10-1997
		EP 0538216 A1	21-04-1993
		ES 2099243 T3	16-05-1997
		JP 6125342 A	06-05-1994
		SE 9102641 A	13-03-1993
		US 5307411 A	26-04-1994
US 4882752 A	21-11-1989	NONE	

BEST AVAILABLE COPY

Petitioner Apple Inc. - Exhibit 1012, p. 1843

FEE TRANSMITTAL FOR FY 2005

Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT | **$180.00**

Complete if Known	
Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. **STEFIK**, *et al.*
Examiner Name	James Reagan
Art Unit	3621
Attorney Docket No.	111325-88 (020700)

USPTO IAP45 OCT 14 2005 PATENT & TRADEMARK OFFICE

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit Card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 19-2380

Deposit Account Name: Nixon Peabody LLP

The Commissioner is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	300	2001	150	Utility filing fee	
1002	200	2002	100	Design filing fee	
1003	200	2003	100	Plant filing fee	
1004	300	2004	150	Reissue filing fee	
1005	200	2005	100	Provisional filing fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

		Extra Claims	Fee from below	Fee Paid
Total Claims	-20** =		X =	0
Independent Claims	-3** =		X =	0
Multiple Dependent			X =	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	50	2202	25	Claims in excess of 20
1201	200	2201	100	Independent claims in excess of 3
1203	360	2203	180	Multiple dependent claim, if not paid
1204	200	2204	100	** Reissue independent claims over original patent
1205	50	2205	25	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	
1051	130	2051	65	Surcharge – late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1,020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1,080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	
1403	1,000	2403	500	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	500	2452	250	Petition to revive – unavoidable	
1453	1,500	2453	750	Petition to revive – unintentional	
1501	1,400	2501	700	Utility issue fee (or reissue)	
1502	800	2502	400	Design issue fee	
1503	1,100	2503	550	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	180.00
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	790	2809	395	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) **$180.00**

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

☐ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop _____, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450

☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) _____.

Date _____ Signature _____

Typed or printed name _____

SUBMITTED BY

				Complete *(if applicable)*	
Name *(Print/Type)*	Carlos R. Villamar	Registration No. *(Attorney/Agent)*	43,224	Telephone	(202) 585-8000
Signature				Date	10/19/05

SEND TO: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

W681968.1

OIPE IAP45 OCT 14 2005 PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of: Mark J. **STEFIK**, *et al.*	)	Examiner: James Reagan
Application No.: 10/015,951	)	Group Art Unit: 3621
Filed: December 17, 2001	)	
For: **DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME**	)	Confirmation No.: 5128

U.S. Patent and Trademark Office
Customer Service Window
Randolph Building
401 Dulany Street
Alexandria, VA 22314

Sir:

INFORMATION DISCLOSURE STATEMENT UNDER 37 C.F.R. § 1.97 (b)

In accordance with the duty of disclosure as set forth in 37 C.F.R. §1.56, Applicants hereby submit the following information in conformance with 37 C.F.R. §§ 1.97 and 1.98. Pursuant to 37 C.F.R. § 1.98, a copy of the listed document is attached.

The Commissioner is hereby authorized to charge the Deposit Account No. 19-2380 in the amount of $180 to comply with the provisions of 37 C.F.R. § 1.97(c).

It is requested that the accompanying PTO-1449 be considered and made of record in the above-identified application. To assist the Examiner, the document is listed on the attached form PTO-1449. It is respectfully requested that an Examiner initial a copy of this form be returned to the undersigned.

10/18/2005 MBEYENE1 00000064 192380 10015951
01 FC:1806 180.00 DA

The Commissioner is hereby authorized to charge any fees connected with this filing which may be required now, or credit any overpayment to Deposit Account No. 19-2380 (111325-88/020700).

Respectfully submitted,

NIXON PEABODY, LLP

By: _____
Carlos R. Villamar
Registration No. 43,224

Date: 10/14/05

NIXON PEABODY LLP
CUSTOMER NO. 22204
401 9th Street, N.W., Suite 900
Washington, DC 20004-2128
Telephone: (202) 585-8000

OIPE IAP45 OCT 14 2005 PATENT & TRADEMARK OFFICE

PTO/SB/08A (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	1	of	1

Complete if Known	
Application Number	10/015,951
Filing Date	December 7, 2001
First Named Inventor	Mark J. STEFIK, *et al.*
Art Unit	3621
Examiner Name	James Reagan
Attorney Docket Number	111325-88 (020700)

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document: Number - Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		6,135,646	October 24, 2000	Kahn et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Application of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Washington, DC 20231.

OIPE IAP45 OCT 14 2005 PATENT & TRADEMARK OFFICE

3621

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. **STEFIK**, *et al.*
Group Art Unit	3621
Examiner Name	James Reagan
Attorney Docket Number	111325-88 (020700)
Confirmation Number	5128

Total Number of Pages in This Submission

ENCLOSURES *(check all that apply)*

- ☒ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☒ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Assignment Papers *(for an Application)*
- ☐ Drawing(s)
- ☐ Declaration and Power of Attorney
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance Communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Application Data Sheet
- ☐ Request for Corrected Filing Receipt with Enclosures
- ☐ A self-addressed prepaid postcard for acknowledging receipt
- ☒ Other Enclosure(s) (*please identify below*):

1. Cited Reference

Remarks

☒ The Commissioner is hereby authorized to charge any additional fees required or credit any overpayments to Deposit Account No. 19-2380 for the above identified docket number.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm *or* Individual name	Carlos R. Villamar Registration No. 43,224 **Nixon Peabody LLP** 401 9th Street, N.W., Suite 900 Washington, D.C. 20004-2128
Signature	
Date 10/14/05	

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

- ☐ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop _____, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450
- ☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) _____.

_____ Date

_____ Signature

_____ Typed or printed name

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,951	12/17/2001	Mark J. Stefik	111325-88	5128

22204 7590 11/16/2005

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

EXAMINER	
REAGAN, JAMES A	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 11/16/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/015,951	STEFIK ET AL.	
	Examiner	Art Unit	
	James A. Reagan	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 January 2005*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. This action is in response to the amendment filed on 27 January 2005.

2. Claims 1, 11, 21, 26, 27, and 34 have been amended.

3. Claims 1-34 have been examined.

4. The rejections of claims 1-34 have been updated to reflect the amendments to the limitations.

Information Disclosure Statement

5. The Information Disclosure Statement filed has been considered. An initialed copy of the Form 1449 is enclosed herewith.

RESPONSE TO ARGUMENTS

6. Applicant's arguments received on 27 January 2005 have been fully considered but they are not persuasive. Referring to the previous Office action, Examiner has cited relevant portions of the references as a means to illustrate the systems as taught by the prior art. As a means of providing further clarification as to what is taught by the references used in the first Office action, Examiner has expanded the teachings for comprehensibility while maintaining the same grounds of rejection of the claims, except as noted above in the section labeled "Status of Claims." This information is intended to assist in illuminating the teachings of the references while providing evidence that establishes further support for the rejections of the claims.

7. Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. Claims 1-3, 6, 9, 10-14, and 21-34 rejected under 35 U.S.C. 103(a) as being unpatentable over Hartrick et al., (US 5,532,920 A) in view of HENRY H. PERRITT JR., Knowbots, "Permissions Headers and Contract Law Papers for the Conference on Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment (30 April 2003).

Claims 1-3, 6, 9, 11, 12, 14, 21, 27 and 28:

Hartrick teaches a digital work distribution system comprising:

- *digital content representing a portion of a digital work rendered on a rendering device* (see at least Figure 1, as well as other relevant and associated text);
- *usage rights associated with said digital content, said usage rights expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols and specifying a manner of use indicating one or more stated purposes for which the digital work can be used and distributed by an authorized party* (see at least Figures 3A-7, as well as other relevant and associated text);
- *storing the digital content and the usage rights as the digital work* (see at least Figure 1, as well as other relevant and associated text);

- *usage rights that further specify status information indicating the status of the digital work and a fee* (revenue) *type and parameter* (e.g. best price fee) (see at least Figures 10 and 11, as well as other relevant and associated text)
- *storing content and rights on the same device* (see at least Figure 1; column 4, lines 40-53, as well as other relevant and associated text)
- *usage rights that include state information indicating the extent of the manner of use exercised by an authorized user* (see at least column 14, lines 15-50; column 15, lines 1-42, as well as other relevant and associated text);

Hartrick does not specifically disclose *said usage rights expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols and specifying a manner of use.* Perritt, However, in at least page 1 as well as other relevant text discloses, "...service identifiers and header descriptors and other forms of labeling and tagging appropriate to allow copyright owners to give different levels of permission, including outright transfer of the copyright interest, use permissions, copy permissions, distribution permission, display permission, and permission to prepare derivative works...how payment authorization procedures should work in conjunction with a permissions header..." It would have been obvious to one of ordinary skill in the art at the time of the invention to add Perritt's service identifiers and header descriptors and other forms of labeling for allowing copyright owners to give different levels of permission with Hartrick's Data processing system and method to enforce payment of royalties when copying softcopy books because the inclusion of Perritt's system goes beyond soft copy books and provides royalty enforcement for all types of digital media.

Claims 10, 13, 29:

Hartrick teaches that usage rights may be integrated within the text or in a separate file (see at least column 4, lines 45-50; column/line 4/66-5/5). Therefore, it would have been obvious to one of ordinary skill at the time the invention was made to store (e.g. floppy disk, CD-ROM) the

rights on a separate disk if additional space was needed because this type of design choice facilitates functionality of copy rights adherences.

Claims 22-24, 26, 30-32 and 34:

The combination of Hartrick/Perritt teaches a multimedia digital content distribution system as shown in the rejections above. Hartrick also discloses that users are charged fees for accessing content (see at least Figures 10 and 11, as well as other relevant text). Hartrick/Perritt do not specifically disclose:

- *the state information comprises information indicating the number of copies of the digital work that are in use;*
- *the state information comprises information indicating the number of time units for which the digital work can be used;*
- *the state information comprises information indicating the revenue owner of the digital work;*
- *the state information comprises information indicating the history of the use and distribution of the digital work;*

Perritt, However, in at least page 1 as well as other relevant text discloses, "...service identifiers and header descriptors and other forms of labeling and tagging appropriate to allow copyright owners to give different levels of permission, including outright transfer of the copyright interest, use permissions, copy permissions, distribution permission, display permission, and permission to prepare derivative works...how payment authorization procedures should work in conjunction with a permissions header..." It would have been obvious to one of ordinary skill in the art at the time of the invention to add Perritt's service identifiers and header descriptors and other forms of labeling for allowing copyright owners to give different levels of permission with Hartrick's Data processing system and method to enforce payment of royalties when copying softcopy books because the inclusion of Perritt's system goes beyond soft copy books and provides royalty enforcement for all types of digital media.

Claims 25 and 33:

Hartrick discloses storing book data such as author, title, copyright date and edition (see at least Figure 5 and associated text). Therefore, it would have been obvious to store other bibliographic data such as publisher and publication date because these data fields are also authoring and publishing data.

10. Claims 4, 5, 7, 8, 15, 16-20, are rejected under 35 U.S.C. 103(a) as being unpatentable over Hartrick/Perritt in view of Sprague et al., (US 5,247,575 A).

Claims 4, 5, 7, 8, and 15-20:

The combination of Hartrick/Perritt teaches a multimedia digital content distribution system as shown in the rejections above. Hartrick also discloses that users are charged fees for accessing content (see at least Figures 10 and 11, as well as other relevant text). Hartrick/Perritt do not specifically recite fees based on time. Sprague, however, teaches a digital content distribution system (see at least abstract; column 24, lines 9-16) where users are charged based on the type or class of content, time or subscription (column 4, lines 8-56; column 13, lines 24-59). Sprague also teaches maintaining a database that stores user fee, account and other statistical information (e.g. usage) (column/line 19/63-20/18; column 23, lines 47-66), as well as fee tables, or schedules and authorized users (column 22, lines 59-66; column 23, lines 46-65). Schedules, fee or tables are familiar and widely used. Similarly, "mark-up" prices are also standard techniques known to those of ordinary skill in retail. Therefore, it would have been obvious to one of ordinary skill to combine the teachings of Hartrick et al. and Sprague et al. in order to allow users the opportunity to select an access method (e.g. rent, purchase, subscription) that best meets their needs.

Conclusion

11. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL.** See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

12. A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **James A. Reagan** whose telephone number is **571.272.6710.** The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **James Trammell** can be reached at **571.272.6712**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

571-273-8300 [Official communications, After Final communications labeled "Box AF"]

571-273-8300 [Informal/Draft communications, labeled "PROPOSED" or "DRAFT"]

Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window**:

Randolph Building

401 Dulany Street

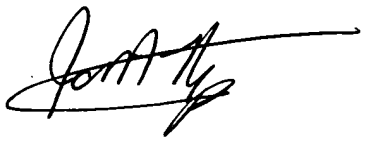
Alexandria, VA 22314.

JAMES A. REAGAN

Primary Examiner

Art Unit 3621

12 October 2005



OIPE JC15
JUL 3 1 2002
PATENT & TRADEMARK OFFICE

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

RECEIVED
AUG 0 2 2002
GROUP 3600

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet	1	of	1

Complete if Known	
Application Number	10/015,951
Filing Date	12/17/2001
First Named Inventor	Mark J. Stefik et al
Group Art Unit	2161
Examiner Name	Unassigned
Attorney Docket Number	111325/000088

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		6,253,193		Ginter et al	06/26/2001	
		4,713,753		Beobert et al	12/15/1987	
		5,052,040		Preston et al	09/24/1991	
		5,301,231		Abraham et al	04/05/1994	
		5,502,766		Boebert et al	03/26/1996	
		5,649,013		Stuckey et al	07/15/1997	
		5,737,416		Cooper et al	04/07/1998	
		5,737,413		Akiyama et al	04/07/1998	
		5,757,907		Cooper et al	05/26/1998	
		6,301,660		Benson	10/09/2001	
		6,327,652		England et al	12/04/2001	
		6,330,670		England et al	12/11/2001	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Office[3]	Number[4]	Kind Code[5] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]

Examiner Signature		Date Considered	2/3/05

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] See attached Kinds of U.S. Patent Documents. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Washington, DC 20231.

NVA234468.1

Form PTO-1449 (Rev. 8-83) U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-8[illegible]	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT	Applicants: Stefik et al.	
	Filing Date: December 17, 2001	Group Art Unit:

OIPE AUG 09 2002 PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date (if appropriate)
JMH	4,827,508	05/02/1989	Shear			
	4,977,594	12/11/1990	Shear			
	5,050,213	09/17/1991	Shear			
	5,410,598	04/25/1995	Shear			
	5,892,900	04/06/1999	Ginter et al.			
	5,910,987	06/08/1999	Ginter et al.			
	5,915,019	06/22/1999	Ginter et al.			
	5,917,912	06/29/1999	Ginter et al.			
	5,920,861	07/06/1999	Hall et al.			
	5,940,504	08/17/1999	Griswold			
	5,943,422	08/24/1999	Van Wie et al.			
	5,949,876	09/07/1999	Ginter et al.			
	5,982,891	11/09/1999	Ginter et al.			
	5,999,949	12/07/1999	Crandall			
	6,112,181	08/29/2000	Shear et al.			
	6,138,119	10/24/2000	Hall et al.			
	6,157,721	12/05/2000	Shear et al.			
	6,185,683	02/06/2001	Ginter et al.			
	6,237,786	05/29/2001	Ginter et al.			
	6,240,185	05/29/2001	Van Wie et al.			
	6,253,193	06/26/2001	Ginter et al.			
	6,292,569	09/18/2001	Shear et al.			
	6,363,488	05/26/2002	Ginter et al.			
	6,389,402	05/14/2002	Ginter et al.			

RECEIVED AUG 13 2002 GROUP 3600

Examiner JMH Date Considered 28 SEP 05

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this formwith next communication to applicant.

Form PTO-1449 (Rev. 8-83) U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-88	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT	Applicants: Stefik et al.	
	Filing Date: December 17, 2001	Group Art Unit:

OIPE JC68 AUG 30 2002 PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date (if appropriate)
JM	3,263,158	07/01/1966	Janis			
	3,609,697	09/28/1971	Blevins et al.			
	3,790,700	02/05/1974	Callais et al.			
	3,798,605	03/19/1974	Feistel			
	4,159,468	06/26/1979	Barnes et al.			
	4,220,991	09/02/1980	Hamano et al.			
	4,278,837	07/14/1981	Best			
	4,323,921	04/06/1982	Guillou			
	4,442,486	04/10/1984	Mayer			
	4,529,870	07/16/1985	Chaum			
	4,558,176	12/10/1985	Arnold et al.			
	4,593,376	06/03/1986	Volk			
	4,614,861	09/30/1986	Pavlov et al.			
	4,644,493	02/17/1987	Chandra et al.			
	4,658,093	04/14/1987	Hellman			
	4,817,140	03/28/1989	Chandra et al.			
	4,868,376	09/19/1989	Lessin et al.			
	4,891,838	01/02/1990	Faber			
	4,924,378	05/08/1990	Hershey et al.			
	4,932,054	06/05/1990	Chou et al.			
	4,937,863	06/26/1990	Robert et al.			
	4,949,187	08/14/1990	Cohen			
	4,953,209	08/28/1990	Ryder, Sr. et al.			
	4,961,142	10/02/1990	Elliott et al.			
	4,975,647	12/04/1990	Downer et al.			
	4,999,806	03/12/1991	Chernow et al.			
	5,010,571	04/23/1991	Katznelson			
	5,014,234	05/07/1991	Edwards, Jr.			
	5,023,907	06/11/1991	Johnson et al.			
	5,047,928	09/10/1991	Wiedemer			
	5,052,040	09/24/1991	Preston et al.			

RECEIVED SEP 04 2002 GROUP 3600

Examiner JM	Date Considered 28SEP05

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this formwith next communication to applicant.

Form PTO-1449 (Rev. 8-83) U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-88	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT	Applicants: Stefik et al.	
	Filing Date: December 17, 2001	Group Art Unit:

OIPE JC16 AUG 30 2002 PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date (if appropriate)
	5,058,164	10/15/1991	Elmer et al.			
	5,103,476	04/07/1992	Waite et al.			
	5,113,519	05/12/1992	Johnson et al.			
	5,136,643	08/04/1992	Fischer			
	5,138,712	08/11/1992	Corbin			
	5,146,499	09/08/1992	Geffrotin			
	5,148,481	09/15/1992	Abraham et al.			
	5,159,182	10/27/1992	Eisele			
	5,183,404	02/02/1993	Aldous et al.			
	5,191,193	03/02/1993	Le Roux			
	5,204,897	04/20/1993	Wyman			
	5,222,134	06/22/1993	Waite et al.			
	5,235,642	08/10/1993	Wobber et al.			
	5,247,575	09/21/1993	Sprague et al.			
	5,255,106	10/19/1993	Castro			
	5,260,999	11/09/1993	Wyman			
	5,263,157	11/16/1993	Janis			
	5,263,158	11/16/1993	Janis			
	5,276,444	01/04/1994	McNair			
	5,276,735	01/04/1994	Boebert et al.			
	5,291,596	03/01/1994	Mita			
	5,311,591	05/10/1994	Fischer			
	5,319,705	06/07/1994	Halter et al.			
	5,337,357	08/09/1994	Chou et al.			
	5,339,091	08/16/1994	Yamazaki et al.			
	5,341,429	08/23/1994	Stringer et al.			
	5,347,579	09/13/1994	Blandford			
	5,381,526	01/10/1995	Ellson			
	5,394,469	02/28/1995	Nagel et al.			
	5,412,717	05/02/1995	Fischer			
	5,428,606	06/27/1995	Moskowitz			

RECEIVED
SEP 04 2002
GROUP 3600

Examiner [signature] Date Considered 28 SEP 05

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this formwith next communication to applicant.

Form PTO-1449 (Rev. 8-83)	U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-88	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT		Applicants: Stefik et al.	
		Filing Date: December 17, 2001	Group Art Unit:

JC#63 OIPE AUG 30 2002 PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date (if appropriate)
JM	5,432,849	07/11/1995	Johnson et al.			
	5,438,508	08/01/1995	Wyman			
	5,444,779	08/22/1995	Daniele			
	5,453,601	09/26/1995	Rosen			
	5,455,953	10/03/1995	Russell			
	5,457,746	10/10/1995	Dolphin			
	5,473,687	12/05/1995	Lipscomb et al.			
	5,473,692	12/05/1995	Davis			
	5,499,298	03/12/1996	Narasimhalu et al.			
	5,504,814	04/02/1996	Miyahara			
	5,504,818	04/02/1996	Okano			
	5,504,837	04/02/1996	Griffeth et al.			
	5,509,070	04/16/1996	Schull			
	5,530,235	06/25/1996	Stefik et al.			
	5,532,920	07/02/1996	Hartrick et al.			
	5,534,975	07/09/1996	Stefik et al.			
	5,539,735	07/23/1996	Moskowitz			
	5,563,946	10/08/1996	Cooper et al.			
	5,568,552	10/22/1996	Davis			
	5,621,797	04/15/1997	Rosen			
	5,629,980	05/13/1997	Stefik et al.			
	5,633,932	05/27/1997	Davis et al.			
	5,634,012	05/27/1997	Stefik et al.			
	5,638,443	06/10/1997	Stefik et al.			
	5,655,077	08/05/1997	Jones et al.			
	5,708,717	01/13/1998	Alasia			
	5,734,823	03/31/1998	Saigh et al.			
	5,734,891	03/31/1998	Saigh			
	5,745,569	04/28/1998	Moskowitz et al.			
	5,748,783	05/05/1998	Rhoads			
	5,761,686	06/02/1998	Bloomberg			

RECEIVED
SEP 0 4 2002
GROUP 3600

Examiner JM Date Considered 28 SEP 05

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this formwith next communication to applicant.

Form PTO-1449 (Rev. 8-83)	U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-88	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT		Applicants: Stefik et al.	
		Filing Date: December 17, 2001	Group Art Unit:

OIPE AUG 30 2002 PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date (If appropriate)
GMR	5,765,152	06/09/1998	Erickson			
	5,768,426	06/16/1998	Rhoads			
	5,825,892	10/20/1998	Braudaway et al.			
	6,047,067	04/04/2000	Rosen			
	6,115,471	09/05/2000	Oki et al.			
	6,233,684	05/15/2001	Stefik et al.			
	6,266,618	05/01/2001	Downs et al.			
	6,345,256	02/05/2002	Milsted et al.			

FOREIGN PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Country	Class	Subclass	Translation Yes	Translation No
	0 084 441	07/27/1983	EP			Full Eng	
	0 180 460	05/07/1986	EP			Full Eng	
	0 332 707	09/01/1989	EP			Full Eng	
	0 651 554	05/03/1995	EP			Full Eng	
	0 668 695	08/23/1995	EP			Full Eng	
	0 725 376	08/07/1996	EP			Full Eng	
	2 136 175	09/12/1984	GB			Full Eng	
	2 236 604	04/10/1991	GB			Full Eng	
	WO 01/63528	08/30/2001	PCT			Full Eng	
	WO 92/20022	11/12/1992	PCT			Full Eng	
	WO 93/01550	01/21/1993	PCT			Full Eng	
	WO 99/49615	09/30/1999	PCT			Full Eng	

RECEIVED
SEP 04 2002
GROUP 3600

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

Examiner Initial	
	"National Semiconductor and EPR Partner for Information Metering/Data Security Cards" March 4, 1994, Press Release from Electronic Publishing Resources, Inc.
	Weber, R., "Digital Rights Management Technology" October 1995
	Flasche, U. et al., "Decentralized Processing of Documents", pp. 119-131, 1986, Comput. & Graphics, Vol. 10, No. 2
	Mori, R. et al., "Superdistribution: The Concept and the Architecture", pp. 1133-1146, 1990, The Transactions of

Examiner	Date Considered 28SEP05

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this formwith next communication to applicant.

Form PTO-1449 (Rev. 8-83)	U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-88	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT		Applicants: Stefik et al.	
		Filing Date: December 17, 2001	Group Art Unit:

O I P E JC169 AUG 30 2002 PATENT & TRADEMARK OFFICE

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

Examiner Initial	
	Weber, R., "Metering Technologies for Digital Intellectual Property", pp. 1-29, Oct. 1994, A Report to the International Federation of Reproduction Rights Organizations
	Clark, P.C. et al., "Bits: A Smartcard protected Operating System", pp. 66-70 and 94, November 1994, Communications of the ACM, Vol. 37, No. 11
	Ross, P.E., "Data Guard", pp. 101, June 6, 1994, Forbes
	Saigh, W.K., "Knowledge is Sacred", 1992, Video Pocket/Page Reader Systems, Ltd.
	Kahn, R.E., "Deposit, Registration and Recordation in an Electronic Copyright Management System", pp. 1-19, August 1992, Corporation for National Research Initiatives, Virginia
	Hilts, P. et al., "Books While U Wait", pp. 48-50, January 3, 1994, Publishers Weekly
	Strattner, A, "Cash Register on a Chip may Revolutionize Software Pricing and Distribution; Wave Systems Corp.", pp. 62, April 1994, Computer Shopper, Vol. 14, No. 4, ISSN 0886-0556
	O'Conner, M., "New Distribution Option for Electronic Publishers; iOpener Data Encryption and Metering System for CD-ROM use; Column", pp. 134, March 1994, CD-ROM Professional, Vol. 7, No. 2, ISSN: 1409-0833
	Willett, S., "Metered PCs: Is Your System Watching You? Wave System beta tests new technology", pp. 84, May 2, 1994, InfoWorld
	Linn, R., "Copyright and Information Services in the Context of the National Research and Education Network ", pp. 9-20, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Perrit, Jr., H., "Permission Headers and Contract Law", pp. 27-48, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Upthegrove, L., "Intellectual Property Header Descriptors: A Dynamic Approach", pp. 63-66, January 1994, IMA Intellectual Property Proceedings, Vol. 1, Issue 1
	Sirbu, M., "Internet Billing Service Design and prototype Implementation", pp. 67-80, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Simmel, S. et al., "Metering and Licensing of Resources: Kala's General Purpose Approach", pp. 81-110, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Kahn, R., "Deposit, Registration and Recordation in an Electronic Copyright Management System", pp. 111-120, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Tygar, J. et al., "Dyad: A System for Using Physically Secure Coprocessors", pp. 121-152, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Griswold, G., "A Method for Protecting Copyright on Networks", pp. 169-178, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Nelson, T., "A Publishing and Royalty Model for Networked Documents", pp. 257-259, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Robinson, E., "Redefining Mobile Computing", pp. 238-240, 247-248 and 252, July 1993, PC Computing
	Abadi, M. et al., "Authentication and Delegation with Smart-cards", 1990, Research Report DEC Systems Research Center
	Mark Stefik, "Letting Loose the Light: Igniting Commerce in Electronic Publication", pp. 219-253, 1996, Internet Dreams: Archetypes, Myths, and Metaphors, IDSN 0-262-19373-6
	Mark Stefik, "Letting Loose the Light: Igniting Commerce in Electronic Publication", pp. 2-35, February 8, 1995, Internet Dreams: Archetypes, Myths and Metaphors,

Examiner _____ Date Considered 28 SEP 05

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this formwith next communication to applicant.

Petitioner Apple Inc. - Exhibit 1012, p. 1864

Form PTO-1449 (Rev. 8-83) U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-88	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT	Applicants: Stefik et al.	
	Filing Date: December 17, 2001	Group Art Unit:

OIPE JC160 AUG 30 2002 PATENT & TRADEMARK OFFICE

N/A

RECEIVED
SEP 04 2002
GROUP 3600

Examiner	Date Considered 28 SEP 05

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this formwith next communication to applicant.

OIPE
JUN 07 2005
PATENT & TRADEMARK OFFICE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. STEFIK, *et al.*
Art Unit	3621
Examiner Name	Calvin L. Hewitt, II
Attorney Docket Number	111325-88 (020700)

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number - Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,882,752	November 21, 1989	Richard P. Lindman, *et al*	
		US-5,224,163	June 29, 1993	Morrie Gasser, *et al.*	
		US-5,299,263	March 29, 1994	Michael J. Beller, *et al.*	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
		EP 0 538 216 A	April 21, 1993	TELEVERKET		

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		HENRY H. PERRITT, JR., "Knowbots, Permissions Headers and Contract Law"; Papers for the conference on Technological Strategies For Protecting Intellectual Property In The Networked Multimedia Environment, April 2, 1993; pages 1-22, XP-002233403	
		European Search Report; mailed September 8, 2004 (European Application No. 03 01 5128).	
		European Search Report; mailed September 13,2004 (European Application No. 03 01 5127).	

Examiner Signature		Date Considered	28 SEP 05

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

OIPE IAP5
OCT 14 2005
PATENT & TRADEMARK OFFICE

PTO/SB/08A (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/015,951
Filing Date	December 7, 2001
First Named Inventor	Mark J. STEFIK, *et al.*
Art Unit	3621
Examiner Name	James Reagan
Attorney Docket Number	111325-88 (020700)

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number - Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
JMK		6,135,646	October 24, 2000	Kahn et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Application of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]

Examiner Signature	JMK	Date Considered	28 SEP 05

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Washington, DC 20231.

Notice of References Cited	Application/Control No. 10/015,951	Applicant(s)/Patent Under Reexamination STEFIK ET AL.	
	Examiner James A. Reagan	Art Unit 3621	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-			
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	HENRY H. PERRITT JR., Knowbots, "Permissions Headers and Contract Law Papers for the Conference on Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment (30 April 2003). Pages 1-22. Retrieved from IDS.
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

XP-002233403

P.D. 30 DEC 1993
P. 1-22 (22)

BEST AVAILABLE COPY

Knowbots, Permissions Headers and Contract Law

paper for the conference on

Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment

April 2-3, 1993 with revisions of 4/30/93

Copyright 1993
Henry H. Perritt, Jr.
Professor of Law
Villanova Law School
Villanova, PA 19085
(215) 645-7078
FAX (215) 645-7033, (215) 896-1723
Internet: perritt@ucis.vill.edu

Introduction

One of the ways to protect intellectual property on the NREN is through a digital library concept. Under this concept, a work would have attached to it a "permissions header," defining the terms under which the copyright owner makes the work available. The digital library infrastructure, implemented on the NREN, would match request messages from users with the permissions headers. If the request message and the permissions header match, the user would obtain access to the work. This concept encompasses major aspects of electronic contracting, which is already in wide use employing Electronic Data Interchange ("EDI") standards developed by ANSI Committee X12.1

This paper explains the relationship between the digital library concept and EDI practice, synthesizing appropriate solutions for contract law, evidence, and agency issues that arise in electronic contracting. The question of how electronic signatures should work to be legally effective is an important part of this inquiry. The paper also defines particular types of service identifiers, header descriptors, and other forms of labeling and tagging appropriate to allow copyright owners to give different levels of permission, including outright transfer of the copyright interest, use permission, copying permission, distribution permission, display permission, and permission to prepare derivative works.The paper considers how payment authorization procedures should work in conjunction with a permissions header and digital library concept in order to integrate the proposed copyright licensing procedures with existing and anticipated electronic payment authorization systems. The paper necessarily considers whether existing standards approaches related to SGML and X12 are sufficient or whether some new standards development efforts will be necessary for implementation of the concepts. The paper considers the relationship between technology and law in enforcing intellectual property, and emphasizes that the traditional adaptation of legal requirements to levels of risk is appropriate as the law is applied to new technologies.

There are certain common issues between the intellectual property question and other applications of wide area

Petitioner Apple Inc. - Exhibit 1012, p. 1869

digital network technology. The question of signatures and writings to reflect the establishment of duties and permissions and the transfer of rights is common to the intellectual property inquiry and to electronic commerce using EDI techniques. There also are common questions involving rights to use certain information channels: First Amendment privileges, and tort liability. These are common not only to technological means of protecting intellectual property but to all forms of wide area networking.

The problem

The law recognizes intellectual property because information technology permits one person to get a free ride on another person's investment in creating information value. Creative activity involving information usually is addressed by copyright, although patent has a role to play in protecting innovative means of processing information.2

Intellectual property arose in the context of letterpress printing technology. Newer technologies like xerography and more recently small computer technology and associated word processing and networking have increased the potential for free rides and accordingly increased the pressure on intellectual property.

The concern about free ride potential is especially great when people envision putting creative works on electronic publishing servers connected to wide area networks intending to permit consumers of information products to access these objects, frequently combining them and generally facilitating "publishing on demand" rather than the well known publishing just in case, typified by guessing how many copies of a work will sell, printing those in advance, and then putting them in inventory until someone wants them.

The concern is that it will be too easy to copy an entire work without detection and without paying for it. Worse, it will be easy to copy an entire work and resell it either by itself or as a part of a new derivative work or collection.

But technology is capable of protecting investment in new ways as well as gaining a free ride. Computer networks make it possible to restrict access and to determine when access occurs. Depending on how new networks are designed, they may actually reduce the potential for a free ride. The digital library is one way of realizing that potential. Professor Pamela Samuelson has observed that the digital library model replaces intellectual property with a system of technological controls.3

Digital Library Concepts

Basic Concepts

A digital library is a set of information resources ("information objects") distributed throughout an electronic network. The objects reside on servers (computers with associated disk drives connected to the network). They can be retrieved remotely by users using "client" workstations.

Origin of Concepts

The phrase "digital library" and the basic concept was first articulated in a 1989 report growing out of a workshop sponsored by the Corporation for National Research Initiatives.4 From its inception, the digital library concept envisioned retrieval of complete information

Petitioner Apple Inc. - Exhibit 1012, p. 1870

resources and not merely bibliographic information.5

The technologies of remote retrieval of complete information objects using electronic technologies is in wide use through the WESTLAW, Dialog, LEXIS, NEXIS, and National Library of Medicine databases. These remotely accessible databases, however, unlike the digital library involved a single host on which most of the data resides. The digital library concept envisions a multiplicity of hosts (servers).

Recent Developments

The remotely accessible database host concept is converging with the digital library concept as more of the electronic database vendors provide gateways to information objects actually residing on other computers. This now is commonplace with WESTLAW access to Dialog, and Dialog's gateways to other information providers.

The most explicit implementation of the digital library concept is the Wide Area Information Service ("WAIS"), which implements ANSI standard Z.39.6 WAIS permits a remote user to formulate a query that is applied to a multiplicity of WAIS servers each of which may contain information responsive to the query. The WAIS architecture permits search engines of varying degrees of sophistication, resident on WAIS information servers to apply the query against their own information objects, reporting matches back to the user.7 Future implementations of WAIS permit automatic refinement of searches according to statistical matching techniques.

The Corporation for National Research Initiatives has proposed a test bed for an electronic copyright management system.8 The proposed system would include four major elements: automated copyright recording and registration, automated, on line clearance of rights, private electronic mail and digital signatures to provide security. It would include three subsystems: a Registration and Recording System (RRS), a Digital Library System (DLS), and a Rights Management System (RMS). The RRS would provide the functions enumerated above and would be operated by the Library of Congress. It would provide "change of title" information.9 The RMS would be an interactive distributed system capable of granting rights on line and permitting the use of copyrighted material in the Digital Library System. The test bed architecture would involve computers connected to the Internet performing the RRS and RMS functions.

Digital signatures would link an electronic bibliographic record with the contents of the work, ensuring against alteration after deposit.10 Multiple RMS servers would be attached to the Internet. A user wishing to obtain rights to an electronically published work would interact electronically with the appropriate RMS. When copyright ownership is transferred, a message could be sent from the RMS to the RRS11 - creating an electronic marketplace for copyrighted material.

The EBR submitted with a new work would "identify the rights holder and any terms and conditions on the use of the document or a pointer to a designated contact for rights and permissions."12 The EBR, thus, is apparently equivalent to the permissions header discussed in this paper. Security in the transfer of rights would be provided by digital signatures using public key encryption, discussed further, infra in the section on encryption.

Basic Architectural Concepts

Petitioner Apple Inc. - Exhibit 1012, p. 1871

The digital library concept in general contemplates three basic architectural elements: a query, also called a "knowbot" in some descriptions; a permissions header attached to each information object; and a procedure for matching the query with the permissions header.

Two kinds of information are involved in all three architectural elements: information about the content of information objects desired and existing, and information about the economic terms on which an information object is made available. For example, a query desiring court opinions involving the enforcement of foreign judgments evidencing a desire to download the full text of such judicial opinions and to pay up to $1.00 per minute of search and downloading time would require that the knowbot appropriately represent the subject matter "enforcement of foreign judgments." It also requires that the knowbot appropriately represent the terms on which the user is willing to deal: downloading and the maximum price. The permissions header similarly must express the same two kinds of information. If the information object to which the permissions header is attached is a short story rather than a judicial opinion, the permissions header must so indicate. Or, if the information object is a judicial opinion and it is about enforcement of foreign judgments, the permission header may indicate that only a summary is available for downloading at a price of $10.00 per minute. The searching, matching, and retrieval procedure in the digital library system must be capable of determining whether there is a match on both subject matter and economic terms, also copying and transmitting the information object if there is a match.

Comparison to EDI

Electronic Data Interchange ("EDI") is a practice involving computer-to-computer commercial dealing without human intervention. In the most widespread implementations, computers are programmed to issue purchase orders to trading partners, and the receiving computer is programmed to evaluate the terms of the purchase order and to take appropriate action, either accepting it and causing goods to be manufactured or shipped or rejecting it and sending an appropriate message. EDI is in wide use in American and foreign commerce, using industry-specific standards for discrete commercial documents like purchase orders, invoices, and payment orders, developed through the American National Standards Institute.

There obviously are similarities between the three architectural elements of the digital library concept and EDI. There is a structured way of expressing an offer or instruction, and a process for determining whether there is a match between what the recipient is willing to do and what the sender requests.

There is also, however, an important difference. In the digital library concept, a match results in actual delivery of the desired goods and services in electronic form. In EDI practice, the performance of the contractual arrangement usually involves physical goods or performance of nonelectronic services.

Nevertheless, the digital library and EDI architectures are sufficiently similar and, it turns out the legal issues associated with both are sufficiently similar to make analogies appropriate.

Elements of Data Structure

For purposes of this paper, the interesting parts of the data structure are those elements that pertain to permission, more than those elements that pertain to content of the information object to which the header is attached. Accordingly, this section will focus on only permissions-related elements, after noting in passing that the content part of the header well might be a pointer to an inverted file to permit full text searching and matching.

The starting point conceptually for identifying the elements of the permissions header are the rights exclusively reserved to the copyright owner by 106 of the copyright statute. But these exclusive rights need not be tracked directly because the owner of an information object free to impose contractual restrictions as well as to enjoy rights granted by the Copyright Act. Accordingly, it seems that the following kinds of privileges in the requester should be addressed in the permissions header:

outright transfer of all rights

use privilege, either unrestricted or subject to restrictions

copying, either unlimited or subject to restrictions like quantitative limits

distribution, either unlimited or subject to restrictions, like geographic ones or limits on the markets to which distribution can occur

preparation of derivative works

Display and presentation rights, separately identified in 106 would be subsumed into the use element, because they are particular uses.

The simplest implementation would allow only binary values for each of these elements. But a binary approach does not permit the permissions header to express restrictions, like those suggested in the enumerated list. Elements could be defined to accept the most common kinds of restrictions on use, and quantitative limits on copying, but it would be much more difficult to define in advance the kinds of geographic or market-definition restrictions that an owner might wish to impose with respect to distribution.

In addition to these discrete privileges, the permissions header must express pricing information. The most sensible way of doing this is to have a price associated with each type of privilege. In the event that different levels of use, copying, or distribution privilege are identified, the data structure should allow a price to be associated with each level.

A complicating factor in defining elements for price is the likelihood that different suppliers would want to price differently. For example, some would prefer to impose a flat fee for the grant of a particular privilege. Others might wish to impose a volume-based fee, and still others might wish to impose a usage or connect-time based fee. The data structure for pricing terms must be flexible enough to accommodate at least these three different approaches to pricing.

Finally, the data structure must allow for a specification of acceptable payment terms and have some kind of trigger for a payment approval procedure. For example,

Petitioner Apple Inc. - Exhibit 1012, p. 1873

the permissions header might require presentation of a credit card number and then trigger a process that would communicate with the appropriate credit card database to obtain authorization. Only if the authorization was obtained would the knowbot and the permissions header "match."

There is a relationship between the data structures and legal concepts. The knowbot is a solicitation of offers. The permissions header is an offer. The matching of the two constitutes an acceptance. Mr. Linn's "envelope" could be the "contract."

There are certain aspects of the data structure design that are not obvious. One is how to link price with specific levels of permission. Another is how to describe particular levels of permission. This representation problem may benefit from the use of some deontic logic, possibly in the form of a grammar developed for intellectual property permissions. Finally, it is not clear what the acceptance should look like. Conceptually, the acceptance occurs when the knowbot matches with a permissions header, but it is unclear how this legally significant event should be represented.

Role of Encryption

The CNRI test bed proposal envisions the use of public key encryption to ensure the integrity of digital signatures and to ensure the authenticity of information objects. Public key encryption permits a person to encrypt a message - like a signature using a secret key, one known only to the sender, while permitting anyone with access to a public key to decrypt it. Use of public key cryptography in this fashion permits any user to authenticate a message, ensuring that it came from the purported sender.13 A related technology called "hashing" permits an encrypted digital signature to be linked to the content of a message. The message can be sent in plain text (unencrypted) form, but if any part of it is changed, it will not match the digital signature. The digital signature and hashing technologies thus permit not only the origin but also the content integrity of a message of arbitrary length to be authenticated without necessitating encryption of the content of the message. This technology has the advantage, among others, that it is usable by someone lacking technological access to public key encryption. An unsophisticated user not wishing to incur the costs of signature verification nevertheless can use the content of the signed information object.

It is well recognized that encryption provides higher levels of security than other approaches. But security through encryption comes at a price. Private key encryption systems require preestablished relationships and exchange of private keys in advance of any encrypted communication. The burdens of this approach have led most proponents of electronic commerce to explore public key encryption instead. But public key systems require the establishment and policing of a new set of institutions. An important infrastructure requirement for practicable public key cryptography is the establishment and maintenance of certifying entities that maintain the public keys and ensure that they are genuine ones rather than bogus ones inserted by forgers. A rough analogy can be drawn between the public key certifying entities and notaries public. Both kinds of institutions verify the authenticity of signature. Both kinds require some level of licensing by governmental entities. Otherwise the word of the "electronic notary"

Petitioner Apple Inc. - Exhibit 1012, p. 1874

(certifying entity) is no better than an uncertified, unencrypted signature. In a political and legal environment in which the limitations of regulatory programs have been recognized and have led to deregulation of major industries, it is not clear that a major new regulatory arrangement for public key encryption is practicable. Nevertheless, experimentation with the concept in support of digital library demonstration programs can help generate more empirical data as to the cost and benefits of public key encryption to reinforce electronic signatures.

On the other hand, it is not desirable to pursue approaches requiring encryption of content. No need to encrypt the contents is apparent in a network environment. Database access controls are sufficient to prevent access to the content if the permissions header terms are not matched by the knowbot. On the other hand, if the electronic publishing is effected through CDROMs or other physical media possessed by a user, then encryption might be appropriate to prevent the user from avoiding the permissions header and going directly to the content.

While encrypted content affords greater security to the owner of copyrighted material. Someone who has not paid the price to the copyright owner must incur much higher cost to steal the material. But the problem is everyone must pay a higher price to use the material. One of the dramatic lessons of the desktop computer revolution was the clear rejection of copyright protection in personal computer software. The reasons that copy protection did not survive in the market place militate against embracing encryption for content. Encryption interferes with realization of electronic markets, because producer and consumer must have the same encryption and description protocols. Encryption burdens processing of electronic information objects because it adds another layer. Some specific implementations have encryption require additional hardware at appreciable costs.

Digital libraries cannot become a reality until consumers perceive that the benefits of electronic formats outweigh the costs, compared to paper formats. Encryption interferes with electronic formats' traditional advantages of density, reusability, editability, and computer search ability and also, by impairing open architectures may perpetuate some of papers' advantages with respect with browsibility.14

The need for encryption of any kind depends upon whether security is available without it. That depends, in turn, on the kinds of free rides that may be obtainable and the legal status of various kinds of electronics transactions in the digital library system.

Legal Issues

Copyright: What legal effect is intended?

The design of the permissions header and the values in the elements of the header must be unambiguous as to whether an outright transfer of a copyright interest is intended or whether only a license is intended. If an outright transfer15 is intended, then the present copyright statute requires a writing signed by the owner of the rights conveyed.16 Recordation of the transfer with the Copyright office is not required, but provides advantages in enforcing transferee rights.17 On the other hand, non exclusive licenses need not be in writing nor registered. If the electronic transaction transfers the copyright in its entirety, then the rights of the transferor are extinguished, and the rights of the

Petitioner Apple Inc. - Exhibit 1012, p. 1875

transferee are determined by the copyright statute. The only significant legal question is whether the conveyance was effective.

On the other hand, when the copyright is not transferred outright but only certain permissions are granted or certain rights conveyed, the legal questions become more varied. Then, the rights of the transferor and the obligations of the transferee are matters of contract law. It is important to understand the degree to which the contract is enforceable and how it is to be interpreted in the event of subsequent disputes. The following sections consider briefly the first sale doctrine as a potential public policy obstacle to enforcing contractual restrictions different from those imposed by the copyright statute and then explore in greater depth whether electronic techniques satisfy the formalities traditionally required for making a contract, whether they adequately ensure against repudiation, and whether they provide sufficient information to permit predictable interpretation of contractual obligations and privileges.

First Sale Doctrine

The first sale doctrine may invalidate restrictions on use. It is impermissible for the holder of a patent to impose restrictions on the use of a patented product after the product has been sold. Restrictions may be imposed, however, on persons who merely license the product.18 The rationale for this limit on the power of the owner of the intellectual property interest is that to allow limitations on use of the product would interfere with competition beyond what the Congress - and arguably the drafters of the Constitution - intended in setting up the patent system.

The first sale doctrine applies to copyright owners.19 Indeed, because of the First Amendment's protection of informational activity, the argument against restrictions after the first sale may be even stronger in the copyright arena then in the patent arena.

The first sale doctrine is potentially important because it may invalidate restrictions imposed on the use of information beyond what is authorized by the Copyright Act and by common law trade secret. Thus, there may be serious questions about the legal efficacy of use restrictions suggested in ___, although such restrictions are common in remote database service agreements. The vendors could argue that the limitations pertain to the contractual terms for delivery of a service rather than use of information as such. The characterization avoids the overlap with copyright and thus may also avoid the conflict between federal policy and contract enforcement.20

Contract Formation Issues

The law does not enforce every promise. Instead, it focuses its power only on promises surrounded with certain formalities to make it likely that the person making the promise (the "promisor") and the person receiving the promise (the "promisee") understood that their communication had legal consequences. A threshold question for the digital library system is whether the traditional formalities for making a contract are present when the contract is made through electronic means. The digital library system considered in this paper clearly contemplates that a contract is formed when the knowbot and the permissions header achieve a match. In this respect, the digital library concept converges with EDI where trading parties contemplate that a contract to perform services or deliver goods is

Petitioner Apple Inc. - Exhibit 1012, p. 1876

formed when a match occurs either upon the receipt of a purchase order or upon the transmission of a purchase order acknowledgment.

It is not altogether clear, however, whether the match between values and computer data structures meets contract formation requirements, particularly those expressed in various statutes of frauds. Statutes of frauds require "writings" and "signatures" for certain kinds of contracts - basically those contemplating performance extending beyond a period of one year.21

In many instances, the digital library contract will be fully performed almost instantaneously upon delivery of the information object after the knowbot and the permissions header match. In such a case, the statute of frauds is not a problem and its requirements need not be satisfied. In other cases, however, as when the intent of the owner of the information object is to grant a license to do things that will extend beyond one year, the statute of frauds writing and signature requirements must be met.

Historical application of Statutes Of Frauds by the courts clearly indicates that there is flexibility in the meaning of "writing" and "signature." A signature is any mark made with the intent that it be a signature.22 Thus an illiterate person signs by making an "X," and the signature is legally effective. Another person may sign a document by using a signature stamp. Someone else may authorize an agent to sign his name or to use the signature stamp. In all three cases the signature is legally effective. There may of course be arguments about who made the X, or whether the person applying the signature stamp was the signer or his authorized agent, but these are evidentiary and agency questions, not arguments about hard and fast contract-law requirements.

Under the generally accepted legal definition of a signature, there is no legal reason why the "mark" may not be made by a computer printer, or for that matter by the write head on a computer disk drive or the data bus in a computer random access memory. The authorization to the computer agent to make the mark may be given by entering a PIN ("Personal Identification Number") on a keyboard. To extend the logic, there is no conceptual reason to doubt the legal efficacy of authority to make a mark if the signer writes a computer program authorizing the application of a PIN upon the existence of certain conditions that can be tested by the program. The resulting authority is analogous to a signature pen that can be operated only with a mechanical key attached to somebody's key ring, coupled with instructions to the possessor of the key.

Which of these various methods should be selected for particular types of transactions must depend, not on what the law requires, because the law permits any of these methods. Rather, it must depend on the underlying purposes of the legal requirement and which method best serves those purposes.

The real issue is how to prove that a particular party made the mark. In other words, the contingency to be concerned about is repudiation, not absence of formalities. Repudiation should be dealt with through usual evidentiary and fact finding processes rather than artificial distinctions between signed and unsigned documents.

Authority is skimpier on how flexible the "writing"

Petitioner Apple Inc. - Exhibit 1012, p. 1877

requirement is. The best approach is to borrow the fixation idea from the copyright statute and conclude that a writing is "embodiment in a copy . . . sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for more a period of more than transitory duration."23

The most important thing conceptually is to understand the purpose of the writing and signature requirements. They have two purposes: awareness or formality and reliability of evidence. Signature requirements, like requirements for writings and for original documents have an essentially evidentiary purpose. If there is a dispute later, they specify what kind of evidence is probative of certain disputed issues, like "who made this statement and for what purpose?" The legal requirements set a threshold of probativeness. Surely the values in a knowbot as well as the values in a permissions header constitute and "mark," and someone who knowingly sets up potential transactions in a digital library scheme can have the intent that the mark be a signature.

When a contract is made through a signed writing, it is more likely that the parties to the contract understand what they are doing. They are aware of the legal affect of their conduct because the writing in the signature involve a greater degree of formality than a simple conversation.

The awareness/formality purpose can be served by computerized contracting systems. This is so not so much because the computers are "aware" of the affect of their "conduct." Rather, it is true because the computers are agents of human principals. The programming of the computer to accept certain contract terms is the granting of authority to the computer agent to enter into a contract. The fact that a principal acts through an agent engaging in conduct at a later point and time never has been thought to defeat contract formation in the traditional evolution of agency and contract law. Nor should it when the agent is a computer.

Fulfillment of the evidentiary purpose depends on the reliability of the information retained by the computer systems making up the digital library. Such systems must be designed to permit the proponent of contract formation to establish the following propositions if the other party to the purported contract attempts to repudiate it.

1.It came from computer X

2.It accurately represents what is in computer X24 now25

3.What is in computer X now is what was in computer X at the time of the transaction

4.What was in computer X at the time of the transaction is what was received from the telecommunications channel26

5.What was received from the telecommunications channel is what was (a) sent, (b) by computer Y.

Two other questions relate to matters other than the authenticity of the message:

6 Computer Y was the agent of B

7 The message content expresses the content of the

Petitioner Apple Inc. - Exhibit 1012, p. 1878

contract (or more narrowly, the offer or the acceptance).27

Factual propositions 1-4 can be established by testimony as to how information is written to and from telecommunications channel processors, primary storage, and secondary storage. Factual proposition 5 requires testimony as to the accuracy of the telecommunications channel and characteristics of the message that associate it with computer Y. Only the last proposition (number 5) relates to signatures, because signature requirements associate the message with its source.28 The other propositions necessitate testimony as to how the basic message and database management system works. It is instructive to compare these propositions with the kinds of propositions that must be established under the business records exception to the hearsay rule when it is applied to computer information.

Those propositions may be supported with non technical evidence, presented by non programmers. A witness can lay a foundation for admission of computer records simply by testifying that the records are generated automatically and routinely in the ordinary course of business. The more inflexible the routine, and the less human intervention in the details of the computer's management of the database the better the evidence.29

The ultimate question is trustworthiness, and if the computer methods are apparently reliable, the information should be admitted unless the opponent of admissibility can raise some reasonable factual question undercutting trustworthiness.30

Contract Interpretation Issues

Assuming that the permissions header and knowbot constitute sufficient writings to permit a contract to be formed and that the signature requirement also is met, through digital signature technology or otherwise, there still are difficult contract interpretation questions. Contract interpretation questions arise not only after contractual relationships are formed, but also in connection with deciding whether there has been offer and acceptance, the prerequisites to contract formation.31 Contract interpretation always seeks to draw inferences about what the parties intended. When contract interpretation issues arise at the contract formation stage, the questions are what the offeror intended the content of the offer to be and what the offeree intended the content of the purported acceptance to be. The proposed Digital Library System envisions extremely cryptic expressions of offer and acceptance - by means of codes. The codes have no intrinsic meaning. Rather, extrinsic reference must be made to some kind of table, standard, or convention associating particular codes with the concepts they represent. Extrinsic evidence is available to resolve contract interpretation questions when the language of the contract itself is ambiguous, and perhaps at other times as well.32 The codes in the permissions header and knowbots certainly are ambiguous and become unambiguous only when extrinsic evidence is considered. So there is no problem in getting a standard or cable into evidence. The problem is whether the parties meant to assent to this standard.

In current EDI practice, this question is resolved by having parties who expect to have EDI transactions with each other to sign a paper trading partner agreement, in which the meaning of values or codes in the transaction sets is established.33 But requiring each pair of suppliers and users

Petitioner Apple Inc. - Exhibit 1012, p. 1879

of information in a digital library to have written contracts with each other in advance would defeat much of the utility of the digital library. Thus the challenge is to establish some ground rules for the meaning of permissions header and knowbot values that all participants are bound by. There are analogous situations. One is a standard credit card agreement that establishes contractual terms among credit card issuer, credit card subscriber, and merchant who accepts the credit card. The intermediary - the credit card company - unilaterally establishes contract terms to which the trading partners assent by using and accepting the credit card.34 Also, it is widely recognized that members of a private association can, through their constitution and bylaws establish contractual relationships that bind all of the members in dealing with each other.35 In the Digital Library System, similar legal arrangements can establish the standards by which electronic transactions between permissions header and knowbots will bind transferor and transferee of information.

Third Party Liability

It is not enough merely to ensure that the licensee is contractually bound. Trading partners also must ensure that the participants in funds transfers have enforceable obligations. For example, if the digital library system envisions that the information object would not be released to the purchaser without simultaneous release of a payment order, the supplier may be interested in enforcing the obligations of financial intermediaries who handle the payment order. This implicates the federal Electronic Funds Transfer Act, and Article 4A of the Uniform Commercial Code, regulating wire transfers.

Solutions

Satisfy the Business Records Exception to the Hearsay Rule

The discussion of contract formalities earlier in this paper concluded that legally enforceable contracts can be formed through electronic means and that the significant legal questions relate to reliability of proof and intent of the parties to be bound by using the electronic techniques. This section considers the reliability of proof further. Traditional evidence law permits computer records to be introduced in evidence when they satisfy the requirements of the business records exception: basically that they are made in the ordinary course of business, that they are relied on for the performance of regular business activities, and that there is no independent reason for questioning their reliability.36

The business records exception shares with the authentication concept statute of frauds and the parol evidence rule a common concern with reliability.37 The same procedural guarantees and established practices that ensure reliability for hearsay purposes also ensure reliability for the other purposes. Under the business records exception, the proponent must identify the source of a record, through testimony by one familiar with a signature on the record, or circumstantially.38 The steps in qualifying a business record under the common law, which since have been relaxed,39 were:

Proving that the record is an original entry made in the routine course of business

Proving that the entries were made upon the personal knowledge of the proponent/witness or someone reporting to him

Petitioner Apple Inc. - Exhibit 1012, p. 1880

Proving that the entries were made at or near the time of the transaction

Proving that the recorder and his informant are unavailable.40

These specific requirements are easier to understand and to adapt to electronic permissions and obligations formed in a digital library system by understanding the rationale for the business records exception. The hearsay rule excludes out of court statements because they are inherently unreliable, primarily because the maker of the statement's demeanor cannot be observed by the jury and because the maker of the statement is not subject to cross examine. On the other hand, there are some out of court statements that have other guarantees of reliability. Business records are one example. If a continuing enterprise finds the records sufficiently reliable to use them in the ordinary course of business, they should be reliable enough for a court. The criteria for the business records exception all aim at ensuring that the records really are relied upon the business to conduct its ordinary affairs.

The Manual for Multidistrict Litigation suggests steps for qualifying computer information under the business records exception:

1.The document is a business record

2.The document has probative value

3.The computer equipment used is reliable

4.Reliable data processing techniques were used41

The key in adapting the business records exception to electronic permissions in a digital library system are points 3 and 4. Establishing these propositions and the propositions set forth in section ___ of this paper requires expert testimony. Any designer of a digital library system must consult with counsel and understand what testimony an expert would give to establish these propositions. Going through that exercise will influence system design.

Reinforce the Evidentiary Reliability by Using Trusted Third Parties

The evidentiary purpose of contract formation requirements can be satisfied by using a trusted third party as an intermediary, when the third party maintains archival records of the transactions. The third party lacks any incentive for tampering with the records and when the third parties archiving system is properly designed, it can provide evidence sufficient to establish all of the propositions identified in ___.

This third party intermediary concept is somewhat different from the concept for a certifying agent in digital signature systems. To be sure, the custodian of transaction records envisioned by this section could be the same as the certifying entity for public and key encryption, but the custodian role can be played in the absence of any encryption. Indeed, the digital library itself is a good candidate for the custodian role. The library has no incentive to manipulate its records in favor of either of the producers of information value or the consumers. In order to carry out its affairs, it must use these transactional records in the ordinary course of business,

Petitioner Apple Inc. - Exhibit 1012, p. 1881

thereby making it likely that digital library records would qualify under the business records exception.

Standardization

Obviously, the digital library concept depends upon the possibility of an automated comparison between the knowbot and the permissions header. This means that potential requesters of information and suppliers of information must know in advance the data structures for representing the elements of the permissions header and the knowbot. This requires compatibility. Compatibility requires standardization. Standardization does not, however, necessarily require "Standard" in the sense that they are developed by some bureaucratic body like ANSI. It may simply imply market acceptance of a particular vendor's approach. Indeed, each digital library might use different data structures. All that is necessary is that the structure of the knowbot and the structure of the permissions header be compatible within any one digital library system. Also, as demands emerge for separate digital libraries to communicate with each other, there can be proprietary translation to assure compatibility between systems much as common word processing programs translate to and from other common formats and much as printers and word processing software communicate with each other through appropriate printer drivers. In neither of these cases has any independent standards organization developed a standard that is at all relevant in the marketplace.

Standardizing the elements of Knowbot and permissions headers involves content standardization, which generally is more challenging than format standardization.42 A permissions header/Knowbot standard is a system for representing legal concepts and for defining legal relations. As such, the standard is basically a grammar for a rule based substantive system in a very narrow domain.43 The data elements must correspond to legally meaningful relational attributes. The allowable values must correspond to legally allowable rights, obligations, privileges and powers. In other words, the standard setter must meet many of the challenges that a legal expert system designer working with Hohfeldian frameworks must meet.44 This adds a constraint to the standards setting process. Unlike setting format standards, where the participants are free to agree on an arbitrary way of expressing format attributes, participants in setting a content standard must remain within the universe of permissible content. The set of permissible values is determined by the law rather than being determined only by the imagination of format creators.

Enforcement and Bottlenecks

One of the many profound observations by Ithiel de Sola Pool was that copyright always has depended upon technological bottlenecks for its enforceability. The printing press was the original enforcement bottleneck. Now, a combination of the printing press and the practical need to inventory physical artifacts representing the work constitute the enforcement bottlenecks. As technologies change, old bottlenecks disappear and enforceability requires a search for new bottlenecks. When there are single hosts, like Westlaw, Dialog, Lexis, and Compuserve, access to that host is the bottleneck. The problem with distributed publishing on an open architecture internet is that there is no bottleneck in the middle of the distribution chain corresponding to the printer, the warehouse or the single host.

Petitioner Apple Inc. - Exhibit 1012, p. 1882

If new bottlenecks are to be found, they almost surely will be found at the origin and at the point of consumption. Encryption and decryption techniques discussed elsewhere in this volume concentrate on those bottlenecks as points of control. It also is possible that rendering software could become the new bottleneck as Mr. Linn suggests.

Even with those approaches, however, a serious problem remains in that the new technologies make it difficult or impossible to distinguish between mere use and copying. Thus the seller cannot distinguish between an end user45 and a potential competitor. On the other hand, the new technologies permit a much better audit trail, potentially producing better evidence for enforcement adjudication.

If network architectures for electronic publishing evolve in the way that Ted Nelson suggests with his Xanadu concept, the real value will be in the network and the pointers, not in the raw content. Thus, the creative and productive effort that the law should reward is the creation and productive effort that the law should reward is the creation and production and delivery of pointers, presentation, distribution, and duplication value. If this is so, then technological means will be particularly important, foreclosing access by those lacking passwords and other keys and limiting through contract what a consumer may do with the information.

In such an architecture, the law either will be relatively unimportant because technology can be counted on to prevent free riding or, the law will need to focus not on prohibiting copying or use without permission, but on preventing circumvention of the technological protections. Thus, legal approaches like that used to prevent the sale of decryption devices for television broadcasts and legal issues associated with contract enforcement may be more important than traditional intellectual property categories.

Weighing Risks and Costs

The law generally imposes sensible levels of transaction costs. Usually, transaction costs are proportional to the risk. Figure 1 shows a continuum of risk and transaction cost in traditional and new technologies. A real estate closing involves significant risks if there is some dispute later about the transaction. Therefore, the law affords much protection, including a constitutional officer called a registrar of deeds who is the custodian of records associated with the transaction. The risk level analogous to this in electronic publishing might be access to an entire library including access software as well as contents. Next, is a transaction involving a will or power of attorney. There, the risk is substantial because the maker of the instrument is not around to help interpret it. The law requires relatively high levels of assurance here, though not as great as those for real estate transactions. The law requires witnesses and attestation by a commissioned minor official called a notary public. The electronic publishing analogy of this level of risk might be the contents of an entire CDROM.

Next, in level of risk is the purchase of a large consumer durable like an automobile. The law requires somewhat less, but still significant protections for this kind of transaction: providing for the filing and enforcement of financing statements under the Uniform Commercial Code. The electronic publishing analogy might be the transfer of copyright to a complete work. Next, down

Petitioner Apple Inc. - Exhibit 1012, p. 1883

the risk continuum, is the purchase of a smaller consumer durable like a television set. Here, the law typically is reflected in written agreements of sale, but no special third party custodial mechanisms. The electronic publishing analogy might be use permission for a complete work.

Finally, is the purchase of a relatively small consumer item, say a box of diskettes. Neither the law or commercial practice involves much more than the exchange of the product for payment, with no written agreement or anything else to perform channeling, cautionary, evidentiary, or protective functions [make sure these function and the citation appears earlier]. The electronic publishing analogy might be use permission for part of a work.

Cost effectiveness = risk-proportional security

traditional transaction equivalent	institutions	electronic
real estate closing software and	registrar of deeds	entire library - contents
will/power of attorney CDROM	witnesses, notary public	contents of entire
auto purchase transfer of	UCC financing statement	complete work - copyright
television set purchase permission	written sale agreement	complete work - use
box of diskettes	-	part of a work - use permission

An encrypted object combined with rendering software is probably inconsistent with an open architecture. Because of the difficulty of setting standards for such technologies, this approach to intellectual property protection probably would be effectuated by proprietary approaches thus frustrating the vision of an open market for electronic publishing.

Conclusion

Realization of the digital library vision requires a method for collecting money and granting permission to use works protected by intellectual property. The concept of a knowbot and a permissions header attached to the work is the right way to think about such a billing and collection system. Standards for the data structures involved must be agreed to, and systems must be designed to satisfy legal formalities aimed at ensuring awareness of the legal significance of transactions and reliable proof of the terms of the transactions.

In the long run, not only must these technological issues be resolved, with appropriate attention to levels of risk and protections available under traditional legal doctrines, but also further conceptual development must be undertaken. Proponents of electronic publishing over wide area networks need to think about the appropriate metaphors: whether it is a library or a bookstore, if a library whether with or without xerox machines, if a bookstore whether it is a retail bookstore, or a mail order operation. Then,

Petitioner Apple Inc. - Exhibit 1012, p. 1884

thought must be given to how standards will be set. Finally, and most important, much more needs to be understood about the need for third party institutions. There is a good deal of enthusiasm for public key encryption. Yet the vulnerability of public key encryption systems is in the integrity of the key authority. In traditional legal protections, the third party custodians or authenticating agents like notary public and registrars of deeds receive state sanction and approval, and in the case of registrars of deeds, public funding. We must be clearer as to whether a similar infrastructure must be developed to protect against substantial risks and the use of EDI and electronic publishing technologies.

Finally, and perhaps most importantly, we must be thoughtful about what legal obligations, imposed on whom, are appropriate? The suggested 102(e) and (f) in the High Performance Computing Act looks very much like King James I's licensing of printing presses. It also looks like the FBI's proposal to prohibit the introduction of new technologies until certain conformity with past legal concepts is assured. Such approaches make the law a hurdle to new technology -- an uncomfortable position for both law and technology.

---

1 The use of EDI techniques to meter usage and determine charges for use of intellectual property is an example of billing and collection value in a typology of different types of value that can be produced in electronic marketplaces for information. See Henry H. Perritt, Jr., Market Structures for Electronic Publishing and Electronic Contracting in Brian Kahin, ed., Building Information Infrastructure: Issues in the Development of the National Research and Education Network (Harvard University and McGraw-Hill 1992) (developing typology for different types of value and explaining how market structures differ for the different types); Henry H. Perritt, Jr., Tort Liability, the First Amendment, and Equal Access to Electronic Networks, 5 Harv.J.Law & Tech. 65 (1992) (using typology of ten types of value to analyze access by competing producers of value).

2 See, e.g.U.S.Pat. No. 5,016,009, Data compression apparatus and method (May 14, 1991); U.S. Pat. No. 4,996,690, Write operator with gating capability (Feb. 26, 1991);U.S. Pat. No. 4,701,745, Data compression system (Oct. 20, 1987); Multi Tech Systems, Inc. v. Hayes Microcomputer Products, Inc., 800 F. Supp. 825 (D. Minn. 1992) (denying summary judgment on claim that patent for modem escape sequence is invalid)..

3 Comments on the 8\21 draft of "Knowbots in the Real World" from the intellectual property workshop participants at page 6 (author unknown, source unknown). Professor Samuelson also observed that the workshop, despite its title, actually did not focus much on intellectual property issues.

4 Corporation for National Research Initiatives, Workshop On The Protection Of Intellectual Property Rights In A Digital Library System: Knowbots in the Real World-May 18-19, 1989 (describing digital library system).

5 See generally Clifford A. Lynch, Visions of Electronic Libraries (libraries of future can follow acquisition-on-demand model rather than acquiring an advance of use; Z39.50 protocol will facilitate realization of that possibility, citing Robert E. Kahn & Vinton G. Serf, An Open Architecture

Petitioner Apple Inc. - Exhibit 1012, p. 1885

for a Digital Library System and a Plan for Its Development. The Digital Library Project, volume 1: The World of Knowbots (draft) (Washington D.C.: Corporation for National Research Initiatives; 1988)).

6 Clifford A. Lynch, The Z39.50 Information Retrieval Protocol: An Overview and Status Report, ACM Sigcomm Computer Communication Review at 58 (describing Z39.50 as an OSI application layer protocol that relieves clients from having to known the structure of data objects to be queried, and specifies a framework for transmitting and managing queries and results and syntax for formulating queries).

7 Brewster Kahle, Wide Area Information Server Concepts (Nov. 3, 1989 working copy; updates available from Brewster @THINK. (describing WAIS as "open protocol for connecting user interfaces on workstations and server computers") (describing information servers as including bulletin board services, shared databases, text searching and automatic indexing and computers containing current newspapers and periodicals, movie and television schedules with reviews, bulletin boards and chat lines, library catalogues, Usenet articles).

8 Robert E. Kahn, Deposit, Registration, Recordation in an Electronic Copyright Management System (August 1992) (Corporation for National Research Initiatives, Reston, Virginia).

9 Kahn 1992 at 4.

10 Kahn 1992 at 6.

11 Kahn 1992 at 10.

12 Kahn 1992 at 12.

13 Kahn 1992 at 15.

14 Browsability through techniques like the collapsible outliner function in Microsoft Word for Windows and competing products require more chunking and tagging value in the form of style and text element codes. Handling this additional formatting information through encryption and description processes is problematic.

15 " A 'transfer of copyright ownership' is an assignment, mortgage, exclusive license, or any other conveyance, alienation, or hypothecation of a copyright or of any of the exclusive rights comprised in a copyright, whether or not it is limited in time or place of effect, but not including a non-exclusive license " 17 U.S.C. 101 (1988).

16 17 U.S.C. 204(a) (1988); Valente-Kritzer Video v. Pinckney, 881 F.2d 772, 774 (9th Cir. 1989) (affirming summary judgment for author; oral agreement unenforceable under Copyright Act); Library Publications, Inc. v. Medical Economics Co., 548 F. Supp. 1231, 1233 (E.D. Pa. 1982) (granting summary judgment against trade book publisher who sought enforcement of oral exclusive distribution agreement; transfer of exclusive rights, no matter how narrow, must be in writing), aff'd mem., 714 F.2d 123 (3d Cir. 1983).

17 17 U.S.C. 205 (1988) provides constructive notice of the contents of the recorded document, determining priority as between conflicting transfers, and determines priority as between recorded transfer and non-exclusive license. The

Petitioner Apple Inc. - Exhibit 1012, p. 1886

former requirement for transfers to be recorded in order for the transferee to maintain an infringement, 17 U.S.C. 205(d), was repealed by the Berne Act Amendments 5.

18 under Adams v. Burke, 84 U.S. (17 Wall.) 453 (1873), a patentee must not attempt to exert control past the first sale. In general, use restrictions may be placed only on licensees, consistent with General Talking Pictures v. Western Elec., 304 U.S. 175 (1938). See generally Baldwin-Lima-Hamilton Corp. v. Tatnall, 169 F. Supp. 1 (E.D. Pa.1958) (applying no control after purchase rule).

19 See Red-Baron-Franklin Park, Inc. v. Taito Corp., 883 F.2d 275, 278 (4th Cir. 1989) (purchase of video game circuit boards did not create privilege to perform video game under first sale doctrine); United States v. Moore, 604 F.2d 1228, 1232 (9th Cir. 1979) (pirated sound recording not within first sale doctrine in criminal copyright infringement prosecution). But see Mirage Editions, Inc. v. Albuquerque A.R.T. Co., 856 F.2d 1341, 1344 (9th Cir. 1988) (first sale doctrine did not create privilege to prepare derivative work by transferring art in book to ceramic tiles).

20 The way in which the first sale doctrine would impact the electronically imposed use restrictions is by frustrating a breach-of-contract lawsuit by the licensor against a licensee who exceeds the use restrictions. The licensee exceeding the use restrictions would argue that it violates public policy to enforce the restrictions and therefore that state contract law may not impose liability for their violation. See generally Restatement (second) of Contracts 178 (1981) (stating general rule for determining when contract term in unenforceable on grounds of public policy).

21 In addition, as ___ of this paper notes, the Copyright Act itself requires signed writings for transfers of copyright interests. 17 U.S.C. 204(a). (1988).

22 Michael S. Baum & Henry H. Perritt, Jr., Electronic Contracting, Publishing and EDI Law ch. 6 (1991) (contract, evidence and agency issues) [hereinafter "Baum & Perritt"]. Accord, Signature Requirements Under EDGAR, Memorandum from D. Goelzer, Office of the General Counsel, SEC to Kenneth A. Fogash, Deputy Executive Director, SEC (Jan. 13, 1986) (statutory and non-statutory requirements for "signatures" may be satisfied by means other than manual writing on paper in the hand of the signatory . . . "In fact, the electronic transmission of an individual's name may legally serve as that person's signature, providing it is transmitted with the present intention to authenticate.").

23 17 U.S.C. 101 (1988). For copyright purposes, a work is created, and therefore capable of protection, when it is fixed for the first time. 17 U.S.C. 101 (1988). "[I]t makes no difference what the form, manner, or medium of fixation may be - whether it is in words, numbers, notes, sounds, pictures, or any other graphic or symbolic indicia, whether embodied in a physical object in written, printed, photographic, sculptural, punched, magnetic, or any other stable form, and whether it is capable of perception directly or by means of any machine or device 'now known or later developed.'" 1976 U.S. Code Cong. & Admin. News 5659, 5665. The legislative history further says that, "the definition of 'fixation' would exclude from the concepts purely of an evanescent or transitory nature -- reproductions such as those projected briefly on a screen

Petitioner Apple Inc. - Exhibit 1012, p. 1887

shown electronically on a television or other video display or captured momentarily in the 'memory' of a computer." 17 U.S.C. 102 note (excerpting from House Report 94-1476).

24 Or, more likely, what is on computer medium read by computer x, such as a magnetic cartridge used for archival records. Further references in the textual discussion to "what is in computer x now" should be understood to include such computer readable media.

25 Cf. Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 Nw.U.L.Rev. 956, 980 (1986) (proof that a printout accurately reflects what is in the computer is too limited a basis for authentication of computer records).

26 In some cases, the electronic transaction will be accomplished by means of a physical transfer of computer readable media. In such a case, this step in the proof would involve proving what was received physically.

27 See generally Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 NW.U.L.Rev. 956, 979 (1986) (citing as examples of authentication Ford Motor Credit Co. v. Swarens, 447 S.W.2d 53 (Ky. 1969) (authentication by establishing relationship between computer-generated monthly summary of account activity and the customer reported on); Ed Guth Realty, Inc. v. Gingold, 34 N.Y.2d 440, 315 N.E.2d 441, 358 N.Y.S.2d 367 (1974) (authentication of summary of taxpayer liability and the taxpayer)).

28 Of course, a paper document signed at the end also is probative of the fact that no alternations have been made. In this sense, a signature requirement telescopes several steps in the inquiry outlined in the text.

29 United States v. Linn, 880 F.2d 209, 216 (9th Cir. 1989) (computer printout showing time of hotel room telephone call admissible in narcotics prosecution). See also United States v. Miller, 771 F.2d 1219, 1237 (9th Cir. 1985) (computer generated toll and billing records in price-fixing prosecution based on testimony by billing supervisor although he had no technical knowledge of system which operated from another office; no need for programmer to testify; sufficient because witness testified that he was familiar with the methods by which the computer system records information).

30 See United States v. Hutson, 821 F.2d 1015, 1020 (5th Cir. 1987) (remanding embezzlement conviction, although computer records were admissible under business records exception, despite trustworthiness challenged based on fact that defendant embezzled by altering computer files; access to files offered in evidence was restricted by special code).

31 Restatement (Second) of Contracts ___ (1981).

32 Cite for when extrinsic evidence is admissible.

33 See Baum & Perritt 2.6; The Electronic Messaging Services Task Force, The Commercial Use of Electronic Data Interchange--A Report and Model Trading Partner Agreement, 45 Bus.Law. 1645 (1990); Jeffrey B. Ritter, Scope of the Uniform Commercial Code: Computer Contracting Cases and Electronic Commercial Practices, 45 Bus.Law. 2533 (1990); Note, Legal Responses to Commercial Transactions Employing

Petitioner Apple Inc. - Exhibit 1012, p. 1888

Novel Communications Media, 90 Mich.L.Rev. 1145 (1992)

34 Garber v. Harris Trust & Savings Bank, 432 N.E.2d 1309, 1311-1312 (Ill. App. 1982) ("each use of the credit card constitutes a separate contract between the parties;" citing cases).

It is not quite this simple, because both merchant and credit card customer have separate written contracts with the credit card issuer. But there is no reason that a supplier of information to a Digital Library System and all customers of that system might not have their own contracts with the Digital Library System in the same fashion.

35 Rowland v. Union Hills Country Club, 757 P.2d 105 (Ariz. 1988) (reversing summary judgment for country club officers because of factual question whether club followed bylaws in expelling members); Straub v. American Bowling Congress, 353 N.W.2d 11 (Neb. 1984) (rule of judicial deference to private associations, and compliance with association requirements, counseled affirmance of summary judgment against member of bowling league who complained his achievements were not recognized). But see Wells v. Mobile County Board of Realtors, Inc., 387 So.2d 140 (Ala. 1980) (claim of expulsion of realtor from private association was justiciable and bylaws, rules and regulations requiring arbitration were void as against public policy; reversing declaratory judgment for defendant association).

36 F.R.E. 803(6) (excluding business records from inadmissibility as hearsay); 28 U.S.C. 1732 ("Business Records Act" permitting destruction of paper copies of government information reliably recorded by any means and allowing admission of remaining reliable record).

37 See Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 NW.U.L.Rev. 956, 978-80, 984-85 (1986) (noting body of commentator opinion saying that business records exception and authentication are parallel ways of establishing reliability).

38 See F.R.E. 901(b)(4) (appearance, contents, substance, internal patterns, as examples of allowable authentication techniques).

39 Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 NW.U.L.Rev. 956, 963-64 (1986) (identifying steps and trend resulting in F.R.E.).

40 Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 NW.U.L.Rev. 956, 963 (1986).

41 Peritz, Computer Data and Reliability: A Call for Authentication of Business Records Under the Federal Rules of Evidence, 80 NW.U.L.Rev. 956, 974 (1986) (reporting four requirements of Manual, and endorsing their use generally).

42 See Henry H. Perritt, Jr., ___, ___ Jurimetrics ___ (1993) (distinguishing between format and content standardization).

43 See Marc Lauritsen, ___ (explaining relationship between substantive legal systems and the field of artificial intelligence).

Petitioner Apple Inc. - Exhibit 1012, p. 1889

44 See Thorne, McCarty; Kevin Ashley; and Gardner.

45 It may not be particularly important to limit competition by consumers, because the consumers will never have the pointers and the rest of the network infrastructure.

Petitioner Apple Inc. - Exhibit 1012, p. 1890

Amendments to the Claims:

1. (Currently amended) A digital work adapted to be distributed within a system for controlling the distribution and use of digital works, said digital work comprising:

digital content representing a portion of a digital work suitable for being rendered by a rendering device; and

usage rights associated with said digital content,

wherein said usage rights are expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use indicating one or more stated purposes for which the digital work can be used and distributed by an authorized party,

said digital work is described by a description structure comprising a plurality of description blocks,

each of said description blocks comprises address information for at least one part of said digital work,

each of said description blocks further comprises zero or more pointers to other description blocks, and

each of said description blocks further comprises a usage rights part for associating one or more of said associated usage rights.

2. (Original) The digital work as recited in claim 1, wherein said usage rights further specify status information indicating the status of the digital work.

3. (Original) The digital work as recited in claim 1, wherein said usage rights further specify a usage fee associated with exercise of the manner of use, said usage fee comprising a fee type and fee parameters.

4. (Original) The digital work as recited in claim 3 wherein said fee type is a metered use fee and said fee parameters comprise a fee unit and a time unit.

5. (Original) The digital work as recited in claim 3 wherein said fee type is a per use fee and said fee parameter comprises a fee unit.

6. (Original) The digital work as recited in claim 3 wherein said fee type is a best price fee and said fee parameters comprise an identifier to identify said best price.

7. (Original) The digital work as recited in claim 3 wherein said fee type is a scheduled fee and said fee parameters comprise time units and fee units.

8. (Original) The digital work as recited in claim 3 wherein said fee type is a mark-up fee and said fee parameters comprise a mark-up percentage.

9. (Original) The digital work as recited in claim 1 wherein said digital content and said usage rights are stored on the same physical device.

10. (Original) The digital work as recited in claim 1, wherein said digital content and said usage rights are stored on different physical devices.

11. (Currently amended) A method for creating a digital work to be used in a system for ~~reporting fees associated with~~ distribution and use of the digital work, said method comprising:

a) obtaining digital content representing a portion of a digital work suitable for being rendered by a rendering device;

b) associating usage rights with the digital content,

wherein the usage rights are expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use indicating one or more stated purposes for which the digital work can be used and distributed by an authorized party,

said digital work is described by a description structure comprising a plurality of description blocks,

each of said description blocks comprises address information for at least one part of said digital work,

each of said description blocks further comprises zero or more pointers to other description blocks, and

each of said description blocks further comprises a usage rights part for associating one or more of said associated usage rights; and

c) storing the digital content and the usage rights as the digital work.

12. (Original) A method as recited in claim 11, wherein said storing step comprises storing the digital content and the usage rights on the same physical device.

13. (Original) A method as recited in claim 11, wherein said storing step comprises storing the digital content and the usage rights on different physical devices.

14. (Original) A method as recited in claim 11, wherein said usage rights further specify a usage fee associated with exercise of the manner of use.

15. (Original) The method as recited in claim 14, wherein said usage fee comprises usage fee information including a fee type and fee parameters.

16. (Original) The method as recited in claim 15 wherein said fee type is a metered use fee and said fee parameters comprise a fee unit and a time unit.

17. (Original) The method as recited in claim 15 wherein said fee type is a per use fee and said fee parameters comprise a fee unit.

18. (Original) The method as recited in claim 15 wherein said fee type is a best price fee and said fee parameters comprise an identifier to identify the best price.

19. (Original) The method as recited in claim 15 wherein said fee type is a scheduled fee and said fee parameters comprise time units and fee units.

20. (Original) The method as recited in claim 17 wherein said fee type is a mark-up fee and said fee parameters comprise a mark-up percentage.

21. (Currently amended) A digital work adapted to be distributed within a system for controlling the distribution and use of digital works, said system having a mechanism for reporting status information relating to digital works, said digital work comprising:

digital content representing a portion of a digital work suitable for being rendered by a rendering device; and

usage rights associated with said digital content,

wherein said usage rights are expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use indicating one or more stated purposes for which the digital work can be used and distributed by an authorized party,

said usage rights also ~~including~~ include state information indicating the extent of the manner of use exercised by the authorized party,

said digital work is described by a description structure comprising a plurality of description blocks,

each of said description blocks comprises address information for at least one part of said digital work,

each of said description blocks further comprises zero or more pointers to other description blocks, and

each of said description blocks further comprises a usage rights part for associating one or more of said associated usage rights.

22. (Original) A digital work as recited in claim 21, wherein the state information comprises information indicating the number of copies of the digital work that are in use.

23. (Original) A digital work as recited in claim 21, wherein the state information comprises information indicating the number of time units for which the digital work can be used.

24. (Original) A digital work as recited in claim 21, wherein the state information comprises information indicating the revenue owner of the digital work.

25. (Original) A digital work as recited in claim 21, wherein the state information comprises information indicating the publication date of the digital work.

26. (Previously Presented) A digital work as recited in claim 21, wherein the state information comprises information indicating the history of the use and distribution of the digital work.

27. (Currently amended) A method for creating a digital work to be used in a system for reporting fees associated with distribution and use of the digital work, said method comprising:

a) obtaining digital content representing a portion of a digital work suitable for being rendered by a rendering device;

b) associating usage rights with the digital content,

wherein the usage rights are expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use indicating one or more stated purposes for which the digital work can be used and distributed by an authorized party,

said usage rights also ~~including~~ include state information indicating the extent of the manner of use exercised by the authorized party,

said digital work is described by a description structure comprising a plurality of description blocks,

each of said description blocks comprises address information for at least one part of said digital work,

each of said description blocks further comprises zero or more pointers to other description blocks, and

each of said description blocks further comprises a usage rights part for associating one or more of said associated usage rights; and

c) storing the digital content and the usage rights as the digital work.

28. (Original) A method as recited in claim 27, wherein said storing step comprises storing the digital content and the usage rights on the same physical device.

29. (Original) A method as recited in claim 27, wherein said storing step comprises storing the digital content and the usage rights on different physical devices.

30. (Original) A method as recited in claim 27, wherein the state information comprises information indicating the number of copies of the digital work that are in use.

31. (Original) A method as recited in claim 27, wherein the state information comprises information indicating the number of time units for which the digital work can be used.

32. (Original) A method as recited in claim 27, wherein the state information comprises information indicating the revenue owner of the digital work.

33. (Original) A method as recited in claim 27, wherein the state information comprises information indicating the publication date of the digital work.

34. (Previously Presented) A method as recited in claim 27, wherein the state information comprises information indicating the history of the use and distribution of the digital work.

REMARKS

Claims 1-34 are pending in the present application, with claims 1, 11, 21, and 27 amended without the introduction of new matter (see, e.g., Applicants' published patent application, FIGs. 5-14 and discussion thereof).

Referring now to the present Office Action, claims 1-3, 6, 9-14, and 21-34 were rejected under 35 U.S.C. §103 based on *Hartrick et al.* (U.S. Patent No. 5,532,920) and *Perrritt* ("Knowbots, Permissions Headers and Contract Law"); and claims 4, 5, 7, 8, and 15-20 were rejected under 35 U.S.C. §103 based on *Hartrick et al.* and *Perritt* in view of *Sprague et al.* (U.S. Patent No. 5,247,575).

The rejection of claims 1-34 is respectfully overcome because *Hartrick et al.*, *Perritt*, and *Sprague et al.*, taken alone or in combination, fail to disclose, teach or suggest all of the features recited in the amended claims. For example, independent claims 1, 11, 21, and 27, as amended, recite that:

> "said digital work is described by a description structure comprising a plurality of description blocks,
> each of said description blocks comprises address information for at least one part of said digital work,
> each of said description blocks further comprises zero or more pointers to other description blocks, and
> each of said description blocks further comprises a usage rights part for associating one or more of said associated usage rights."

By contrast, *Hartrick et al.* discloses a data processing system and method to enforce payment of royalties when copying softcopy books, wherein a publisher of a softcopy book includes royalty payment information either within the structured document text of the book or in a royalty payment information file which accompanies the book, and to read the book from the storage disk, the user applies a special softcopy book reading program. *Hartrick et al.* further discloses employing a structured document having tags for indicating royalty payment information for collecting fees for copying the softcopy books (Figs. 3A-3C, and cols. 7-8). However, *Hartrick et al.* fails to disclose, teach or suggest the claimed "description structure," as recited in independent claims 1, 11, 21, and 27, as amended.

Perritt discloses use of " ... service identifiers, header descriptors, and other forms of labeling and tagging appropriate to allow copyright owners to give different levels of permission, including outright transfer of the copyright interest, use permission, copying permission, distribution permission, display permission, and permission to prepare

Petitioner Apple Inc. - Exhibit 1012, p. 1897

derivative works [and] ... how payment authorization procedures should work in conjunction with a permissions header". However, *Perritt* fails to disclose, teach or suggest the claimed "description structure," as recited in independent claims 1, 11, 21, and 27, as amended.

Sprague et al. discloses an information distribution system that provides information to a user, when the information corresponds to criteria individually selected by the user, and then charges the user only for the selected information thus provided, wherein encrypted information packages (IP's) are provided at the user site, via high and/or low density storage media and/or by broadcast transmission. However, *Sprague et al.* fails to disclose, teach or suggest the claimed "description structure," as recited in independent claims 1, 11, 21, and 27, as amended.

Employing the claimed "description structure," as recited in independent claims 1, 11, 21, and 27, as amended, provides the following advantages, as disclosed in Applicants' published patent application, for example, as follows:

> **[0051]** Usage rights are associated with digital works. Thus, it is important to understand the structure of a digital work. The structure of a digital work, in particular composite digital works, may be naturally organized into an acyclic structure such as a hierarchy. For example, a magazine has various articles and photographs which may have been created and are owned by different persons. Each of the articles and photographs may represent a node in a hierarchical structure. Consequently, controls, i.e. usage rights, may be placed on each node by the creator. By enabling control and fee billing to be associated with each node, a creator of a work can be assured that the rights and fees are not circumvented.

By contrast, *Hartrick et al., Perritt*, and *Sprague et al.*, taken alone or in combination, fail to disclose, teach or suggest the noted features recited in independent claims 1, 11, 21, and 27, nor the advantages thereof.

Dependent claims 2-10, 12-26, and 28-34 are allowable over *Hartrick et al., Perritt*, and *Sprague et al.*, taken alone or in combination, on their on merits and for at least the reasons as argued above with respect to independent claims 1, 11, 21, and 27.

The present amendment is submitted in accordance with the provisions of 37 C.F.R. §1.116, which after Final Rejection permits entry of amendments placing the claims in better form for consideration on appeal. As the present amendment is believed to overcome outstanding rejections under 35 U.S.C. § 103, the present amendment places the application in better form for consideration on appeal. It is therefore respectfully

requested that 37 C.F.R. §1.116 be liberally construed, and that the present amendment be entered.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. If, however, the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

Respectfully submitted,
NIXON PEABODY, LLP

/Carlos R. Villamar, Reg. # 43,224/
Carlos R. Villamar
Reg. No. 43,224

NIXON PEABODY LLP
CUSTOMER NO.: 22204
401 9th Street, N.W., Suite 900
Washington, DC 20004
Tel: 202-585-8000
Fax: 202-585-8080

Petitioner Apple Inc. - Exhibit 1012, p. 1899

OIPE IAP40
FEB 14 2006
PATENT & TRADEMARK OFFICE

AF

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. **STEFIK**, *et al.*
Group Art Unit	3621
Examiner Name	James Reagan
Total Number of Pages in This Submission	**Attorney Docket Number** 111325-88 (020700)

ENCLOSURES *(check all that apply)*

- ☐ Fee Transmittal Form
  - ☐ Fee Attached
- ☒ Amendment / Reply
  - ☒ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Assignment Papers *(for an Application)*
- ☐ Drawing(s)
- ☐ Declaration and Power of Attorney
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance Communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Application Data Sheet
- ☐ Request for Corrected Filing Receipt with Enclosures
- ☐ A self-addressed prepaid postcard for acknowledging receipt
- ☐ Other Enclosure(s) (*please identify below*):

Remarks

☒ The Commissioner is hereby authorized to charge any additional fees required or credit any overpayments to Deposit Account No. 19-2380 for the above identified docket number.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm *or* Individual name	Carlos R. Villamar Registration No. 43,224 **Nixon Peabody LLP** 401 9th Street, N.W., Suite 900 Washington, D.C. 20004-2128
Signature	
Date	February 14, 2006

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

- ☐ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop _____, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450
- ☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) _____.

_____ Date

_____ Signature

_____ Typed or printed name

OIPE IAP40
FEB 14 2006
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	
Mark J. **STEFIK,** *et al.*	)	Group Art Unit: 3621
Serial No. 10/015,951	)	Examiner: James Reagan
Filed: December 17, 2001	)	Confirmation No. 5128
For: DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME	))	

U.S. Patent and Trademark Office
Customer Services Window, Mail Stop AF
Randolph Building
401 Dulany Street
Alexandria, VA 22314

AMENDMENT AFTER FINAL REJECTION

Sir:

In response to the final Office Action mailed **November 16, 2005**, please amend the above-identified patent application, as follows:

Petitioner Apple Inc. - Exhibit 1012, p. 1901

PATENT APPLICATION FEE DETERMINATION RECORD
Effective October 1, 2001

Application or Docket Number: 10.015957

CLAIMS AS FILED - PART I

	(Column 1)	(Column 2)
TOTAL CLAIMS	34	
FOR	NUMBER FILED	NUMBER EXTRA
TOTAL CHARGEABLE CLAIMS	34 minus 20=	* 14
INDEPENDENT CLAIMS	4 minus 3 =	* 1
MULTIPLE DEPENDENT CLAIM PRESENT		☐

* If the difference in column 1 is less than zero, enter "0" in column 2

SMALL ENTITY TYPE ☐		OR	OTHER THAN SMALL ENTITY	
RATE	FEE		RATE	FEE
BASIC FEE	370.00	OR	BASIC FEE	740.00
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL		OR	TOTAL	

CLAIMS AS AMENDED - PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 34	Minus	** 34	= 1
Independent	* 4	Minus	*** 4	= 1
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

SMALL ENTITY		OR	OTHER THAN SMALL ENTITY	
RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

2-14-06

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	* 34	Minus	** 34	=
Independent	* 4	Minus	*** 4	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

AMENDMENT C

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA
Total	*	Minus	**	=
Independent	*	Minus	***	=
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM				☐

RATE	ADDITIONAL FEE		RATE	ADDITIONAL FEE
X$ 9=		OR	X$18=	
X42=		OR	X84=	
+140=		OR	+280=	
TOTAL ADDIT. FEE		OR	TOTAL ADDIT. FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20."
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3."
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Best Available Copy

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,951	12/17/2001	Mark J. Stefik	111325-88	5128

22204 7590 03/03/2006

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

EXAMINER	
REAGAN, JAMES A	
ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 03/03/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Advisory Action Before the Filing of an Appeal Brief	**Application No.** 10/015,951	**Applicant(s)** STEFIK ET AL.	
	Examiner James A. Reagan	**Art Unit** 3621	

--The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

THE REPLY FILED 14 February 2006 FAILS TO PLACE THIS APPLICATION IN CONDITION FOR ALLOWANCE.

1. ☒ The reply was filed after a final rejection, but prior to or on the same day as filing a Notice of Appeal. To avoid abandonment of this application, applicant must timely file one of the following replies: (1) an amendment, affidavit, or other evidence, which places the application in condition for allowance; (2) a Notice of Appeal (with appeal fee) in compliance with 37 CFR 41.31; or (3) a Request for Continued Examination (RCE) in compliance with 37 CFR 1.114. The reply must be filed within one of the following time periods:
   a) ☒ The period for reply expires 3 months from the mailing date of the final rejection.
   b) ☐ The period for reply expires on: (1) the mailing date of this Advisory Action, or (2) the date set forth in the final rejection, whichever is later. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of the final rejection.

   Examiner Note: If box 1 is checked, check either box (a) or (b). ONLY CHECK BOX (b) WHEN THE FIRST REPLY WAS FILED WITHIN TWO MONTHS OF THE FINAL REJECTION. See MPEP 706.07(f).

Extensions of time may be obtained under 37 CFR 1.136(a). The date on which the petition under 37 CFR 1.136(a) and the appropriate extension fee have been filed is the date for purposes of determining the period of extension and the corresponding amount of the fee. The appropriate extension fee under 37 CFR 1.17(a) is calculated from: (1) the expiration date of the shortened statutory period for reply originally set in the final Office action; or (2) as set forth in (b) above, if checked. Any reply received by the Office later than three months after the mailing date of the final rejection, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

NOTICE OF APPEAL

2. ☐ The Notice of Appeal was filed on _____. A brief in compliance with 37 CFR 41.37 must be filed within two months of the date of filing the Notice of Appeal (37 CFR 41.37(a)), or any extension thereof (37 CFR 41.37(e)), to avoid dismissal of the appeal. Since a Notice of Appeal has been filed, any reply must be filed within the time period set forth in 37 CFR 41.37(a).

AMENDMENTS

3. ☒ The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because
   (a) ☒ They raise new issues that would require further consideration and/or search (see NOTE below);
   (b) ☐ They raise the issue of new matter (see NOTE below);
   (c) ☐ They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal; and/or
   (d) ☐ They present additional claims without canceling a corresponding number of finally rejected claims.

   NOTE: *See Continuation Sheet*. (See 37 CFR 1.116 and 41.33(a)).
4. ☐ The amendments are not in compliance with 37 CFR 1.121. See attached Notice of Non-Compliant Amendment (PTOL-324).
5. ☐ Applicant's reply has overcome the following rejection(s): _____.
6. ☐ Newly proposed or amended claim(s) _____ would be allowable if submitted in a separate, timely filed amendment canceling the non-allowable claim(s).
7. ☒ For purposes of appeal, the proposed amendment(s): a) ☒ will not be entered, or b) ☐ will be entered and an explanation of how the new or amended claims would be rejected is provided below or appended.
   The status of the claim(s) is (or will be) as follows:
   Claim(s) allowed: _____.
   Claim(s) objected to: _____.
   Claim(s) rejected: *1-34*.
   Claim(s) withdrawn from consideration: _____.

AFFIDAVIT OR OTHER EVIDENCE

8. ☐ The affidavit or other evidence filed after a final action, but before or on the date of filing a Notice of Appeal will not be entered because applicant failed to provide a showing of good and sufficient reasons why the affidavit or other evidence is necessary and was not earlier presented. See 37 CFR 1.116(e).
9. ☐ The affidavit or other evidence filed after the date of filing a Notice of Appeal, but prior to the date of filing a brief, will not be entered because the affidavit or other evidence failed to overcome all rejections under appeal and/or appellant fails to provide a showing a good and sufficient reasons why it is necessary and was not earlier presented. See 37 CFR 41.33(d)(1).
10. ☐ The affidavit or other evidence is entered. An explanation of the status of the claims after entry is below or attached.

REQUEST FOR RECONSIDERATION/OTHER

11. ☐ The request for reconsideration has been considered but does NOT place the application in condition for allowance because: _____.
12. ☐ Note the attached Information Disclosure Statement(s). (PTO/SB/08 or PTO-1449) Paper No(s). _____
13. ☐ Other: _____.

Continuation of 3. NOTE: The addition of limitations to various claims may have altered the scope of the claims and therefore will require additional research and/or consideration to better ascertain the condition of the pending application.

OIPE IAP34
MAR 10 2006
PATENT & TRADEMARK OFFICE

RCE 2nd 5

REQUEST FOR CONTINUED EXAMINATION (RCE) TRANSMITTAL

Subsection (b) of 35 U.S.C. § 132, effective on May 29, 2000, provides for continued examination of an utility or plant application filed on or after June 8, 1995. See The American Inventors Protection Act of 1999 (AIPA).

Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. **STEFIK**, *et al.*
Group Art Unit	3621
Examiner Name	James A. Reagan
Attorney Docket Number	111325-88 (020700)

This is a Request for Continued Examination (RCE) under 37 C.F.R. § 1.114 of the above-identified application.

NOTE: 37 C.F.R. § 1.114 is effective on May 29, 2000. If the above-identified application was filed prior to May 29, 2000, applicant may wish to consider filing a continued prosecution application (CPA) under 37 C.F.R. § 1.53(d) (PTO/SB/29) instead of a RCE to be eligible for the patent term adjustment provisions of the AIPA. See Changes to Application Examination and Provisional Application Practice, Final Rule, 65 Fed. Reg. 50092 (Aug. 16, 2000); Interim Rule, 65 Fed. Reg. 14865 (Mar. 20, 2000), 1233 Off. Gaz. Pat. Office 47 (Apr. 11, 2000), which established RCE practice.

1. Submission required under 37 C.F.R. § 1.114
   - a. ☒ Previously submitted
     - i. ☒ Consider the amendment(s)/reply under 37 C.F.R. § 1.116 previously filed on **February 14, 2006.** (Any unentered amendment(s) referred to above will be entered).
     - ii. ☐ Consider the arguments in the Appeal Brief or Reply Brief previously filed on _____
     - iii. ☐ Other:_____.
   - b. ☒ Enclosed
     - i. ☐ Amendment/Reply
     - ii. ☐ Affidavit(s)/Declaration(s)
     - iii. ☐ Information Disclosure Statement (IDS)
     - iv. ☐ Submission of Formal Drawings
     - v. ☒ Petition for One-month Extension of Time
     - vi. ☐ Other:
2. Miscellaneous
   - a. ☐ Suspension of action on the above-identified application is requested under 37 C.F.R. § 1.103(c) for a period of _____ months. (Period of suspension shall not exceed 3 months; Fee under 37 C.F.R. § 1.17(I) required)
   - b. ☐ Other _____
3. Fees — The RCE fee under 37 C.F.R. § 1.17(e) is required by 37 C.F.R. § 1.114 when the RCE is filed.
   - a. ☒ The Director is hereby authorized to charge the following fees, additional fees which may be required, or credit any overpayments, to Deposit Account No. 19-2380
     - i. ☒ RCE fee required under 37 C.F.R. § 1.17(e)
     - ii. ☒ Extension of time fee (37 C.F.R. §§ 1.136 and 1.17)
     - iii. ☐ Other _____
   - b. ☐ Check in the amount of $_____ enclosed
   - c. ☐ Payment by credit card (Form PTO-2038 enclosed)

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT REQUIRED

Name *(Print/Type)*	Carlos R. Villamar	Registration No. *(Attorney/Agent)*	43,224
Signature		Date	March 10, 2006

CERTIFICATE OF MAILING OR TRANSMISSION
[37 CFR 1.8(a)]

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to: Mail Stop RCE, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, or being facsimile transmitted to the USPTO at _____, on _____.

Signature:	
Name:	

03/13/2006 JADD01 00000051 192380 10015951
02 FC:1801 790.00 DA

SEND TO: Mail Stop RCE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

W709446.1

OIPE
MAR 10 2006
PATENT & TRADEMARK OFFICE

PETITION FOR EXTENSION OF TIME UNDER 37 CFR 1.136(a)	Docket Number (Optional) 111325-88 (020700)

CERTIFICATE OF MAILING OR TRANSMISSION
[37 CFR 1.8(a)]

I hereby certify that this correspondence is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to Mail Stop _____, Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450, or being facsimile transmitted to the USPTO at _____, on _____.

Signature: _____

Name: _____

In re Application of
Mark J. **STEFIK** *et al.*

Application Number: 10/015,951 | Filed: December 17, 2001

For: **DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME**

Group Art Unit: 3621 | Examiner: James A. Reagan

This is a request under the provisions of 37 CFR 1.136(a) to extend the period for filing a reply in the above identified application.

The requested extension and appropriate entity fee are as follows (check time period desired):

- ☒ One month (37 CFR 1.17(a)(1)) - ($60/$120) $ 120.00
- ☐ Two months (37 CFR 1.17(a)(2)) - ($225/$450) $ _____
- ☐ Three months (37 CFR 1.17(a)(3)) - ($510/$1020) $ _____
- ☐ Four months (37 CFR 1.17(a)(4)) - ($795/$1590) $ _____
- ☐ Five months (37 CFR 1.17(a)(5)) - ($1080/$2160) $ _____

☐ Applicant claims small entity status.

☐ A check to cover the fee is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Commissioner has already been authorized to charge fees in this application to a Deposit Account.

☒ The Commissioner is hereby authorized to charge any fees which may be required, or credit any overpayment, to Deposit Account Number 19-2380.
I have enclosed a duplicate copy of this sheet.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

I am the ☐ applicant/inventor

☐ assignee of record of the entire interest. See 37 CFR 3.71.
Statement under 37 CFR 3.73(b) is enclosed. (Form PTO/SB/96).

☐ attorney or agent of record.

☒ attorney or agent under 37 CFR 1.34(a).
Registration number if acting under 37 CFR 1.34(a) **43,224**.

_____
Signature

March 10, 2006
Date

Carlos R. Villamar
Typed or printed name

(202) 585-8204
Telephone Number

03/13/2006 [illegible] 00000051 192380 10015951
01 FC:1251 120.00 DA

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below.

☐ Total of _____ forms are submitted.

SEND TO: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

W709458.1

FEE TRANSMITTAL FOR FY 2005

Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT | **$910.00**

MAR 10 2006 PATENT & TRADEMARK OFFICE

Complete if Known	
Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. STEFIK, *et al.*
Examiner Name	James A. Reagan
Art Unit	3621
Attorney Docket No.	111325-88 (020700)

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit Card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 19-2380

Deposit Account Name: Nixon Peabody LLP

The Commissioner is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	300	2001	150	Utility filing fee	
1002	200	2002	100	Design filing fee	
1003	200	2003	100	Plant filing fee	
1004	300	2004	150	Reissue filing fee	
1005	200	2005	100	Provisional filing fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

		Extra Claims		Fee from below		Fee Paid
Total Claims	-20** =		X		=	0
Independent Claims	-3** =		X		=	0
Multiple Dependent			X		=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	50	2202	25	Claims in excess of 20
1201	200	2201	100	Independent claims in excess of 3
1203	360	2203	180	Multiple dependent claim, if not paid
1204	200	2204	100	** Reissue independent claims over original patent
1205	50	2205	25	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	
1051	130	2051	65	Surcharge – late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	120	2251	60	Extension for reply within first month	120.00
1252	450	2252	225	Extension for reply within second month	
1253	1,020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1,080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	
1403	1,000	2403	500	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	500	2452	250	Petition to revive – unavoidable	
1453	1,500	2453	750	Petition to revive – unintentional	
1501	1,400	2501	700	Utility issue fee (or reissue)	
1502	800	2502	400	Design issue fee	
1503	1,100	2503	550	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	790	2809	395	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	790.00
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid **SUBTOTAL (3)** $910.00

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

☐ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop _____, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450

☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) _____.

Date _____ Signature _____

Typed or printed name _____

SUBMITTED BY				Complete *(if applicable)*	
Name *(Print/Type)*	Carlos R. Villamar	Registration No. *(Attorney/Agent)*	43,224	Telephone	(202) 585-8204
Signature				Date	March 10, 2006

SEND TO: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

W709448.1

Notice of References Cited	Application/Control No. 10/015,951	Applicant(s)/Patent Under Reexamination STEFIK ET AL.	
	Examiner James A. Reagan	Art Unit 3621	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,708,157 B2	03-2004	Stefik et al.	705/59
	B	US-			
	C	US-			
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,951	12/17/2001	Mark J. Stefik	111325-88	5128

22204 7590 05/24/2006

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

EXAMINER	
REAGAN, JAMES A	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 05/24/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/015,951	STEFIK ET AL.	
	Examiner	Art Unit	
	James A. Reagan	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 March 2006*.

2a)☒ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. This action is in response to the amendment filed on 14 February 2006 and subsequent RCE filed on 10 March 2006.
2. Claims 1, 11, 21, and 27 have been amended.
3. Claims 1-34 are pending in the present application and have been examined.

RESPONSE TO ARGUMENTS

4. Applicant's arguments received on 14 February 2006 have been fully considered but they are not persuasive. Referring to the previous Office action, Examiner has cited relevant portions of the references as a means to illustrate the systems as taught by the prior art. As a means of providing further clarification as to what is taught by the references used in the first Office action, Examiner has expanded the teachings for comprehensibility while maintaining the same grounds of rejection of the claims, except as noted above in the section labeled "Status of Claims." This information is intended to assist in illuminating the teachings of the references while providing evidence that establishes further support for the rejections of the claims. Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

Double Patenting

5. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection

is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

6. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

7. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

8. Claims 1-34 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-23 of U.S. Patent No. 6,708,157 B2. Although the conflicting claims are not identical, they are not patentably distinct from each other because US 6,708,157 B2 to Stefik et al. does not disclose:

- *said digital work is described by a description structure comprising a plurality of description blocks;*
- *each of said description blocks comprises address information for at least one part of said digital work;*

- *each of said description blocks further comprises zero or more pointers to other description blocks; and*
- each of said description blocks further comprises a usage rights part for associating one or more of said associated usages rights;

Although US 6,708,157 B2 does disclose a system for controlling the distribution and use of digital works comprising a means for associating one or more usage rights with a digital work, said one or more usage rights specifying a manner of use indicating a particular manner of how said digital work may be used and at least one condition that must be satisfied in order to exercise the manner of use, US 6,708,157 B2 does not disclose the descriptor block limitations as shown above. Utilization of said descriptor block as claimed is an obvious modification because processing languages routinely use pointers to store addresses and to associate data stored in memory. In this case, each digital work is associated with a usage right description block by using pointers in memory.

Claim Rejections - 35 USC § 101

9. Claims 1-10 and 21-26 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. Computer programs claimed as computer listings per se, i.e., the descriptions or expressions of the programs, are not physical "things." They are neither computer components nor statutory processes, as they are not "acts" being performed. Such claimed computer programs do not define any structural and functional interrelationships between the computer program and other claimed elements of a computer, which permit the computer program's functionality to be realized. In contrast, a claimed computer-readable medium encoded with a computer program is a computer element which defines structural and functional interrelationships between the computer program and the rest of the computer which permit the computer program's functionality to be realized, and is thus statutory. Accordingly, it is

important to distinguish claims that define descriptive material per se from claims that define statutory inventions. Since a computer program is merely a set of instructions capable of being executed by a computer, the computer program itself is not a process and the Examiner therefore will treat a claim for a computer program, without the computer-readable medium needed to realize the computer program's functionality, as nonstatutory functional descriptive material.

NON-FUNCTIONAL DATA

10. Since the application currently before the Examiner is a utility patent, the claims must be directed to systems, methods, or articles of manufacture that have a clear utility. See MPEP 706.03(a). Over the years, numerous court decisions have analyzed the content of various claim language for meaningful, useful differences in structure or acts performed between the claims and the prior art. Some of these decisions have found that certain language adds little, if anything, to the claimed structure or acts and therefore do not serve as a limitation on the claims to distinguish over the prior art. Thus, the limitations on the claim can broadly be thought of then as its ability to make a meaningful contribution to the definition of the invention in a claim. In other words, language that is not functionally interrelated with the useful acts, structure, or properties of the claimed invention will not serve as a limitation. See *In re Gulack*, 217 USPQ 401 (CAFC 1983), *Ex parte Carver*, 227 USPQ 465 (BPAI 1985) and *In re Lowry*, 32 USPQ2d 1031 (CAFC 1994), where language provided certain limitations because of specific relationships required by the claims. In the computer arts we frequently examine claims that are directed to systems, methods, and articles (computer program products) that process data. In these specific cases, nonfunctional descriptive material is material that cannot exhibit any functional interrelationship with the way in which computing processes are performed.

As a result, when analyzing claim language for its limited effect, the Examiner will perform two basic steps:

i) Review the claimed as a whole to see whether or not any descriptive material is being recited; and

ii) If a descriptive material is found, determine how this descriptive material is being used in the claim as a whole.

In this case, the claim language contains nonfunctional data in the form of. This nonfunctional data is not processed by the computer, nor does it alter the process steps. It only means something to the human mind.

Although US 6,708,157 B2 does disclose a system for controlling the distribution and use of digital works comprising a means for associating one or more usage rights with a digital work, said one or more usage rights specifying a manner of use indicating a particular manner of how said digital work may be used and at least one condition that must be satisfied in order to exercise the manner of use, US 6,708,157 B2 does not disclose the descriptor block limitations and zero or more pointers as shown above. However, these differences are only found in the nonfunctional descriptive material and are not functionally involved in the steps recited. Therefore, it would have been obvious to one of ordinary skill in the art at the time of the invention to utilize processing languages and pointers for storing addresses and associating data stored in memory. In this case, each digital work is associated with a usage right description block by using pointers in memory.

Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **James A. Reagan** whose telephone number is **571.272.6710.** The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **James Trammell** can be reached at **571.272.6712**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to:

571-273-8300 [Official communications, After Final communications labeled "Box AF"]

571-273-8300 [Informal/Draft communications, labeled "PROPOSED" or "DRAFT"]

Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window**:

Randolph Building

401 Dulany Street

Alexandria, VA 22314.

JAMES A. REAGAN

Primary Examiner

Art Unit 3621

18 May 2006

JAMES A. REAGAN
PRIMARY EXAMINER

OIPE IAP40
FEB 14 2006
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	
Mark J. **STEFIK**, *et al.*	)	Group Art Unit: 3621
Serial No. 10/015,951	)	Examiner: James Reagan
Filed: December 17, 2001	)	Confirmation No. 5128
For: DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME	)	

U.S. Patent and Trademark Office
Customer Services Window, Mail Stop AF
Randolph Building
401 Dulany Street
Alexandria, VA 22314

ENTER
9AM2
18 MAY 06

AMENDMENT AFTER FINAL REJECTION

Sir:

In response to the final Office Action mailed **November 16, 2005**, please amend the above-identified patent application, as follows:

Petitioner Apple Inc. - Exhibit 1012, p. 1918

Amendments to the Claims:

1. (Currently amended) A computer readable medium having embedded thereon a digital work adapted to be distributed within a system for controlling ~~the distribution and~~ use of digital works, said digital work comprising:

a digital content ~~representing a~~ portion ~~of a digital work suitable for being rendered~~ that is renderable by a rendering device; ~~and~~

a usage rights portion associated with said digital content portion and comprising one or more computer readable instructions configured to permit or prohibit said rendering device to render said digital content portion, ~~wherein~~ said usage rights ~~are~~ portion being expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use ~~indicating~~ relating to one or more ~~stated~~ purposes for which the digital work can be used ~~and distributed~~ by an authorized party[[,]]; and

~~said digital work is described by~~ a description structure comprising a plurality of description blocks, each of said description blocks ~~comprises~~ comprising address information for at least one part of said digital work, ~~each of said description blocks further comprises~~ zero or more pointers to other description blocks, and ~~each of said description blocks further comprises~~ a usage rights part for associating one or more ~~of said associated~~ usage rights portions.

2. (Currently amended) The digital work as recited in claim 1, wherein said usage rights portion further ~~specify~~ specifies status information indicating the status of the digital work.

3. (Currently amended) The digital work as recited in claim 1, wherein said usage rights portion further ~~specify~~ specifies a usage fee associated with exercise of the manner of use, said usage fee comprising a fee type and fee parameters.

4. (Original) The digital work as recited in claim 3 wherein said fee type is a metered use fee and said fee parameters comprise a fee unit and a time unit.

5. (Original) The digital work as recited in claim 3 wherein said fee type is a per use fee and said fee parameter comprises a fee unit.

6. (Original) The digital work as recited in claim 3 wherein said fee type is a best price fee and said fee parameters comprise an identifier to identify said best price.

7. (Original) The digital work as recited in claim 3 wherein said fee type is a scheduled fee and said fee parameters comprise time units and fee units.

8. (Original) The digital work as recited in claim 3 wherein said fee type is a mark-up fee and said fee parameters comprise a mark-up percentage.

9. (Currently amended) The digital work as recited in claim 1 wherein said digital content portion and said usage rights portion are stored on the same physical device.

10. (Currently amended) The digital work as recited in claim 1, wherein said digital content portion and said usage rights portion are stored on different physical devices.

11. (Currently amended) A method for creating a digital work to be used in a system for ~~distribution and~~ use of the digital work, said method comprising:

[[a)]] obtaining a digital content ~~representing a~~ portion ~~of a digital work suitable for being rendered~~ that is renderable by a rendering device;

[[b)]] associating a usage rights portion with the digital content portion, ~~wherein~~ the usage rights portion comprising one or more computer readable instructions configured to permit or prohibit said rendering device to render said digital content portion, said usage rights ~~are~~ portion being expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use ~~indicating~~ relating to one or more ~~stated~~ purposes for which the digital work can be used ~~and distributed~~ by an authorized party[[,]];

describing said digital work ~~is described~~ by a description structure comprising a plurality of description blocks, each of said description blocks ~~comprises~~ comprising address information for at least one part of said digital work, ~~each of said description blocks further comprises~~ zero or more pointers to other description blocks, and ~~each of~~

~~said description blocks further comprises~~ a usage rights part for associating one or more ~~of said associated~~ usage rights portions; and

[[c)]] ~~storing~~ combining the digital content portion and the usage rights portion to create [[as]] the digital work.

12. (Currently amended) A method as recited in claim 11, wherein said ~~storing~~ combining step comprises storing the digital content portion and the usage rights portion on the same physical device.

13. (Currently amended) A method as recited in claim 11, wherein said ~~storing~~ combining step comprises storing the digital content portion and the usage rights portion on different physical devices.

14. (Currently amended) A method as recited in claim 11, wherein said usage rights portion further ~~specify~~ specifies a usage fee associated with exercise of the manner of use.

15. (Original) The method as recited in claim 14, wherein said usage fee comprises usage fee information including a fee type and fee parameters.

16. (Original) The method as recited in claim 15 wherein said fee type is a metered use fee and said fee parameters comprise a fee unit and a time unit.

17. (Original) The method as recited in claim 15 wherein said fee type is a per use fee and said fee parameters comprise a fee unit.

18. (Original) The method as recited in claim 15 wherein said fee type is a best price fee and said fee parameters comprise an identifier to identify the best price.

19. (Original) The method as recited in claim 15 wherein said fee type is a scheduled fee and said fee parameters comprise time units and fee units.

20. (Original) The method as recited in claim 17 wherein said fee type is a mark-up fee and said fee parameters comprise a mark-up percentage.

21. (Currently amended) A computer readable medium having embedded thereon a digital work adapted to be distributed within a system for controlling ~~the distribution and~~ use of digital works~~, said system having a mechanism for reporting status information relating to digital works~~, said digital work comprising:

a digital content ~~representing a~~ portion ~~of a digital work suitable for being rendered~~ that is renderable by a rendering device;~~ and~~

a usage rights portion associated with said digital content portion and comprising one or more computer readable instructions configured to permit or prohibit said rendering device to render said digital content portion, ~~wherein~~ said usage rights ~~are~~ portion being expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying ~~a manner of use indicating~~ conditions relating to one or more ~~stated~~ purposes for which the digital work can be used ~~and distributed~~ by an authorized party~~, said usage rights also include state information indicating the extent of the manner of use exercised by the authorized party,~~; and

~~said digital work is described by~~ a description structure comprising a plurality of description blocks, each of said description blocks ~~comprises~~ comprising address information for at least one part of said digital work, ~~each of said description blocks further comprises~~ zero or more pointers to other description blocks, and ~~each of said description blocks further comprises~~ a usage rights part for associating one or more ~~of said associated~~ usage rights portions.

22. (Currently amended) A digital work as recited in claim 21, wherein the ~~state information comprises information indicating~~ conditions relate to the number of copies of the digital work that are in use.

23. (Currently amended) A digital work as recited in claim 21, wherein the ~~state information comprises information indicating~~ conditions relate to the number of time units for which the digital work can be used.

24. (Currently amended) A digital work as recited in claim 21, wherein the ~~state information comprises information indicating~~ conditions relate to the revenue owner of the digital work.

25. (Currently amended) A digital work as recited in claim 21, wherein the ~~state information comprises information indicating~~ conditions relate to the publication date of the digital work.

26. (Currently amended) A digital work as recited in claim 21, wherein the ~~state information comprises information indicating~~ conditions relate to the history of the use and distribution of the digital work.

27. (Currently amended) A method for creating a digital work to be used in a system for ~~reporting fees associated with distribution and~~ controlling use of the digital work, said method comprising:

[[a)]] obtaining a digital content ~~representing a~~ portion ~~of a digital work suitable for being rendered~~ that is renderable by a rendering device;

[[b)]] associating a usage rights portion with the digital content portion, ~~wherein~~ the usage rights portion comprising one or more computer readable instructions configured to permit or prohibit said rendering device to render said digital content portion, the usage rights ~~are~~ portion being expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying ~~a manner of use indicating~~ conditions relating to one or more ~~stated~~ purposes for which the digital work can be used ~~and distributed~~ by an authorized party~~, said usage rights also include state information indicating the extent of the manner of use exercised by the authorized party~~[[,]];

describing said digital work ~~is described~~ by a description structure comprising a plurality of description blocks, each of said description blocks ~~comprises~~ comprising address information for at least one part of said digital work, ~~each of said description blocks further comprises~~ zero or more pointers to other description blocks, and ~~each of said description blocks further comprises~~ a usage rights part for associating one or more ~~of said associated~~ usage rights portions; and

[[c)]] ~~storing~~ combining the digital content portion and the usage rights portion to create [[as]] the digital work.

28. (Currently amended) A method as recited in claim 27, wherein said ~~storing~~ combining step comprises storing the digital content portion and the usage rights portion on the same physical device.

29. (Currently amended) A method as recited in claim 27, wherein said ~~storing~~ combining step comprises storing the digital content portion and the usage rights portion on different physical devices.

30. (Currently amended) A method as recited in claim 27, wherein the ~~state information comprises information indicating~~ conditions relate to the number of copies of the digital work that are in use.

31. (Currently amended) A method as recited in claim 27, wherein the ~~state information comprises information indicating~~ conditions relate to the number of time units for which the digital work can be used.

32. (Currently amended) A method as recited in claim 27, wherein the ~~state information comprises information indicating~~ conditions relate to the revenue owner of the digital work.

33. (Currently amended) A method as recited in claim 27, wherein the ~~state information comprises information indicating~~ conditions relate to the publication date of the digital work.

34. (Currently amended) A method as recited in claim 27, wherein the ~~state information comprises information indicating~~ conditions relate to the history of the use and distribution of the digital work.

REMARKS

Claims 1-34 are pending in the present application, with claims 1-3, 9-14, and 21-34 amended without the introduction of new matter (see, e.g., Applicants' published patent application, FIGs. 5-14 and discussion thereof).

Referring now to the present Office Action, claims 1-34 were rejected based on obviousness type double patenting over USP 6,708,157, and claims 1-10 and 21-26 were rejected as under 35 U.S.C. §101 based on non-statutory subject matter.

In response to the double patenting rejection, Applicants will submit a Terminal Disclaimer over USP 6,708,157, if still needed in view of the present claim amendments and after the case is otherwise in condition for allowance.

In response to the 35 U.S.C. §101 rejection, Applicants have amended claims 1-3, 9-14, and 21-34 to correct the noted and discovered informalities. No new matter is introduced. Accordingly, all of the pending claims are in compliance with 35 U.S.C. § 101 and no further rejections on such basis is anticipated. If, however, the Examiner disagrees, the Examiner is invited to contact the undersigned attorney, who will be happy to work with the Examiner in a joint effort to derive a mutually satisfactory claim language.

Dependent claims 2-10, 12-26, and 28-34 are allowable for at least the reasons as argued above.

In view of the foregoing, it is submitted that the present application is in condition for allowance and a notice to that effect is respectfully requested. If, however, the Examiner deems that any issue remains after considering this response, the Examiner is invited to contact the undersigned attorney to expedite the prosecution and engage in a joint effort to work out a mutually satisfactory solution.

Respectfully submitted,
NIXON PEABODY, LLP

/Carlos R. Villamar, Reg. # 43,224/
Carlos R. Villamar
Reg. No. 43,224

NIXON PEABODY LLP

CUSTOMER NO.: 22204

401 9th Street, N.W., Suite 900

Washington, DC 20004

Tel: 202-585-8000

Fax: 202-585-8080

Electronic Acknowledgement Receipt

EFS ID:	1130694
Application Number:	10015951
Confirmation Number:	5128
Title of Invention:	Digital works having usage rights and method for creating the same
First Named Inventor:	Mark J. Stefik
Customer Number:	22204
Filer:	Carlos Rafael Villamar/Kisha Avery
Filer Authorized By:	Carlos Rafael Villamar
Attorney Docket Number:	111325-88
Receipt Date:	27-JUL-2006
Filing Date:	17-DEC-2001
Time Stamp:	17:08:43
Application Type:	Utility
International Application Number:	

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part	Pages
1	Amendment - After Non-Final Rejection	111325-020700_US_response_to_NFOA_24_MAY_06.pdf	46393	no	9

Warnings:	
Information:	
Total Files Size (in bytes):	46393

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	
Mark J. **STEFIK,** *et al.*	)	Group Art Unit: 3621
Serial No. 10/015,951	)	Examiner: James A. Reagan
Filed: December 17, 2001	)	Confirmation No. 5128
For: DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME	)	

U.S. Patent and Trademark Office
Customer Window, Mail Stop Non-Fee Amendment
Randolph Building
401 Dulany Street
Alexandria, VA 22314

AMENDMENT

Sir:

In response to the non-final Office Action mailed **May 25, 2005**, please amend the above-identified patent application, as follows:

PTO/SB/06 (12-04)
Approved for use through 7/31/2006. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD

Substitute for Form PTO-875

Application or Docket Number: 10/015,951

APPLICATION AS FILED – PART I

FOR	(Column 1) NUMBER FILED	(Column 2) NUMBER EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY FEE ($)
BASIC FEE (37 CFR 1.16(a), (b), or (c))							
SEARCH FEE (37 CFR 1.16(k), (l), or (m))							
EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))							
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X =		OR	X =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X =			X =	
APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
			TOTAL			TOTAL	

* If the difference in column 1 is less than zero, enter "0" in column 2.

APPLICATION AS AMENDED – PART II

AMENDMENT A

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	SMALL ENTITY RATE ($)	SMALL ENTITY ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	OTHER THAN SMALL ENTITY ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	* 34	Minus	** 34	=	X =		OR	X =	
Independent (37 CFR 1.16(h))	* 4	Minus	*** 4	=	X =		OR	X =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

AMENDMENT B

	(Column 1) CLAIMS REMAINING AFTER AMENDMENT		(Column 2) HIGHEST NUMBER PREVIOUSLY PAID FOR	(Column 3) PRESENT EXTRA	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
Total (37 CFR 1.16(i))	*	Minus	**	=	X =		OR	X =	
Independent (37 CFR 1.16(h))	*	Minus	***	=	X =		OR	X =	
Application Size Fee (37 CFR 1.16(s))									
FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
					TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

OIPE IAP48
SEP 12 2006
PATENT & TRADEMARK OFFICE

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76) AND POWER OF ATTORNEY

Attorney Docket No. 111325-020700 (088)

Title of Invention	**DIGITAL WORKS HAVING USAGE RIGHT AND METHOD FOR CREATING THE SAME**

As the below named inventor(s), I/we declare that:

This declaration is directed to:

- ☐ The attached application, or
- ☒ Application No. 10/015,951 filed on December 17, 2001
  - ☐ as amended on _____ (if applicable);

I/We believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;

I/We have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;

I/We acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

All statements made herein of my/own knowledge are true, all statements made herein on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon.

I/We hereby appoint:

Practitioners at Customer Number 22204 as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

FULL NAME OF INVENTOR(S)

Inventor one: Mark J. **STEFIK**

Signature: Mark Stefik Citizen of: UNITED STATES

Inventor two: Peter L. **PIROLLI**

Signature: Peter Pirolli Citizen of: CANADIAN

Inventor three: Ralph C. **MERKLE**

Signature: _____ Citizen of: UNITED STATES

☒ Additional inventors are being named on the additional form(s) attached hereto.

OIPE IAP SEP 12 2006 PATENT & TRADEMARK OFFICE

DECLARATION (37 CFR 1.63) FOR UTILITY OR DESIGN APPLICATION USING AN APPLICATION DATA SHEET (37 CFR 1.76) AND POWER OF ATTORNEY

Attorney Docket No. 111325-020700 (088)

Title of Invention	**DIGITAL WORKS HAVING USAGE RIGHT AND METHOD FOR CREATING THE SAME**

As the below named inventor(s), I/we declare that:

This declaration is directed to:

- ☐ The attached application, or
- ☒ Application No. 10/015,951 filed on December 17, 2001
  - ☐ as amended on _____ (if applicable);

I/We believe that I/we am/are the original and first inventor(s) of the subject matter which is claimed and for which a patent is sought;

I/We have reviewed and understand the contents of the above-identified application, including the claims, as amended by any amendment specifically referred to above;

I/We acknowledge the duty to disclose to the United States Patent and Trademark Office all information known to me/us to be material to patentability as defined in 37 CFR 1.56, including for continuation-in-part applications, material information which became available between the filing date of the prior application and the national or PCT International filing date of the continuation-in-part application.

All statements made herein of my/own knowledge are true, all statements made herein on information and belief are believed to be true, and further that these statements were made with the knowledge that willful false statements and the like are punishable by fine or imprisonment, or both, under 18 U.S.C. 1001, and may jeopardize the validity of the application or any patent issuing thereon.

I/We hereby appoint:

Practitioners at Customer Number 22204 as my/our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

FULL NAME OF INVENTOR(S)

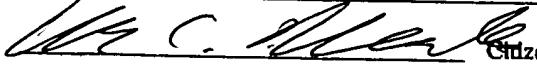
Inventor one: Mark J. **STEFIK**

Signature: _____ Citizen of: UNITED STATES

Inventor two: Peter L.T. **PIROLLI**

Signature: _____ Citizen of: CANADIAN

Inventor three: Ralph C. **MERKLE**

Signature:  Citizen of: UNITED STATES

☒ Additional inventors are being named on the additional form(s) attached hereto.

Petitioner Apple Inc. - Exhibit 1012, p. 1932

SEP 12 2006
PATENT & TRADEMARK OFFICE

APPLICATION DATA SHEET

Electronic Version v14
Stylesheet Version v14.1

Applicant Information:

Inventor 1:

Applicant Authority Type:	Inventor
Citizenship:	US
Given Name:	Mark
Middle Name:	J.
Family Name:	STEFIK
City of Residence:	Portola Valley
State of Residence:	CA
Country of Residence:	US
Address-1 of Mailing Address:	10 Portola Green Circle
Address-2 of Mailing Address:	
City of Mailing Address:	Portola Valley
State of Mailing Address:	CA
Postal Code of Mailing Address:	94028
Country of Mailing Address:	US
Phone:	
Fax:	
E-mail:	

Inventor 2:

Applicant Authority Type:	Inventor
Citizenship:	CA
Given Name:	Peter
Middle Name:	L.T.
Family Name:	Pirolli
City of Residence:	San Francisco
State of Residence:	CA
Country of Residence:	US
Address-1 of Mailing Address:	2958 Sloat Boulevard
Address-2 of Mailing Address:	

Petitioner Apple Inc. - Exhibit 1012, p. 1933

City of Mailing Address:	San Francisco
State of Mailing Address:	CA
Postal Code of Mailing Address:	94116
Country of Mailing Address:	US
Phone:	
Fax:	
E-mail:	

Inventor 3:

Applicant Authority Type:	Inventor
Citizenship:	US
Given Name:	Ralph
Middle Name:	C.
Family Name:	Merkle
City of Residence:	Sunnyvale
State of Residence:	CA
Country of Residence:	US
Address-1 of Mailing Address:	1134 Pimento Avenue
Address-2 of Mailing Address:	
City of Mailing Address:	Sunnyvale
State of Mailing Address:	CA
Postal Code of Mailing Address:	94087
Country of Mailing Address:	US
Phone:	
Fax:	
E-mail:	

Correspondence Information:

Customer Number:	22204	*22204*

Application Information:

Title of Invention:	DIGITAL WORKS HAVING USAGE RIGHT AND METHOD FOR CREATING THE SAME
Application Type:	regular, utility

Petitioner Apple Inc. - Exhibit 1012, p. 1934

Attorney Docket Number: 111325/020700

Botanic Information:

Publication Information:
Suggested Figure for Publication -
Suggested Classification -
Suggested Technology Center -
Total Number of Drawing Sheets -

Representative Information:

practitioner(s) at Customer Number:

22204 *22204*

as our attorney(s) or agent(s) to prosecute the application identified above, and to transact all business in the United States Patent and Trademark Office connected therewith.

Domestic Priority Information:

This is a Continuation of US application number 09/778,001, filed 2001-02-07, now which is a divisional of Serial No. 08/967,084; filed on November 10, 1997, now U.S. Patent No. 6,236,971, which is a continuation of Serial No. 08/344,760, filed on November 23, 1994,now abandoned..

Foreign Priority Information:

Assignee Information:

Assignee 1:

Organization Name:	ContentGuard Holding, Inc.
Address-1 of Mailing Address:	103 Foulk Road
Address-2 of Mailing Address:	Suite 200-M
City of Mailing Address:	Wilmington
State of Mailing Address:	DE
Postal Code of Mailing Address:	19803
Country of Mailing Address:	US

Petitioner Apple Inc. - Exhibit 1012, p. 1935

Phone:
Fax:
E-mail:

Petitioner Apple Inc. - Exhibit 1012, p. 1936

OIPE IAP48
SEP 12 2006
PATENT & TRADEMARK OFFICE

IFW

Attorney's Docket No. 111325-020700 (088)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	Confirmation No.: 5128
Mark J. **STEFIK,** *et al.*	)	Group Art Unit: 3621
Serial No. 10/015,951	)	Examiner: James A. Reagan
Filed: December 17, 2001	)	
For: **DIGITAL WORKS HAVING RIGHT AND METHOD FOR CREATING THE SAME**	)	

United States Patent and Trademark Office
Customer Services Window
Randolph Building
401 Dulany Street
Alexandria, VA 222314

STATEMENT BY MARK J. STEFIK

IN SUPPORT OF THE LETTER RE CORRECTION OF INVENTORSHIP

UNDER 37 C.F.R. 1.48

Sir:

Pursuant to the requirements of 37 C.F.R. 1.48(a)(2), it is hereby stated that the error in failing to list Ralph C. Merkle as third inventor for the above identified patent application occurred without deceptive intention on my part.

Respectfully submitted,

Date: 19 June 2006

Mark J. Stefik

W727955.1

OIPE
SEP 12 2006
PATENT & TRADEMARK OFFICE

Attorney's Docket No. 111325-020700 (088)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	Confirmation No.: 5128
Mark J. **STEFIK**, *et al.*	)	Group Art Unit: 3621
Serial No. 10/015,951	)	Examiner: James A. Reagan
Filed: December 17, 2001	)	
For: **DIGITAL WORKS HAVING USAGE RIGHT AND METHOD FOR CREATING THE SAME**	)	

United States Patent and Trademark Office
Customer Services Window
Randolph Building
401 Dulany Street
Alexandria, VA 222314

STATEMENT BY PETER L.T. PIROLLI

IN SUPPORT OF THE LETTER RE CORRECTION OF INVENTORSHIP

UNDER 37 C.F.R. 1.48

Sir:

Pursuant to the requirements of 37 C.F.R. 1.48(a)(2), it is hereby stated that the error in failing to list Ralph C. Merkle as third inventor for the above identified patent application occurred without deceptive intention on my part.

Respectfully submitted,

Date: 6/15/2006

Peter L.T. Pirolli

W727957.1

OIPE IAP48
SEP 12 2006
PATENT & TRADEMARK OFFICE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re PATENT Application of	) Confirmation No. 5128
Mark J. **STEFIK,** *et al.*	) Group Art Unit: 3621
Application Serial No.: 10/015,951	) Examiner: James A. Reagan
Filed: December 17, 2001	)
For: **DIGITAL WORKS HAVING USAGE RIGHT AND METHOD FOR CREATING THE SAME**	)))

United States Patent and Trademark Office
Customer Services Window
Randolph Building
401 Dulany Street
Alexandria, VA 222314

LETTER REQUESTING CORRECTION OF INVENTORSHIP

UNDER 37 C.F.R. 1.48

Sir:

This letter requests the correction for the incorrect original naming of inventors in the above noted application filed on December 17, 2001. It is requested that the inventorship of the above identified application be corrected to add:

Ralph C. Merkle

1134 Pimento Avenue

Sunnyvale, California 94087

Pursuant to the requirements of 37 C.F.R. 1.48(a), please find attached a newly executed Declaration and Assignment by all the inventors, and letters from Mark J. Stefik and Peter L.T. Pirolli stating that the error in omission of Ralph Merkle as an inventor of the subject matter of at least one claim of the instant application occurred without deceptive intent on their part.

Respectfully submitted,
NIXON PEABODY, LLP

By: _____
Carlos R. Villamar
Registration No. 43,224

Date: 9/12/06

NIXON PEABODY LLP
401 9th Street, N.W., Suite 900
Washington, DC 20004
Telephone: (202) 585-8000
Facsimile (202) 585-8080

OIPE 1449 SEP 12 2006 PATENT & TRADEMARK OFFICE

Attorney's Docket No. 111325-020700 (088)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	Confirmation No.: 5128
Mark J. **STEFIK**, *et al.*	)	Group Art Unit: 3621
Serial No. 10/015,951	)	Examiner: James A. Reagan
Filed: December 17, 2001	)	
For: **DIGITAL WORKS HAVING USAGE RIGHT AND METHOD FOR CREATING THE SAME**	)	

United States Patent and Trademark Office
Customer Services Window
Randolph Building
401 Dulany Street
Alexandria, VA 222314

STATEMENT BY RALPH C. MERKLE
IN SUPPORT OF THE LETTER RE CORRECTION OF INVENTORSHIP
UNDER 37 C.F.R. 1.48

Sir:

Pursuant to the requirements of 37 C.F.R. 1.48(a)(2), it is hereby stated that the error in failing to list myself as inventor of the above identified patent application occurred without deceptive intention on my part.

Respectfully submitted,

Date: June 11, 2006

Ralph C. Merkle

W727958.1

OIPE IAP48
SEP 12 2006
PATENT & TRADEMARK OFFICE

Attorney's Docket No. 111325-020700 (088)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:	)	Confirmation No.: 5128
Mark J. **STEFIK,** *et al.*	)	Group Art Unit: 3621
Serial No. 10/015,951	)	Examiner: James A. Reagan
Filed: December 17, 2001	)	
For: **DIGITAL WORKS HAVING USAGE RIGHT AND METHOD FOR CREATING THE SAME**	)	

United States Patent and Trademark Office
Customer Services Window
Randolph Building
401 Dulany Street
Alexandria, VA 222314

WRITTEN CONSENT OF THE ASSIGNEE

IN SUPPORT OF THE LETTER RE CORRECTION OF INVENTORSHIP

UNDER 37 C.F.R. 1.48

Sir:

Pursuant to the requirements of 37 C.F.R. 1.48(a)(2), it is hereby stated that the error in failing to list Ralph C. Merkle as third inventor for the above identified patent application occurred without deceptive intention on the part of the Assignee.

Respectfully submitted,

Date: 6/13/06

Robert Logan, Chief Executive Officer
ContentGuard Holdings, Inc.
Assignee

W727960.1

OIPE IAP48
SEP 12 2006
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. **STEFIK**, *et al.*
Group Art Unit	3621
Examiner Name	James A. Reagan
Total Number of Pages in This Submission	
Attorney Docket Number	111325-020700 (088)

ENCLOSURES *(check all that apply)*

- ☒ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☒ Assignment Papers *(for an Application)*
- ☐ Drawing(s)
- ☒ Declaration and Power of Attorney
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance Communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Status Letter
- ☒ Application Data Sheet
- ☐ Request for Corrected Filing Receipt with Enclosures
- ☐ A self-addressed prepaid postcard for acknowledging receipt
- ☒ Other Enclosure(s) (*please identify below*):
  1. Letter Requesting Correction of Inventorship Under 37 C.F.R. 1.48
  2. Statements by Mark J. Stefik, Peter L.T. Pirolli and Ralph C. Merkle in Support of the Letter re Correction of Inventorship Under 37 C.F.R. 148
  3. Written Consent of the Assignee in Support of the Letter re Correction of Inventorship Under 37 C.F.R. 148
  4. Assignment Recordation Cover Sheet

Remarks

☒ The Commissioner is hereby authorized to charge any additional fees required or credit any overpayments to Deposit Account No. 19-2380 for the above identified docket number.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm *or* Individual name	Carlos R. Villamar Reg. No. 43,224 **Nixon Peabody LLP** 401 9th Street, N.W., Suite 900 Washington, D.C. 20004-2128
Signature	
Date	9/12/06

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

- ☐ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop _____, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450
- ☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) _____.

_____ Date

_____ Signature

_____ Typed or printed name

FEE TRANSMITTAL FOR FY 2005

Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT | **$40.00**

OIPE SEP 12 2006 PATENT & TRADEMARK OFFICE

Complete if Known	
Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. STEFIK, *et al.*
Examiner Name	James A. Reagan
Art Unit	3621
Attorney Docket No.	111325-020700 (088)

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit Card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 19-2380

Deposit Account Name: Nixon Peabody LLP

The Commissioner is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	300	2001	150	Utility filing fee	
1002	200	2002	100	Design filing fee	
1003	200	2003	100	Plant filing fee	
1004	300	2004	150	Reissue filing fee	
1005	200	2005	100	Provisional filing fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

		Extra Claims		Fee from below		Fee Paid
Total Claims	-20** =		X		=	0
Independent Claims	-3** =		X		=	0
Multiple Dependent			X		=	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	50	2202	25	Claims in excess of 20
1201	200	2201	100	Independent claims in excess of 3
1203	360	2203	180	Multiple dependent claim, if not paid
1204	200	2204	100	** Reissue independent claims over original patent
1205	50	2205	25	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	
1051	130	2051	65	Surcharge – late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1,020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1,080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	
1403	1,000	2403	500	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	500	2452	250	Petition to revive – unavoidable	
1453	1,500	2453	750	Petition to revive – unintentional	
1501	1,400	2501	700	Utility issue fee (or reissue)	
1502	800	2502	400	Design issue fee	
1503	1,100	2503	550	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	40.00
1809	790	2809	395	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify) _____

*Reduced by Basic Filing Fee Paid

SUBTOTAL (3) **$40.00**

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

☐ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop _____, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450

☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) _____.

Date _____ Signature _____

Typed or printed name _____

SUBMITTED BY

				Complete *(if applicable)*	
Name *(Print/Type)*	Carlos R. Villamar	Registration No. *(Attorney/Agent)*	43,224	Telephone	(202) 585-8204
Signature				Date	9/11/06

SEND TO: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

W727951.1

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,951	12/17/2001	Mark J. Stefik	111325-88	5128

22204 7590 10/05/2006

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

EXAMINER	
REAGAN, JAMES A	

ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 10/05/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/015,951	STEFIK ET AL.	
	Examiner	Art Unit	
	James A. Reagan	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *27 July 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Status of Claims

1. This action is in response to the amendment filed on 27 July 2006.
2. Claims 1-3, 9-14, and 21-34 have been amended.
3. Claims 1-34 are pending in the present application and have been examined.
4. The rejection of claims 1-34 has been updated to include a rejection under 35 U.S.C § 112, 2nd paragraph.

Previous Claim Rejections - 35 USC § 101

5. Claims 1-10 and 21-26 were rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter. The examiner thanks the Applicant for amending the claims and hereby withdraws the rejections under 35 USC § 101.

RESPONSE TO ARGUMENTS

6. Applicant's arguments received on 27 July 2006 have been fully considered. Referring to the previous Office action, Examiner has cited relevant portions of the references as a means to illustrate the systems as taught by the prior art. As a means of providing further clarification as to what is taught by the references used in the first Office action, Examiner has expanded the teachings for comprehensibility while maintaining the same grounds of rejection of the claims, except as noted above in the section labeled "Status of Claims." This information is intended to assist in illuminating the teachings of the references while providing evidence that establishes

further support for the rejections of the claims. Applicant's arguments with respect to claims have been considered but are moot in view of the new ground(s) of rejection.

Double Patenting

7. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. A nonstatutory obviousness-type double patenting rejection is appropriate where the conflicting claims are not identical, but at least one examined application claim is not patentably distinct from the reference claim(s) because the examined application claim is either anticipated by, or would have been obvious over, the reference claim(s). See, e.g., *In re Berg*, 140 F.3d 1428, 46 USPQ2d 1226 (Fed. Cir. 1998); *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

8. A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) or 1.321(d) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent either is shown to be commonly owned with this application, or claims an invention made as a result of activities undertaken within the scope of a joint research agreement.

9. Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

10. Claims 1-34 are rejected on the ground of nonstatutory obviousness-type double patenting as being unpatentable over claims 1-23 of U.S. Patent No. 6,708,157 B2. Although the conflicting claims are not identical, they are not patentably distinct from each other because US 6,708,157 B2 to Stefik et al. does not disclose:

- *said digital work is described by a description structure comprising a plurality of description blocks;*
- *each of said description blocks comprises address information for at least one part of said digital work;*
- *each of said description blocks further comprises zero or more pointers to other description blocks; and*
- *each of said description blocks further comprises a usage rights part for associating one or more of said associated usages rights;*

Although US 6,708,157 B2 does disclose a system for controlling the distribution and use of digital works comprising a means for associating one or more usage rights with a digital work, said one or more usage rights specifying a manner of use indicating a particular manner of how said digital work may be used and at least one condition that must be satisfied in order to exercise the manner of use, US 6,708,157 B2 does not disclose the descriptor block limitations as shown above. Utilization of said descriptor block as claimed is an obvious modification because processing languages routinely use pointers to store addresses and to associate data stored in memory. In this case, each digital work is associated with a usage right description block by using pointers in memory.

Claim Rejections - 35 USC § 112

11. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

12. Claims 1, 11, 21, and 27 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. These independent claims refer to "zero or more pointers." In the case that there are zero pointers, the limitations appears to become meaningless. The Applicant is invited to respond.

Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **James A. Reagan** whose telephone number is **571.272.6710.** The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **ANDREW J. FISCHER** can be reached at **571.272.6779**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to **571-273-8300**.

Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window**:

Randolph Building

401 Dulany Street

Alexandria, VA 22314.

JAMES A. REAGAN

Primary Examiner

Art Unit 3621

20 September 2006

JAMES A. REAGAN
PRIMARY EXAMINER

Electronic Acknowledgement Receipt

EFS ID:	1301393
Application Number:	10015951
International Application Number:	
Confirmation Number:	5128
Title of Invention:	Digital works having usage rights and method for creating the same
First Named Inventor/Applicant Name:	Mark J. Stefik
Customer Number:	22204
Filer:	Carlos Rafael Villamar/Kisha Avery
Filer Authorized By:	Carlos Rafael Villamar
Attorney Docket Number:	111325-88
Receipt Date:	08-NOV-2006
Filing Date:	17-DEC-2001
Time Stamp:	16:54:10
Application Type:	Utility

Payment information:

Submitted with Payment	yes
Payment was successfully received in RAM	$130
RAM confirmation Number	468
Deposit Account	192380
The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows: Charge any Additional Fees required under 37 C.F.R. Section 1.16 and 1.17	

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)	Multi Part /.zip	Pages (if appl.)
1	Terminal Disclaimer Filed	111325_020700_Terminal_Disclaimer_over_US_Patent_6_708_157.pdf	28965	no	1
Warnings:					
Information:					
2	Fee Worksheet (PTO-875)	fee-info.pdf	8161	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	37126		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

Electronic Patent Application Fee Transmittal

Application Number:	10015951
Filing Date:	17-Dec-2001
Title of Invention:	Digital works having usage rights and method for creating the same
First Named Inventor/Applicant Name:	Mark J. Stefik
Filer:	Carlos Rafael Villamar/Kisha Avery
Attorney Docket Number:	111325-88

Filed as Large Entity

Utility Filing Fees

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				
Post-Allowance-and-Post-Issuance:				
Statutory disclaimer	1814	1	130	130
Extension-of-Time:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Miscellaneous:				
		Total in USD ($)		**130**

TERMINAL DISCLAIMER TO OBVIATE A DOUBLE PATENTING REJECTION OVER A PRIOR PATENT	Docket Number (Optional) 111325-020700

In re Application of: Mark J. **STEFIK**, *et al.*

Application No.: 10/015,951

Filed: December 17, 2001

For: **DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME**

The owner*, ContentGuard Holdings, Inc., of 100 percent interest in the instant application hereby disclaims, except as provided below, the terminal part of the statutory term of any patent granted on the instant application, which would extend beyond the expiration date of the full statutory term defined in 35 U.S.C. 154 to 156 and 173, as presently shortened by any terminal disclaimer, of prior **Patent No. 6,708,157**. The owner hereby agrees that any patent so granted on the instant application shall be enforceable only for and during such period that it and the prior patent are commonly owned. This agreement runs with any patent granted on the instant application and is binding upon the grantee, its successors or assigns.

In making the above disclaimer, the owner does not disclaim the terminal part of any patent granted on the instant application that would extend to the expiration date of the full statutory term as defined in 35 U.S.C. 154 to 156 and 173 of the prior patent, as presently shortened by any terminal disclaimer, in the event that it later: expires for failure to pay a maintenance fee, is held unenforceable, is found invalid by a court of competent jurisdiction, is statutorily disclaimed in whole or terminally disclaimed under 37 CFR 1.321, has all claims canceled by a reexamination certificate, is reissued, or is in any manner terminated prior to the expiration of its full statutory term as presently shortened by any terminal disclaimer.

Check either box 1 or 2, if appropriate.

1. ☐ For submissions on behalf of an organization (e.g., corporation, partnership, university, government agency, etc.), the undersigned is empowered to act on behalf of the organization.

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

2. ☒ The undersigned is an attorney or agent of record.

/Carlos R. Villamar, Reg. # 43,224/ — Signature
11/08/06 — Date

Carlos R. Villamar, Reg. No. 43,224
Typed or printed name

☒ Terminal disclaimer fee under 37 CFR 1.20(d) is included.

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

*Statement under 37 CF 3.73(b) is required if terminal disclaimer is signed by the assignee (owner). Form PTO/SB/96 may be used for making this statement. See MPEP § 324.

Petitioner Apple Inc. - Exhibit 1012, p. 1956

Dialog LOG OFF

Search results: **0** titles

Search Report

Database Name	Database Number
SCISEARCH 1990+	34
DISSERTATION ABS	35
GLOBALBASE	583
INSIDE CONFERENCES	65
INSPEC, 1898+	2
APPLIED SCI & TECH	99
NTIS	6
JICST-EPLUS	94
FT ABSTRACTS	473
SCISEARCH 74-89	434
NYT ABSTRACTS	474
TECTRENDS	256
WSJ ABSTRACTS	475

Set	Description
S1	PY=((1970:1994))
S2	S1 (((drm) AND digital AND rights AND management AND descriptor AND block))and ((UNCYPHER? OR UNENCYPHER? OR UNENCIPHER? OR UNCIPHER? OR ENCYPHER? OR UNCRYPT? OR DECRYPT? OR DECYPHER? OR UNENCOD? OR ENCIPHER? OR KEY? ?(1W)PAIR? ? OR SECRET()(CODE? ? OR CODING)) or (CYPHER? OR UNENCRYPT? OR DESCRAMBL? OR UNSCRAMBL? OR CIPHER? OR DECRYPT? OR DECIPHER? OR (SECRET OR PUBLIC OR PRIVATE)(1W)KEY? ? OR SECURE(2W)(TRANSACT? OR PROCESS???) OR CRYPT? OR SCRAMBL? OR ENCRYPT?))
S3	RD

Petitioner Apple Inc. - Exhibit 1012, p. 1957

Help Tips for 'Zero Records' - How To Get More Records

- Don't over-specify: use only the search options you really need -- leave the others blank.
- Exclude "implied concepts": leave out words like 'research' or 'effects.'
- Use more wildcards to search different word endings: use COMPUTER? in place of COMPUTER.
- Check the format of your entry. Follow the Search Tips examples shown on the search page.
- Check for misspelled words.
- Check that you are using parentheses correctly when you combine words with AND, OR, NOT.

For more tips on searching, see the Help page.

Petitioner Apple Inc. - Exhibit 1012, p. 1958

powered by Dialog LOG OFF

Search results: **0** titles

Search Report

Database Name	Database Number
ABI/INFORM	15
COMPUTER DATABASE	275
NEW PRODUCT ANNMNT	621
NEWSLETTER DB	636
TRADE&INDUSTRY	148
PROMT (90-PRESENT)	16
PROMT (1972-1989)	160

Set	Description
S1	((drm) AND digital AND rights AND management AND descriptor AND block)
S2	PY=((1970:1994))
S3	S1 and S2
S4	S3 and ((UNCYPHER? OR UNENCYPHER? OR UNENCIPHER? OR UNCIPHER? OR ENCYPHER? OR UNCRYPT? OR DECRYPT? OR DECYPHER? OR UNENCOD? OR ENCIPHER? OR KEY? ?(1W)PAIR? ? OR SECRET(1w)(CODE? ? OR CODING)) or (CYPHER? OR UNENCRYPT? OR DESCRAMBL? OR UNSCRAMBL? OR CIPHER? OR DECRYPT? OR DECIPHER? OR (SECRET OR PUBLIC OR PRIVATE)(1W) KEY? ? OR SECURE(2W)(TRANSACT? OR PROCESS???) OR CRYPT? OR SCRAMBL? OR ENCRYPT?))
S5	RD
S6	SORT /ALL/pd,a

Help Tips for 'Zero Records' - How To Get More Records

- Don't over-specify: use only the search options you really need -- leave the others blank.
- Exclude "implied concepts": leave out words like 'research' or 'effects.'
- Use more wildcards to search different word endings: use COMPUTER? in place of COMPUTER.

Realtime Data LLC - Exhibit 1012, p. 1959

- Check the format of your entry. Follow the Search Tips examples shown on the search page.
- Check for misspelled words.
- Check that you are using parentheses correctly when you combine words with AND, OR, NOT.

For more tips on searching, see the Help page.

Petitioner Apple Inc. - Exhibit 1012, p. 1960

POWERED BY Dialog LOGOFF

Search results: **0** titles

Search Report

Database Name	Database Number
AMERICAN BANKER	625
BOND BUYER	626
BUSINESS & INDUS	9
BUSINESS WIRE	610
BUSINESS WIRE	810
DIALOG FIN & BANK	267
KR/T BUS NEWS	608
MATHSCI	239
MCGRAW-HILL PUBS	624
PR NEWSWIRE	613
PR NEWSWIRE	813
SAN JOSE MERCURY	634
GLOBAL REPORTER	20
FT INFORMATION LTD	476

Set	Description
S1	(((drm) AND digital AND rights AND management AND descriptor AND block))
S2	PY=((1970:1994))
S3	S1 and S2
	S3 and ((UNCYPHER? OR UNENCYPHER? OR UNENCIPHER? OR UNCIPHER? OR ENCYPHER? OR UNCRYPT? OR DECRYPT? OR DECYPHER? OR UNENCOD? OR ENCIPHER? OR KEY? ?(1W)PAIR? ? OR SECRET(1w)

Petitioner Apple Inc. - Exhibit 1012, p. 1961

S4	(CODE? ? OR CODING)) or (CYPHER? OR UNENCRYPT? OR DESCRAMBL? OR UNSCRAMBL? OR CIPHER? OR DECRYPT? OR DECIPHER? OR (SECRET OR PUBLIC OR PRIVATE)(1W)KEY? ? OR SECURE(2W) (TRANSACT? OR PROCESS???) OR CRYPT? OR SCRAMBL? OR ENCRYPT?))
S5	RD

Help Tips for 'Zero Records' - How To Get More Records

- Don't over-specify: use only the search options you really need -- leave the others blank.
- Exclude "implied concepts": leave out words like 'research' or 'effects.'
- Use more wildcards to search different word endings: use COMPUTER? in place of COMPUTER.
- Check the format of your entry. Follow the Search Tips examples shown on the search page.
- Check for misspelled words.
- Check that you are using parentheses correctly when you combine words with AND, OR, NOT.

For more tips on searching, see the Help page.

Patriot Apache Inc. - Exhibit 1012, p. 1962

PLUS Search Results for S/N 10015951, Searched Thu Nov 16 11:13:05 EST 2006

The Patent Linguistics Utility System (PLUS) is a USPTO automated search system for U.S. Patents from 1971 to the present PLUS is a query-by-example search system which produces a list of patents that are most closely related linguistically to the application searched. This search was prepared by the staff of the Scientific and Technical Information Center, SIRA.

5629980 78
5634012 78
5715403 78
6236971 78
20010014882 78
20010023417 78
5638443 69
5765152 69
6708157 69
6714921 69
6865551 69
6895392 69
6898576 69
6910022 69
6920436 69
6925448 69
6928419 69
6934693 69
6944600 69
6957193 69
6957194 69
6959290 69
6963859 69
7024392 69
7039613 69
7043453 69
7058606 69
7065505 69
7096202 69
7113912 69
7117180 69
20010010045 69
20020128856 69
20020128972 69
20020133465 69
20030023561 69
20030069849 69
20030115144 69
20030167236 69
20030208447 69
20030217010 69
20030225698 69
20030225699 69
20040015446 69
20040059678 69
20040064417 69
20040073513 69
20040073514 69
20040073515 69
20040107166 69
20040220880 69
20040225611 69
20040243834 69
20050086172 69
20050108173 69
20050149450 69
20050160048 69
20050165687 69
20050216415 69
20050251482 69
20050273432 69
20050273433 69
20050289068 69
20060004665 69
20060041512 69
20060106722 69
20060129492 69
20060129493 69
20060149680 69
20060167801 69
20060190404 69
20060200417 69
20050044016 68
6876984 60
20020184158 60
20030236886 60
20040210535 60
20040210765 60
20050043960 60
20050197963 60
20030163724 60
20050105728 59
5896535 58
6253193 58
6363488 58
6389402 58
6427140 58
5838911 57
6282573 57
6735699 57
6882979 57
6885748 57
7068787 57
20030191946 57
20040199471 57
6330672 57
5825883 56
5848154 56
20020198845 56
20020198846 56
4937863 55
5887192 55
5933503 55
20020017977 55
6052119 54
6058478 54
20040215757 53
6173446 52
6226652 51
6226652 51
6292830 51
5291600 51
6075768 51
6202056 50
6233684 50
6857071 50
6889206 50
6973445 50
6999946 50
7031471 50
7051004 50
7089315 50
20010008557 50
20010016837 50
20010032187 50
20020023219 50
20020184156 50
20020184159 50
20030007640 50
20030009681 50
20040073516 50
20040148503 50
20040255138 50
20050080735 50
20050080910 50
20050187877 50
20060085348 50
20060095387 50
20060112015 50
20060116963 50
20060116964 50
20060122942 50
20060107330 50
4884068 50
6282653 50
5809301 49
6148189 49

6220413 49
6220413 49
5787175 48
5519825 48
5719786 48
5754761 48
5950822 48
6061608 48
6061608 48
6421750 48
6769075 48
20020144180 48
20050144200 48
4577288 48
4918759 48
5014222 48
5828742 48
5530520 48
6807534 48
6826546 48
7047241 48
20020002543 48
20040167858 48
20040205358 48
20050039000 48
20050097059 48
20050119975 48
20050278258 48
20060004669 48
5889515 48
4851830 48
4853688 48
4857915 48
5884280 48
5886274 48
6081897 48
6080207 48
6459501 48
6522936 48
7007166 48
20020141584 48
20030097299 48
20030105831 48
20030177362 48
20040103044 48
20050055624 48
20050177516 48
20050278256 48
20060093309 48
20060122842 48
20060155648 48
5819156 47
6278704 47
4479249 47
5886898 47
5905404 47
6070160 47
6871200 47
20030225697 47
20040010486 47
20060161578 47
4802030 47
5625889 47
5845281 47
6005659 47
6246703 47
5313616 47
5629508 47
5745569 47
5444779 47
6477649 47
6824051 47
20020002466 47
20030004888 47
20030009423 47
20030023564 47
20030066884 47
20030078891 47
20030101142 47
20030140003 47
20040024688 47
20040149121 47
5499298 46
5999860 46
6014183 46
4284977 46
4413318 46
5254813 46
5351276 46
5504911 46
5539667 46
5559626 46
5603049 46
5608418 46
5841476 46
5903647 46
6040985 46
6091508 46
6287765 46
6292569 46
6405132 46
6419636 46
4977594 46
5410598 46
5539828 46
6499106 46
6832318 46
20010032312 46
20020002468 46
20030177074 46
20030182574 46
20030217171 46
20040039916 46
20040054893 46
20040193545 46
20050076334 46
20050182731 46
20050209972 46
20050278716 46
20060143690 46
4394103 45
20050071280 45
20060010076 45
20060253400 45
5768387 45
5737414 45
5751723 45
5857575 45
5898689 45
5905436 45
5920861 45
6041946 45
6089384 45
6138119 45
6249865 45
6272126 45
20020077985 45
20020077986 45
20030046545 45
20050108538 45
20060022963 45
5809105 45
5275285 45
5416819 45
5500938 45
5890997 45
5008827 44
5363650 44
5966642 44
4920506 44
5313592 44
5416781 44
5436968 44

CLS1

Most frequently occurring classifications of patents returned from a search Of 10015951 on Nov 16 , 2006

Original Classifications

54	705/51
18	705/57
16	705/52
10	705/54
10	705/59
7	713/176
6	705/1
5	707/9
4	705/50
4	713/193
3	709/229
3	705/53
3	705/55
3	726/26
3	705/26
3	713/165
3	340/7.25
3	211/40
2	705/39
2	726/27
2	705/58
2	380/202
2	713/182
2	717/127
2	707/203
2	705/64
2	705/40
2	191/12.4
2	700/240
2	399/366
2	370/352
2	370/524

Cross-Reference Classifications

26	705/57
25	705/51
22	705/54
21	705/52
20	705/59
18	705/53
17	380/201
15	705/50
11	705/56
10	705/1
10	705/58
8	380/200
8	713/168
7	707/9
7	713/176
6	380/204
6	713/182
6	713/193
5	707/10
5	705/55
5	707/104.1
5	713/185
4	380/202
4	713/184

Petitioner Apple Inc. - Exhibit 1012, p. 1965

4	713/186
4	713/183
4	713/179
4	713/181
4	713/194
4	705/26
4	705/78
3	707/1
3	380/227
3	380/230
3	726/27
3	713/155
3	380/231
3	726/26
3	726/5
3	380/54
3	713/189
3	380/277
3	707/102
3	380/30
2	705/39
2	709/229
2	380/228
2	380/229
2	380/278
2	726/31
2	380/232
2	380/55
2	380/203
2	713/157
2	713/170
2	709/203
2	709/224
2	707/204
2	715/511
2	715/840
2	715/866
2	717/122
2	713/165
2	707/3
2	726/10
2	713/180
2	715/716
2	222/55
2	700/231
2	358/462
2	380/51
2	340/7.46
2	340/7.49
2	705/27
2	380/46
2	707/4
2	707/5

Combined Classifications

79	705/51
44	705/57
37	705/52
32	705/54
30	705/59
21	705/53
19	705/50
18	380/201

Petitioner Apple Inc. - Exhibit 1012, p. 1966

16	705/1
14	713/176
12	707/9
12	705/58
11	705/56
10	713/193
8	705/55
8	380/200
8	713/182
8	713/168
7	705/26
6	380/204
6	380/202
6	726/26
5	709/229
5	707/10
5	726/27
5	707/104.1
5	713/185
5	713/181
5	713/165
4	705/39
4	707/1
4	713/184
4	713/186
4	713/183
4	713/155
4	713/179
4	380/231
4	713/194
4	705/78
4	713/189
4	707/102
3	380/227
3	380/230
3	380/203
3	709/203
3	726/5
3	380/54
3	709/224
3	707/204
3	380/277
3	705/40
3	380/30
3	340/7.25
3	705/27
3	707/4
3	211/40
2	705/44
2	380/228
2	380/229
2	380/278
2	726/31
2	380/232
2	380/55
2	713/157
2	713/156
2	726/2
2	726/7
2	713/170
2	705/30
2	709/225
2	717/131

Petitioner Apple Inc. - Exhibit 1012, p. 1967

2 705/14
2 705/80
2 705/37
2 709/217
2 713/191
2 713/173
2 709/223
2 717/127
2 707/203
2 715/511
2 715/840
2 715/866
2 717/122
2 705/64
2 707/3
2 726/10
2 191/12.4
2 713/180
2 715/716
2 700/240
2 222/55
2 700/231
2 358/1.1
2 399/366
2 358/462
2 380/51
2 340/7.46
2 340/7.49
2 715/500
2 726/32
2 717/172
2 717/177
2 380/46
2 370/352
2 707/5
2 370/524
2 235/382
2 235/380
2 379/88.17

Petitioner Apple Inc. - Exhibit 1012, p. 1968

EAST Search History

L12	296	(US-6449367-$ or US-6427140-$ or US-6363488-$ or US-6237786-$ or US-6948070-$ or US-6658568-$ or US-6640304-$ or US-6253193-$ or US-6389402-$ or US-6185683-$ or US-5982891-$ or US-5949876-$ or US-5917912-$ or US-5915019-$ or US-5910987-$ or US-5892900-$ or US-5713032-$ or US-6363357-$ or US-6330670-$ or US-6327652-$ or US-5260999-$ or US-6775779-$ or US-5745879-$ or US-6772340-$ or US-6697944-$ or US-6519700-$).did. or (US-6763464-$ or US-5204897-$ or US-6754642-$ or US-6240185-$ or US-6138119-$ or US-6233684-$ or US-6236971-$ or US-6651171-$ or US-6775655-$ or US-5438508-$ or US-5943422-$ or US-5920861-$ or US-5715403-$ or US-5638443-$ or US-5634012-$ or US-5629980-$ or US-6112181-$ or US-6618484-$ or US-6611812-$ or US-6587837-$ or US-6574609-$ or US-6418421-$ or US-6398245-$ or US-6389538-$ or US-6389403-$ or US-6345256-$ or US-6292830-$).did. or (US-6282573-$ or US-6141754-$ or US-6018724-$ or US-6263313-$ or US-6226618-$ or US-6170014-$ or US-6006332-$ or US-5983236-$ or US-5933841-$ or US-5806078-$ or US-5774661-$ or US-6449718-$ or US-5530235-$ or US-6886038-$ or US-6820063-$ or US-6055526-$ or US-6976175-$ or US-6976009-$ or US-6973445-$ or US-6968996-$ or US-6963859-$ or US-6963858-$ or US-6959289-$ or US-6959288-$ or US-6957193-$ or US-6954738-$ or US-6948073-$).did. or (US-6944776-$ or US-6931545-$ or US-6928419-$ or US-6925448-$ or US-6920436-$ or US-6912294-$ or US-6910022-$ or US-6898706-$ or US-6895503-$ or US-6889206-$ or US-6442696-$ or US-6871200-$ or US-6859791-$ or US-6859533-$ or US-6834110-$ or US-6829708-$ or US-6824051-$ or US-6816596-$ or US-6813640-$ or US-6799302-$ or US-6789188-$ or US-6738744-$ or US-6704797-$ or US-6640307-$ or US-6640302-$ or US-6597891-$ or US-6591365-$).did. or (US-6535871-$ or US-6516416-$	USPAT	OR	ON	2006/11/17 10:20

Petitioner Apple Inc. - Exhibit 1012, p. 1969

EAST Search History

L13	164	("5629508" "5745569" "5444779" "6477649" "6824051" "20020002466" "20030004888" "20030009423" "20030023564" "20030066884" "20030078891" "20030101142" "20030140003" "20040024688" "20040149121" "5499298" "5999860" "6014183" "4284977" "4413318" "5254813" "5351276" "5504911" "5539667" "5559626" "5603049" "5608418" "5841476" "5903647" "6040985" "6091508" "6287765" "6292569" "6405132" "6419636" "4977594" "5410598" "5539828" "6499106" "6832318" "20010032312" "20020002468" "20030177074" "20030182574" "20030217171" "20040039916" "20040054893" "20040193545" "20050076334" "20050182731" "20050209972" "20050278716" "20060143690" "4394103" "20050071280" "20060010076" "20060253400" "5768387" "5737414" "5751723" "5857575" "5898689" "5905436" "5920861" "6041946" "6089384" "6138119" "6249865" "6272126" "20020077985" "20020077986" "20030046545" "20050108538" "20060022963" "5809105" "5275285" "5416819" "5500938" "5890997" "5008827" "5363650" "5966642" "4920506" "5313592" "5416781" "5436968").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/17 10:21

Petitioner Apple Inc. - Exhibit 1012, p. 1970

EAST Search History

L14	166	("20030007640" "20030009681" "20040073516" "20040148503" "20040255138" "20050080735" "20050080910" "20050187877" "20060085348" "20060095387" "20060112015" "20060116963" "20060116964" "20060122942" "20060107330" "4884068" "6282653" "5809301" "6148189" "6220413" "6220413" "5787175" "5519825" "5719786" "5754761" "5950822" "6061608" "6061608" "6421750" "6769075" "20020144180" "20050144200" "4577288" "4918759" "5014222" "5828742" "5530520" "6807534" "6826546" "7047241" "20020002543" "20040167858" "20040205358" "20050039000" "20050097059" "20050119975" "20050278258" "20060004669" "5889515" "4851830" "4853688" "4857915" "5884280" "5886274" "6081897" "6080207" "6459501" "6522936" "7007166" "20020141584" "20030097299" "20030105831" "20030177362" "20040103044" "20050055624" "20050177516" "20050278256" "20060093309" "20060122842" "20060155648" "5819156" "6278704" "4479249" "5886898" "5905404" "6070160" "6871200" "20030225697" "20040010486" "20060161578" "4802030" "5625889" "5845281" "6005659" "6246703" "5313616").pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/17 10:21

Petitioner Apple Inc. - Exhibit 1012, p. 1971

EAST Search History

L15	123	("20050165687" "20050216415" "20050251482" "20050273432" "20050273433" "20050289068" "20060004665" "20060041512" "20060106722" "20060129492" "20060129493" "20060149680" "20060167801" "20060190404" "20060200417" "20050044016" "6876984" "20020184158" "20030236886" "20040210535" "20040210765" "20050043960" "20050197963" "20030163724" "20050105728" "5896535" "6253193" "6363488" "6389402" "6427140" "5838911" "6282573" "6735699" "6882979" "6885748" "7068787" "20030191946" "20040199471" "6330672" "5825883" "5848154" "20020198845" "20020198846" "4937863" "5887192" "5933503" "20020017977" "6052119" "6058478" "20040215757" "6173446" "6226652" "6226652" "6292830" "5291600" "6075768" "6202056" "6233684" "6857071" "6889206" "6973445" "6999946" "7031471" "7051004" "7089315" "20010008557" "20010016837" "20010032187" "20020023219" "20020184156" "20020184159"). pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/17 10:21

Petitioner Apple Inc. - Exhibit 1012, p. 1972

EAST Search History

L16	72	("5629980" "5634012" "5715403" "6236971" "20010014882" "20010023417" "5638443" "5765152" "6708157" "6714921" "6865551" "6895392" "6898576" "6910022" "6920436" "6925448" "6928419" "6934693" "6944600" "6957193" "6957194" "6959290" "6963859" "7024392" "7039613" "7043453" "7058606" "7065505" "7096202" "7113912" "7117180" "20010010045" "20020128856" "20020128972" "20020133465" "20030023561" "20030069849" "20030115144" "20030167236" "20030208447" "20030217010" "20030225698" "20030225699" "20040015446" "20040059678" "20040064417" "20040073513" "20040073514" "20040073515" "20040107166" "20040220880" "20040225611" "20040243834" "20050086172" "20050108173" "20050149450" "20050160048"). pn.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/11/17 10:21
S1	946	"digital rights management" or DRM	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/01/17 14:09
S2	409	("digital rights management" or DRM) and (play or copy or save or transfer or crop or extract or embed or delete or render)	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:13
S3	207	(("digital rights management" or DRM) and (play or copy or save or transfer or crop or extract or embed or delete or render)) and distribut$	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:02
S4	172	((("digital rights management" or DRM) and (play or copy or save or transfer or crop or extract or embed or delete or render)) and distribut$) and (NOT ginter)	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 15:47
S5	33	wyman WITH robert	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:34
S6	5225	grammar	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:07

Petitioner Apple Inc. - Exhibit 1012, p. 1973

EAST Search History

S7	162	grammar and permission	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:06
S8	203	grammar and (permission or privilege)	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:06
S9	1763	grammar and rights	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:06
S10	127	(grammar and rights) and permission	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:06
S11	1197	grammar and rule and (permission or priviliege or rights)	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:08
S12	109	grammar and rule and (permission or priviliege) and rights	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:10
S13	1034	(grammar or language) and rule and (permission or priviliege) and rights	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:10
S14	107	(grammar and language) and rule and (permission or priviliege) and rights	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:11
S15	106	((grammar and language) and rule and (permission or priviliege) and rights) and (play or copy or save or transfer or crop or extract or embed or delete or render)	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:13
S16	73	embed$ WITH extract$ WITH digital and rights	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:22
S17	295	embed$ WITH extract$ WITH digital	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:30
S18	438	embed$ WITH extract$ SAME digital	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:30

Petitioner Apple Inc. - Exhibit 1012, p. 1974

EAST Search History

S19	4	wyman WITH robert and fee	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 14:34
S20	4	wyman WITH robert and fee and distribut$	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 15:39
S21	4	(("5335346") or ("5295266")).PN.	USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/08/27 15:28
S22	4	wyman WITH robert and fee and distribut$ AND PRINT	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 15:39
S23	6	((("digital rights management" or DRM) and (play or copy or save or transfer or crop or extract or embed or delete or render)) and distribut$) and (NOT ginter) and print and repository	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 15:48
S24	28	((("digital rights management" or DRM) and (play or copy or save or transfer or crop or extract or embed or delete or render)) and distribut$) and (NOT ginter) and print	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 15:49
S25	3250	repository and print$	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 15:55
S26	1750	repository and print$ and "rights"	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 15:50
S27	566	repository and print$ and "rights" and copyright	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 15:53
S28	26	repository and print$ and "copy rights"	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 15:54
S29	498	repository SAME print$	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/08/27 15:56

Petitioner Apple Inc. - Exhibit 1012, p. 1975

EAST Search History

S30	4	(("5295266") or ("5335346")).PN.	USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/10/18 12:15
S31	2	("5138712").PN.	USPAT; USOCR; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2004/10/18 14:09
S32	350	705/51.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:10
S33	158	705/52.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:10
S34	74	705/53.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:10
S35	81	705/54.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:10
S36	78	705/55.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:10
S37	78	705/56.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:10
S38	281	705/57.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:10
S39	105	705/58.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:10
S40	156	705/59.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:11

Petitioner Apple Inc. - Exhibit 1012, p. 1976

EAST Search History

S41	71	705/50.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:12
S42	246	380/201.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:15
S43	723	707/9.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:18
S44	0	707/9.CCLS. AND DRM	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:16
S45	2281	707/104.1.ccls.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:16
S46	2	707/104.1.ccls. and "digital rights management"	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:17
S47	220	713/182.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:18
S48	189	713/183.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:18
S49	109	713/184.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:18
S50	241	713/185.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:19
S51	166	713/186.CCLS.	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/10/18 14:19
S53	0	stefik.in. and (less SAME restrict$)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/11/05 13:42

Petitioner Apple Inc. - Exhibit 1012, p. 1977

EAST Search History

S54	30	stefik.in. and (more SAME restrict$)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/02/28 16:38
S55	0	stefik.in. and (least SAME restrict$)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2004/11/05 13:43
S59	33	stefik.in. and (more SAME restrict$)	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/11 11:04
S60	1	S59 and watermark	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/08 13:37
S61	7	stefik.in. and watermark	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/03/08 13:37
S62	37	stefik.in. and delete	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/11 11:04
S63	148	stefik.in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/10/06 14:30
S64	0	stefik.in. and (more SAME restrict$) and "digital image"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/11 11:04
S65	2	stefik.in. and "digital image"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/05/11 11:04
S66	0	stefik.in. AND "MOST RESTRICTIVE"	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/10/06 14:30

Petitioner Apple Inc. - Exhibit 1012, p. 1978

EAST Search History

S67	3	stefik.in. AND RESTRICTIVE	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/10/06 14:30
S68	0	("digital rights management" or DRM) and "manner of use" and restrictive	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/10/06 14:32
S69	0	"manner of use" and restrictive	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/10/06 14:32
S70	190	"least restrictive"	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/10/06 14:34
S71	2614	"more restrictive"	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/10/06 14:34
S72	651	S71 and digital	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/10/06 14:35
S73	345	S72 and rights	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/10/06 14:35
S74	103	S73 and management	USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2005/10/06 14:35
S75	2	("6,741,921").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/28 11:04
S76	3	("6,714,921").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2005/11/28 11:04
S77	3	("6714921").PN.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	OFF	2006/01/17 14:09

Petitioner Apple Inc. - Exhibit 1012, p. 1979

EAST Search History

S78	296	(US-6253193-$ or US-6363488-$ or US-6389402-$ or US-6427140-$ or US-6754642-$ or US-6282653-$ or US-6824051-$ or US-6895503-$ or US-6968996-$ or US-6973445-$ or US-6976009-$ or US-5765152-$ or US-6954738-$ or US-6389403-$ or US-5530235-$ or US-6963858-$ or US-6233684-$ or US-5937160-$ or US-6041355-$ or US-6546405-$ or US-6885748-$ or US-6876984-$ or US-5673316-$ or US-6098056-$ or US-6112181-$ or US-6185683-$).did. or (US-6141754-$ or US-6263313-$ or US-6345256-$ or US-6389538-$ or US-6398245-$ or US-6418421-$ or US-6574609-$ or US-6587837-$ or US-6611812-$ or US-6834110-$ or US-6859791-$ or US-6959288-$ or US-6983371-$ or US-5204897-$ or US-5260999-$ or US-5438508-$ or US-6343738-$ or US-6519700-$ or US-6763464-$ or US-6018724-$ or US-6230173-$ or US-5737442-$ or US-5956422-$ or US-6912294-$ or US-5933841-$ or US-5963949-$ or US-5983227-$).did. or (US-5991756-$ or US-6049801-$ or US-6076166-$ or US-6163844-$ or US-6182078-$ or US-6225993-$ or US-5619571-$ or US-5787175-$ or US-6938021-$ or US-6189043-$ or US-6006332-$ or US-6122648-$ or US-6081900-$ or US-5638443-$ or US-6535871-$ or US-6292830-$ or US-6073160-$ or US-6058383-$ or US-4321672-$ or US-5930788-$ or US-6565000-$ or US-6697944-$ or US-6772340-$ or US-6775655-$ or US-6816596-$ or US-6829708-$ or US-6948073-$).did. or (US-6973444-$ or US-6226618-$ or US-6282573-$ or US-6363357-$ or US-5388196-$ or US-5519608-$ or US-5537526-$ or US-5768580-$ or US-5781732-$ or US-5845067-$ or US-6061675-$ or US-6101515-$ or US-6112201-$ or US-6237099-$ or US-6240410-$ or US-6292271-$ or US-6311176-$ or US-5949491-$ or US-5983369-$ or US-6185602-$ or US-5539893-$ or US-5745879-$ or US-5905496-$ or US-6799302-$ or US-5629980-$ or US-5715403-$ or US-6442696-$).did. or (US-5892900-$ or US-5910987-$	USPAT	OR	ON	2006/01/17 14:29

Petitioner Apple Inc. - Exhibit 1012, p. 1980

EAST Search History

S79	356	ginter.in.	US-PGPUB; USPAT; EPO; JPO; DERWENT; IBM_TDB	OR	ON	2006/02/28 16:38

Petitioner Apple Inc. - Exhibit 1012, p. 1981

Notice of Allowability	Application No.	Applicant(s)	
	10/015,951	STEFIK ET AL.	
	Examiner	Art Unit	
	James A. Reagan	3621	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the Terminal Disclaimer filed on 08 November 2006*.

2. ☒ The allowed claim(s) is/are *1-38*.

3. ☒ The drawings filed on *17 December 2001* are accepted by the Examiner.

4. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

5. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

6. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

7. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

Status of Claims

1. This action is in response to the Terminal Disclaimer filed on 08 November 2006.
2. Claims 1, 8, 21, and 27 have been amended by Examiner's Amendment below.
3. Claims 36-38 have been added by Examiner's Amendment below.
4. Claims 1-38 have been examined.

Terminal Disclaimer

5. The terminal disclaimer filed on 08 November 2006 disclaiming the terminal portion of any patent granted on this application which would extend beyond the expiration date of 23 November 2014 has been reviewed and is accepted. The terminal disclaimer has been recorded.

Allowable Subject Matter

6. Claims 1-38 are allowed. See Reasons for Allowance under separate heading.

EXAMINER'S AMENDMENT

7. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

8. Authorization for this examiner's amendment was given in a telephone interview with Carlos Villamar on 30 October 2006.

The application has been amended as follows:

1. (Currently amended) A computer readable medium having embedded thereon a digital work adapted to be distributed within a system for controlling use of digital works, said digital work comprising:

a digital content portion that is renderable by a rendering device;

a usage rights portion associated with said digital content portion and comprising one or more computer readable instructions configured to permit or prohibit said rendering device to render said digital content portion, said usage rights portion being expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use relating to one or more purposes for which the digital work can be used by an authorized party; and

a description structure comprising a plurality of description blocks, each of said description blocks comprising address information for at least one part of said digital work, ~~zero or more pointers to other description blocks,~~ and a usage rights part for associating one or more usage rights portions.

2. (Previously presented) The digital work as recited in claim 1, wherein said usage rights portion further specifies status information indicating the status of the digital work.

3. (Previously presented) The digital work as recited in claim 1, wherein said usage rights portion further specifies a usage fee associated with exercise of the manner of use, said usage fee comprising a fee type and fee parameters.

4. (Original) The digital work as recited in claim 3 wherein said fee type is a metered use fee and said fee parameters comprise a fee unit and a time unit.

5. (Original) The digital work as recited in claim 3 wherein said fee type is a per use fee and said fee parameter comprises a fee unit.

6. (Original) The digital work as recited in claim 3 wherein said fee type is a best price fee and said fee parameters comprise an identifier to identify said best price.

7. (Original) The digital work as recited in claim 3 wherein said fee type is a scheduled fee and said fee parameters comprise time units and fee units.

8. (Original) The digital work as recited in claim 3 wherein said fee type is a mark-up fee and said fee parameters comprise a mark-up percentage.

9. (Previously presented) The digital work as recited in claim 1 wherein said digital content portion and said usage rights portion are stored on the same physical device.

10. (Previously presented) The digital work as recited in claim 1, wherein said digital content portion and said usage rights portion are stored on different physical devices.

11. (Currently amended) A method for creating a digital work to be used in a system for use of the digital work, said method comprising:

obtaining a digital content portion that is renderable by a rendering device;

associating a usage rights portion with the digital content portion, the usage rights portion comprising one or more computer readable instructions configured to permit or prohibit said rendering device to render said digital content portion, said usage rights portion being expressed

as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use relating to one or more purposes for which the digital work can be used by an authorized party;

describing said digital work by a description structure comprising a plurality of description blocks, each of said description blocks comprising address information for at least one part of said digital work, ~~zero or more pointers to other description blocks,~~ and a usage rights part for associating one or more usage rights portions; and

combining the digital content portion and the usage rights portion to create the digital work.

12. (Previously presented) A method as recited in claim 11, wherein said combining step comprises storing the digital content portion and the usage rights portion on the same physical device.

13. (Previously presented) A method as recited in claim 11, wherein said combining step comprises storing the digital content portion and the usage rights portion on different physical devices.

14. (Previously presented) A method as recited in claim 11, wherein said usage rights portion further specifies a usage fee associated with exercise of the manner of use.

15. (Original) The method as recited in claim 14, wherein said usage fee comprises usage fee information including a fee type and fee parameters.

16. (Original) The method as recited in claim 15 wherein said fee type is a metered use fee and said fee parameters comprise a fee unit and a time unit.

17. (Original) The method as recited in claim 15 wherein said fee type is a per use fee and said fee parameters comprise a fee unit.

18. (Original) The method as recited in claim 15 wherein said fee type is a best price fee and said fee parameters comprise an identifier to identify the best price.

19. (Original) The method as recited in claim 15 wherein said fee type is a scheduled fee and said fee parameters comprise time units and fee units.

20. (Original) The method as recited in claim 17 wherein said fee type is a mark-up fee and said fee parameters comprise a mark-up percentage.

21. (Currently amended) A computer readable medium having embedded thereon a digital work adapted to be distributed within a system for controlling use of digital works, said digital work comprising:

a digital content portion that is renderable by a rendering device;

a usage rights portion associated with said digital content portion and comprising one or more computer readable instructions configured to permit or prohibit said rendering device to render said digital content portion, said usage rights portion being expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying conditions relating to one or more purposes for which the digital work can be used by an authorized party; and

a description structure comprising a plurality of description blocks, each of said description blocks comprising address information for at least one part of said digital work, ~~zero or more pointers to other description blocks,~~ and a usage rights part for associating one or more usage rights portions.

22. (Previously presented) A digital work as recited in claim 21, wherein the conditions relate to the number of copies of the digital work that are in use.

23. (Previously presented) A digital work as recited in claim 21, wherein the conditions relate to the number of time units for which the digital work can be used.

24. (Previously presented) A digital work as recited in claim 21, wherein the conditions relate to the revenue owner of the digital work.

25. (Previously presented) A digital work as recited in claim 21, wherein the conditions relate to the publication date of the digital work.

26. (Previously presented) A digital work as recited in claim 21, wherein the conditions relate to the history of the use and distribution of the digital work.

27. (Previously presented) A method for creating a digital work to be used in a system for controlling use of the digital work, said method comprising:

obtaining a digital content portion that is renderable by a rendering device;

associating a usage rights portion with the digital content portion, the usage rights portion comprising one or more computer readable instructions configured to permit or prohibit said rendering device to render said digital content portion, the usage rights portion being expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying conditions relating to one or more purposes for which the digital work can be used by an authorized party;

describing said digital work by a description structure comprising a plurality of description blocks, each of said description blocks comprising address information for at least one part of

said digital work, ~~zero or more pointers to other description blocks,~~ and a usage rights part for associating one or more usage rights portions; and

combining the digital content portion and the usage rights portion to create the digital work.

28. (Previously presented) A method as recited in claim 27, wherein said combining step comprises storing the digital content portion and the usage rights portion on the same physical device.

29. (Previously presented) A method as recited in claim 27, wherein said combining step comprises storing the digital content portion and the usage rights portion on different physical devices.

30. (Previously presented) A method as recited in claim 27, wherein the conditions relate to the number of copies of the digital work that are in use.

31. (Previously presented) A method as recited in claim 27, wherein the conditions relate to the number of time units for which the digital work can be used.

32. (Previously presented) A method as recited in claim 27, wherein the conditions relate to the revenue owner of the digital work.

33. (Previously presented) A method as recited in claim 27, wherein the conditions relate to the publication date of the digital work.

34. (Previously presented) A method as recited in claim 27, wherein the conditions relate to the history of the use and distribution of the digital work.

35. (Previously presented) The digital work as recited in claim 1, wherein said description blocks further include one or more pointers to other description blocks.

36. (New) A method as recited in claim 11, wherein said description blocks further include one or more pointers to other description blocks.

37. (New) A digital work as recited in claim 21, wherein said description blocks further include one or more pointers to other description blocks.

38. (New) A method as recited in claim 27, wherein said description blocks further include one or more pointers to other description blocks.

Reasons For Allowance

9. The following is an Examiner's statement of reasons for allowance:

None of the art of record, taken individually or combination, disclose at least the method step or system components of:

- *obtaining a digital content portion that is renderable by a rendering device;*
- *associating a usage rights portion with the digital content portion, the usage rights portion comprising one or more computer readable instructions configured to permit or prohibit said rendering device to render said digital content portion, the usage rights portion being expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying conditions relating to one or more purposes for which the digital work can be used by an authorized party;*

- *describing said digital work by a description structure comprising a plurality of description blocks, each of said description blocks comprising address information for at least one part of said digital work, and a usage rights part for associating one or more usage rights portions; and*
- *combining the digital content portion and the usage rights portion to create the digital work.*

More specifically, the prior art of record fails to disclose attaching usage rights to a protected digital work specifically identifying descriptor blocks that that assign usage rights to the digital work.

Independent Claims 1, 8, 21, and 27 are distinguished over the closest prior art of Perritt, which teaches various levels of permission for digital works. See at least page 1 of the white paper. As recited in independent claims 1, 8, 21, and 27, it is clear that the Applicant's invention is distinguished over the Perritt disclosure in at least the method step of *describing said digital work by a description structure comprising a plurality of description blocks, each of said description blocks comprising address information for at least one part of said digital work, and a usage rights part for associating one or more usage rights portions, etc.* Although Perritt does disclose various levels of permission for digital works, Perritt does not disclose usage based upon descriptor blocks.

Conclusion

10. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- Rule Generation Device For Utilizing A Software Component by Mihoko Kishi and Koichi Kachi, 30 March 1990, discloses "...automatically formulating, by using formal language...restriction script texts."

- Fabbio (US 5,335,346 A) discloses a system and method that provides an access control list which spans across object boundaries in an object-oriented database. In addition to providing read and write access permissions, the access control list provides execute semantics which apply to the execution of methods in an object oriented database. Within the entries of the access control lists, each of the permissions for read, write, and execute can be assigned separately to each of a number of ids representing user ids or group ids. Upon request for access to the data by the user, the user id of the user and the group ids for which the user is a member are searched for within the entries to determine whether the user has the privileges to perform the operation requested against the objects. In addition, the access control policies are inherited from an object's superobject; resulting in a least privilege for the object (abstract).

- Hinsley et al. (US 5,295,266 A) discloses user roles a system has an associated user privilege set indicating the privileges granted to that role that may be selectively enabled or disabled by that role (column 2, lines 25-27).

- Corbin (US 5,138,712 A) discloses a software application that provides verification and license check out functions that are normally performed by a license server of a network software license system. The encrypted license information is contained in a license token, and is sorted in the database controlled by the license server (abstract).
- Weber (Digital Rights Management Technologies) discusses the general purpose and guiding framework with regard to DRM.

Any inquiry of a general nature or relating to the status of this application or concerning this communication or earlier communications from the Examiner should be directed to **James A. Reagan** whose telephone number is **571.272.6710.** The Examiner can normally be reached on Monday-Friday, 9:30am-5:00pm. If attempts to reach the examiner by telephone are unsuccessful, the Examiner's supervisor, **ANDREW J. FISCHER** can be reached at **571.272.6779**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://portal.uspto.gov/external/portal/pair . Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at **866.217.9197** (toll-free).

Any response to this action should be mailed to:

Commissioner of Patents and Trademarks

Washington, D.C. 20231

or faxed to **571-273-8300**.

Hand delivered responses should be brought to the **United States Patent and Trademark Office Customer Service Window**:

Randolph Building

401 Dulany Street

Alexandria, VA 22314.

JAMES A. REAGAN

Primary Examiner

Art Unit 3621

15 November 2006

JAMES A. REAGAN
PRIMARY EXAMINER

UNITED STATES PATENT AND TRADEMARK OFFICE

COMMISSIONER FOR PATENTS
UNITED STATES PATENT AND TRADEMARK OFFICE
WASHINGTON, D.C. 20231
www.uspto.gov

Bib Data Sheet

CONFIRMATION NO. 5128

SERIAL NUMBER	FILING DATE	CLASS	GROUP ART UNIT	ATTORNEY DOCKET NO.
10/015,951	12/17/2001 RULE	705	2161	111325-88

APPLICANTS

Mark J. Stefik, Portola Valley, CA;
Peter L.T. Pirolli, San Francisco, CA;

**** CONTINUING DATA ***************************

THIS APPLICATION IS A CON OF 09/778,001 02/07/2001
WHICH IS A DIV OF 08/967,084 11/10/1997 PAT 6,236,971
WHICH IS A CON OF 08/344,760 11/23/1994 ABN

**** FOREIGN APPLICATIONS *********************

IF REQUIRED, FOREIGN FILING LICENSE GRANTED
**** 01/10/2002**

		STATE OR COUNTRY	SHEETS DRAWING	TOTAL CLAIMS	INDEPENDENT CLAIMS
Foreign Priority claimed	☐ yes ☑ no	CA	13	34 30	4
35 USC 119 (a-d) conditions met	☐ yes ☑ no ☐ Met after Allowance				
Verified and Acknowledged	Examiner's Signature Initials				

ADDRESS

22204

TITLE

Digital works having usage rights and method for creating the same

FILING FEE RECEIVED		
1206	FEES: Authority has been given in Paper No. _____ to charge/credit DEPOSIT ACCOUNT No. _____ for following:	☐ All Fees ☐ 1.16 Fees (Filing) ☐ 1.17 Fees (Processing Ext. of time) ☐ 1.18 Fees (Issue) ☐ Other _____ ☐ Credit

Issue Classification	Application No.	Applicant(s)	
	10/015,951	STEFIK ET AL.	
	Examiner	Art Unit	
	James A. Reagan	3621	

ISSUE CLASSIFICATION

ORIGINAL CLASS	ORIGINAL SUBCLASS	CROSS REFERENCE(S) CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)						
705	51	705	52	53	54	55	56	57	58
INTERNATIONAL CLASSIFICATION		705	59	50					
G 06 Q	99/00	380	201						
H 04 K	1/00	707	9	104.1					
H 04 L	9/00	713	182	183	184	185	186		
	/								
	/								

****
****
(Assistant Examiner) (Date)

(Legal Instruments Examiner) 12/4/06 (Date)

JAMES A. REAGAN
15 November 2006
(Primary Examiner) (Date)

Total Claims Allowed: 38

O.G. Print Claim(s)	O.G. Print Fig.
1	1

☐ Claims renumbered in the same order as presented by applicant ☐ CPA ☒ T.D. ☐ R.1.47

Final	Original	Final	Original	Final	Original	Final	Original	Final	Original	Final	Original
1	1	34	31		61		91		121		151		181
2	2	35	32		62		92		122		152		182
3	3	36	33		63		93		123		153		183
4	4	37	34		64		94		124		154		184
7	5	11	35		65		95		125		155		185
8	6	22	36		66		96		126		156		186
6	7	29	37		67		97		127		157		187
5	8	38	38		68		98		128		158		188
9	9		39		69		99		129		159		189
10	10		40		70		100		130		160		190
12	11		41		71		101		131		161		191
13	12		42		72		102		132		162		192
14	13		43		73		103		133		163		193
15	14		44		74		104		134		164		194
16	15		45		75		105		135		165		195
17	16		46		76		106		136		166		196
18	17		47		77		107		137		167		197
20	18		48		78		108		138		168		198
21	19		49		79		109		139		169		199
19	20		50		80		110		140		170		200
23	21		51		81		111		141		171		201
24	22		52		82		112		142		172		202
25	23		53		83		113		143		173		203
26	24		54		84		114		144		174		204
27	25		55		85		115		145		175		205
28	26		56		86		116		146		176		206
30	27		57		87		117		147		177		207
31	28		58		88		118		148		178		208
32	29		59		89		119		149		179		209
33	30		60		90		120		150		180		210

Petitioner Apple Inc. - Exhibit 1012, p. 1996

Digital Rights Management Technologies

October, 1995

Prepared for:

Joseph S. Alen, Chairman

Committee On New Technologies

International Federation of Reproduction Rights Organizations

c/o Copyright Clearance Center

222 Rosewood Drive

Danvers, MA 01923

U.S.A.

Voice: (508) 750-8400

Fax: (508) 750-4343

E-mail: jalen@copyright.com

Web: http://www.copyright.com

Prepared by:

Dr. Robert Weber Principal Northeast Consulting Resources, Inc. One Liberty Square, 11th Floor Boston, MA 02109-4825 U.S.A. Voice: (617) 654-0621 FAX: (617) 654-0654 E-mail: weber@ncri.com Web: http://www.ncri.com

Table of Contents

---

1. INTRODUCTION

This year marks the emergence of a growing consensus that technology will provide new opportunities to proactively manage copyrights and permissions and to protect copyright for all kinds of digital content. Indicators of this growing consensus include:

* The number of companies who have said they are developing rights protection technologies or services has grown substantially;

* Working with vendors and clearinghouses to establish major standards for content control and rights management.

The Appendix (Chapter 5) provides brief overviews of the relevant vendors and their respective technologies.

2. TECHNOLOGY MODELS

This chapter identifies models of rights protection and rights management technologies. Each model describes the technology, characterizes its advantages and limitations, and identifies the leading suppliers of the technology. Some of the technologies described here support features of two or more models even though we have characterized them as implementing a single model. And again, more detailed discussions of specific vendors can be found in the Appendix (Chapter 5) to this report.

Neither this overview of rights protection and rights management technology models nor the vendor descriptions in the Appendix are exhaustive. Some who have spoken with us prefer to remain unacknowledged in this report. And we're sure we inadvertently missed a few new companies that have not wanted to attract attention just now. Finally, there are undoubtedly large technology companies working on rights management who have not yet come forward. Notwithstanding these limitations, this chapter is likely to cover most, if not all, important models for rights protection and rights management now being discussed in the American market.

2.1 Secure Delivery

The simplest form of rights protection involves the secure delivery of content from seller to buyer over the Internet. The simplest level of protection eliminates the possibility that a third party can obtain the digital content in a usable form by monitoring the transmission of that content from seller to buyer. For example, a sophisticated student might be able to intercept Internet traffic between the bookstore and a publisher and, thereby, obtain an electronic copy of an article or book chapter that would have been sold by the bookstore. Many solutions to this kind of problem are now in the marketplace. To illustrate, we give a World Wide Web example.

A number of vendors of World Wide Web browser and server software have incorporated methods for encrypting all communications between a buyer and seller in a given "session." The encryption keys are typically changed from one session to the next. In this approach, information, such as credit card numbers, expiration dates, ordering information, and the delivery of the content itself are encrypted prior to transmission. Even if someone is monitoring the network traffic, they cannot obtain either the digital content or credit card numbers in the clear because they cannot obtain the session keys.

At present, there are two competing standards, and there is agreement among those involved to rationalize the two approaches and create a single, unified standard. The first standard is known as Secure HTTP (HTTP being the underlying standard of the World Wide Web) developed by Enterprise Integration Technologies and CommerceNet. The second standard is known as Secure Socket Layer (SSL) that was developed by Netscape, the market leader in Web browser software. Backed by several interested parties, Terisa Systems will create a single, rationalized standard.

The export version of Netscape with short encryption keys has recently been broken by three different groups. However, the American version with much longer keys remains secure from attack for some time to come. Netscape is working to correct these deficiencies.

2.2 Secure Vending Machines

A number of vendors, including AT&T, CD-MAX, InfoSafe Systems, Spyrus, Inc., and Wave Systems, make

and PCs, are evolving to become services distributed in the network. Thus, search, rights management, security, billing, and payment are likely to become common services distributed in the network, rather than having devices as the important focal point. This means that the interfaces to these services reside in PCs, but the services themselves are delivered through the network.

2.4 Secure Software Containers

EPR continues to be the leader in bringing secure software container technology to market. Their complete InterTrust model includes the same hardware-based security protections found in other models, but they go beyond others in two important respects. They have developed secure software containers or envelopes that provide a substantial degree of security for any kind of digital content. Although less secure than their own or others' hardware based models, the EPR "DigiBox" container technology provides good security for all, but, perhaps, the most expensive content. The DigiBox and related system elements were designed so that it would take an effort substantially disproportionate to the value of the content to break a container. Second, the DigiBox is engineered so that even if one were able to compromise a particular container, the larger InterTrust system would not be compromised.

A second important feature of InterTrust technology is that these secure software containers can be sent from one computer to another over the network while maintaining the confidentiality and security of the digital property and rights and pricing control information. Thus, one customer can create new customers whose payments are credited to the appropriate rightsholders.

A third important feature of EPR's InterTrust is the ability for participants in the distribution chain to modify permissions and pricing information. This patented InterTrust capability is known as "chain of handling and control." Here is a simple example.

As an author, I convey an article to a publisher in a secure software container along with a set of permissions and pricing (royalty) information. To keep this example simple, I might require 50 cents each time the article is sold, prohibit exporting the article from the secure container, and authorize publishers to add to, but not negate the control information I've just created. The system has mechanisms for determining that a publisher, rather than a user, is trying to modify the control information.

Having established with InterTrust that either I'm a publisher or a particular publisher, I can now use the chain of handling and control mechanisms to increase the price to $1 each time the article is sold, with half coming back to me and half going to the author. I can, for example, also include this article in a digital anthology and impose the condition that subsequent users cannot include the article in a larger, encompassing digital work. In short, the chain of handling and control mechanisms enable secure information commerce all along the distribution chain from author to consumer. An extended example is presented in Section 3.5 of this report.

2.5 Other Models and Services

Not all relevant rights management technology and services falls into the preceding categories. Two of note are Folio's integration of rights protection and metering capabilities into their applications, and Copyright Clearance Center's announced program to provide digital rights and permissions clearinghouse services. Details of these efforts are discussed in the Appendix.

2.5.1 Application Integration

Folio Corporation has taken the clear lead in integrating metering capabilities in their line of information applications. They have announced relationships with several meter makers, including InfoSafe Systems, CD-MAX, Wave Systems, and Copyright Clearance Center for rights clearinghouse services. They are publishing a set of Application Program Interfaces (APIs) that allow meters from various vendors to exchange information with Folio

technologies.

3. MANAGING RIGHTS PROACTIVELY

Last year's report focused on "Metering Technologies For Digital Intellectual Property" and principally addressed copyright protection, counting, and charging for what could be counted. In the past year, the thinking of leading-edge rightsholder and technology companies has evolved to focus on proactively managing pre-approved rights and permissions.

In some segments of the copyright industries, rightsholders have wanted the ability to deny permission for uses deemed inappropriate or that may benefit one's competitor as much as oneself. While broad guidelines developed by each rightsholder often made specific decisions relatively easy, seeking and granting permissions became a labor-intensive activity in many publishing segments, most notably in book publishing. Individual permission request letters were processed one at a time. Royalties often varied depending upon use and by competitive implications, if any.

Last year at this time, rights management technologies were the province of a few small start-ups, some with real products, some with great ideas in search of partners and customers. That at least some technologies will prevail in the marketplace seems assured. Chapter 3 addresses emerging key issues, specifically, how might rightsholders:

* Think about technology standards?

* Manage rights proactively, rather than to just protect rights?

* Utilize the services of a rights and permissions clearinghouse on the net?

* Distribute content and convey rights and prices to other distribution chain participants?

3.1 Standards For Rights Management

Each of the rights management technology vendors would very much like to have their technology become a prevailing standard. Being a standard means that the technology is widely available on personal computers and is used by many large publishers and information distributors. In short, there is wide agreement on which rights management technology to use, how it will be used, and the benefits of this technology to information creators, publishers, distributors, and information consumers.

It is not necessarily the case that the best technology becomes the widely accepted standard. The triumph in the US of VHS over technologically superior Beta format for home video players is a well-known example. It's worth noting that the recent agreement by Philips, Sony, and others on a single new standard for CDs reflect increasing sophistication around standards issues. Rather than fragment the market into warring camps, they preferred a single standard. The rising tide will raise all boats.

Some companies may do well as big players in important niches. Companies like InfoSafe Systems, CD-MAX, and Spyrus may profitably exploit the CD-ROM niche. CDs are inexpensive and convenient ways to distribute and dispense a broad range of information. The coming high performance, high capacity (about 5 gigabytes) CDs that support both music, video, and other types of data will undoubtedly create expanded opportunities for those focused on physical distribution media.

However, at least in developed and many developing countries, information distribution is highly likely to be based

"stored value" (money stored in "purses" on the user computer or smart card), debit cards related to bank accounts, and EDI (Electronic Data Interchange) transactions for business to business purchases and payments.

6. Secure Delivery Of Content. Content in any digital form is delivered from the information distributor only to the authorized customer. Others cannot gain useful access to the content merely by copying the network transmission.

7. Secure Redistribution of Content. If one person desires to send a copy of the digital content to another, this redistribution should also be as secure as the original distribution to the initial customer. Also, the recipient should be able to pay for use and be subjected to the same restrictions as the initial customer.

8. Persistent Control of Content. There are always limitations to rights management and content control technologies. Nothing will prevent someone from scanning a printed page of a protected document (although fingerprinting or digital watermarking techniques may make it easier to trace and prosecute such infringements). Still, the best rights management technologies will be capable of protecting digital content after it is delivered to the customer and regardless of redistribution.

9. Control and Metering of Nested Objects. Many rightsholders believe it will be important to keep track of the individual objects that comprise larger ones. Multimedia products usually consist of content within content: an image and sound clip within an instructional module, for example.

10. Wide Range of Granularity of Metered Objects. Some observers have suggested that it will be desirable to meter content consisting of a few bits or a few characters. Many objects will be very large, a digitized film clip for example. Others will be very small, a sentence or two from another document. It will be important to find the right balance between practicality and rights management.

11. Rights Modification Along The Distribution Chain. The information industry consists of several different roles: author, publisher, aggregator, and repackager (and of course, customer). Technology for content control and metered usage should allow each of the different players to modify appropriately the permissions and pricing as the "chunk" of content moves from one to the next and as value is added.

12. Strong System Security. The rights management technology should be very difficult to "crack" or compromise. In addition, if it is compromised, the result of the attack should be the compromise of a particular piece of content destined for a particular customer, rather than the compromise of the rights management system as a whole.

Widely deployed technologies that enable these capabilities will provide options for new business models for authors, publishers, aggregators (like Dialog, Lexis-Nexis, AOL, Prodigy, CompuServe, etc.), and repackagers (like Individual, Hoover, Profound, etc.). Besides the enabling rights management technologies, another critical prerequisite is that rightsholders manage rights proactively.

3.2 Proactive Rights Management

Burgeoning markets for digital content of all kinds will force changes in the ways that authors, publishers, and other rightsholders deal with rights and permissions. Many publishers have still not yet rationalized their management of rights and permissions. Specifically, rightsholders should consider:

* Building internal rights management database applications

* Standard contract terms for electronic rights

* Anticipating the evolution to new, additional pricing models

* Aggressively instituting pre-approved permissions

forward copies of the property. In both circumstances the rights protection and management system protects the content. Let's assume that Alice sends Bill a market research report, music, or video clip in a cryptographic envelope that also contains pricing and rights information. Let's also assume that Bill has the appropriate envelope opening software on his PC. When Bill begins to open the envelope, the software will inform him of the price and of the relevant permissions. Or, we may assume that Bill has set some system defaults so that if the price is less than or equal to a specified amount, and if a minimal set of usage rights are conveyed, the system will allow him to open and, thereby, automatically agree to the rightsholder's prices and permissions. These scenarios assume that Bill has sufficient credit or funds stored on his PC or that the system can get his credit or charge card transaction approved.

The rightsholder may not have known immediately that the first buyer was, in fact, Alice and would not know that the second buyer was Bill until after the transaction was consummated. It is in this sense, that the business and rights relationships are ad hoc, rather than formal.

Automated rights clearinghouses play an important role in a fully deployed, best of breed rights management system. The next section examines their function.

3.3 Rights and Permissions Clearinghouse Services

As noted earlier, some rightsholders will create their own automated clearinghouses, but many are likely to leverage important economies of scale by outsourcing this function to a specialist organization. Copyright Clearance Center has announced their intention to provide automated clearinghouse services in support of several rights management technologies. This section briefly explains rights clearinghouse services and some of the issues that rightsholders should consider as rights management technologies become more widely deployed.

In support of advanced metering technologies, two kinds of clearinghouses may exist on the Internet and other large networks:

* A Financial Clearinghouse. The interface between systems for rights management and metered usage and the various financial services systems such as those for credit, debit, and stored value plus financial EDI transactions.

* A Rights and Permissions Clearinghouse (RPCH) The interface between systems for rights management and metered usage and authors, publishers and other rightsholders.

To help understand what an RPCH actually does, it is useful to distinguish between a rights template and a particular rights model. A rights template indicates what rights might be conveyed by the rightsholder; a particular rights model indicates for a particular piece of information which of the possible rights are being conveyed and which are being withheld. Every rights model incorporates a particular rights template. Example 1 presents a rights template and rights model for a particular hypothetical feature news story.

Example 1. Combined Rights Template and Rights Model For Particular Hypothetical Feature News Story

Transaction	Permission	Comments
Viewing title	Granted	
Viewing abstract	Granted	
Viewing article	Granted conditionally	after payment
Modifying abstract	Prohibited	
Modifying article	Prohibited	
Printing abstract	Granted	
Printing article	Granted conditionally	after payment
Cut and paste, excerpting	Prohibited	
Exporting from envelope	Prohibited	

A similar distinction can be made between "pricing templates" and "pricing models." A "pricing template" indicates

		or modify information (headlines, dates, copyright notice, on-line service branding, etc.)
Repackager (e.g., newsletter or current awareness products)	Repackager gets articles from on-line service and creates new electronic publication from several objects, and modifies pricing, rights, and other control set information. Note that royalties must be returned to the rightsholders for each of the constituent objects in addition to individual receiving its own royalties	Controls could prevent disaggregation of the digital newsletter into its constituent objects for example
Corporate info. server (Fortune 1000 company)	Objects are stored in corporate information base where people within the company can search/browse, download, etc.	Usage information could be aggregated on corporate information server
User	In conjunction with container opener and metering system, transactions are enabled, metered, and paid for	A variety of pricing models and payment methods can be enforced
Other User Outside Company	First user sends encrypted container and content to another user in another company. The metering system on that user's machine must be able to eventually reach a financial and rights clearinghouse	The object needs to phone home to establish payment and verify rights

The rights clearinghouse system will be able to receive, store, aggregate, and report usage information to rightsholders. The frequency of reporting and the level of data aggregation, by person, company, industry, etc., remains to be determined by rightsholders and CCC.

The rights and pricing templates described above are a subset of the information required by various content control and metering systems. Depending on market demand and acceptance, we expect the CCC clearinghouse to supply clearinghouse services through several different rights management technologies.

4. NEXT YEAR: WHAT MATTERS?

In the year ahead, rightsholders might want to pay attention to: (1) fixing internal policies, contracts, and systems for rights management. (2) participating in the various "betas" that will be announced in order to experiment with different rights and pricing models; and (3) working with vendors and clearinghouses to establish one (or two) major standards for content control and rights management. We address each of these in turn.

4.1 Fixing Internal Systems

Advanced technologies provide fine-grained capabilities for copyright control and rights management. The discussion in Section 3.3 of pricing and rights templates and models gives an overview of the level of detail incorporated in emerging technologies and clearinghouse services. To be an active participant, publishers and other rightsholders will have to make important changes in policies, contracts, and internal systems for rights management. It continues to be the case, we believe, that most large publishing houses have not modified their standard contracts and agreements to take into account the expanded range of pricing, rights, and permissions options that will become available over the

generally. For example, the AT&T announcement mentions a broad range of information vending and electronic commerce applications, including video-on-demand, electronic publishing, electronic news and alerting services, software distribution, computer program license control, program execution metering, home shopping, remote gaming, bank-at-home service, electronic contracting, etc.

Table 5.1: IVES Supported Security Services

Security Service	Description
(SSI) Security Service Interface	Calls that access IVES services
Secure network communications protocols	Means for secure messaging across a network, including secure addressing
Security applications protocols	Application-dependent protocols, such as methods for dispensing entitlements for the service IVES is supporting
Authentication protocols	Methods for securely and reliably identifying system entities
Key management	Cryptographic key generation, distribution, and maintenance methods supporting the various security functions
Local, off-chip memory protection mechanisms	Capabilities for storing valuable information, including digital cash balances in security containers of arbitrary size, off-chip
Security kernel	Atomic security services that cannot be interrupted or interfered with
Physical layer security	Silicon-layer anti-tamper, memory protection, bus isolation, etc.

While technical details of the IVES architecture have not yet been made public, IVES appears to be a well thought out cryptographic key management system based on a secure co-processor, the RSA public key crypto system for user and device authentication and secure secret key exchange, and triple DES for content encryption/decryption.

The IVES system is based on a security co-processor manufactured for AT&T by VLSI Technology. The chips include tamper resistant memory, a 32-bit RISC processor, support for any of the standard interfaces (PCMCIA, ISA, 16550 serial, and others), a security kernel in masked ROM, a hardware randomizer, a high-speed Triple-DES processor with key cache, and a variety of non-security applications ranging from data and audio compression to communications protocols.

Devices that, in principle, can incorporate IVES chip technology range from personal computers in homes or businesses, servers, settop boxes, video game players, off-track betting machines. Once incorporated in the business or home customer device, the IVES chip supports several security services. APIs that developers can write to will be published later this year.

The IVES architecture encompasses a sophisticated lock/unlock content control system. Figure 5.1 shows a schematic view of IVES system functions. Digital content is first encrypted with a triple DES key and stored on a content server that might be another computer or static storage device such as a CD-ROM. The content and the entitlement to use that content can be stored and transmitted separately. Encrypted content can be stored anywhere on a public or private network. The content may be any digital data ranging from software to business information to video clips to feature length movies.

Commercial availability is expected in late 1995 or early 1996.

Wave Systems' CEO Peter Sprague and InfoSafe Systems' CEO Thomas Lipscomb have been granted one relevant patent. The status of other Wave patents is unknown.

Wave Systems has entered into a number of alliances and created a number of new services based on WaveMeter and WaveNet:

* Folio Corporation. In March, 1995, Wave Systems announced support for Folio's Metering Applications Programming Interface. The $API provides an interface between the WaveMeter and Folio's applications.

* VLSI Technology. Wave and VLSI announced a strategic licensing agreement in March, 1995. The two firms will collaborate on the design and manufacture of Wave-enabled encryption chips for targeted markets such as electronic commerce.

* Wave Interactive Network. In August, 1995, Wave Systems announced formation of a new subsidiary company, Wave Interactive Network (WIN), that will provide pay-per-use multimedia to the consumer market.

* Network News Corporation. In August, 1995, Wave Systems announced formation of Network News Corporation to provide secure satellite delivery of news and information to the corporate desktop for sale by the story. Network News will deliver content via satellite using Hughes Network Systems' new DirecPC service, and Wave's patented metering technologies. Announced content partners include Knight Ridder/Tribune Business News, PR *Newswire*, and Businesswire.

WSC claims to have received permission from the Department of Commerce to export the WaveMeter to all non-communist countries. (This is because the user cannot control the encryption keys or the operation of the WaveMeter device; hence the WaveMeter cannot be used to encrypt data.)

5.2 Hardware Container Models

5.2.1 Xerox PARC

A team at Xerox is building rights management technology based on research at the Xerox Palo Alto Research Center. The approach lends itself to a range of implementations for different kinds of digital works, different security requirements, and different transaction costs. A key to the approach is a usage rights language, which describes rights and fees associated with particular uses of a digital work. Rights and fees are determined by authors and publishers, described in the rights language, and attached to a digital work. (Contact: Bettie Steiger, Principal, Technology and Market Development, Xerox PARC, 3333 Coyote Hill Road, Palo Alto, CA 94304, Voice: 415-812-4072; Fax: 415-812-4274; Mark Stefik, Principal Scientist, Xerox PARC, 3333 Coyote Hill Road, Palo Alto, CA 94304, Voice: 415-812-4366; Fax: 415-812-4241.)

The basic idea is that rights and fees for a digital work are written in a machine-readable language and subsequently enforced by hardware and software for using the digital work. There are distinct categories of rights for such uses as playing (or displaying), printing, copying, loaning, and transferring, as well as rights related to the making of derivative works and making and restoring backup copies. Any given right on a digital work can be governed by required digital licenses or prepaid via digital tickets. Payment for usage of a digital work is handled via secure transactions, by realtime or periodic connections with an on-line financial clearinghouse.

Different digital works have different requirements for security. At the low end are standard personal computer systems with software for handling the encryption. At the high end are trusted systems with tamper-resistant hardware. In the middle are trusted systems that have co-processors for encryption and protected storage for keys and

information use, but offers a basis for a complete solution to secure ad hoc commerce transactions in a networked environment. Unlike the other technologies mentioned in this report, EPR's system provides for the persistent, on-going control, authorization, billing, and metering of digital information without having to integrate the EPR system into each and every application being used to access the protected information.

EPR's business model is based on a tiny part of each transaction fee collected at clearinghouses plus licensing fees from computer companies and software tool and operating system companies.

EPR is negotiating agreements with major companies to provide critical parts of the distribution chain, and major announcements are expected by the end of 1995. EPR has announced a strategic alliance with Copyright Clearance Center who will provide rights and permissions clearinghouse services.

Victor Shear has four granted patents involving content control and metering technologies. Extensive other patent materials are currently pending.

EPR does not yet have an export license for InterTrust, but believes there are no significant obstacles in creating an exportable version.

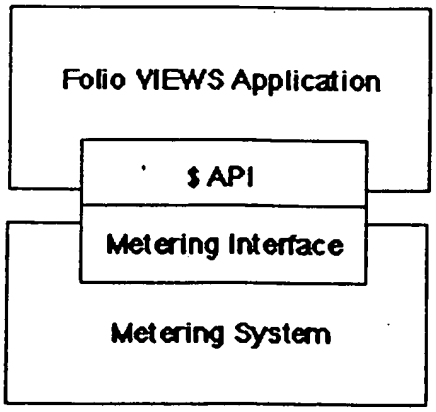
5.4 Metering Aware Applications

5.4.1 Folio Corporation

Folio Corporation, a division of Reed Elsevier plc, (Contact: Curt Allen, Executive Vice President, Folio Corporation, 5072 North Information Way (300W), Provo, UT 84604. Voice: 801-229-6700; Fax: 801-229-6785. Web home page. Folio develops and markets information base applications (infobases) worldwide. In use on more than 30 million desktops in the form of Folio VIEWSreg., on-line help for various software products and as a delivery mechanism for some 2,000 electronic titles from nearly 500 commercial publishers.

Among applications developers, Folio has taken a significant leadership position regarding the integration of metering and rights management technologies into their end user and server applications. They are adding to their applications and server software code that either tracks certain kinds of usage or that limits certain kinds of operations. An example of the former is the ability to count the number of times a document was opened, which pages were viewed on the screen, and how many pages were printed. An example of the latter is prohibiting modification of the document.

To leverage its core competency in user applications and server software, they have created a general interface, an Applications Programming Interface (API), that can be used by any maker of rights management and usage metering software. To use the API, any of Folio's metering partners would write new software that was the interface between the application and the meter.



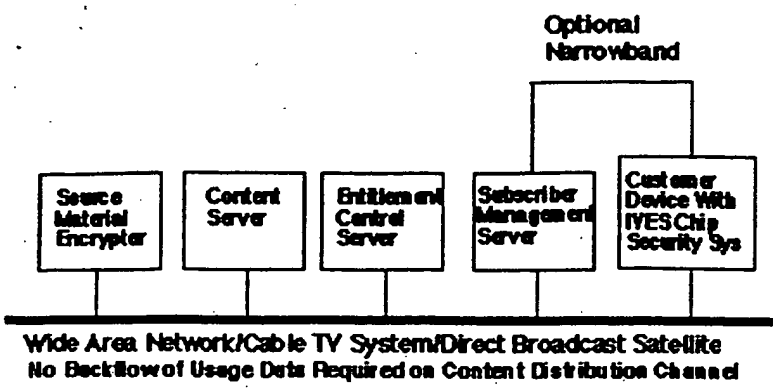


Figure 5.1. Schematic Representation of General IVES Architecture

The decryption key is stored on an "entitlement" control server. Entitlements are marketed on the network. When a customer purchases an entitlement for a specific piece of content, the entitlement is addressed to a specific device or set of devices designated by the customer.

The architecture also envisions a subscriber management server and applications that can respond to requests to purchase entitlements and see that the appropriate entitlements are distributed to the correct customer device or devices. The administrative system also handles billing and financial transactions.

Having purchased an entitlement for a particular piece of digital content, the user's system decrypts the content with the keys associated with the entitlement. As in other lock/unlock systems, once the content is paid for, no further protection is provided by the system. It appears, for example, that the user could record a video program for subsequent playback or redistribute the unencrypted content over networks or other media.

Supported payment systems include count-down and count-up credit. In the former, the user pre-pays some amount into an account. The system debits the account as usage occurs. In the latter, credit is authorized up to a specified amount and usage charges accumulated until that amount is reached. In either case, when the account is exhausted or the credit limit reached, no further entitlements will be dispensed. Credit information can be stored either on the customer device or on a server or both.

No further information is available at this time regarding AT&T's patent position, business model, exportability, or position on customer privacy issues.

5.1.2 CD-MAX, Inc.

CD-MAX, Inc. is a wholly owned subsidiary of InfoServe, Inc. with principal offices in New Jersey (219 South Street, Suite 203, Murray Hill, NJ 07974-2100, voice: (908) 771-0022, fax: (908) 771-0444, contact: David B. Boelio, Executive Vice President, Marketing, (908) 464-1878). Their chief business activities are copyright protection and usage billing services to information providers based on patented technology.

CD-MAX's approach to controlling content and metering begins with encrypting the content during development of the information base and before the CD-ROM is manufactured. CD-MAX provides a security program that is installed on the customer's PC. This security program transparently decrypts the information on the CD-ROM as it is accessed by the customer. DOS and Windows versions of the system have been delivered to client publishers. MAC and UNIX versions will be developed in response to demand.

Selected files on the CD-ROM is marked with a security code and the contents is encrypted with a proprietary encryption algorithm. This encryption method was designed especially for the PC environment. CD-MAX claims that the computing overhead for decryption is minimal and is not apparent to the user.

According to CD-MAX, their security, metering, and billing solutions are media-independent and multi-platform in their design. While CD-ROM and local area networks have been their first priority, they intend to demonstrate in the near future CD-MAX's ability to operate effectively in wide area networks, including the Internet.

CD-MAX, Inc. claims protection, in part, from at least four patents granted and applied for by Dr. John David Wiedemer, a founder of the company.

CD-MAX's business model is based on performing clearinghouse functions for billing and taking a small fee for handling each billing transaction. Details of pricing and other financial information were not available.

Since last year, CD-MAX has entered into a number of strategic alliances:

* Folio. In March, 1995, CD-MAX announced that it has been designated a Technology Partner by Folio Corporation. The relationship plans to incorporate CD-MAX technology with Folio Metering Application Programming Interface and Folio VIEWSreg. software.

* Mitchell International. In June, 1995, CD-MAX announced that Mitchell International will include CD-MAX's copyright and billing technology in Mitchell's new version of Mitchell On-Demand(TM) Repair Information System product line. 10,000 service stations and dealerships presently use this product line. The new version of Metered On-Demand was released in August, 1995.

* Disclosure. In August, 1995, CD-MAX and Disclosure, Inc. announced an alliance to produce a metered product entitled, "Metered New Issues Database." The product is expected to be released in September, 1995. Disclosure has plans to use CD-MAX's technology to offer new customers a free trial of the database while also using CD-MAX's technology to register, track information usage and bill customers. Reporting is planned to be completed via modem or mailing in a disk.

Regarding user privacy issues, CD-MAX endorses the Information Industry Association's "Fair Information Practices Guidelines" and has implemented procedures and policies to ensure security and privacy. The exact nature of these procedures and policies has remained confidential.

5.1.3 Infosafe Systems, Inc.

Infosafe Systems, Inc. offers a hardware-based system for protecting and metering information (Contact: Thomas H. Lipscomb, President, Infosafe Systems, Inc., 342 Madison Avenue, Suite 622, New York, NY 10173, Voice: 212-867-7200; Fax: 212-867-7227. Web home page.

Their technology is proprietary and employs both hardware and software. An external "box," the Infosafe-Mark III, is connected via an SCSI interface (Small Computer System Interface) to either an individual's computer, or to a server machine capable of supporting several users. Presently supported are Macintosh and Intel Architecture computers (DOS, Windows). Infosafe provides software to run on the subscriber's computer; no modifications are required to the operating system that runs the subscriber's computer.

Prior to delivery to the customer, the publisher/rightsholder identifies appropriate chunks of information such as articles, paragraphs, images, and the like that would constitute a basic "packet" of information that could be priced and charged for separately. Typically, the publisher also creates a separate abstract and/or index for each packet. As part of the production process, each packet is assigned a separate encryption key, encrypted, and put on the CD-ROM or other delivery media together with the un-encrypted and hence, searchable, abstracts and indices. Packets may be of any size, including a single graph, photograph, article, paragraph, typeface, word, statistic, or data-point.

In a typical application, the user browses the abstracts or search results at no charge and is informed of the costs

monitoring subscriber usage information, conveying electronic information regarding credit balances and requests between the subscriber and publisher, and coordinating management of publisher mailings and processing of bills; and (4) market support services, which involve frequent communications between Infosafe Systems, Inc. and the publisher to assist the publisher in realizing the maximum return on their investment in the Infosafe system. Based on information returned from the metering device, publishers can analyze usage information to yield marketing information showing patterns of use. This allows rightsholders to re-configure or update products or change prices, either universally or at specific locations, using the memory storage available in each Mark III.

While Infosafe can perform clearinghouse operations, the Mark III is compatible with each publisher or their delegated agent performing clearinghouse functions. Infosafe's business model appears to be based on receiving a portion of the publisher's revenue stream from the protected data.

Additionally, Infosafe works with its clients to design, configure, and sell digital streams of information delivered through the Mark III. It charges a fee for initial configuration and software design and takes a portion of the publisher's revenue from the data it protects and delivers through the system. The size of the initial fee varies and depends, in part, on the extent of revenue sharing going forward. No detailed pricing information was made available by Infosafe.

One patent has been granted to Robert Nagel (InfoSafe Chief Scientist) and Thomas Lipscomb (CEO). At least one other is pending. In addition, Lipscomb and Peter Sprague (Wave Systems' CEO) have been granted a relevant patent.

In the past year, InfoSafe has entered into a number of strategic alliances and made one acquisition:

* Folio. In March, 1995, Folio Corporation, a division of Reed-Elsevier, announced Infosafe as a key supplier for its new Folio Metering API (application programming interface). Folio Corporation is a leading provider of infobase software with products installed on an estimated 30 million desktops in the form of Folio VIEWSreg., on-line help for various software products, and as the delivery mechanism for some 2,000 electronic titles from nearly 500 commercial publishers.

* Design Palette(TM). InfoSafe has branched out from being a supplier of copyright protection systems to a provider of content. In April, 1995, Infosafe Systems, Inc. announced that it purchased Design Palette from one of its largest customers, International Typeface Corporation (ITC). The vendor relationship between Infosafe and ITC will continue. ITC will remain responsible for managing 25 vendors' content for a 40 plus CD-ROM library. Vendors include PhotoDics, AGFA, Adobe and Letraset.

* Copyright Clearance Center. In August, 1995, InfoSafe Systems and Copyright Clearance Center announced they will work together to develop fully secure, auditable and interactive digital clearance for copyrighted materials.

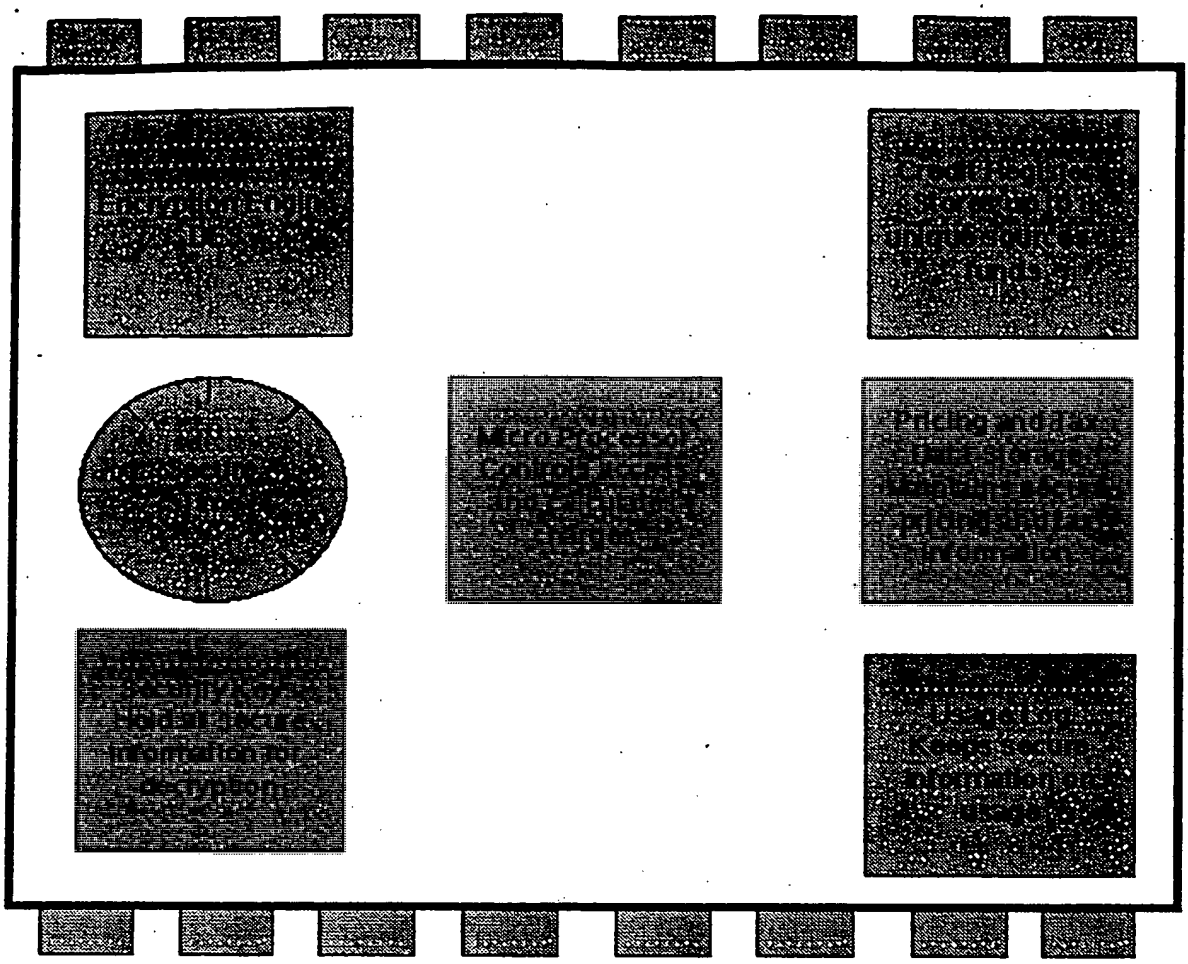
InfoSafe has applied for, but not yet been granted, an export license by the Department of Commerce for the Mark III.

5.1.4 Spyrus, Inc.

Spyrus, Inc. is a small designer and implementor of strong security systems based on cryptography that is well-respected in the cryptography and security communities. (Contact: Sue Pontius, CEO, Spyrus, Inc., 2841 Junction Ave., Suite 110, San Jose, CA 95134, Voice: 408-432-8180; Fax: 408-432-8415). For example, they are among the leaders in security tokens on PCMCIA cards that authenticate individuals to various security systems.

Spryus has brought to market a third party software developer's kit (SDK) for content protection and usage metering. The SDK implements strong cryptographic methods for secure communications between publishers and users and between users and data bases principally on CD-ROM.

Spyrus does not itself develop the complete metering application, but instead relies on third party partners.



BEST AVAILABLE COPY

Figure 5.5 WaveMeter Functional Schematic

Data Preparation. In preparing the information to be protected by the Wave System, the publisher performs four basic tasks. First, the publisher defines logical groupings of information that can be purchased as a single item. This might be an article, a page, an entire volume or database, and so on. Next, the publisher sets the pricing for each logical unit of information, such as an article and what is called the "pricing factor," for each database. The "pricing factor" is a multiplier to be applied against the prices set for each unit in the database. Pricing factors can be changed over time by the publisher. WSC provides a publisher interface to WaveNet for this purpose. The third data preparation step is to define abstracts and keywords. Wave System stores information in packets that have an encrypted part and a "clear" area in which publishers typically put abstracts and keywords that can be searched easily. The fourth and final step consists of encrypting the information to be protected. The encryption is fully automated and represents no burden to the publisher. Wave uses the Data Encryption Standard (DES).

Information Delivery. Once encrypted, the information can be delivered to customer locations by a variety of means. Early implementations of Wave System will be CD-ROM based. Later versions are expected to use Wide Area Networks, such as the Internet, satellite, or sideband FM radio broadcasting (combining text information with FM radio broadcasts that don't interfere with the primary content of the broadcast).

Search and Retrieval Applications. WSC does not provide its own search and retrieval or other end-user applications. Instead, WSC provides what are known as Application Programming Interfaces (APIs) that define how software developers can incorporate WaveMeter functions in their applications.

WaveNet is comprised of all the "back office" data communications and information processing systems. The way to think about WaveNet is as a transaction processing system for electronic commerce. Each transaction is initiated by the user through the WaveMeter over dial-up lines to WaveNet. Each call results in one of four types of transactions:

payment, usage reporting, and new or additional permissions.

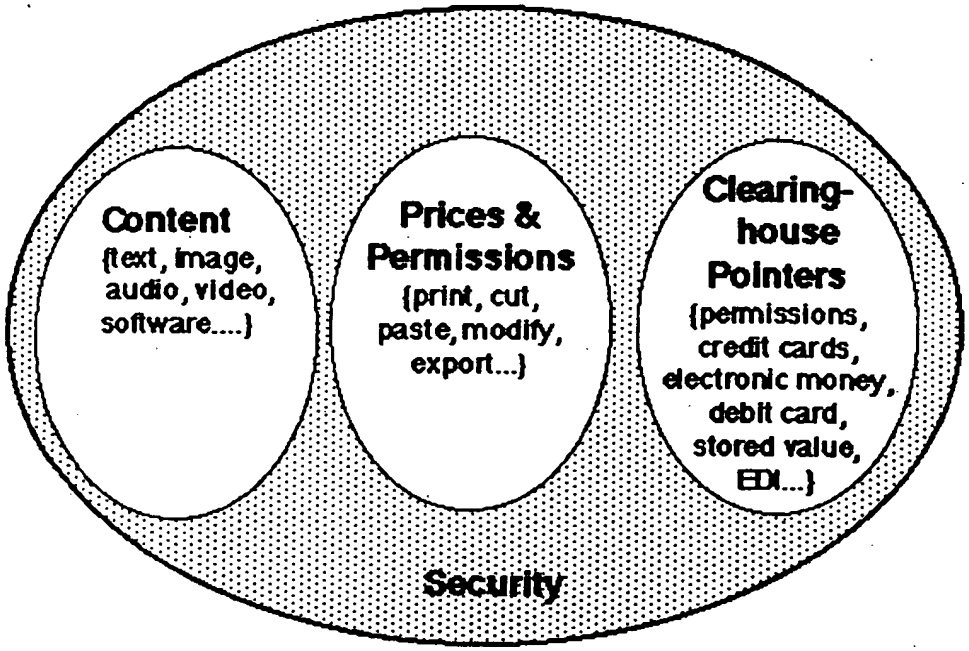


Figure 5.7. EPR DigiBox Container Schematic

Figure 5.9. Schematic View of Folio $ API

Figure 5.9 presents a schematic representation of the $ API. Each of Folio's partners will create their own metering interface that will exchange rights management and usage information to the application by communicating with the $ API.

Thus far, Folio has announced strategic alliances with CD-MAX, Inc., InfoSafe Systems, and Wave Systems. Another alliance with Copyright Clearance Center for clearinghouse services has also been announced. Additional announcements are expected in late 1995 and early 1996.

No public information is available on Folio patents in this area.

Since encryption/decryption is likely to be performed by the metering systems, rather than by the Folio applications, there does not appear to be limitations on exportability of the Folio software.

5.5 Rights Clearinghouses

This section reports one American and one Canadian effort to create on-line rights clearinghouses.

In conjunction with the deployment of rights management technologies, some meter makers and some rightsholders may elect to operate their own on-line clearinghouses. In addition, there is likely to be one or more on-line clearinghouses that are not operated directly by meter makers or by any one publisher or other rightsholder organization. As noted in Chapter 3 of this report, Copyright Clearance Center will operate a vendor and publisher neutral clearinghouse.

In addition, a consortium of Canadian rights, technology, and academic organizations have put together the IVY Consortium to develop rights clearinghouse technologies.

5.5.1 Copyright Clearance Center

In support of several announced partnerships, Copyright Clearance Center (CCC) will provide rights and permissions clearinghouse services. (Contact: Kelly Frey, Director, New Business Development, Copyright Clearance Center, 222 Rosewood Drive, Danvers, MA 01923, Voice: 508-750-8400; Fax: 508-750-4343; E-mail: kellyfrey@copyright.com; Web Home Page. CCC's base business has been in the permissions and usage royalties for photocopying. They license on behalf of over 9,200 publishers who, in turn, represent hundreds of thousands of authors. For the past several years, CCC has instituted several new programs focused on permissions for digital content in the business and higher education markets. This brief section augments the discussion of rights and permissions clearinghouses in Chapter 3 of this report.

companies, schools and governments.

IVY was developed at York University, Toronto by CulTech Research Centre who partnered with Disus and SOCAN to bring IVY to commercial reality. Disus is a well known telecommunications software firm and SOCAN is Canada's largest copyright collective with more than $70 million annual income from music performances. Contact: Paul Hoffert, Executive Director, 4700 Keele Street, North York, Ontario, Canada M3J 1P3, Voice: 416-736-5405, Fax: 416-736-5404, Web Home Page; contact: Tom Jurenka, Director, Empirics/Disus, 47 Colborne Ave, Suite 303, Toronto, Ontario, Canada M5E 1P8; Voice: 416-417-7035, Fax: 416-461-8439.

According to Paul Hoffert, Director of CulTech, IVY is an intellectual property management and accounting system that incorporates:

* Intellectual property accounting software

* Trusted rights administration

* Accommodations for financial clearinghouses

* Interactive network and CD-ROM delivery

A simplified diagram of IVY's structure of rights administration is shown in Figure 5.11. There is both a financial clearinghouse to handle billing and payment and a separate agency - The IVY League - for rights clearings.

The owner licenses limited exploitation rights to a producer who licenses distributors, who in turn, license retailers who sell to users. The structure may be collapsed so that an owner may be a producer, distributor, and retailer or any other permutation of functions among the food chain categories. Owners and producers must enroll a work with the rights administration agency so that it may grant a license to the user.

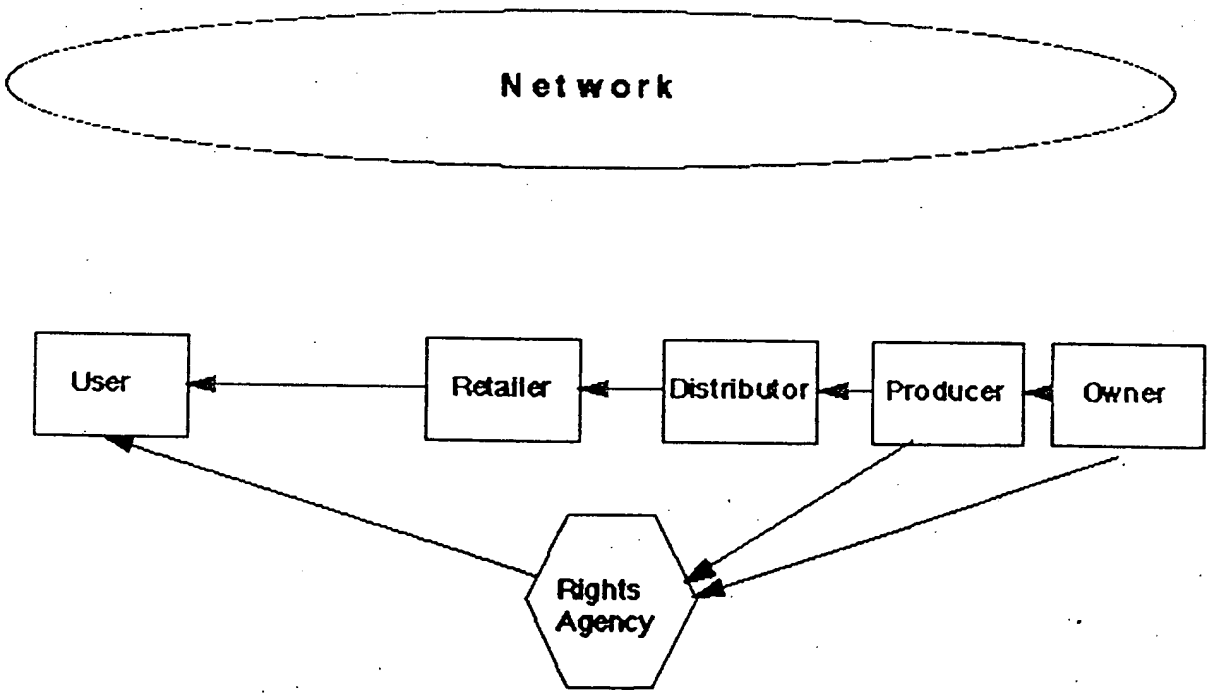


Figure 5.11. Typical Flow of Rights

At the same time, various distribution chain participants need to be authenticated: how do we know that the person claiming to be user "Laura-who-lives-on Maple-Street" is really the person she says she is. The authentication and security methods being implemented in IVY similar to the Kerberos system for security and authentication developed

Figure 5.13. The IVY Vision

The IVY effort is backed by several major technologies, telecommunications, and content companies. Although their initial focus is video-on-demand and other multimedia over broadband applications, the rights management issues IVY addresses are generic. Thus, their rights clearinghouse may service content distribution business other than video-on-demand.

The IVY group is less interested in developing new technologies than applying existing technologies to rights and financial clearinghouse activities.

IVY will likely be the first IP management system to go into regular operation with backing from a broad range of content collectives, network operators and users. No public information is yet available on the business models for their financial and rights clearinghouses.

PTO 04-3950

Japanese Patent

Document No. H03-282733

RULE GENERATION DEVICE FOR UTILIZING A SOFTWARE COMPONENT

[Sofutowea Buhin Riyo Ruru Seisei Sochi]

Mihoko Kishi and Koichi Kachi

UNITED STATES PATENT AND TRADEMARK OFFICE

Washington, D.C. June 2004

Translated by: Schreiber Translations, Inc.

Petitioner Apple Inc. - Exhibit 1012, p. 2015

Country	:	Japan
Document No.	:	H03-282733
Document Type	:	Kokai
Language	:	Japanese
Inventor	:	Mihoko Kishi and Koichi Kachi
Applicant	:	Toshiba Corp.
IPC	:	G 06 F 9/06
Application Date	:	December 12, 1991
Publication Date	:	March 30, 1990
Foreign Language Title	:	Sofutowea Buhin Riyo Ruru Seisei Sochi
English Title	:	RULE GENERATION DEVICE FOR UTILIZING A SOFTWARE COMPONENT

Petitioner Apple Inc. - Exhibit 1012, p. 2016

/1[1]

Specification

1. Title of the invention

Rule generation device for utilizing a software component

2. Patent Claim

A rule generation device for utilizing a software component characterized by the possession of

A component packaging mechanism designed to collect & package software components provided, in relation to the respective targets handled in a given field, for operating said targets,

An inter-component utility restriction scripting mechanism designed to script restrictions on the joint utilities of multiple software components within each component package generated by said component packaging mechanism,

An inter-package relationship definition mechanism designed to define the relationships among the respective component packages generated by the aforementioned component packaging mechanism, and

An inter-component utility restriction fusion mechanism designed to extract, from the script texts of the restrictions on the joint utilities of multiple software components within each component package scripted by the aforementioned inter-component utility restriction scripting mechanism, script portions on the software components actually utilized for program formulation and

[1] Numbers in the margin indicate pagination in the foreign text.

Petitioner Apple Inc. - Exhibit 1012, p. 2017

to generate, by fusing these script portions based on the relationships among the respective component packages defined by the aforementioned inter-package relationship definition mechanism, a restriction script text on the joint utilities of multiple software components actually utilized for the aforementioned program formulation.

3. Detailed explanation of the invention

(Objective of the invention)

(Industrial application fields)

The present invention concerns a rule generation device for utilizing a software component, which is used for verifying a program formulated by coupling software components.

(Prior art)

A program formulated in the prior art by coupling software components is verified based on any of the following methods:

<1>: After a program has been formulated by synthesizing components, it is verified in compliance with test specifications according to procedures comparable to those for verifying a program formulated by an ordinary method without recourse to component synthesis;

Petitioner Apple Inc. - Exhibit 1012, p. 2018

<2>: After a program has been formulated by synthesizing components, whether or not restrictive conditions on component utility are being satisfied is checked; /2

<3>: Restrictive conditions among the respective components are preliminarily defined, and whether or not such restrictive conditions are being satisfied by a given component is checked on an occasion for utilizing said component.

The respective methods listed above, however, are plagued with the following problems.

Despite the fact that a program has been formulated by means of component synthesis according to the method of <1>, the advantage of this history cannot be inherited by the test. In other words, despite the guaranteed reliability of each component, it is necessary to formulate, in a redundant manner, test specifications comparable to those of a program formulated without recourse to component synthesis.

The method of <2> is a test method that exploits the advantage of the component synthesis, for only the combination of components with guaranteed qualities needs to be checked, although it is difficult to automate the test in that it is cumbersome to formally script the entire relationships among large numbers of components.

The method of <3> is advantageous in the sense that a program with a high reliability can be formulated since the component synthesis is perpetually checked, although it is difficult to automate the test, as in the method of <2>.

Petitioner Apple Inc. - Exhibit 1012, p. 2019

(Problems to be solved by the invention)

Thus, it has been difficult to automate operations of the prior art for verifying programs formulated by means of component synthesis due to the cumbersomeness of formally scripting restrictions on the utilities among the entire components.

The objective of the present invention, which has been conceived for solving these problems, is to provide a rule generation device for utilizing a software component capable of automating program verifying operations.

(Constitution of the invention)

(Mechanism for solving the problems)

The rule generation device of the present invention for utilizing a software component possesses, for the purpose of achieving the aforementioned objective, a component packaging mechanism designed to collect & package software components provided, in relation to the respective targets handled in a given field, for operating said targets, an inter-component utility restriction scripting mechanism designed to script restrictions on the joint utilities of multiple software components within each component package generated by said component packaging mechanism, an inter-package relationship definition mechanism designed to define the relationships among the respective component packages generated by the aforementioned component packaging mechanism, and

Petitioner Apple Inc. - Exhibit 1012, p. 2020

an inter-component utility restriction fusion mechanism designed to extract, from the script texts of the restrictions on the joint utilities of multiple software components within each component package scripted by the aforementioned inter-component utility restriction scripting mechanism, script portions on the software components actually utilized for program formulation and to generate, by fusing these script portions based on the relationships among the respective component packages defined by the aforementioned inter-package relationship definition mechanism, a restriction script text on the joint utilities of multiple software components actually utilized for the aforementioned program formulation.

(Functions)

As far as the rule generation device of the present invention for utilizing a software component is concerned, software components for operating targets handled in a given field are collected & packaged by the component packaging mechanism in relation to the respective targets, whereas the relationships among the respective component packages are defined by the inter-package relationship definition mechanism, whereas restrictions on the joint utilities of multiple software components within each component package are scripted by the inter-component utility restriction scripting mechanism. The inter-component utility restriction fusion mechanism, furthermore, extracts, from the script texts of the restrictions on the joint utilities of

Petitioner Apple Inc. - Exhibit 1012, p. 2021

multiple software components within each component package scripted by the inter-component utility restriction scripting mechanism, script portions on the software components actually utilized for program formulation and generates, by fusing these script portions based on the relationships among the respective component packages defined by the inter-package relationship definition mechanism, a restriction script text on the joint utilities of multiple software components actually utilized for the aforementioned program formulation.

According to the present invention, therefore, it becomes possible to automatically formulate, by using a formal language, the restriction script texts on the joint utilities of multiple software components utilized for the aforementioned program formulation and, as a result, to automate the program verifying operation.

(Application examples)

In the following, an application example of the present invention will be explained with reference to figures.

Figure 1 is a block diagram provided for explaining the constitution of an application example of the rule generation device of the present invention for utilizing a software component. /3

In the same figure, (1) is a component packaging unit which collects & packages software components (hereafter referred to simply as "components") used for operating data that define

Petitioner Apple Inc. - Exhibit 1012, p. 2022

targets handled in a given field (i.e., application program) in relation to the respective targets.

(2) is an inter-component utility restriction scripting unit which scripts, by using a formal language, restrictions on the joint utilities of multiple components within each component package generated by the component packaging unit (1).

(3) is an inter-package relationship definition unit which defines the relationships among the respective component packages generated by the component packaging unit (1) [e.g., parent-offspring (is-a) relationship, etc.]. It should be noted that the relationships among targets hereby serve as the relationships among targets as they are.

(4) is an inter-component utility restriction fusion unit which extracts, from the script texts of the restrictions on the joint utilities of multiple software components within each component package scripted by the inter-component utility restriction scripting unit (2), script portions on the software components actually utilized for program formulation and generates, by fusing these script portions based on the relationships among the respective component packages defined by the inter-package relationship definition unit (3), a restriction script text on the joint utilities of multiple software components actually utilized for the aforementioned program formulation.

Next, the actions of the rule generation device for utilizing a software component characterized by the foregoing constitution

Petitioner Apple Inc. - Exhibit 1012, p. 2023

will be explained with reference mainly to Figure 2 as well as to Figures 3 through 7.

First, the component packaging unit (1) extracts targets handled in a given field, whereas the relationships among the respective component packages are defined by the inter-package relationship definition unit (3) (step a). Figure 3 shows examples of such relationships among the respective packages (relationships of targets handled by a window system).

Subsequently, the component packaging unit (1) formulates a component package by collecting components for operating each target (step b). Figure 4 shows a component package for operating an "I/O sub-window," which represents one of such targets.

Next, the inter-component utility restriction scripting unit (2) scripts, by using a formal language, restrictions on the joint utilities of multiple components within each package (step c) and then stores them within a database (step d).

The corresponding example is shown in Figures 5 and 6.

Figure 5 shows a restriction script text on the joint utilities of multiple components within the "main window" package. The following are expressed by this text:

"In order to utilize a component within this package, it is necessary to use 'window-create,' namely a component for securing a main window, in the first place";

"In a case where a component within this package is used, it is necessary to use 'window-destroy,' namely a component for releasing the main window region, at the end."

Petitioner Apple Inc. - Exhibit 1012, p. 2024

Figure 6, furthermore, shows a restriction script text on the joint utilities of multiple components within the "I/O sub-window" package.

The following are expressed by this text:

"In order to utilize a component within this package, it is necessary to use 'io-open,' namely a component for opening the I/O sub-window, in the first place";

"In a case where a component within this package is used, it is necessary to use 'io-close,' namely a component for closing the I/O sub-window, at the end."

Subsequently, the inter-component utility restriction fusion unit (4) proceeds, upon the reception of a list of utilized components from the program formulator, to extract, from the script texts of the restrictions on the joint utilities of multiple software components within each component package scripted by the inter-component utility restriction scripting unit (2), script portions on the utilized components mentioned in the list (step e), to judge the relationships among the component packages inclusive of said utilized components (step f), to fuse the extracted restriction script texts based on the ascertained relationships among the component packages (step g), and to formulate a restriction script text on the joint uses of the utilized components (component utility rules) (step g).

Figure 7 shows an example of restriction script text formulated by this inter-component utility restriction fusion unit (4) (component utility rules).

Petitioner Apple Inc. - Exhibit 1012, p. 2025

The following is expressed by this text:

"The components must be used in the prescribed order, although another component(s) may intervene in-between." /4

Thus, the rule generation device of this application example for utilizing a software component is capable of automatically formulating restriction script texts on multiple components utilized jointly for the formulation of a program, and in a case where such texts are used as test specifications, it becomes possible to automate the program verifying operation.

In a case where the present device is integrated with a component synthesizing system, furthermore, the component synthesis can be executed in a concomitantly verified state, and it becomes possible to formulate a program with a high reliability in a highly efficient manner.

(Effects of the invention)

As the foregoing explanations have demonstrated, the rule generation device of the present invention for utilizing a software component is capable of automatically formulating, by using a formal language, restriction script texts on the joint utilities of multiple software components utilized for the aforementioned program formulation, as a result of which it becomes possible to automate the program verifying operation.

Petitioner Apple Inc. - Exhibit 1012, p. 2026

4. Brief explanation of the figures

Figure 1 is a block diagram provided for explaining the constitution of an application example of the rule generation device of the present invention for utilizing a software component. Figure 2 is a flow chart provided for explaining the actions of the rule generation device for utilizing a software component shown in Figure 1, whereas Figure 3 is a diagram which shows the relationships among the respective packages, whereas Figure 4 is a diagram which shows an example of package, whereas Figures 5 and 6 are each diagrams which show examples of restriction script texts on joint utilities of multiple components within a package, whereas Figure 7 is a diagram which shows an example of component utility rules generated by the rule generation device for utilizing a software component shown in Figure 1.

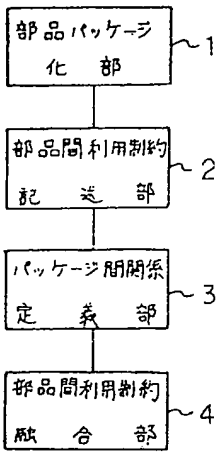
(1): Component packaging unit; (2): Inter-component utility restriction scripting unit; (3): Inter-package relationship definition unit; (4): Inter-component utility restriction fusion unit.

Applicant: Toshiba Corp.

Agent: Saichi Suyama, patent attorney

Petitioner Apple Inc. - Exhibit 1012, p. 2027

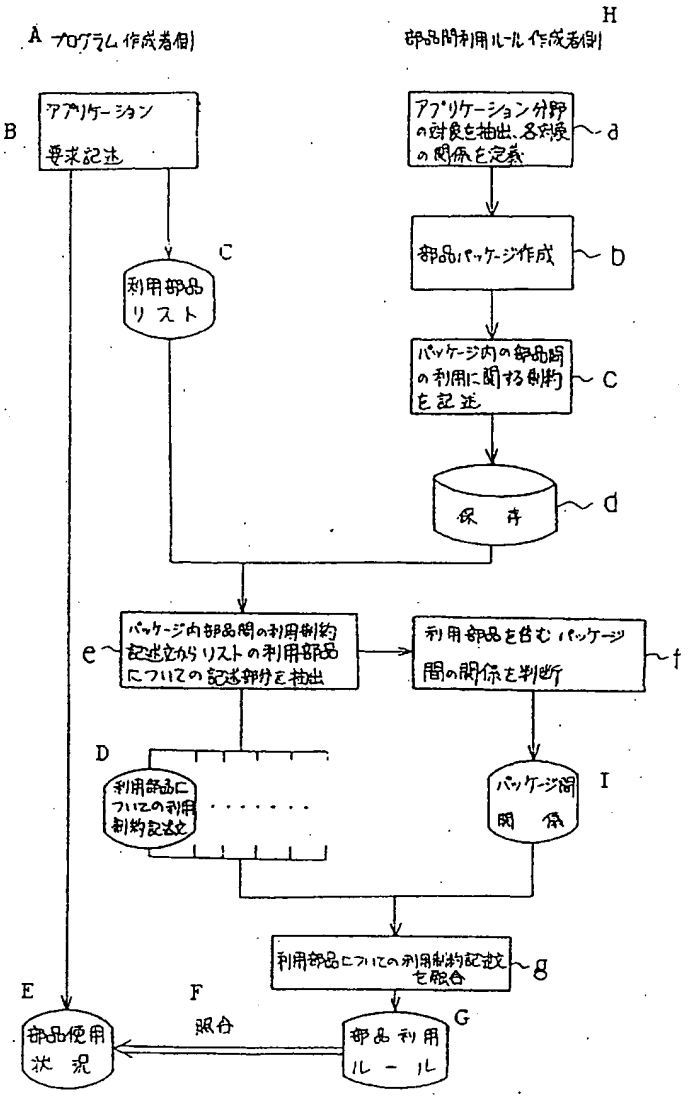
Figure 1



[(1): Component packaging unit; (2): Inter-component utility restriction scripting unit; (3): Inter-package relationship definition unit; (4): Inter-component utility restriction fusion unit]

Petitioner Apple Inc. - Exhibit 1012, p. 2028

Figure 2



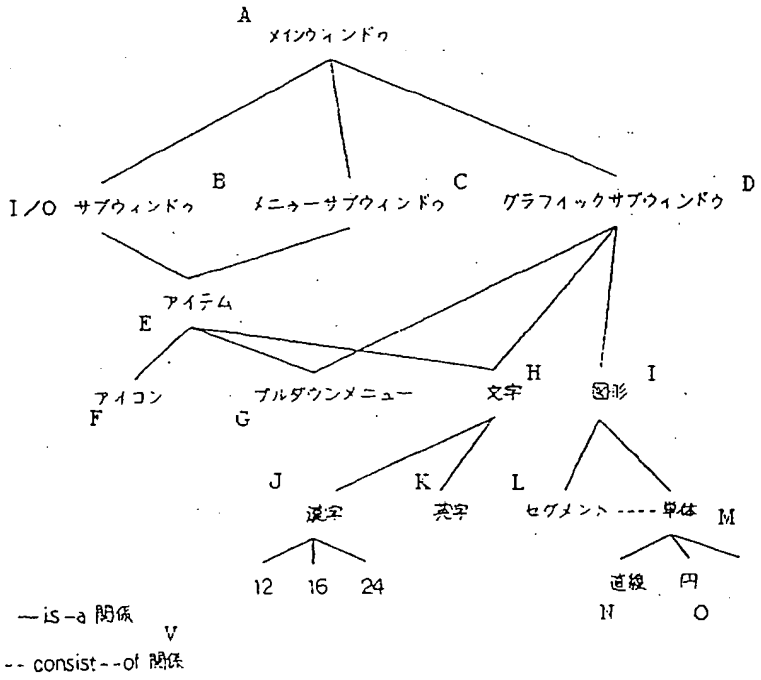
第 2 図

[(A): Program formulator side; (B): Application request script; (C): Utilized component list; (D): Utility restriction script text on utilized components; (E): Component utility state; (F): Matching; (G): Component utility rule; (a): Extraction of targets within an application field & definition of relationships among

Petitioner Apple Inc. - Exhibit 1012, p. 2029

the respective targets; (b): Component package formulation; (c): Script on restrictions on joint utilities of multiple components within a package; (d): Storage; (e): Extraction, from the script texts of the restrictions on the joint utilities of multiple software components within each component package, script portions on the utilized components mentioned in the list; (f): Judgment of relationships among packages inclusive of utilized components; (g): Fusion of utility restriction script texts on the utilized components]

Figure 3



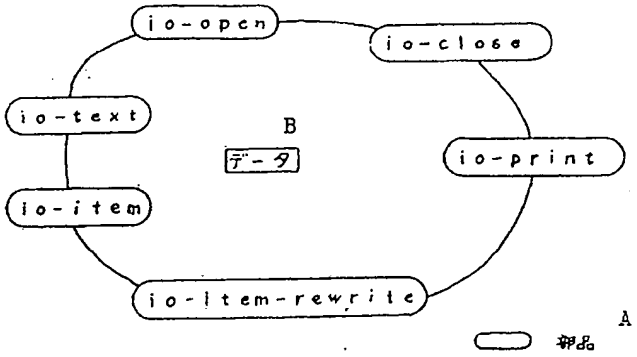
第 3 図

[(A): Main window; (B): I/O sub-window; (C): Menu sub-window; (D): Graphic sub-window; (E): Item; (F): Icon; (G): Pull-down menu;

Petitioner Apple Inc. - Exhibit 1012, p. 2030

(H): Characters; (I): Patterns; (J): *Kanji* characters; (K): European characters; (L): Segment; (M): Singular entity; (N): Line; (O): Circle; (V): Relationship]

Figure 4 /4



第 4 図

[(A): Component; (B): Data]

Figure 5

INIT: window-create
END: window-destroy

第 5 図

Figure 6

INIT: io—open
END: io—close

第 6 図

Figure 7

Petitioner Apple Inc. - Exhibit 1012, p. 2031

```
order:window_create, io_open, io_close, window_destroy
```

第 7 図

Petitioner Apple Inc. - Exhibit 1012, p. 2032

Notice of References Cited	Application/Control No. 10/015,951	Applicant(s)/Patent Under Reexamination STEFIK ET AL.	
	Examiner James A. Reagan	Art Unit 3621	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
	A	US-5,138,712 A	08-1992	Corbin, John R.	713/200
	B	US-5,295,266 A	03-1994	Hinsley et al.	718/101
	C	US-5,335,346 A	08-1994	Fabbio, Robert A.	711/163
	D	US-			
	E	US-			
	F	US-			
	G	US-			
	H	US-			
	I	US-			
	J	US-			
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N	H03-282733	03-1990	JAPAN	KISHI	G06F 9/06
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Weber, Robert. Digital Rights Management Technologies. October 1995. Retrieved from IDS.
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

22204 7590 01/24/2007

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

EXAMINER	
REAGAN, JAMES A	
ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 01/24/2007

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,951	12/17/2001	Mark J. Stefik	111325-88	5128

TITLE OF INVENTION: DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1400	$300	$0	$1700	04/24/2007

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 07/06) Approved for use through 04/30/2007.

Petitioner Apple Inc. - Exhibit 1012, p. 2034

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22204 7590 01/24/2007

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission
I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,951	12/17/2001	Mark J. Stefik	111325-88	5128

TITLE OF INVENTION: DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1400	$300	$0	$1700	04/24/2007

EXAMINER	ART UNIT	CLASS-SUBCLASS
REAGAN, JAMES A	3621	705-050000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,
(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.
1 _____
2 _____
3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
☐ Issue Fee
☐ Publication Fee (No small entity discount permitted)
☐ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**
☐ A check is enclosed.
☐ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Petitioner Apple Inc. - Exhibit 1012, p. 2035

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,951	12/17/2001	Mark J. Stefik	111325-88	5128

22204 7590 01/24/2007

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

EXAMINER	
REAGAN, JAMES A	
ART UNIT	PAPER NUMBER
3621	

DATE MAILED: 01/24/2007

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 325 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 325 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 07/06) Approved for use through 04/30/2007.

Petitioner Apple Inc. - Exhibit 1012, p. 2036

Search Notes

Application No.	Applicant(s)	
10/015,951	STEFIK ET AL.	
Examiner	**Art Unit**	
James A. Reagan	3621	

SEARCHED			
Class	Subclass	Date	Examiner
705	50-59	11/15/2006	JAR
380	201	11/15/2006	JAR
707	9	11/15/2006	JAR
707	104.1	11/15/2006	JAR
713	182-186	11/15/2006	JAR

INTERFERENCE SEARCHED			
Class	Subclass	Date	Examiner
705	**50-59**	**10/18/2004**	**JAR**
380	201	10/18/2004	JAR
707	9; 104.1	10/18/2004	JAR
713/182-186		10/18/2004	JAR

SEARCH NOTES (INCLUDING SEARCH STRATEGY)		
	DATE	EXMR
UPDATED EAST	11/16/2006	JAR
UPDATED DIALOG	11/15/2006	JAR
EIC PLUS	11/16/2006	JAR

OIPE
JUN 07 2005
PATENT & TRADEMARK OFFICE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. STEFIK, *et al.*
Art Unit	3621
Examiner Name	Calvin L. Hewitt, II
Attorney Docket Number	111325-88 (020700)

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number - Kind Code[2] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
JAR		US-4,882,752	November 21, 1989	Richard P. Lindman, *et al*	
		US-5,224,163	June 29, 1993	Morrie Gasser, *et al.*	
		US-5,299,263	March 29, 1994	Michael J. Beller, *et al.*	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3] Number[4] Kind Code[5] *(if known)*	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
		EP 0 538 216 A	April 21, 1993	TELEVERKET		

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		HENRY H. PERRITT, JR., "Knowbots, Permissions Headers and Contract Law"; Papers for the conference on Technological Strategies For Protecting Intellectual Property In The Networked Multimedia Environment, April 2, 1993; pages 1-22, XP-002233403	
		European Search Report; mailed September 8, 2004 (European Application No. 03 01 5128).	
		European Search Report; mailed September 13,2004 (European Application No. 03 01 5127).	

Examiner Signature	/James Reagan/ (11/15/2006)	Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

OIPE JC17
JUL 31 2002
PATENT & TRADEMARK OFFICE

Please type a plus sign (+) inside this box → [+]

PTO/SB/08A (08-00)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

RECEIVED
AUG 02 2002
GROUP 3600

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/015,951
Filing Date	12/17/2001
First Named Inventor	Mark J. Stefik et al
Group Art Unit	2161
Examiner Name	Unassigned
Attorney Docket Number	111325/000088

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number	Kind Code[2] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		6,253,193		Ginter et al	06/26/2001	
		4,713,753		Beobert et al	12/15/1987	
		5,052,040		Preston et al	09/24/1991	
		5,301,231		Abraham et al	04/05/1994	
		5,502,766		Boebert et al	03/26/1996	
		5,649,013		Stuckey et al	07/15/1997	
		5,737,416		Cooper et al	04/07/1998	
		5,737,413		Akiyama et al	04/07/1998	
		5,757,907		Cooper et al	05/26/1998	
		6,301,660		Benson	10/09/2001	
		6,327,652		England et al	12/04/2001	
		6,330,670		England et al	12/11/2001	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Office[3]	Number[4]	Kind Code[5] (if known)	Name of Patentee or Applicant of Cited Document	Date of Publication of Cited Document MM-DD-YYYY	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[6]

Examiner Signature		Date Considered	2/5/05

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Unique citation designation number. [2] See attached Kinds of U.S. Patent Documents. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

[1] Unique citation designation number. [2] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Washington, DC 20231.

NVA234468.1

Form PTO-1449 (Rev. 8-83) U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-8[illegible]	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT	Applicants: Stefik et al.	
	Filing Date: December 17, 2001	Group Art Unit:

U.S. PATENT & TRADEMARK OFFICE AUG 09 2002

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date (if appropriate)
QMR	4,827,508	05/02/1989	Shear			
	4,977,594	12/11/1990	Shear			
	5,050,213	09/17/1991	Shear			
	5,410,598	04/25/1995	Shear			
	5,892,900	04/06/1999	Ginter et al.			
	5,910,987	06/08/1999	Ginter et al.			
	5,915,019	06/22/1999	Ginter et al.			
	5,917,912	06/29/1999	Ginter et al.			
	5,920,861	07/06/1999	Hall et al.			
	5,940,504	08/17/1999	Griswold			
	5,943,422	08/24/1999	Van Wie et al.			
	5,949,876	09/07/1999	Ginter et al.			
	5,982,891	11/09/1999	Ginter et al.			
	5,999,949	12/07/1999	Crandall			
	6,112,181	08/29/2000	Shear et al.			
	6,138,119	10/24/2000	Hall et al.			
	6,157,721	12/05/2000	Shear et al.			
	6,185,683	02/06/2001	Ginter et al.			
	6,237,786	05/29/2001	Ginter et al.			
	6,240,185	05/29/2001	Van Wie et al.			
	6,253,193	06/26/2001	Ginter et al.			
	6,292,569	09/18/2001	Shear et al.			
	6,363,488	05/26/2002	Ginter et al.			
	6,389,402	05/14/2002	Ginter et al.			

RECEIVED AUG 13 2002 GROUP 3600

Examiner [signature] Date Considered 28 SEP 05

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this formwith next communication to applicant.

Form PTO-1449 (Rev. 8-83) U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-88	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT	Applicants: Stefik et al.	
	Filing Date: December 17, 2001	Group Art Unit:

OIPE AUG 30 2002 PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date (if appropriate)
JM	3,263,158	07/01/1966	Janis			
	3,609,697	09/28/1971	Blevins et al.			
	3,790,700	02/05/1974	Callais et al.			
	3,798,605	03/19/1974	Feistel			
	4,159,468	06/26/1979	Barnes et al.			
	4,220,991	09/02/1980	Hamano et al.			
	4,278,837	07/14/1981	Best			
	4,323,921	04/06/1982	Guillou			
	4,442,486	04/10/1984	Mayer			
	4,529,870	07/16/1985	Chaum			
	4,558,176	12/10/1985	Arnold et al.			
	4,593,376	06/03/1986	Volk			
	4,614,861	09/30/1986	Pavlov et al.			
	4,644,493	02/17/1987	Chandra et al.			
	4,658,093	04/14/1987	Hellman			
	4,817,140	03/28/1989	Chandra et al.			
	4,868,376	09/19/1989	Lessin et al.			
	4,891,838	01/02/1990	Faber			
	4,924,378	05/08/1990	Hershey et al.			
	4,932,054	06/05/1990	Chou et al.			
	4,937,863	06/26/1990	Robert et al.			
	4,949,187	08/14/1990	Cohen			
	4,953,209	08/28/1990	Ryder, Sr. et al.			
	4,961,142	10/02/1990	Elliott et al.			
	4,975,647	12/04/1990	Downer et al.			
	4,999,806	03/12/1991	Chernow et al.			
	5,010,571	04/23/1991	Katznelson			
	5,014,234	05/07/1991	Edwards, Jr.			
	5,023,907	06/11/1991	Johnson et al.			
	5,047,928	09/10/1991	Wiedemer			
	5,052,040	09/24/1991	Preston et al.			

RECEIVED SEP 04 2002 GROUP 3600

Examiner JM Date Considered 28SEP05

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

08/27/2002

Form PTO-1449 (Rev. 8-83)	U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-88	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT		Applicants: Stefik et al.	
		Filing Date: December 17, 2001	Group Art Unit:

OIPE JC16 AUG 10 2007 PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date (if appropriate)
GMR	5,058,164	10/15/1991	Elmer et al.			
	5,103,476	04/07/1992	Waite et al.			
	5,113,519	05/12/1992	Johnson et al.			
	5,136,643	08/04/1992	Fischer			
	5,138,712	08/11/1992	Corbin			
	5,146,499	09/08/1992	Geffrotin			
	5,148,481	09/15/1992	Abraham et al.			
	5,159,182	10/27/1992	Eisele			
	5,183,404	02/02/1993	Aldous et al.			
	5,191,193	03/02/1993	Le Roux			
	5,204,897	04/20/1993	Wyman			
	5,222,134	06/22/1993	Waite et al.			
	5,235,642	08/10/1993	Wobber et al.			
	5,247,575	09/21/1993	Sprague et al.			
	5,255,106	10/19/1993	Castro			
	5,260,999	11/09/1993	Wyman			
	5,263,157	11/16/1993	Janis			
	5,263,158	11/16/1993	Janis			
	5,276,444	01/04/1994	McNair			
	5,276,735	01/04/1994	Boebert et al.			
	5,291,596	03/01/1994	Mita			
	5,311,591	05/10/1994	Fischer			
	5,319,705	06/07/1994	Halter et al.			
	5,337,357	08/09/1994	Chou et al.			
	5,339,091	08/16/1994	Yamazaki et al.			
	5,341,429	08/23/1994	Stringer et al.			
	5,347,579	09/13/1994	Blandford			
	5,381,526	01/10/1995	Ellson			
	5,394,469	02/28/1995	Nagel et al.			
	5,412,717	05/02/1995	Fischer			
	5,428,606	06/27/1995	Moskowitz			

RECEIVED
SEP 04 2002
GROUP 3600

Examiner GMR Date Considered 28 SEP 05

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

08/27/2002

Form PTO-1449 (Rev. 8-83)	U.S. Department of Commerce Patent and Trademark Office	Atty Docket 111325-88	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT		Applicants: Stefik et al.	
		Filing Date: December 17, 2001	Group Art Unit:

OIPE JC16 AUG 30 2002 PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date (if appropriate)
JMR	5,432,849	07/11/1995	Johnson et al.			
	5,438,508	08/01/1995	Wyman			
	5,444,779	08/22/1995	Daniele			
	5,453,601	09/26/1995	Rosen			
	5,455,953	10/03/1995	Russell			
	5,457,746	10/10/1995	Dolphin			
	5,473,687	12/05/1995	Lipscomb et al.			
	5,473,692	12/05/1995	Davis			
	5,499,298	03/12/1996	Narasimhalu et al.			
	5,504,814	04/02/1996	Miyahara			
	5,504,818	04/02/1996	Okano			
	5,504,837	04/02/1996	Griffeth et al.			
	5,509,070	04/16/1996	Schull			
	5,530,235	06/25/1996	Stefik et al.			
	5,532,920	07/02/1996	Hartrick et al.			
	5,534,975	07/09/1996	Stefik et al.			
	5,539,735	07/23/1996	Moskowitz			
	5,563,946	10/08/1996	Cooper et al.			
	5,568,552	10/22/1996	Davis			
	5,621,797	04/15/1997	Rosen			
	5,629,980	05/13/1997	Stefik et al.			
	5,633,932	05/27/1997	Davis et al.			
	5,634,012	05/27/1997	Stefik et al.			
	5,638,443	06/10/1997	Stefik et al.			
	5,655,077	08/05/1997	Jones et al.			
	5,708,717	01/13/1998	Alasia			
	5,734,823	03/31/1998	Saigh et al.			
	5,734,891	03/31/1998	Saigh			
	5,745,569	04/28/1998	Moskowitz et al.			
	5,748,783	05/05/1998	Rhoads			
	5,761,686	06/02/1998	Bloomberg			

RECEIVED
SEP 0 4 2002
GROUP 3600

Examiner JMR Date Considered 28 SEP 05

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this formwith next communication to applicant.

08/27/2002

Form PTO-1449 (Rev. 8-83)	U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-88	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT		Applicants: Stefik et al.	
		Filing Date: December 17, 2001	Group Art Unit:

O I P E
AUG 30 2002
PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date (If appropriate)
GMF	5,765,152	06/09/1998	Erickson			
	5,768,426	06/16/1998	Rhoads			
	5,825,892	10/20/1998	Braudaway et al.			
	6,047,067	04/04/2000	Rosen			
	6,115,471	09/05/2000	Oki et al.			
	6,233,684	05/15/2001	Stefik et al.			
	6,266,618	05/01/2001	Downs et al.			
	6,345,256	02/05/2002	Milsted et al.			

FOREIGN PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Country	Class	Subclass	Translation Yes	Translation No
	0 084 441	07/27/1983	EP			Full Eng	
	0 180 460	05/07/1986	EP			Full Eng	
	0 332 707	09/01/1989	EP			Full Eng	
	0 651 554	05/03/1995	EP			Full Eng	
	0 668 695	08/23/1995	EP			Full Eng	
	0 725 376	08/07/1996	EP			Full Eng	
	2 136 175	09/12/1984	GB			Full Eng	
	2 236 604	04/10/1991	GB			Full Eng	
	WO 01/63528	08/30/2001	PCT			Full Eng	
	WO 92/20022	11/12/1992	PCT			Full Eng	
	WO 93/01550	01/21/1993	PCT			Full Eng	
	WO 99/49615	09/30/1999	PCT			Full Eng	

RECEIVED
SEP 04 2002
GROUP 3600

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

Examiner Initial	
	"National Semiconductor and EPR Partner for Information Metering/Data Security Cards" March 4, 1994, Press Release from Electronic Publishing Resources, Inc.
	Weber, R., "Digital Rights Management Technology" October 1995
	Flasche, U. et al., "Decentralized Processing of Documents", pp. 119-131, 1986, Comput. & Graphics, Vol. 10, No. 2
	Mori, R. et al., "Superdistribution: The Concept and the Architecture", pp. 1133-1146, 1990, The Transactions of

Examiner	Date Considered 28SEP05

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this formwith next communication to applicant.

08/27/2002

Form PTO-1449 (Rev. 8-83)	U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-88	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT		Applicants: Stefik et al.	
		Filing Date: December 17, 2001	Group Art Unit:

OIPE JC100 AUG 30 2002 PATENT & TRADEMARK OFFICE

Examiner Initial	OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)
	Weber, R., "Metering Technologies for Digital Intellectual Property", pp. 1-29, Oct. 1994, A Report to the International Federation of Reproduction Rights Organizations
	Clark, P.C. et al., "Bits: A Smartcard protected Operating System", pp. 66-70 and 94, November 1994, Communications of the ACM, Vol. 37, No. 11
	Ross, P.E., "Data Guard", pp. 101, June 6, 1994, Forbes
	Saigh, W.K., "Knowledge is Sacred", 1992, Video Pocket/Page Reader Systems, Ltd.
	Kahn, R.E., "Deposit, Registration and Recordation in an Electronic Copyright Management System", pp. 1-19, August 1992, Corporation for National Research Initiatives, Virginia
	Hilts, P. et al., "Books While U Wait", pp. 48-50, January 3, 1994, Publishers Weekly
	Strattner, A, "Cash Register on a Chip may Revolutionize Software Pricing and Distribution; Wave Systems Corp.", pp. 62, April 1994, Computer Shopper, Vol. 14, No. 4, ISSN 0886-0556
	O'Conner, M., "New Distribution Option for Electronic Publishers; iOpener Data Encryption and Metering System for CD-ROM use; Column", pp. 134, March 1994, CD-ROM Professional, Vol. 7, No. 2, ISSN: 1409-0833
	Willett, S., "Metered PCs: Is Your System Watching You? Wave System beta tests new technology", pp. 84, May 2, 1994, InfoWorld
	Linn, R., "Copyright and Information Services in the Context of the National Research and Education Network ", pp. 9-20, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Perrit, Jr., H., "Permission Headers and Contract Law", pp. 27-48, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Upthegrove, L., "Intellectual Property Header Descriptors: A Dynamic Approach", pp. 63-66, January 1994, IMA Intellectual Property Proceedings, Vol. 1, Issue 1
	Sirbu, M., "Internet Billing Service Design and prototype Implementation", pp. 67-80, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Simmel, S. et al., "Metering and Licensing of Resources: Kala's General Purpose Approach", pp. 81-110, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Kahn, R., "Deposit, Registration and Recordation in an Electronic Copyright Management System", pp. 111-120, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Tygar, J. et al., "Dyad: A System for Using Physically Secure Coprocessors", pp. 121-152, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Griswold, G., "A Method for Protecting Copyright on Networks", pp. 169-178, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Nelson, T., "A Publishing and Royalty Model for Networked Documents", pp. 257-259, January 1994, IMA Intellectual Property Project Proceedings, Vol. 1, Issue 1
	Robinson, E., "Redefining Mobile Computing", pp. 238-240, 247-248 and 252, July 1993, PC Computing
	Abadi, M. et al., "Authentication and Delegation with Smart-cards", 1990, Research Report DEC Systems Research Center
	Mark Stefik, "Letting Loose the Light: Igniting Commerce in Electronic Publication", pp. 219-253, 1996, Internet Dreams: Archetypes, Myths, and Metaphors, IDSN 0-262-19373-6
	Mark Stefik, "Letting Loose the Light: Igniting Commerce in Electronic Publication", pp. 2-35, February 8, 1995, Internet Dreams: Archetypes, Myths and Metaphors,

Examiner _____ Date Considered 28 SEP 05

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this formwith next communication to applicant.

08/27/2002

Form PTO-1449 (Rev. 8-83) U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-88	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT	Applicants: Stefik et al.	
	Filing Date: December 17, 2001	Group Art Unit:

OIPE JC160 AUG 30 2002 PATENT & TRADEMARK OFFICE

N/A

RECEIVED
SEP 04 2002
GROUP 3600

Examiner	Date Considered 28 SEP 05

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this formwith next communication to applicant.

08/27/2002

OIPE SC174
JUN 07 2005
PATENT & TRADEMARK OFFICE

Substitute for form 1449A/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. STEFIK, *et al.*
Art Unit	3621
Examiner Name	Calvin L. Hewitt, II
Attorney Docket Number	111325-88 (020700)

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document: Number - Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,882,752	November 21, 1989	Richard P. Lindman, *et al*	
		US-5,224,163	June 29, 1993	Morrie Gasser, *et al.*	
		US-5,299,263	March 29, 1994	Michael J. Beller, *et al.*	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]
		EP 0 538 216 A	April 21, 1993	TELEVERKET		

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[7]
		HENRY H. PERRITT, JR., "Knowbots, Permissions Headers and Contract Law"; Papers for the conference on Technological Strategies For Protecting Intellectual Property In The Networked Multimedia Environment, April 2, 1993; pages 1-22, XP-002233403	
		European Search Report; mailed September 8, 2004 (European Application No. 03 01 5128).	
		European Search Report; mailed September 13,2004 (European Application No. 03 01 5127).	

Examiner Signature		Date Considered	28 SEP 05

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

OIPE MAIL
OCT 14 2005
PATENT & TRADEMARK OFFICE

PTO/SB/08A (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/015,951
Filing Date	December 7, 2001
First Named Inventor	Mark J. STEFIK, *et al.*
Art Unit	3621
Examiner Name	James Reagan
Attorney Docket Number	111325-88 (020700)

U.S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	U.S. Patent Document Number - Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
JAN		6,135,646	October 24, 2000	Kahn et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3] Number[4]	Foreign Patent Document: Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T[6]

OTHER PRIOR ART – NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]

Examiner Signature	JAN	Date Considered	28 SEP 05

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, Washington, DC 20231.

OIPE IAP44
MAR 07 2007
PATENT & TRADEMARK OFFICE

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. **STEFIK**, *et al.*
Group Art Unit	3621
Examiner Name	James A. Reagan
Total Number of Pages in This Submission	**Attorney Docket Number** 111325-020700
	Confirmation Number 5128

ENCLOSURES *(check all that apply)*

- ☒ Fee Transmittal Form
  - ☐ Fee Attached
- ☐ Amendment / Reply
  - ☐ After Final
  - ☐ Affidavits/declaration(s)
- ☐ Extension of Time Request
- ☐ Express Abandonment Request
- ☐ Information Disclosure Statement
- ☐ Certified Copy of Priority Document(s)
- ☐ Response to Missing Parts/ Incomplete Application
  - ☐ Response to Missing Parts under 37 CFR 1.52 or 1.53
- ☐ Assignment Papers *(for an Application)*
- ☐ Drawing(s)
- ☐ Declaration and Power of Attorney
- ☐ Licensing-related Papers
- ☐ Petition
- ☐ Petition to Convert to a Provisional Application
- ☐ Power of Attorney, Revocation Change of Correspondence Address
- ☐ Terminal Disclaimer
- ☐ Request for Refund
- ☐ CD, Number of CD(s) _____
- ☐ After Allowance Communication to Group
- ☐ Appeal Communication to Board of Appeals and Interferences
- ☐ Appeal Communication to Group (Appeal Notice, Brief, Reply Brief)
- ☐ Proprietary Information
- ☐ Status Letter
- ☐ Application Data Sheet
- ☐ Request for Corrected Filing Receipt with Enclosures
- ☐ A self-addressed prepaid postcard for acknowledging receipt
- ☒ Other Enclosure(s) (*please identify below*):
  1. Part B – Fee(s) Transmittal Form (Duplicate)

Remarks

☒ The Commissioner is hereby authorized to charge any additional fees required or credit any overpayments to Deposit Account No. 19-2380 for the above identified docket number.

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm *or* Individual name	Marc S. Kaufman Registration No.35,212 **Nixon Peabody LLP** 401 9th Street, N.W., Suite 900 Washington, D.C. 20004-2128
Signature	
Date	3-07-07

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

☐ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop _____, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450

☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) _____.

_____ Date

_____ Signature

_____ Typed or printed name

FEE TRANSMITTAL FOR FY 2007

Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	$1,730.00

Complete if Known	
Application Number	10/015,951
Filing Date	December 17, 2001
First Named Inventor	Mark J. STEFIK, *et al.*
Examiner Name	James A. Reagan
Art Unit	3621
Attorney Docket No.	111325-020700
Confirmation No.	5128

USPTO OIPE IAP44 MAR 07 2007 PATENT & TRADEMARK OFFICE

METHOD OF PAYMENT *(check all that apply)*

☐ Check ☐ Credit Card ☐ Money Order ☐ Other ☐ None

☒ Deposit Account:

Deposit Account Number: 19-2380

Deposit Account Name: Nixon Peabody LLP

The Commissioner is authorized to: *(check all that apply)*

☒ Charge fee(s) indicated below ☒ Credit any overpayments

☒ Charge any additional fee(s)

☐ Charge fee(s) indicated below, **except for the filing fee** to the above-identified deposit account.

FEE CALCULATION

1. BASIC FILING FEE

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1001	300	2001	150	Utility filing fee	
1002	200	2002	100	Design filing fee	
1003	200	2003	100	Plant filing fee	
1004	300	2004	150	Reissue filing fee	
1005	200	2005	100	Provisional filing fee	

SUBTOTAL (1) ($) 0

2. EXTRA CLAIM FEES FOR UTILITY AND REISSUE

		Extra Claims	Fee from below	Fee Paid
Total Claims	-20** =		X =	0
Independent Claims	-3** =		X =	0
Multiple Dependent			X =	0

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description
1202	50	2202	25	Claims in excess of 20
1201	200	2201	100	Independent claims in excess of 3
1203	360	2203	180	Multiple dependent claim, if not paid
1204	200	2204	100	** Reissue independent claims over original patent
1205	50	2205	25	** Reissue claims in excess of 20 and over original patent

SUBTOTAL (2) ($) 0

**or number previously paid, if greater; For Reissues, see above

FEE CALCULATION (continued)

3. ADDITIONAL FEES

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	
1051	130	2051	65	Surcharge – late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet	
1053	130	1053	130	Non-English specification	
1812	2,520	1812	2,520	For filing a request for *ex parte* reexamination	
1804	920*	1804	920*	Requesting publication of SIR prior to Examiner action	
1805	1,840*	1805	1,840*	Requesting publication of SIR after Examiner action	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1,020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1,080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	
1403	1,000	2403	500	Request for oral hearing	
1451	1,510	1451	1,510	Petition to institute a public use proceeding	
1452	500	2452	250	Petition to revive – unavoidable	
1453	1,500	2453	750	Petition to revive – unintentional	
1501	1,400	2501	700	Utility issue fee (or reissue)	1,400.00
1502	800	2502	400	Design issue fee	
1503	1,100	2503	550	Plant issue fee	
1460	130	1460	130	Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
8021	40	8021	40	Recording each patent assignment per property (times number of properties)	
1809	790	2809	395	Filing a submission after final rejection (37 CFR 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR 1.129(b))	
1801	790	2801	395	Request for Continued Examination (RCE)	
1802	900	1802	900	Request for expedited examination of a design application	

Other fee (specify): 10 Advance Copies 30.00

Publication Fee 300.00

*Reduced by Basic Filing Fee Paid SUBTOTAL (3) $1,730.00

CERTIFICATE OF MAILING OR TRANSMISSION [37 CFR 1.8(a)]

I hereby certify that this correspondence is being:

☐ deposited with the United States Postal Service on the date shown below with sufficient postage as first class mail in an envelope addressed to: Mail Stop _____, Commissioner for Patents, P. O. Box 1450, Alexandria, VA 22313-1450

☐ transmitted by facsimile on the date shown below to the United States Patent and Trademark Office at (703) _____.

Date _____ Signature _____

Typed or printed name _____

SUBMITTED BY				Complete *(if applicable)*	
Name *(Print/Type)*	Marc S. Kaufman	Registration No. *(Attorney/Agent)*	35,212	Telephone	(202) 585-8000
Signature				Date	3-07-07

SEND TO: Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

10331235.1

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

BEST AVAILABLE COPY

OIPE IAP44 MAR 07 2007 PATENT & TRADEMARK OFFICE

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

22204 7590 01/24/2007

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)

(Signature)

(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,951	12/17/2001	Mark J. Stefik	111325-88	5128

TITLE OF INVENTION: DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1400	$300	$0	$1700	04/24/2007

EXAMINER	ART UNIT	CLASS-SUBCLASS
REAGAN, JAMES A	3621	705-050000

03/08/2007 MAHMED2 00000003 192380 10015951
01 FC:1501 1400.00 DA
02 FC:1504 300.00 DA
03 FC:8001 30.00 DA

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 Marc S. Kaufman
2 Carlos R. Villamar
3 Nixon Peabody, LLP

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: ContentGuard Holdings, Inc.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): Wilmington, Delaware

Please check the appropriate assignee category or categories (will not be printed on the patent) : ☐ Individual ☒ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☒ Issue Fee

☒ Publication Fee (No small entity discount permitted)

☒ Advance Order - # of Copies 10

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

☐ A check is enclosed.

☐ Payment by credit card. Form PTO-2038 is attached.

☒ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number 19-2380 (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

☐ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date 3-07-07

Typed or printed name Marc S. Kaufman Registration No. 35,212

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

Petitioner Apple Inc. - Exhibit 1012, p. 2051

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,951	12/17/2001	Mark J. Stefik	111325-88	5128

22204 7590 04/03/2007

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

EXAMINER	
AUGUSTIN, EVENS J	

ART UNIT	PAPER NUMBER
3621	

MAIL DATE	DELIVERY MODE
04/03/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
10. 015951			

EXAMINER	
ART UNIT	PAPER
	20070320

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

1. The Information Disclosure Statement received on 27 September 2002 has been considered.

2. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Evens Augustin whose telephone number is 571-272-6860. The examiner can normally be reached on Monday thru Friday 10 to 7 pm.

3. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Andrew Fischer can be reached on 571-272-6779.

Evens J. Augustin
March 20, 2007
Art Unit 3621

3/24/07
ANDREW J. FISCHER
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 3600

Form PTO-1449 (Rev. 8-83)	U.S.Department of Commerce Patent and Trademark Office	Atty Docket 111325-88	Serial No. 10/015,951
INFORMATION DISCLOSURE STATEMENT		Applicants: Stefik et al.	
		Filing Date: December 17, 2001	Group Art Unit:

OIPE SEP 27 2002 PATENT & TRADEMARK OFFICE

U.S. PATENT DOCUMENTS

Examiner Initial	Document Number	Date	Name	Class	Subclass	Filing Date (if appropriate)
	4,796,220	01/03/1989	Wolfe			

FOREIGN PATENT DOCUMENTS

RECEIVED OCT 01 2002 GROUP 3600

Examiner Initial	Document Number	Date	Country	Class	Subclass	Translation Yes	Translation No
EA	0 715 241	06/05/1996	JP			Full Eng	
	04-369068	12/21/1992	JP			Eng Abst	
	05-268415	10/15/1993	JP			Eng Abst	
	06-175794	06/24/1994	JP			Eng Abst	
	06-215010	08/05/1994	JP			Eng Abst	
	07-084852	03/31/1995	JP			Eng Abst	
	07-200317	08/04/1995	JP			Eng Abst	
	07-244639	09/19/1995	JP			Eng Abst	
	62-241061	10/21/1987	JP			Eng Abst	
	64-068835	03/14/1989	JP			Eng Abst	
	WO 94/01821	01/20/1994	PCT			Full Eng	
	WO 96/24092	08/08/1996	PCT			Full Eng	
	WO 97/48203	12/18/1997	PCT			Full Eng	
	WO 98/11690	03/19/1998	PCT			Full Eng	
	WO 98/42098	09/24/1998	PCT			Full Eng	

OTHER DOCUMENTS (Including Author, Title, Date, Pertinent Pages, Etc.)

Examiner Initial	
	Henry H. Perritt, Jr., "Technological Strategies for Protecting Intellectual Property in the Networked Multmedia Enviroment", April 2-3, 1993, Knowbots, Permissions Headers & Contract Law

Examiner	Date Considered 3/20/07

*EXAMINER: Initial if citation considered, whether or not citation is in conformance with MPEP 609; Draw line through citation if not in conformance and not considered. Include copy of this formwith next communication to applicant.

09/25/2002

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/015,951	05/29/2007	7225160	111325-88	5128

22204 7590 05/09/2007

NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 325 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Mark J. Stefik, Portola Valley, CA;
Peter L.T. Pirolli, San Francisco, CA;
Ralph C Merkle, Sunnyvale, CA;

PTO/SB/96 (07-09)
Approved for use through 07/31/2012. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

STATEMENT UNDER 37 CFR 3.73(b)

Applicant/Patent Owner: MARK J. STEFIK, et al.

Application No./Patent No.: 08/967,084 Filed/Issue Date: 11-10-1997

Titled: SYSTEM FOR CONTROLLING THE DISTRIBUTION AND USE OF DIGITAL WORKS USING DIGITAL TICKETS

CONTENTGUARD HOLDINGS, INC. , a Corporation

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.

states that it is:

1. ☒ the assignee of the entire right, title, and interest in;

2. ☐ an assignee of less than the entire right, title, and interest in (The extent (by percentage) of its ownership interest is _____ %); or

3. ☐ the assignee of an undivided interest in the entirety of (a complete assignment from one of the joint inventors was made)

the patent application/patent identified above, by virtue of either:

A. ☒ An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel 011122, Frame 0204, or for which a copy therefore is attached.

OR

B. ☐ A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

2. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

3. From: _____ To: _____

The document was recorded in the United States Patent and Trademark Office at

Reel _____, Frame _____, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☒ As required by 37 CFR 3.73(b)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (*i.e.*, a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Stephen M. Hertzler, Reg. No. 58,247/	2010-09-16
Signature	Date
Stephen M. Hertzler, Reg. No. 58,247	
Printed or Typed Name	Title

This collection of information is required by 37 CFR 3.73(b). The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

AUTHORIZATION TO ACT ON BEHALF OF THE ASSIGNEE

UNDER 37 CFR 3.73(b)(2)(i)

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

The practitioners associated with Customer Number 98804 have been authorized (or empowered) to act on behalf of ContentGuard Holdings, Inc. before the United States Patent and Trademark Office (i.e. to sign the enclosed submission on behalf of the assignee), pursuant to 37 CFR 3.73(b)(2)(i).

If any additional information is required in this regard, please contact the undersigned as soon as possible.

Respectfully submitted,

Date: September 16, 2010

/Stephen M. Hertzler, Reg. No. 58,247/
Stephen M. Hertzler
Registration No. 58,247

REED SMITH LLP
CUSTOMER NO.: 98804
1301 K Street N.W.
Suite 1100 – East Tower
Washington, D.C. 20005

Petitioner Apple Inc. - Exhibit 1012, p. 2058

Electronic Acknowledgement Receipt

EFS ID:	8554680
Application Number:	10015951
International Application Number:	
Confirmation Number:	5128
Title of Invention:	DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME
First Named Inventor/Applicant Name:	Mark J. Stefik
Customer Number:	22204
Filer:	Stephen M. Hertzler
Filer Authorized By:	
Attorney Docket Number:	111325-020700
Receipt Date:	05-OCT-2010
Filing Date:	17-DEC-2001
Time Stamp:	11:48:55
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Miscellaneous Incoming Letter	020700_-_2010-10-05_-_Authorization_Statement.pdf	407008 01ab114e39275dc6ed116c6a0a5e5b8130820f04	no	1

Warnings:	
Information:	

2	Power of Attorney	020700_-_2010-10-05_-_POA.pdf	1217636 e6ce4e7be6e5cb0ed814e488d50f9a970815e583	no	2
Warnings:					
Information:					
3	Assignee showing of ownership per 37 CFR 3.73(b).	020700_-_2010-10-05_-_Statement_under_37_CFR_373.pdf	413936 64ca835f087405a0dd7375f4856349e299cdd5f4	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	2038580		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PTO/SB/80 (11-08)
Approved for use through 11/30/2011. OMB 0651-0035
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

POWER OF ATTORNEY TO PROSECUTE APPLICATIONS BEFORE THE USPTO

I hereby revoke all previous powers of attorney given in the application identified in the attached statement under 37 CFR 3.73(b).

I hereby appoint:

☑ Practitioners associated with the Customer Number: 98804

OR

☐ Practitioner(s) named below (if more than ten patent practitioners are to be named, then a customer number must be used):

Name	Registration Number	Name	Registration Number

as attorney(s) or agent(s) to represent the undersigned before the United States Patent and Trademark Office (USPTO) in connection with any and all patent applications assigned only to the undersigned according to the USPTO assignment records or assignment documents attached to this form in accordance with 37 CFR 3.73(b).

Please change the correspondence address for the application identified in the attached statement under 37 CFR 3.73(b) to:

☑ The address associated with Customer Number: 98804

OR

☐ Firm or Individual Name			
Address			
City		State	Zip
Country			
Telephone		Email	

Assignee Name and Address:

ContentGuard Holdings, Inc.
222 N. Sepulveda Blvd., Suite 1400
El Segundo, CA 90245

A copy of this form, together with a statement under 37 CFR 3.73(b) (Form PTO/SB/96 or equivalent) is required to be filed in each application in which this form is used. The statement under 37 CFR 3.73(b) may be completed by one of the practitioners appointed in this form if the appointed practitioner is authorized to act on behalf of the assignee, and must identify the application in which this Power of Attorney is to be filed.

SIGNATURE of Assignee of Record

The individual whose signature and title is supplied below is authorized to act on behalf of the assignee

Signature	[signature]	Date	9/16/2010
Name	Eddie Chen	Telephone	
Title	Chief Technology Officer		

This collection of information is required by 37 CFR 1.31, 1.32 and 1.33. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to take 3 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
10/015,951	12/17/2001	Mark J. Stefik	111325-020700

CONFIRMATION NO. 5128

98804
Reed Smith LLP
P.O. Box 488
Pittsburgh, PA 15230

POA ACCEPTANCE LETTER

OC000000043924441

Date Mailed: 10/14/2010

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/05/2010.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

/sleutchit/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Petitioner Apple Inc. - Exhibit 1012, p. 2063

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
10/015,951	12/17/2001	Mark J. Stefik	111325-020700

CONFIRMATION NO. 5128

POWER OF ATTORNEY NOTICE

22204
NIXON PEABODY, LLP
401 9TH STREET, NW
SUITE 900
WASHINGTON, DC 20004-2128

OC000000043924424

Date Mailed: 10/14/2010

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 10/05/2010.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

/sleutchit/

Office of Data Management, Application Assistance Unit (571) 272-4000, or (571) 272-4200, or 1-888-786-0101

Petitioner Apple Inc. - Exhibit 1012, p. 2064

Best Available Copy

Trials@uspto.gov
571-272-7822

Paper 12
Entered: June 19, 2013

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ZTE CORPORATION AND ZTE (USA) INC.
Petitioner

v.

CONTENTGUARD HOLDINGS INC.
Patent Owner

Case IPR2013-00134
U.S. Patent No. 7,225,160

Before JAMESON LEE, MICHAEL W. KIM, and
MICHAEL R. ZECHER, *Administrative Patent Judges*.

ZECHER, *Administrative Patent Judge*

DECISION
Institution of *Inter Partes* Review
37 C.F.R. § 42.108

Best Available Copy

I. INTRODUCTION

ZTE Corporation and ZTE (USA) Inc. ("ZTE") filed a petition ("Pet.") requesting *inter partes* review of claims 1-38 of U.S. Patent No. 7,225,160 ("the '160 patent"). Paper 3. In response, Patent Owner, ContentGuard Holdings Inc. ("ContentGuard"), filed a preliminary response ("Prel. Resp."). Paper 9. We have jurisdiction under 35 U.S.C. § 314.

The standard for instituting an *inter partes* review is set forth in 35 U.S.C. § 314(a), which provides:

> THRESHOLD --The Director may not authorize an inter partes review to be instituted unless the Director determines that the information presented in the petition filed under section 311 and any response filed under section 313 shows that there is a reasonable likelihood that the petitioner would prevail with respect to at least 1 of the claims challenged in the petition.

For the reasons set forth below, we conclude that the information presented in the petition demonstrates that there is a reasonable likelihood that ZTE will prevail in establishing claims 12-22 and 30-38 as unpatentable. However, we conclude that the information presented in the petition does not demonstrate that there is a reasonable likelihood that ZTE will prevail in establishing claims 1-11 and 23-29 as unpatentable. Pursuant to 35 U.S.C. § 314, we hereby authorize an *inter partes* review to be instituted only as to claims 12-22 and 30-38 of the '160 patent.

A. Related Matters

ZTE indicates that the '160 patent was asserted against it in *ContentGuard Holdings Inc. v. ZTE Corporation et al.*, Civil Action No.

Best Available Copy

1:12-cv-0206-CMH-TCB, filed in the U.S. District Court for the Eastern District of Virginia on February 27, 2012. Pet. 1. According to ZTE, this patent infringement lawsuit was transferred to the U.S. District Court for the Southern District of California on May 21, 2012. *Id.* ContentGuard does not dispute that it asserted the '160 patent against ZTE.

ZTE also filed five other petitions seeking *inter partes* review of the following patents: U.S. Patent No. 7,523,072 (IPR2013-00133); U.S. Patent No. 7,359,884 (IPR2013-00136); U.S. Patent No. 6,963,859 (IPR2013-00137); U.S. Patent No. 7,139,736 (IPR2013-00138); and U.S. Patent No. 7,269,576 (IPR2013-00139). Pet. 1-2.

B. The Invention of the '160 Patent (Ex. 1001)

The invention of the '160 patent generally relates to distributing and enforcing usage rights for digital works. Ex. 1001, 1:15-16. A digital work refers to any work that has been reduced to a digital representation, including any audio, video, text, or multimedia work, and any accompanying interpreter, *e.g.*, software, which may be required to recreate or render the content of the digital work. Ex. 1001, 5:20-24. Usage rights refer to rights granted to a recipient of a digital work that define the manner in which a digital work may be used and distributed. Ex. 1001, 5:26-30. According to the '160 patent, the disclosed invention permits the owner of a digital work, or other authorized party, to specify a manner of use of the content associated therewith. Ex. 1001, 3:51-54.

Best Available Copy

The '160 patent discloses dividing a digital work into two files: (1) a contents file; and (2) a description tree file. Ex. 1001, 7:65-67. The contents file is a stream of addressable bytes, the format of which completely depends on the interpreter or rendering engine used to play, display, or print the digital work. Ex. 1001, 7:67-8:4. The description tree file makes it possible to examine the rights and fees associated with the digital work without reference to the content of the digital work. Ex. 1001, 8:4-6.

Figure 5 of the '160 patent illustrates a contents file layout for a digital work. Ex. 1001, 4:16-18, 8:10. Figure 5 of the '160 patent is reproduced below:

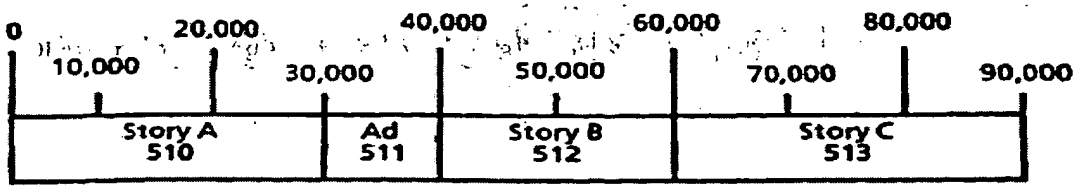


Figure 5

Figure 5 illustrates the format of the contents file of a digital work.

According to the contents file illustrated above, digital work 509 includes story A 510, advertisement 511, story B 512, and story C 513. Ex. 1001, 8:11-12. Assuming that digital work 509 is stored starting at a relative address of 0, the aforementioned portions of digital work 509 are stored so

Best Available Copy

that story A 510 occupies the address of 0-30,000, advertisement 511 occupies the address of 30,001-40,000, story B 512 occupies the address of 40,0001-60,000, and story C 513 occupies the address of 60,0001-90,000. Ex. 1001, 8:12-18.

Figure 8 of the '160 patent illustrates the description tree layout or structure of digital work 509. Ex. 1001, 4:26-27, 8:55-56. Figure 8 of the '160 patent is reproduced below:

Figure 8

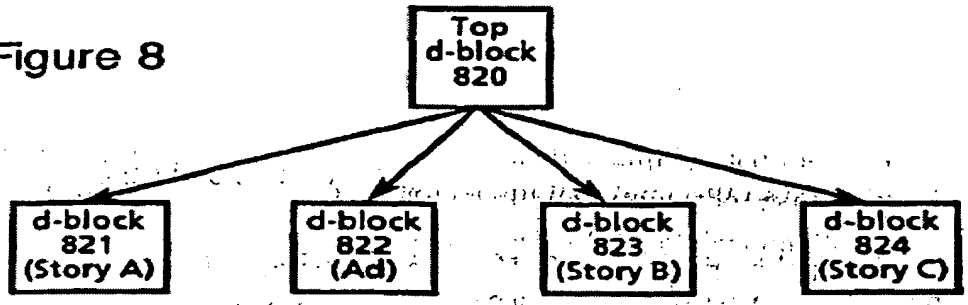


Figure 8 illustrates the structure of the description tree portion of a digital work.

According to the description tree illustrated above, the top descriptor block ("d-block") 820 of the digital work refers to the various stories and advertisement contained therein. Ex. 1001, 8:56-58. The top d-block 820 points to the following: (1) d-block 821, which represents story A 510; (2) d-block 822, which represents advertisement 511; (3) d-block 823, which represents story B 512; and (4) d-block 824, which represents story C 513. Ex. 1001, 8:58-61.

Figure 9 of the '160 patent further illustrates a portion of the description tree associated with d-block 821, which represents story A 510.

Best Available Copy

Ex. 1001, 4:28-29, 8:62-63. Figure 9 of the '160 patent is reproduced below:

Figure 9

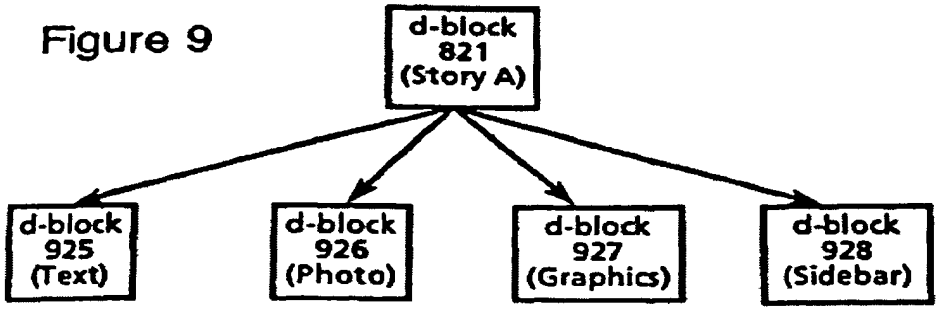


Figure 9 illustrates another level of the description tree associated with d-block 821.

Figure 10 of the '160 patent illustrates the usage rights portions of an individual d-block. Ex. 1001, 4:30-32, 8:66-67. Figure 10 of the '160 patent is reproduced below:

Figure 10

Figure 10 illustrates the usage rights portion of a d-block.

The usage right for each individual d-block has a right code field 1050 and a status information field 1052. Ex. 1001, 9:2-3. The right code field 1050 contains a unique code assigned to the usage right. Ex. 1001, 9:3-4.

Best Available Copy

The status information field 1052 contains information relating to the state of the usage right and the corresponding digital work. Ex. 1001, 9:4-6.

C. Illustrative Claims

Claims 1, 12, 23, and 30 are independent claims. Independent claims 1 and 12 are illustrative:

> 1. A computer readable medium having embedded thereon a digital work adapted to be distributed within in a system for controlling the use of digital works, said digital work comprising:
>
> a digital content portion that is renderable by a rendering device;
>
> a usage rights portion associated with said digital content portion and comprising one or more computer readable instructions configured to permit or prohibit said rendering device to render said digital content portion, said usage rights portion being expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use relating to one or more purposes for which the digital work can be used by an authorized party; and
>
> ***a description structure comprising a plurality of description blocks, each of said description blocks comprising address information for a least one part of said digital work, and a usage rights part for associating one or more usage rights portions.***

Ex. 1001, Claims—48:32-51 (emphasis added).

Best Available Copy

12. A method for creating a digital work to be used in a system for use of the digital work, said method comprising:

obtaining a digital content portion that is renderable by a rendering device;

associating a usage rights portion with the digital content portion, the usage rights portion comprising one or more computer readable instructions configured to permit or prohibit said rendering device to render said digital content portion, said usage rights portion being expressed as statements from a usage rights language having a grammar defining a valid sequence of symbols, and specifying a manner of use relating to one or more purposes for which the digital work can be used by an authorized party;

describing said digital work by a description structure comprising a plurality of description blocks, each of said description blocks comprising addressing information for a least one part of said digital work, and a usage rights part for associating one or more usage rights portions; and

combining the digital content portion and the usage rights portion to create the digital work.

Ex. 1001, Claims—49:16-37 (emphasis added).

D. Prior Art Relied Upon

ZTE relies upon the following prior art references:

Wyman	US 5,260,999	Nov. 9, 1993	Ex. 1013
Porter, Jr. (hereinafter "Porter")	US 5,263,160	Nov. 16, 1993	Ex. 1014
Hartrick (hereinafter "EP '306")	EP 0464306 A2	Jan. 8, 1992	Ex. 1010

Best Available Copy

Hartrick EP 0567800 A1 Nov. 3, 1993 Ex. 1011
(hereinafter "EP '800")

Henry H. Perritt, Jr., "*Knowbots, Permissions Headers and Contract Law*," Paper for the Conference on Technological Strategies for Protecting Intellectual Property in the Networked Multimedia Environment (Apr. 30, 1993) (retrieved from http://archive.ifla.org/documents/infopol/copyright/perh2.txt on Jan. 4, 2013) (Ex. 1006) (hereinafter "Perritt").

Admitted Prior Art—During the original prosecution, the Examiner rejected dependent claim 8 (now dependent claim 5) because "'mark-up prices' are old and well known to those of ordinary skill in retail." Ex. 1002-001347 (Non-Final Rejection dated July 27, 2004, p. 4). Patent Owner did not traverse the Examiner's position that "mark-up prices" are common knowledge in the retail art. As such, the Examiner's statement regarding "mark-up prices" is taken to be admitted prior art.

E. Alleged Grounds of Unpatentability

ZTE seeks to cancel claims 1-38 of the '160 patent based on the following alleged grounds of unpatentability:

1. Claims 1, 2, 9, 12, 13, 23, 30, and 31 as anticipated under 35 U.S.C. § 102(b) by EP '306. Pet. 12-22.

2. Claims 1-3, 8, 9, 12, 13, 15, 16, 20, 23, 30, and 31 as anticipated under 35 U.S.C. § 102(b) by EP '800. *Id.* at 22-33.

3. Claims 2-4, 6, 7, 15-18, 21, 25, 26, 34, and 35 as unpatentable under 35 U.S.C. § 103(a) over the combination of EP '306 and Perritt. *Id.* at 34-38.

Best Available Copy

4. Claims 2-4, 6, 7, 15-18, 21, 25, 26, 34, and 35 as unpatentable under 35 U.S.C. § 103(a) over the combination of EP '800 and Perritt. *Id.* at 38-39.

5. Claims 2, 10, 14, 24-28, and 32-37 as unpatentable under U.S.C. § 103(a) over the combination of EP '306 and Wyman. *Id.* at 39-44.

6. Claims 2, 10, 14, 24-28, and 32-37 as unpatentable under U.S.C. § 103(a) over the combination of EP '800 and Wyman. *Id.* at 44-46.

7. Claims 5 and 19 as unpatentable under 35 U.S.C. § 103(a) over the combination of EP '306, Perritt, and Admitted Prior Art. *Id.* at 47.

8. Claims 5 and 19 as unpatentable under U.S.C. § 103(a) over the combination of EP '800, Perritt, and Admitted Prior Art. *Id.* at 48.

9. Claims 11, 22, 29, and 38 as unpatentable under U.S.C. § 103(a) over the combination of EP '306 and Porter. *Id.* at 48-51.

10. Claims 11, 22, 29, and 38 as unpatentable under U.S.C. § 103(a) over the combination of EP '800 and Porter. *Id.* at 51-53.

II. FINDINGS OF FACT

The following findings of facts are supported by a preponderance of the evidence.

EP '800 (Ex. 1011)

The invention disclosed in EP '800 relates to a data processor that ensures the copying and printing operations for a softcopy book, *e.g.*, electronic book, comply with the royalty payment requirements for making copies of the softcopy book. Ex. 1011, 1:3-8. According to EP '800, the

Best Available Copy

disclosed invention ensures compliance with the royalty requirements of a softcopy book by providing the following improved methods: (1) managing the softcopy text of a structured document in a data processing system; (2) managing the printing of pages of a structured document; (3) managing the writing of a structured document into a bulk storage medium; and (4) managing the telecommunication of softcopies of a structured document. Ex. 1011, 5:19-38.

Figure 3A of EP '800 illustrates the element tags and associated text of a structured document, such as a softcopy book. Ex. 1011, 7:53-54; *see, e.g.*, 2:21-28 and 3:9-11. Figure 3A is reproduced below:

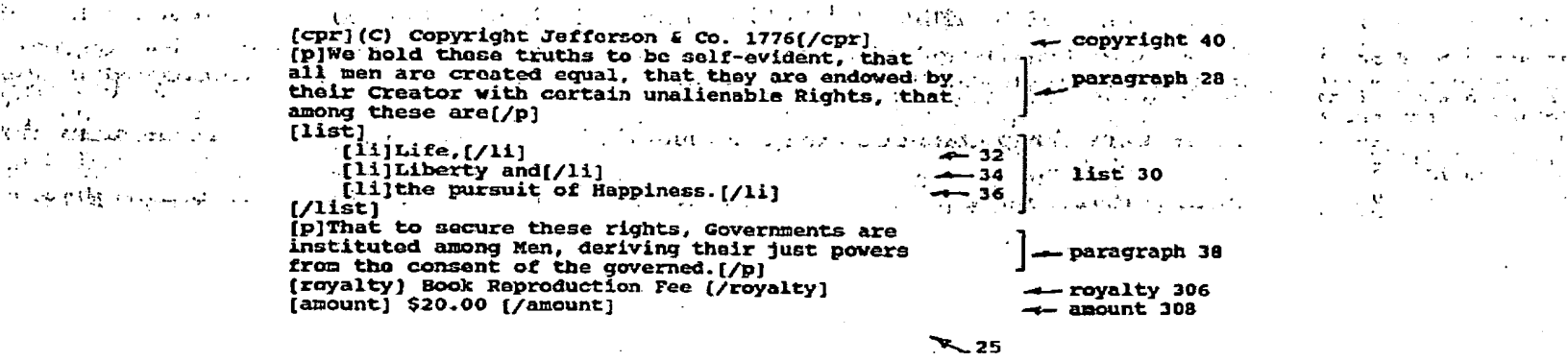


Figure 3A. Example of Control Element Tags and Associated Text

Figure 3A of EP '800 illustrates the organization of document elements 38-42 in a formatted text stream 25 having an ordered sequence. Ex. 1011, 9:35-41. Each element is a structured document element having a begin tag and an end tag. Ex. 1011, 9:43-47. The begin tag and end tag serve to identify the element type. Ex. 1011, 9:47-49. For instance,

Best Available Copy

paragraph 28 is shown in the structured document notation between begin tag [p] and end tag [/p]. Ex. 1011, 9:41-43.

The invention of the EP '800 embeds special strings, such as royalty message 306, within document elements having special structured document tags in the structured document. Ex. 1011, 10:1-5. In particular, Figure 3A of the EP '800 illustrates that royalty message 306 is embedded between a begin tag [royalty] and end tag [/royalty]. Ex. 1011, 10:5-7. When the processor 20 (illustrated in Figure 1) detects the presence of a special tag, such as a royalty begin tag, it makes a note of its presence within memory 22 (illustrated in Figure 1) so when specific functions are requested by various components of the data processing system, copying of the structured document is inhibited and a royalty payment process is invoked. Ex. 1011, 10:7-14. For instance, if a royalty message 306 is identified in the formatted text stream 25, the data processing system inhibits the printer function so that a prospective user cannot print the structured document containing the royalty element. Ex. 1011, 10:14-18.

Figure 3B of EP '800 illustrates the memory organization of element tags and associated text in Figure 3A. Ex. 1011, 7:55-57. Figure 3B is reproduced below:

Petitioner Apple Inc. - Exhibit 1012, p. 2076

Best Available Copy

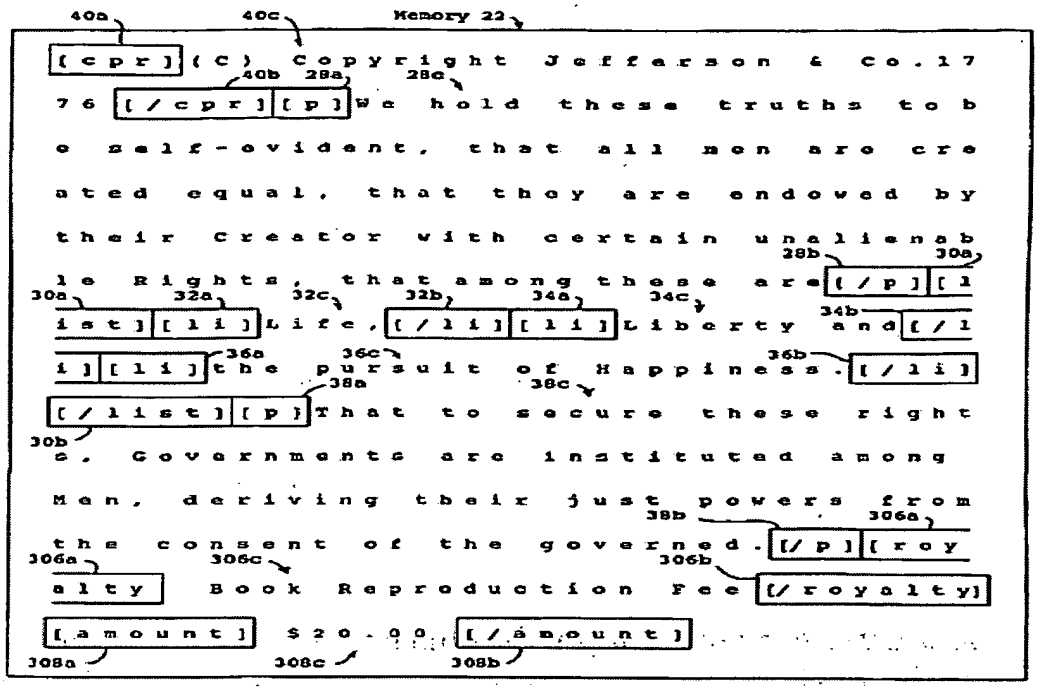


Figure 3B – Memory Organization of Control Element Tags and Associated Text

Figure 3B of EP '800 illustrates storing the structured document and its corresponding tags in memory 22 in a linear sequential order, *i.e.*, the formatted text stream 25. Ex. 1011, 10:24-27. A special copyright notice element is represented by begin tag 40a and end tag 40b, which surrounds copyright notice string 40c. Ex. 1011, 10:38-40. Similarly, the special royalty message element is represented by begin tag 306a and end tag 306b, which surrounds the "Book Reproduction Fee" string 306c. Ex. 1011, 10:41-44.

When the royalty payment program 45 (illustrated in Figure 1) is loaded into the memory 22 of the data processing system, a default parameter table 56 is loaded into memory 22 as well. Ex. 1011, 10:55-11:1.

Best Available Copy

The default parameter table 56 includes a set of default values. Ex. 1011, 11:2-4. Alternatively, a prospective user can enter a profile of values for the parameter table. Ex. 1011, 11:4-6. The parameter table 56 loaded during the initial program loading stage includes characters representing each special tag, such as the royalty tag "[royalty]". Ex. 1011, 11:6-9. The default parameter table 56 also includes values indicating how the data processing system should respond when particular tagged strings are identified in the document text loaded into memory 22. Ex. 1011, 11:10-14. For instance, if a royalty tag "[royalty]" is detected in the structured document, the default parameter table 56 indicates that if the document is displayed on display 26 (illustrated in Figure 1), then the page displayed should include the royalty message. Ex. 1011, 11:14-19.

Figure 7 of EP '800 illustrates the default parameter table 56 after it has been loaded with information pertaining to the document elements associated with each special tag. Ex. 1011, Ex. 8:13-15. Figure 7 is reproduced below:

Best Available Copy

Loaded Parameter Table 56L

	360 Special Tags	362 Text String Loaded from Elements with Special Tags	156 Element Coordinates bk	h1	h2	h3	p	el	364 Display Text	366 Book Royalty Flag	368 Chapter Royalty Flag
300L	bk	Book Title	1	0	0	0	0	1	yes		
302L	ed	Second Edition	1	0	0	0	1	1	yes		
304L	cpr	(C) ABC Co. 1990	1	0	0	0	2	1	yes		
306L	royalty	Book Repro...Fee	1	0	0	0	3	1	yes	x	
308L	amount	$20.00	1	0	0	0	3	2	yes		
310L	phone	1-800-123-1234	1	0	0	0	3	3	yes		
312L	public key	13A723F9...6	1	0	0	0	3	4	no		
314L	validation	The Book ... Paid	1	0	0	0	3	5	no		
318L	royalty	Chapt...Repro Fee	1	1	0	0	1	1	yes		x
320L	amount	$ 1.00	1	1	0	0	1	2	yes		
322L	validation	First Chapt...Paid	1	1	0	0	1	3	no		
344L	royalty	Chapt...Repro Fee	1	2	0	0	1	1	yes		x
346L	amount	$ 2.00	1	2	0	0	1	2	yes		
348L	validation	Second Chapt...Paid	1	2	0	0	1	3	no		

Fig. 7

Figure 7 illustrates default table 56 populated with document elements and special tags.

Figure 7 of EP '800 illustrates that default table 56 includes column 364, which indicates what strings should be displayed on the display 26. Ex. 1011, 11:49-51. For instance, column 364 indicates that royalty message 306, which is represented by the special royalty message string "Book Reproduction Fee" surrounded by being tag [royalty] and end tag [/royalty], should be displayed on display 26. Ex. 1011, 11:46-49.

When the royalty message 306 occurs first in the structured document, and does not occur within a chapter heading, *e.g.*, [h1], it is considered a global element that affects the entire softcopy book. Ex. 1011, 11:51-56. As a consequence, royalty message 306 is flagged in the book royalty flag

Best Available Copy

column 366 of default parameter table 56. Ex. 1011, 11:56-57. Because royalty message 306 is the first occurring royalty element in the structured document, it represents the royalty message for copying the entire softcopy book. Ex. 1011, 11:57-12:3. In addition, the corresponding royalty information in the special tags that occur immediately following royalty message 306 are considered global elements that apply when the entire book is copied. Ex. 1011, 12:3-7. The special tags associated with royalty message 306 include the following: (1) "[amount] $20.00 [/amount]" 308; (2) "[phone] 1-800-123-1234 [/phone]" 310; (3) "[public key] 13A723F9 . . . 6 [/public key]" 312; and (4) "[validation] The Book Repo Fee Is Paid [/validation]" 314. Ex. 1011, 12:7-12.

III. CLAIM CONSTRUCTION

Consistent with the statute and legislative history of the Leahy-Smith America Invents Act, Pub. L. 112-29, 125 Stat. 284, 329 (2011) ("AIA"), we construe claims by applying the broadest reasonable interpretation in light of the specification. 37 C.F.R. § 42.100(b); *see also Office Patent Trial Practice Guide*, 77 *Fed. Reg.* 48756, 48766 (Aug. 14, 2012). There is a "heavy presumption" that a claim term carries its ordinary and customary meaning. *CCS Fitness, Inc. v. Brunswick Corp.*, 288 F.3d 1359, 1366 (Fed. Cir. 2002). However, a "claim term will not receive its ordinary meaning if the patentee acted as his own lexicographer and clearly set forth a definition of the disputed claim term in either the specification or prosecution history." *Id.* "Although an inventor is indeed free to define the specific terms used to

Best Available Copy

describe his or her invention, this must be done with reasonable clarity, deliberateness, and precision." *In re Paulsen*, 30 F.3d 1475, 1480 (Fed. Cir. 1994). Also, we must be careful not to read a particular embodiment appearing in the specification into the claim if the claim language is broader than that embodiment. *See In re Van Geuns*, 988 F.2d 1181, 1184 (Fed. Cir. 1993).

A. Preambles (Claims 1, 12, 23, and 30)

ContentGuard contends that the preambles of independent claims 1, 12, 23, and 30 are limiting and, therefore, are entitled to patentable weight. Prel. Resp. 18-22. ContentGuard correctly notes that the claim terms "the digital work" and "said digital work" recited in the bodies of independent claims 1 and 23 refer back to the recitation of "a digital work" in the claims' preambles for antecedent basis. *Id.* at 19-20. ContentGuard also correctly notes that the bodies of independent claims 1 and 23 are directed to describing the necessary components of the claimed "digital work." *Id.* at 20. But then ContentGuard asserts that the recitation in the preamble of "a digital work adapted to be distributed within a system for controlling the use of digital works" is a necessary and defining aspect of the claimed invention and, as a consequence, should be treated as a limitation of independent claims 1 and 23. *Id.* at 20-21. As to this assertion, we do not agree with ContentGuard.

In general, a preamble is construed as a limitation "if it recites essential structure or steps, or if it is 'necessary to give life, meaning, and vitality' to the claim." *Catalina Mktg. Int'l, Inc. v. Coolsavings.com, Inc.*,

Petitioner Apple Inc. - Exhibit 1012, p. 2081

Best Available Copy

289 F.3d 801, 808 (Fed. Cir. 2002) (quoting *Pitney Bowes, Inc. v. Hewlett-Packard Co.*, 182 F.3d 1298, 1305 (Fed. Cir. 1999)). However, a preamble is not limiting "'where a patentee defines a structurally complete invention in the claim body and uses the preamble only to state a purpose or intended use for the invention.'" *Catalina Mktg.*, 289 F.3d at 808 (quoting *Rowe v. Dror*, 112 F.3d 473, 478 (Fed. Cir. 1997)); *see also Symantec Corp. v. Computer Assocs. Int'l Inc.*, 522 F.3d 1279, 1288 (Fed. Cir. 2008).

In this case, the recitations in the preambles of independent claims 1 and 23 immediately following "a digital work"—namely "adapted to be distributed within a system for controlling use of digital works"—are mere statements of intended use for an invention that is already structurally complete as defined in the body of each claim. Accordingly, the aforementioned recitations in the preambles of independent claims 1 and 23 provide no patentable significance to the claimed subject matter.

ContentGuard relies upon essentially the same argument presented for independent claims 1 and 23 to assert that all portions of the preambles of independent claims 12 and 30 are limiting and, therefore, are entitled to patentable weight. Pet. 21-22. Once again, we do not agree with ContentGuard.

Similar to our analysis above, the recitations in the preambles of independent claims 12 and 30 immediately following "a digital work"—namely "to be used in a system for use of the digital work"— are mere statements of intended use. The preambles of independent claims 12 and 30 do not recite any essential method steps. Moreover, the claimed method

Best Available Copy

steps of "obtaining," "associating," "describing," and "combining" are already complete and do not require more from the preamble for meaning. As a result, the aforementioned recitations in the preambles of independent claims 12 and 30 provide no patentable significance to the claimed subject matter.

B. Description Structure (Claims 1, 12, 23, and 30)

ZTE contends that upon reviewing the specification of the '160 patent, the broadest reasonable interpretation of the claim term "description structure" includes at least a description tree, which is "a structure which describes the location of content and the usage rights and usage fees for a digital work." Pet. 6 (citing to Ex. 1001, 47:31-37). In response, ContentGuard contends that ZTE's claim construction for the claim term "description structure" is based on a partial quotation of the "description tree" as disclosed in the glossary of the '160 patent. Prel. Resp. 17. ContentGuard argues that, at best, the claim term "description structure" could include a "description tree," but the specification of the '160 patent does not support that a "description structure" must necessarily include a "description tree." *Id.* Instead, ContentGuard argues that independent claims 1, 12, 23, and 30 explicitly recite the necessary elements that make up the claimed "description structure." *Id.* at 18. For instance, ContentGuard alleges that the "description structure" recited in independent claim 1 must be part of the claimed "digital work" and include "a plurality of description blocks," "address information for at least one part of said

Petitioner Apple Inc. - Exhibit 1012, p. 2083

Best Available Copy

digital work," and "a usage rights part for associating one or more usage rights portions." *Id.*

ContentGuard's argument is misplaced. While a claim may recite other claim features which further limit a "description structure," the pivotal issue is the meaning of the claim term "description structure." The additional claim features recited in independent claim 1, 13, 23, and 30 narrow the scope of each claim, but do not convey a definition for the claim term "description structure." At issue is the meaning of claim term "description structure," not what type of description structure is within the scope of the claim.

ZTE correctly indicates that the glossary of the '160 patent explicitly sets forth a special definition for a "description tree." For convenience, the entire glossary definition for a "description tree" is reproduced below:

> Description Tree—A structure which describes the location of content and usage rights and usage fees for a digital work. A description tree is comprised of description blocks. Each description block corresponds to a digital work or to an interest (typically a revenue bearing interest) in a digital work.

Ex. 1001, 47:31-36.

We agree with ContentGuard that there is not an express indication in the specification of the '160 patent that the claim term "description structure" necessarily encompasses a "description tree." However, upon reviewing the specification of the '160 patent in its entirety, as well as the prosecution history of the '160 patent, we determine that it is unreasonable to accord a meaning to the claim term "description structure" that is different

Best Available Copy

from the meaning of a "description tree." In the context of the specification as filed and the prosecution history, ContentGuard uses the two terms "description structure" and "description tree" synonymously, *i.e.*, without distinction.

This is evident by the fact that the term "description structure" is not used in the specification as filed. Nor does the term appear in any of the original claims of the application. The term "description structure" was added during prosecution in a claim amendment. Ex. 1002-00335 (Claim Amendment date Feb. 14, 2006). In contrast, the term "description tree" is used throughout the specification as filed. It is simply unclear what is covered by a "description structure," but not covered by a "description tree," and vice-versa. ContentGuard does not identify any written description support for the claim term "description structure" beyond that which also supports a "description tree" and, on this record, we find none.

In addition, the term "description structure," as a claim term, is no less important than a "description tree." Yet, the term "description structure" cannot be found in the glossary, but the glossary does contain a special definition for a "description tree." Moreover, the special definition in the glossary for a "description tree" begins with "***a structure***." Emphasis added. All of the foregoing reasons support the conclusion that the claim term "description structure" has the same meaning as a "description tree." Consequently, we look to the discussion of a "description tree" in the specification of the '160 patent to construe the meaning of the claim term "description structure."

Best Available Copy

Indeed, the specification of the '160 patent actually provides two meanings for a "description tree." As discussed above, the glossary of the '160 patent explicitly sets forth a special definition for a "description tree." In addition, the specification of the '160 patent states that "the term description tree as used herein refers to any type of acyclic structure used to represent the relationship between the various components of a digital work." Ex. 1001, 8:6-9. Therefore, the specification sets forth two meanings for a "description tree," one broad and one narrow. The two meanings are not contradictory. Rather, they reflect a difference in scope, as one encompasses the other. In view of the foregoing, noting that the second definition is the broader one and, thereafter, applying the broadest reasonable interpretation standard, we conclude that a "description tree"—otherwise known as a "description structure"—is any acyclic structure that represents the relationship between the components of a digital work.

While we agree with ContentGuard that independent claims 1, 12, 23, and 30 provide additional claim features that serve to further limit the claimed "description structure," the claim features recited in each independent claim do not provide a basis for construing the claim term "description structure" as innately or inherently possessing such features. In other words, the claim term "description structure" does not itself require the additional claim features recited in independent claims 1, 12, 23, and 30.

Accordingly, we construe the claim term "description structure" recited in independent claims 1, 12, 23, and 30 as any acyclic structure that represents the relationship between the components of a digital work.

Best Available Copy

C. Remaining Claim Terms

All remaining claim terms recited in claims 1-38 are given their ordinary and customary meaning as would be understood by one with ordinary skill in the art, and need not be further construed at this time.

IV. ANALYSIS

A. 35 U.S.C. § 102(b) Ground of Unpatentability—EP '800

ZTE contends that claims 1-3, 8, 9, 12, 13, 15, 16, 20, 23, 30, and 31 are anticipated under 35 U.S.C. § 102(b) by EP '800. Pet. 22-33. In particular, ZTE relies upon claim charts to explain how EP '800 allegedly describes the subject matter recited in these claims, and the Declaration of Dr. Vijay K. Madisetti (Ex. 1015) to support its positions. *Id.* In response, ContentGuard presents arguments predicated on two claim groupings—(1) for independent claims 1 and 23, EP '800 does not disclose "[a] computer readable medium having embedded thereon a digital work . . . said digital work comprising . . . a description structure"; and (2) for independent claims 12 and 30, EP '800 does not disclose a "method for creating a digital work" that includes the step of "describing . . . by a description structure." *See* Prel. Resp. 32-35. We will address ContentGuard's arguments with respect to each group of independent claims in turn.

Claims 1 and 23

ContentGuard contends that ZTE has not demonstrated that EP '800 discloses a "description structure" that is part of a "digital work," as required

Petitioner Apple Inc. - Exhibit 1012, p. 2087

Best Available Copy

by in independent claims 1 and 23. Prel. Resp. 35. We agree with ContentGuard.

We begin our analysis by determining the scope and breadth of independent claims 1 and 23. Both independent claims 1 and 23 recite "[a] computer readable medium having embedded thereon a digital work . . . said digital work comprising" three elements: (1) "a digital content portion;" (2) "a usage rights portion associated with said digital content portion;" and (3) "a description structure." Accordingly, the cited prior art must disclose "a digital work" that includes "a description structure" in order to anticipate independent claims 1 and 23.

To establish anticipation, each and every element in a claim, arranged as is recited in the claim, must be found in a single prior art reference. *Karsten Mfg. Corp. v. Cleveland Golf Co.*, 242 F.3d 1376, 1383 (Fed. Cir. 2001); *see also NetMoneyIn, Inc. v. Verisign, Inc.*, 545 F.3d 1359, 1369 (Fed. Cir. 2008). ZTE takes the position that EP '800 discloses a parameter table that describes a structured document of a softcopy book. Pet. 23-25 and 27-28 (citing to Ex. 1011, Fig. 7; 11:46-12:12 and 13:44-58). However, contrary to ZTE's position, EP '800's parameter table is not included within, or part of, the softcopy book as is required by independent claims 1 and 23.

Figure 3A of EP '800 illustrates a softcopy book in the form of a structured document, *i.e.*, the claimed "digital work," that contains special tags and associated text. Ex. 1011, 7:53-54; *see, e.g.*, 2:21-28 and 3:9-11. EP '800 discloses that the processor in the data processing system loads a

Petitioner Apple Inc. - Exhibit 1012, p. 2088

Best Available Copy

default parameter table with information pertaining to each special tag found in the structured document. Ex. 1011, 8:13-15 and 11:6-9. Figure 7 of EP '800 illustrates a parameter table, *i.e.*, the claimed "description structure," populated with the information pertaining to the document elements associated with each special tag. Ex. 1011, 11:46-12:12. Based on these cited disclosures, EP '800 discloses that the special tags found in the structured document are used to create the parameter table, but the structured document does not itself include the parameter table. In other words, EP '800's parameter table is not included within, or part of, the structured document, but rather is a mutually exclusive data structure created from the document elements and special tags derived from the structured document.

Because ZTE's position with respect to EP '800 does not properly account for "a digital work" that includes "a description structure," ZTE has not demonstrated a reasonable likelihood of prevailing on its assertion that independent claims 1 and 23 are anticipated by EP '800.

Claims 2, 3, 8, and 9

Claims 2, 3, 8, and 9 each depend directly or indirectly from independent claim 1. Therefore, for the same reasons set forth above with respect to independent claim 1, ZTE has not demonstrated a reasonable likelihood of prevailing on its assertion that dependent claims 2, 3, 8, and 9 are anticipated by EP '800.

Claims 12 and 30

To rebut the grounds of unpatentability asserted by ZTE against independent claims 12 and 30, ContentGuard relies upon essentially the

Petitioner Apple Inc. - Exhibit 1012, p. 2089

Best Available Copy

same arguments it presented in rebutting the grounds of unpatentability asserted by ZTE against independent claims 1 and 23. Prel. Resp. 35. In order to determine whether those arguments have merit, we first must determine the scope and breadth of independent claims 12 and 30. Both independent claims 12 and 30 recite "a method for creating a digital work . . . said method comprising" the following method steps: (1) "obtaining a digital content portion;" (2) "associating a usage rights portion with the digital content portion;" (3) "describing said digital work by a description structure;" and (4) "combining the digital content portion and the usage rights portion to create the digital work." In contrast to independent claims 1 and 23, independent claims 12 and 30 do not require that "a description structure" be included within "a digital work." Instead, there need only be "a description structure" that describes "a digital work."

As discussed above, ZTE contends that EP '800 discloses a parameter table that describes a structured document of a softcopy book. Pet. 23-25 and 27-28 (citing to Ex. 1011, Fig. 7; 11:46-12:12 and 13:44-58). We agree with ZTE. Figure 7 of EP '800 illustrates a parameter table, *i.e.*, the claimed "description structure," populated with the information pertaining to the document elements associated with each special tag found in the structured document, *i.e.*, the claimed "digital work." Ex. 1011, 11:46-12:12. Based on that cited disclosure, EP '800's parameter table describes the document elements and special tags derived from the structured document. As such, ZTE has presented sufficient evidence to warrant a finding that EP '800

Best Available Copy

discloses "a description structure" that describes "a digital work," as required by independent claims 12 and 30.

Because ZTE's position with respect to EP '800 properly accounts for "a description structure" that describes "a digital work," ZTE has demonstrated a reasonable likelihood of prevailing on its assertion that independent claims 12 and 30 are anticipated by EP '800.

Claim 13, 15, 16, 20, and 31

To rebut the grounds of unpatentability asserted by ZTE against dependent claims 13, 15, 16, 20, and 31, ContentGuard relies upon essentially the same arguments it presented in rebutting the grounds of unpatentability asserted by ZTE against independent claims 12 and 30. Prelim. Resp. 32-35. As discussed above, those arguments are not persuasive. In addition, the explanations provided by ZTE as to how EP '800 describes the claimed subject matter recited in dependent claims 13, 15, 16, 20, and 31 have merit and are otherwise unrebutted. As a result, ZTE has demonstrated a reasonable likelihood of prevailing on its assertion that dependent claims 13, 15, 16, 20, and 31 are anticipated by EP '800.

B. 35 U.S.C. § 103(a) Grounds of Unpatentability Based in Part on EP '800

ZTE contends that: (1) claims 2-4, 6, 7, 15-18, 21, 25, 26, 34, and 35 are unpatentable under 35 U.S.C. § 103(a) over the combination of EP '800 and Perritt (Pet. 35-39); (2) claims 2, 10, 14, 24-28, and 32-37 are unpatentable under 35 U.S.C. § 103(a) over the combination of EP '800 and Wyman (*id.* at 41-46); (3) claims 5 and 19 are unpatentable under 35 U.S.C. § 103(a) over the combination of EP '800, Perritt, and Admitted Prior Art

Best Available Copy

(*id.* at 47-48); and (4) claims 11, 22, 29, and 38 are unpatentable under 35 U.S.C. § 103(a) over the combination of EP '800 and Porter (*id.* at 50-53). In particular, ZTE relies upon claim charts to explain how EP '800, Perritt, Wyman, Admitted Prior Art, or Porter allegedly describe the subject matter recited in these claims, and the Declaration of Dr. Madisetti (Ex. 1015) to support its positions. *Id.* ZTE also provides articulated reasons with rational underpinnings to combine EP '800 with Perritt, Wyman, Admitted Prior Art, and Porter. *Id.*

In response, ContentGuard contends that ZTE does not provide an articulated reason with a rational underpinning to support each of the alleged grounds of unpatentability based on obviousness. Prel. Resp. 36-38. In particular, ContentGuard directs our attention to ZTE's rationale for combining EP '306 and Perritt, and generally alleges that ZTE does not adequately explain why one with ordinary skill in the art would make the proffered combination. *Id.* at 37. ContentGuard also argues that merely pointing out that the cited prior art references are in the same field of endeavor is insufficient to vitiate patentability. *Id.* at 38.

Similar to our analysis above, we will address ContentGuard's arguments with respect to the claims that depend from each group of independent claims—namely (1) claims that depend from independent claims 1 and 23; and (2) claims that depend from independent claims 12 and 30.

Best Available Copy

Claims 2-7, 10, 11, and 24-29

Claims 2-7, 10, 11, and 24-29 each depend directly or indirectly from independent claims 1 or 23. As discussed above, ZTE's position with respect to EP '800 does not properly account for "a digital work" that includes "a description structure," as required by independent claims 1 and 23. As applied by ZTE, Perritt, Wyman, Admitted Prior Art, and Porter do not remedy the above-noted deficiency in EP '800. Therefore, for the same reasons set forth above with respect to independent claims 1 and 23, ZTE has not demonstrated a reasonable likelihood of prevailing on its assertion that: (1) dependent claims 2-4, 6, 7, 25 and 26 are unpatentable over the combination of EP '800 and Perritt; (2) dependent claims 2, 10, and 24-28 are unpatentable over the combination of EP '800 and Wyman; (3) dependent claim 5 is unpatentable over the combination of EP '800, Perritt, and Admitted Prior Art; and (4) dependent claims 11 and 29 are unpatentable over the combination of EP '800 and Porter.

Claims 14-19, 21, 22, and 32-38

Claims 14-19, 21, 22, and 32-38 each depend directly or indirectly from independent claims 12 or 30. With respect to these claims, we are not persuaded by ContentGuard's argument that ZTE does not provide an articulated reason with a rationale underpinning to support each of the alleged grounds of unpatentability based on obviousness. Prel. Resp. 36-38. Contrary to ContentGuard's argument, ZTE provides an articulated reason with a rationale underpinning to combine EP '800 with each of the following

Best Available Copy

prior art references: (1) Perritt; (2) Wyman; (3) Perritt and Admitted Prior Art; and (4) Porter. *See, e.g.,* Pet. 39, 46, and 52-53.

For instance, ZTE contends that dependent claims 15-18, 21, 34, and 35 are unpatentable under 35 U.S.C. § 103(a) over the combination of EP '800 and Perritt. Pet. 35-39. To support combining the teachings of EP '800 and Perritt, ZTE states:

> As EP '800 and Perritt each relate to protecting a copyright owner's interests in a digital work, one of ordinary skill in the art would have been motivated to combine the teaching of EP '800 with Perritt to provide a system that offers increased flexibility in copyright protection by specifying varying economic terms and conditions for using the digital work. (Perritt, pp. 1; 3-6; *see also* Madisetti Decl. ¶¶ 100-102.)

Id. at 39. ZTE's explanation constitutes an articulated reason with a rational underpinning to justify the legal conclusion of obvious. ContentGuard does not provide a sufficient or credible explanation indicating why the proposed combination of EP '800 and Perritt is improper. For example, ContentGuard did not submit credible evidence or argument regarding technological difficulties that might prevent one with ordinary skill in the art from combining EP '800 and Perritt in the manner proposed by ZTE. Nor does ContentGuard provide persuasive evidence or technological reasoning pertaining to why the proffered combination would produce an unexpected result.

As a result, ZTE has demonstrated a reasonable likelihood of prevailing on its assertion that: (1) dependent claims 15-18, 21, 34, and 35 are unpatentable over EP '800 and Perritt; (2) dependent claims 14 and 32-

Best Available Copy

37 are unpatentable over the combination of EP '800 and Wyman; (3) dependent claim 19 is unpatentable over the combination of EP '800, Perritt, and Admitted Prior Art; and (4) dependent claims 22 and 38 are unpatentable over the combination of EP '800 and Porter.

C. Declaration of Dr. Vijay K. Madisetti (Ex. 1015)

ContentGuard contends that Dr. Madisetti's declaration is entitled to little or no weight because it merely parrots the arguments made by ZTE in the petition. Prel. Resp. 40. ContentGuard's argument is inconsequential. Even if we were to give Dr. Madisetti's declaration little or no weight, the content of cited prior art references and the arguments of the parties still constitute sufficient evidence supporting a reasonable likelihood that ZTE will prevail on its assertion that claims 12-22 and 30-38 of the '160 are unpatentable.

D. Remaining 35 U.S.C. §§ 102(b) and 103(a) Grounds of Unpatentability Based in Whole or in Part on EP '306

Claims 1-7, 9-19, and 21-38

ZTE contends that claims 1-7, 9-19, and 21-38 are unpatentable under 35 U.S.C. §§ 102(b) and 103(a) based in whole or in part on EP '306. Pet. 12-22, 34-37, 39-44, and 47-51. The disclosures for EP '306 and EP '800 are essentially the same. *Compare* Ex. 1010, Figs. 3 and 5, *with* Ex. 1011, Figs. 3B and 7. As such, the alleged grounds of unpatentability proposed for claims 1-7, 9-19, and 21-38 that are based in whole or in part on EP '306 are essentially the same as the alleged grounds of unpatentability proposed for the same claims that are based in whole or in part on EP '800.

Best Available Copy

For the alleged grounds of unpatentability directed to claims 1-7, 9-11, and 23-29 that are based in whole or in part on EP '306, ZTE has not demonstrated a reasonable likelihood of prevailing on its assertion that these claims are anticipated by, or unpatentable over, EP '306 for essentially the same reasons discussed above with respect to EP '800. For the alleged grounds of unpatentability directed to claims 12-19, 21, 22, and 30-38 that are based in whole or in part on EP '306, these grounds of unpatentability are redundant to the grounds of unpatentability on which we initiate an *inter partes* review for the same claims. Accordingly, we do not authorize an *inter partes* review on the remaining grounds of unpatentability asserted by ZTE against claims 1-7, 9-19, and 21-38 of the '160 patent. *See* 37 C.F.R. § 42.108(a).

V. ORDER

Accordingly, it is

ORDERED that pursuant to 35 U.S.C. § 314(a), an *inter partes* review is hereby instituted as to claims 12-22 and 30-38 of the '160 patent for the following grounds of unpatentability:

A. Claims 12, 13, 15, 16, 20, 30, and 31 as anticipated under 35 U.S.C. § 102(b) by EP '800;

B. Claims 15-18, 21, 34, and 35 as unpatentable under 35 U.S.C. § 103(a) over the combination of EP '800 and Perritt;

C. Claims 14 and 32-37 as unpatentable under 35 U.S.C. § 103(a) over the combination of EP '800 and Wyman;

Best Available Copy

D. Claim 19 as unpatentable under 35 U.S.C. § 103(a) over the combination of EP '800, Perritt, and Admitted Prior Art;

E. Claims 22 and 38 as unpatentable under 35 U.S.C. § 103(a) over the combination of EP '800 and Porter;

FURTHER ORDERED that an *inter partes* review is not instituted as to claims 1-11 and 23-29 of the '160 patent;

FURTHER ORDERED that pursuant to 35 U.S.C. § 314(c) and 37 C.F.R. § 42.4, notice is hereby given of the institution of a trial. The trial will commence on the entry date of this decision.

FURTHER ORDERED that an initial conference call with the Board is scheduled for 2 PM on July 23, 2013. The parties are directed to the Office Trial Practice Guide, 77 *Fed. Reg.* 48756, 48765-66 (Aug. 14, 2012) for guidance in preparing for the initial conference call, and should come prepared to discuss any proposed changes to the Scheduling Order entered herewith and any motions the parties anticipate filing during the trial.

Best Available Copy

Case IPR2013-00134
U.S. Patent No. 7,225,160

For PETITIONER:

Jon H. Beaupre
Jeremy S. Snodgrass
Richard K. DeMille
BRINKS HOFER GILSON AND LIONE
jbeaupre@brinkshofer.com
jsnodgrass@brinkshofer.com
rdemille@brinkshofer.com

For PATENT OWNER:

Robert Greene Sterne
Jon E. Wright
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C
rsterne-PTAB@skgf.com
jwright-PTAB@skgf.com

This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ **BLACK BORDERS**
- ☐ **IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- ☒ **FADED TEXT OR DRAWING**
- ☐ **BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- ☐ **SKEWED/SLANTED IMAGES**
- ☐ **COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- ☐ **GRAY SCALE DOCUMENTS**
- ☒ **LINES OR MARKS ON ORIGINAL DOCUMENT**
- ☐ **REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- ☐ **OTHER:**

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

Trials@uspto.gov
571-272-7822

Paper 34
Entered: August 6, 2013

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

ZTE CORPORATION AND ZTE (USA) INC.
Petitioner,

v.

CONTENTGUARD HOLDINGS INC.
Patent Owner.

Case IPR2013-00134 (JL)
Patent 7,225,160

Before JAMESON LEE, MICHAEL W. KIM, and MICHAEL R. ZECHER, *Administrative Patent Judges.*

LEE, *Administrative Patent Judge.*

JUDGMENT
Request for Adverse Judgment
37 C.F.R. § 42.73(b)

Introduction

On July 24, 2013, the Patent Owner ("ContenGuard") requested cancellation of claims 12-22 and 30-38, all of the involved claims in this *inter partes* review, and entry of adverse judgment. (Paper 28.) Petitioner ("ZTE") did not file an

opposition within the ten (10) calendar day period it was provided for such an opposition (Paper 25), but in a conference call held on July 29, 2013, indicated that it desires and prefers that the Board does not act on ContentGuard's request until ZTE's Motion for Joinder in IPR2013-00454, filed on July 19, 2013, has been considered. In that motion, ZTE seeks to join IPR2013-00454 with this *inter partes* review.

Discussion

Under 35 U.S.C. § 42.73(b), a party may request judgment against itself at any time during a proceeding. Also, under 37 C.F.R. § 42.73(b)(2), actions construed as a request for entry of adverse judgment include cancellation of a claim such that the party has no remaining claim in the trial.

ContentGuard has not only requested cancellation of all claims involved in this *inter partes* review, such that after the cancellation it will have no remaining claim in the trial, but also expressly requested entry of adverse judgment.

Although ZTE desires and prefers that the Board does not act on ContentGuard's request for cancellation of claims and request for entry of adverse judgment until such time as when ZTE's Motion for Joinder filed in IPR2013-00454 has been considered, the Board sees no reason for delay. The two cases have not yet been joined and this case is now ready for entry of judgment.

The Motion for Joinder in IPR2013-00454 does not, and should not, act as an automatic stay of this proceeding. While ZTE expressed its desire and preference that ContentGuard's Request for Entry of Adverse Judgment not be considered until the Motion for Joinder in IPR2013-00454 has been considered, it has not sought to file a motion to stay this proceeding.

Order

For the foregoing reasons, it is

ORDERED that ContentGuard's request to cancel claims 12-22 and 30-38 and request for entry of adverse judgment are *granted*;

FURTHER ORDERED that judgment is herein entered against ContentGuard with respect to claims 12-22 and 30-38 of Patent 7,225,160; and

FURTHER ORDERED that claims 12-22 and 30-38 of Patent 7,225,160 are herein cancelled.

Petitioner Apple Inc. - Exhibit 1012, p. 2102

For PETITIONER:

Jon H. Beaupre
Richard K. DeMille
David Bluestone
Miyoung Shin
Peter Lee
Lawrence Chen
BRINKS HOFER GILSON AND LIONE
jbeaupre@brinkshofer.com
rdemille@brinkshofer.com
dbluestone@brinkshofer.com
mshin@brinkshofer.com
plee@brinkshofer.com
lchen@brinkshofer.com

For PATENT OWNER

Robert Greene Sterne
Jon E. Wright
STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C
rsterne-PTAB@skgf.com
jwright-PTAB@skgf.com

Doc Code: **TRIAL.CERT** Date (for IFW TOC): 11/14/2013
(Date sent to IFW scanning)

PATENT NUMBER: 7,225,160 APPLICATION NO.: 10/015,951
ISSUED: 5/29/2007

CHECKLIST FOR ISSUANCE OF AIA TRIAL CERTIFICATE

CASE NUMBER: IPR2013-00134 PETITION FILING DATE: 2/11/2013

The results of IPR2013-00134

_____

_____

[*insert proceeding no(s). and filing date(s) and indicate if joined or consolidated*]

are reflected in this:

☒ **INTER PARTES REVIEW (IPR) CERTIFICATE UNDER 35 U.S.C. 318(b).**
[*Kind Code* K]

☐ **POST-GRANT REVIEW (PGR) CERTIFICATE UNDER 35 U.S.C. 328(b).**
[*Kind Code* J]

☐ **DERIVATION (DER) CERTIFICATE UNDER 35 U.S.C. 135(d).**
[*Kind Code* O]

PETITIONER: ZTE Corporation & ZTE (USA), Inc.

PATENT OWNER: Contentguard Holdings, Inc.

BIBLIOGRAPHIC DATA:

Abstract of Title of Patent attached: ☒ Yes ☐ No*

If no Abstract of Title available, then Front Page of Patent and any Certificate of Corrections and/or Reexamination Certificates attached: ☐ Yes ☐ No*

****NOTE: If "No" to both, then Trial Paralegal please complete the following:**

Title: _____

_____

Inventor(s): _____

_____

Petitioner Apple Inc. - Exhibit 1012, p. 2104

Doc Code: **TRIAL.CERT** Date (for IFW TOC): 11/14/2013
(Date sent to IFW scanning)

PATENT NUMBER: 7,225,160 **APPLICATION NO.:** 10/015,951
ISSUED: 5/29/2007

Applicants (complete only if original patent application was filed on or after Sep. 16, 2012):

_____

_____

_____

Assignee(s): _____

_____

Patent No.: _____
Issued: _____
Appl. No.: _____
Filed: _____

TRIAL CERTIFICATE WILL INDICATE THE FOLLOWING:

a. Change in Specification: ☒ **No** ☐ **Yes If "Yes"** ☐ **Substitution(s) to Column No(s). are attached. (please enter column and line nos.):** _____

b. Change in Drawings: ☒ **No** ☐ **Yes If "Yes"** ☐ **Substitution(s) to Figure No(s).** _____ **are attached.**

c. Status of the Claims (list each claim *only once*):

☐ **Patent Claims Found Patentable:** _____

_____

☒ **Patent Claims Cancelled:** 12-22 & 30-38

_____

☐ **Substitute Claims:** _____

_____

_____

☐ **Substitute Claims attached.**

☐ **Patent Claims Disclaimed:** _____

d. Other Changes: Trial Paralegal please enter the Patent Owner Motion to Amend and [date filed] containing the approved change, and either enter the change below or attach a copy of the approved change to this checklist. Only changes approved for entry by the Trial Judges are to be included.

☐ **Title:** _____

_____

Petitioner Apple Inc. - Exhibit 1012, p. 2105

Doc Code: **TRIAL.CERT** Date (for IFW TOC): 11/14/2013
(Date sent to IFW scanning)

PATENT NUMBER: 7,225,160 APPLICATION NO.: 10/015,951
ISSUED: 5/29/2007

☐ **Inventors:**

_____

_____

☐ **Applicants (complete if original patent application was filed on or after Sep. 16, 2012):**

_____

_____

☐ **Assignee:** _____

_____

☐ **Abstract:** _____

☐ **Substitute Abstract attached.**

Petitioner Apple Inc. - Exhibit 1012, p. 2106

Patent Assignment Abstract of Title

Total Assignments: 2

Application #: 10015951 **Filing Dt:** 12/17/2001 **Patent #:** 7225160 **Issue Dt:** 05/29/2007

PCT #: NONE **Publication #:** US20020128972 **Pub Dt:** 09/12/2002

Inventors: Mark J. Stefik, Peter L.T. Pirolli, Ralph C Merkle

Title: DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME

Assignment: 1

Reel/Frame: 012685 / 0424 **Received:** 03/21/2002 **Recorded:** 03/11/2002 **Mailed:** 05/14/2002 **Pages:** 2

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignors: STEFIK, MARK J. **Exec Dt:** 02/05/2002

PIROLLI, PETER L.T. **Exec Dt:** 02/05/2002

Assignee: CONTENTGUARD HOLDINGS, INC.
103 FOULK ROAD, SUITE 200-M
WILMINGTON, DELAWARE 19803

Correspondent: NIXON PEABODY LLP
MARC S. KAUFMAN
SUITE 800
8180 GREENSBORO DR.
MCLEAN, VA 22102

Assignment: 2

Reel/Frame: 018298 / 0399 **Received:** 09/15/2006 **Recorded:** 09/12/2006 **Mailed:** 09/25/2006 **Pages:** 3

Conveyance: ASSIGNMENT OF ASSIGNORS INTEREST (SEE DOCUMENT FOR DETAILS).

Assignors: STEFIK, MARK J. **Exec Dt:** 08/03/2006

PIROLLI, PETER L.T. **Exec Dt:** 08/08/2006

MERKLE, RALPH C. **Exec Dt:** 06/11/2006

Assignee: CONTENTGUARD HOLDINGS, INC.
103 FOULK ROAD, SUITE 200-M
WILMINGTON, DELAWARE 19803

Correspondent: NIXON PEABODY LLP
CARLOS R. VILLAMAR
401 9TH STREET, N.W.
SUITE 900
WASHINGTON, D.C. 20004

Search Results as of: 11/14/2013 03:30 PM

If you have any comments or questions concerning the data displayed, contact PRD / Assignments at 571-272-3350. v.2.2.4
Web interface last modified: Jul 8, 2013 v.2.2.4

To:	Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Southern District of California on the following: _X_ Patents or ___ Trademarks:

DOCKET NO.	**DATE FILED**	**US District Court** Southern District of California
3:13-cv-03073-LAB-JMA	12/17/13	San Diego, CA
PLAINTIFF		DEFENDANT
ZTE Corporation, et al.		ContentGuard Holdings, Inc.

PATENT OR TRADEMARK NO.	**PATENT OR TRADEMARK NO.**	**PATENT OR TRADEMARK NO.**
1. 6,963,859	6. 7,523,072	11.
2. 7,139,736	7.	12.
3. 7,225,160	8.	13.
4. 7,269,576	9.	14.
5. 7,359,884	10.	15.

In the above-entitled case, the following patents(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY __ Amendment __ Answer __ Cross Bill __ Other Pleading	
PATENT OR TRADEMARK NO.	**PATENT OR TRADEMARK NO.**	**PATENT OR TRADEMARK NO.**
1.	6.	11.
2.	7.	12.
3.	8.	13.
4.	9.	14.
5.	10.	15.

In the above-entitled case, the following decision has been rendered or judgment issued:

DECISION/JUDGMENT

CLERK	(BY) DEPUTY CLERK	DATE
John Morrill, Acting Clerk of Court		

(12) **INTER PARTES REVIEW CERTIFICATE** (1st)
United States Patent
Stefik et al.

(10) **Number: US 7,225,160 K1**
(45) **Certificate Issued: Jan. 14, 2014**

(54) **DIGITAL WORKS HAVING USAGE RIGHTS AND METHOD FOR CREATING THE SAME**

(75) Inventors: **Mark J. Stefik**; **Peter L.T. Pirolli**; **Ralph C Merkle**

(73) Assignee: **Contentguard Holdings, Inc.**

Trial Number:

IPR2013-00134 filed Feb. 11, 2013

Petitioner: ZTE Corporation & ZTE (USA), Inc.

Patent Owner: Contentguard Holdings, Inc.

Inter Partes Review Certificate for:

Patent No.:	**7,225,160**
Issued:	**May 29, 2007**
Appl. No.:	**10/015,951**
Filed:	**Dec. 17, 2001**

The results of IPR2013-00134 are reflected in this inter partes review certificate under 35 U.S.C. 318(b).

INTER PARTES REVIEW CERTIFICATE
U.S. Patent 7,225,160 K1
Trial No. IPR2013-00134
Certificate Issued Jan. 14, 2014

AS A RESULT OF THE INTER PARTES REVIEW PROCEEDING, IT HAS BEEN DETERMINED THAT:

Claims **12**-**22** and **30**-**38** are canceled.

* * * * *