

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE PATENT TRIAL AND APPEAL BOARD

DOLBY LABORATORIES, INC.
Petitioner,

v.

INTERTRUST TECHNOLOGIES CORPORATION

Patent Owner

Case IPR2020-00663

U.S. Patent No. 7,406,603

DECLARATION OF DR. VIJAY K. MADISETTI



I. INTRODUCTION

A. Engagement

1. I submit this report on behalf of Dolby Laboratories, Inc. in connection with their request for *inter partes* review of U.S. Patent No. 7,406,603 (the “’603 patent”)—to review and to provide my opinion on the scope and content of “prior art” predating the application for the ’603 patent and regarding the subject matter recited in the claims of the ’603 patent. I understand that this Declaration relates to a Petition for the above-captioned *inter partes* review (IPR) of the ’603 patent.

2. For my efforts in connection with the preparation of this declaration, I have been compensated at my standard hourly consulting rate of \$550. My compensation is in no way contingent on the results of these or any other proceedings relating to the above-captioned patent. I have no expectation or promise of additional business with the Petitioner in exchange for the positions explained herein.

3. I make this declaration based on personal knowledge.

B. Background and Qualifications

4. A detailed description of my professional qualifications, including a listing of my specialties/expertise and professional activities, is contained in my curriculum vitae, a copy of which is attached as Appendix A. In what follows, I provide a short summary of my professional qualifications.

5. I have over thirty years of experience as an electrical and computer engineer in industry, education, and consulting.

6. I am a Professor in Electrical and Computer Engineering at Georgia Tech. I have worked extensively in the field of information systems (including information security), digital communications and have studied telecommunications and systems engineering since 1981. I also have over 20 years of industry experience in computer engineering, secure information systems, distributed computer systems, networking, software engineering, signal processing, and telecommunications, including wireless communications and signal processing. Throughout this time, I have designed, implemented, and tested various products in the fields of electronics, computer engineering, and communications.

7. In 1984, I received a Bachelor of Technology in Electronics and Electrical Communications Engineering from the Indian Institute of Technology (IIT). In 1989, I received my Ph.D. in Electrical Engineering and Computer Sciences (EECS) from the University of California, Berkeley. That year, I also received the Demetri Angelakos Outstanding Graduate Student Award from the University of California, Berkeley, and the IEEE/ACM Ira M. Kay Memorial Paper Prize.

8. In 1989, I also joined the faculty of Georgia Tech. I began working at Georgia Tech as an assistant professor, became an associate professor in 1995, and have held my current position since 1998. As a member of the faculty at Georgia

Tech, I have been active in, among other technologies, cloud computing, distributed computing, image and video processing, computer engineering, information security, embedded systems, chip design, software systems, wireless networks and cellular communications.

9. I have been involved in research and technology in the area of computing and digital signal processing since the late 1980s, and I am the Editor-in-Chief the IEEE Press/CRC Press's 3-volume Digital Signal Processing Handbook (Editions 1 & 2) (1998, 2010).

10. Over the past three decades, I studied, used, and designed distributed systems, including one of the first published works in distributed secure content delivery networks, that included processing of multimedia signals over the internet, called BEEHIVE, in addition to image and video processing and wireless networking circuits for several applications, including digital and video cameras, mobile phones and networking products for leading commercial firms.

11. Between 1994-1998 as part of a research initiative in collaboration with the US Army Research Laboratory and Georgia Tech, I and my students developed one of the first published implementations of a distributed signal processing environment, where secure sensor data (from US Army) was accessed over the network and processed and rendered/displayed at distributed and protected server locations (Georgia Tech, Rice University, and Spelman College) utilizing Java-

based object broker technologies. This secure environment, BEEHIVE, is shown in the figure below, implemented within Java, utilized resource objects (including servers), data sources (such as cameras and sensors), sink sources (such as display), and service objects (representing Java applications), broker objects (e.g., schedulers), and user COE interfaces (e.g., GUIs) that download applications that run locally on secure data obtained from networked sources consistent with information policies and user privileges.

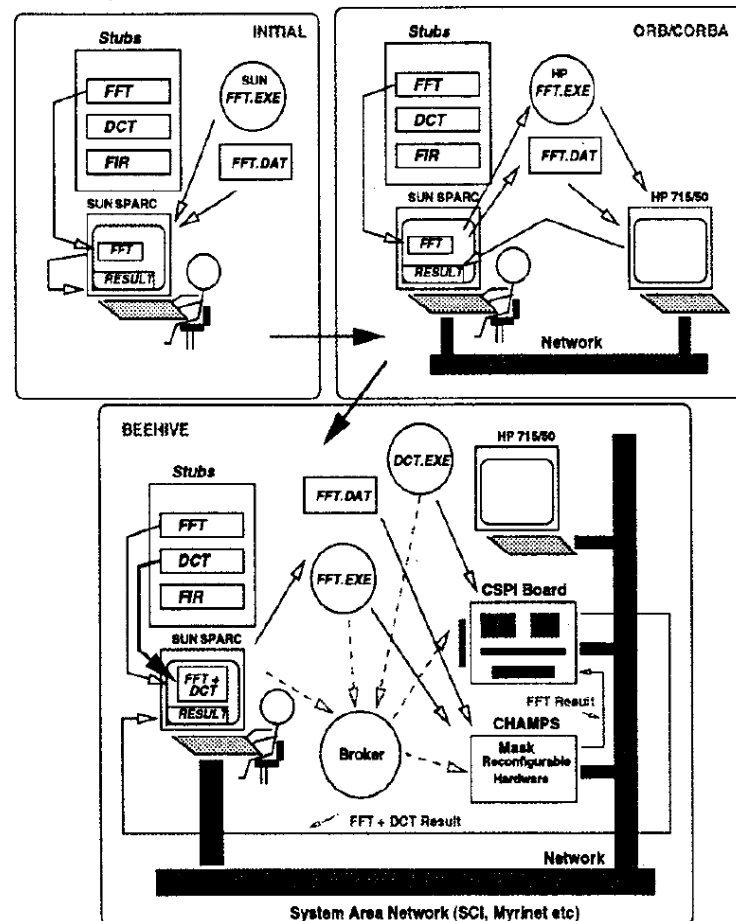


Figure 1. Evolution of the BEEHIVE Project.

12. A detailed description of the distributed environment is described in the Figure 4 below.

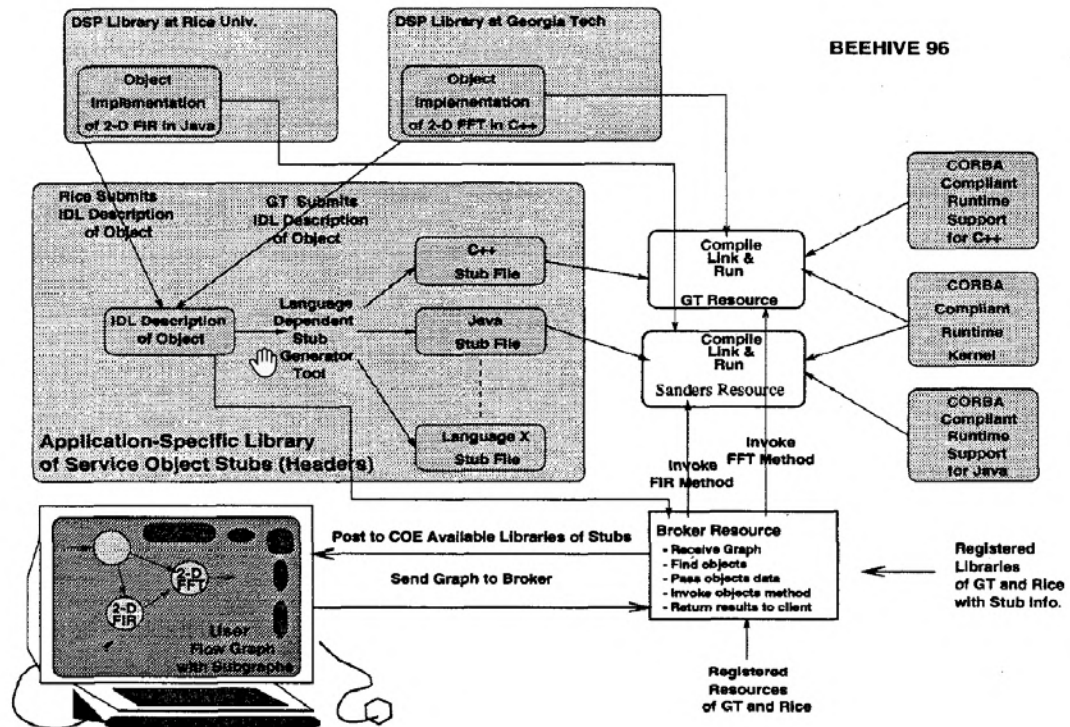


Figure 4. BEEHIVE Environment v0.1. Next version plans to include seamless support for BEEHIVE-compliant DSP cards and FPGA boards.

13. Prior to or around the timeframe of the filing the '603 Patent, some of my significant work in the area of digital image processing, video processing, networking technologies, and software engineering include the following:

- i. M. Romdhane, V. Madiseti, "All Digital Oversampled Front-End Sensors", IEEE Signal Processing Letters, Vol 3, Issue 2, 1996;

- ii. A. Hezar, V. Madiseti, “Efficient Implementation of Two-Band PR-QMF Filterbanks”, IEEE Signal Processing Letters, Vol 5, Issue 4, 1998; and
- iii. R. Tummala, V. Madiseti, System on Chip or System on Package”, IEEE Design & Test of Computers, Vol 16, Issue 2, 1999

14. I have also designed code and compilation tools for chipsets used for advanced imaging and document cameras used in photocopying and other applications, such as the Intel MXP 5800 family of image processing chipsets that have been widely used in commercial document imaging and video products since the late 1990s. I have also implemented H.264 and AVC video compression and rendering codecs for a large commercial semiconductor vendor in the mid 2000 timeframe. I have published several papers on audio, video and image content processing in a distributed environment over the two decades.

15. I also have significant experience in designing and implementing electronic equipment using various source code languages, including C, assembly code, VHDL, and Verilog. In 2000, I published a book entitled “VHDL: Electronics Systems Design Methodologies.” In 1997, I was awarded the VHDL International Best PhD Dissertation Advisor for my contributions in the area of rapid prototyping.

16. Since 1995, I have authored, co-authored, or edited several books in the areas of communications, signal processing, chip design, and software engineering, including VLSI Digital Signal Processors (1995), Quick-Turnaround ASIC Design in VHDL (1996), The Digital Signal Processing Handbook (1997 & 2010), Cloud Computing: A Hands-On Approach (2013), Internet of Things: A Hands-On Approach (2014), Big Data Science & Analytics (2016).

17. I have authored over 100 articles, reports, and other publications pertaining to electrical engineering, and in the areas of computer engineering, communications signal processing, and communications. All of my publications, including the ones identified above, are set forth in my attached CV.

18. I have implemented several electronic devices, including audio and video codecs, echo cancellers, equalizers, and multimedia audio/video compression applications and modules for a leading commercial mobile phone manufacturer. I have also designed tools for porting mobile applications from one platform to another for a leading mobile phone manufacturer. I have also developed hardware and software designs for a leading set-top box manufacturer. I am familiar with the design, test and implementation of embedded systems, such as image and video processing systems, security systems, barrier control systems, and associated software and hardware architectures.

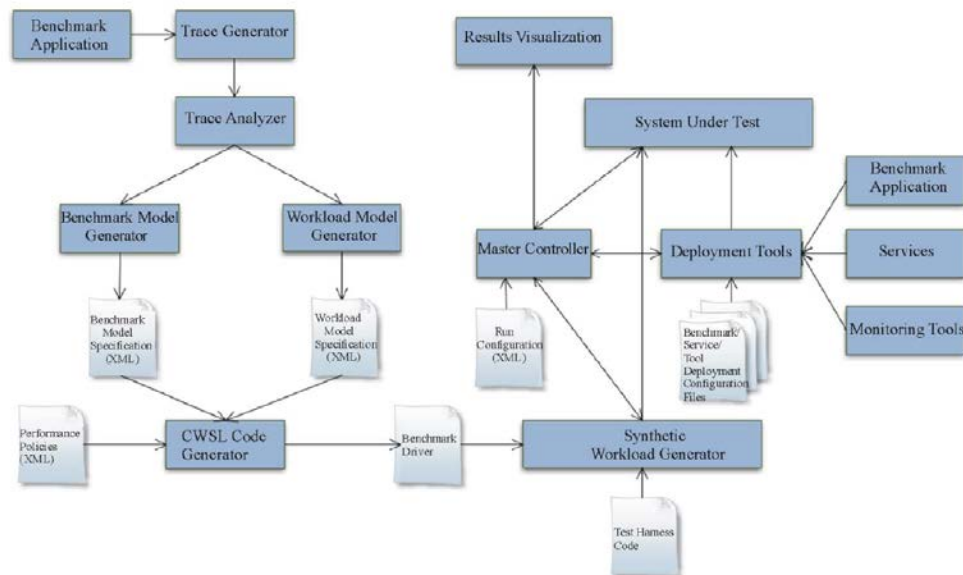
19. I have been elected a Fellow of the Institute of Electrical and Electronics Engineers (“IEEE”) in recognition of my contributions to embedded computing systems. The IEEE is a worldwide professional body consisting of more than 300,000 electrical and electronic engineers. Fellow is the highest grade of membership of the IEEE, with only one-tenth of one percent of the IEEE membership being elected to the Fellow grade each year.

20. In 2006, I was awarded the Frederick Emmons Terman Medal from the American Society of Engineering Education (ASEE) and HP Corporation for my contribution to electrical engineering while under the age of 45.

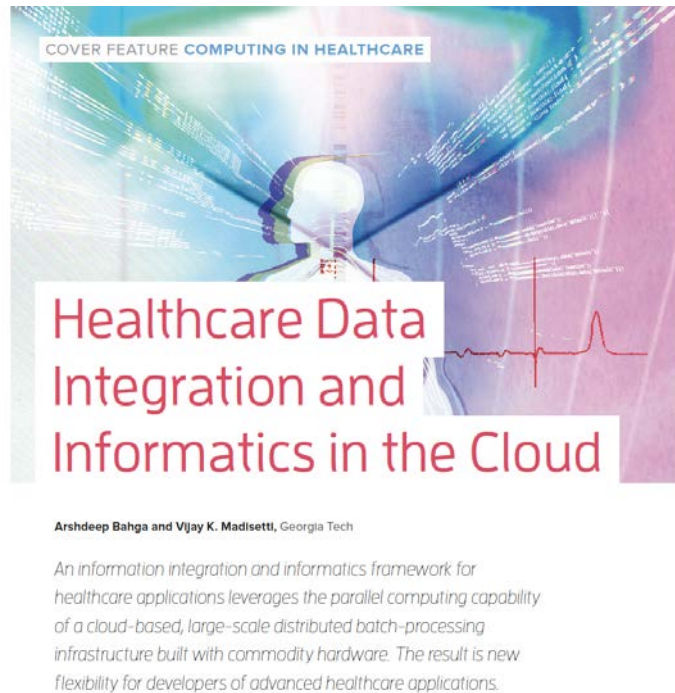
21. I have been working in the areas of secure cloud computing, workload modeling, virtualization, and benchmarking for over ten years.

22. In the area of characterization, modeling and generation of workloads for cloud computing applications I have created a synthetic workload generator for virtual environments that accepts benchmark and workload model specifications. I also developed a cloud workload specification language called, GT-CWSL, to provide a structured way for specification of application workloads. These approaches allow accurate characterization of virtualization and cloud performance, and have been published in “Synthetic Workload Generation for Cloud Computing Applications”, Journal of Software Engineering and Applications, 2011, Vol 4, pp. 396-410.

23. Our methodology for analysis of virtual workloads on cloud platforms is shown in the figure below.



24. In other work related to distributed computing, virtualization, performance modeling, and data integration, I have developed cloud-based information integration and informatics framework, called CHISTAR, that allows integration of secure distributed and heterogeneous healthcare data into a common virtual environment (on commodity hardware running hypervisors) allow easier analysis and analytics to be performed. This research was presented as a cover feature in the Special Issue on Computing in Healthcare, IEEE Computer Magazine, in 2015.



25. In my work on rapid prototyping of cloud-based virtual services and systems, I proposed a new methodology using loosely coupled virtual components that are not restricted by architecture or programming styles. This approach, shown below, creates virtual components that are then integrated and deployed effectively to realize improvements in deployment efficiency and time to deployment, as shown below.

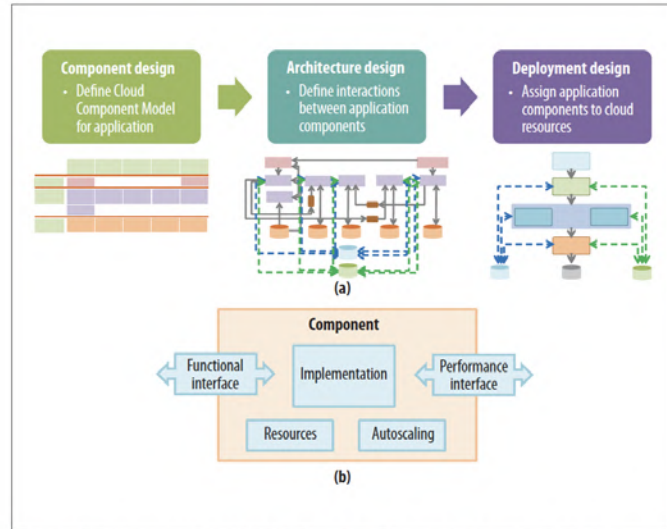


Figure 2. Cloud Component Model (CCM)-based development: (a) design methodology, which comprises component, architecture, and deployment design; and (b) CCM component architecture. CCM's component-based approach is suitable for both Web-based and mobile applications.

26. Use of our CCM-based virtualization and distributed cloud component methodology improved throughput and response times as shown below. These results were published in flagship journal, IEEE Computer Magazine, in November 2013.

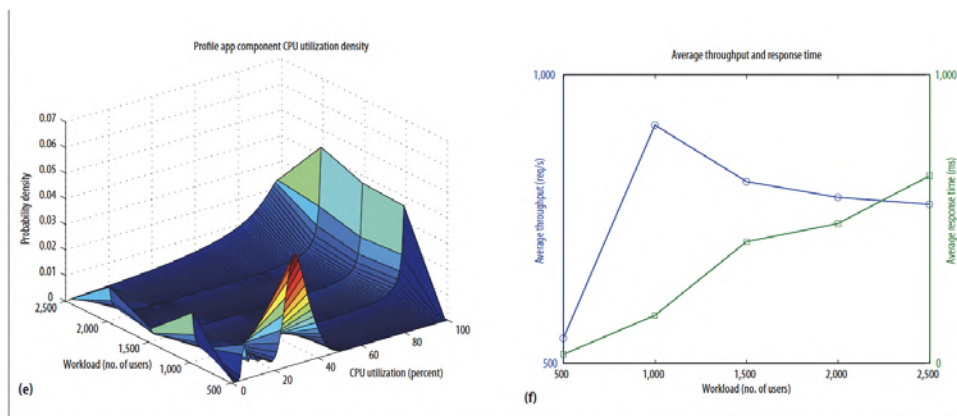
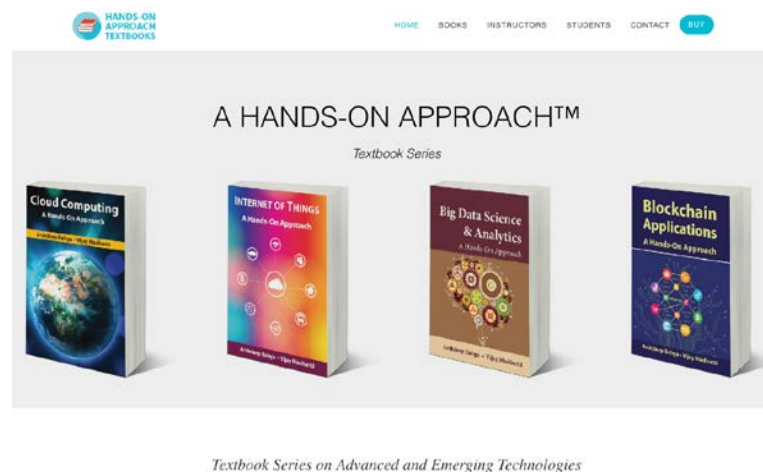


Figure 4. Results of performance monitoring in Experiments 1 and 2. (a) Average CPU use in Experiment 1. (b) CPU use density of the catalog component in Experiment 1. (c) Throughput and response time in Experiment 1. (d) Average CPU use in Experiment 2. (e) CPU use density of the customer profile component in Experiment 2. (f) Throughput and response time in Experiment 2. The two experiments show that scaling up the catalog component can increase throughput and decrease response time.

27. In addition to research and commercialization projects in secure computing, in virtualization and cloud computing and advanced cloud applications and data

analytics, I have also taught courses and written books in these areas. These books are widely used by dozens of universities all over the world.

28. I also have nearly thirty issued or pending applications for US Patents in the past twenty years in areas that include content management and digital rights management, encryption and crypto-currency applications.



C. Basis of My Opinion and Materials Considered

29. I have reviewed the '603 patent and the prior art and other documents and materials cited herein. For ease of reference, the full list of documents that I have considered is included in Appendix B.

30. My opinions in this declaration are based on my review of these documents, as well as upon my education, training, research, knowledge, and experience.

31. I have reviewed, had input into, and endorse as set forth fully herein the discussions in the accompanying Petition.

D. Legal Standards for Patentability

32. I am not an attorney and I offer no opinions on the law itself. My understanding of the relevant law principles this section is based on information provided to me by counsel.

1. Priority

33. I was informed and understand that for a patent to claim the benefit of an earlier provisional application, each application in the chain leading back to the provisional must comply with the written description requirement of 35 U.S.C. § 112. To satisfy the written description requirement, the specification of the provisional must contain a written description of the claimed invention and the manner and process of making and using it, in such full, clear, concise, and exact terms to enable an ordinarily skilled artisan to practice the invention. Moreover, the provisional application must describe the later claimed invention in sufficient detail that a person of ordinary skill in the art can clearly conclude that the inventor had possession of the claimed invention as of the provisional filing date.

2. Obviousness

34. I have been informed that a claim may be unpatentable under 35 U.S.C. § 103(a) if the subject matter described by the claim as a whole would have been obvious to a hypothetical person of ordinary skill in the art in view of a prior art reference or in view of a combination of references at the time the alleged

invention was made. I have been informed that obviousness is determined from the perspective of a hypothetical person of ordinary skill in the art and that the asserted claims of the patent should be read from the point of view of such a person at the time the alleged invention was made. I have been informed that a hypothetical person of ordinary skill in the art is assumed to know and to have all relevant prior art in the field of endeavor covered by the patent in suit, and would thus have been familiar with each of the references cited herein, as well as the background knowledge in the art discussed in Section VII, and the full range of teachings they contain.

35. I have been informed that there are two criteria for determining whether prior art is analogous and thus can be considered prior art: (1) whether the art is from the same field of endeavor, regardless of the problem addressed, and (2) if the reference is not within the field of the patentee's endeavor, whether the reference still is reasonably pertinent to the particular problem with which the patentee is involved. I have also been informed that the field of endeavor of a patent is not limited to the specific point of novelty, the narrowest possible conception of the field, or the particular focus within a given field. I have also been informed that a reference is reasonably pertinent if, even though it may be in a different field from that of the patentee's endeavor, it is one which, because of the matter with which it

deals, logically would have commended itself to a patentee's attention in considering his problem.

36. I have also been informed that an analysis of whether an alleged invention would have been obvious should be considered in light of the scope and content of the prior art, the differences (if any) between the prior art and the alleged invention, and the level of ordinary skill in the pertinent art involved. I have been informed as well that a prior art reference should be viewed as a whole.

37. I have also been informed that in considering whether an invention for a claimed combination would have been obvious, I may assess whether there are apparent reasons to combine known elements in the prior art in the manner claimed in view of interrelated teachings of multiple prior art references, the effects of demands known to the design community or present in the market place, and/or the background knowledge possessed by a person having ordinary skill in the art. I have been informed that other principles may be relied on in evaluating whether an alleged invention would have been obvious, and that these principles include the following:

- A combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results;
- When a device or technology is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the

same field or in a different one, so that if a person of ordinary skill can implement a predictable variation, the variation is likely obvious;

- If a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill;
- An explicit or implicit teaching, suggestion, or motivation to combine two prior art references to form the claimed combination may demonstrate obviousness, but proof of obviousness does not depend on or require showing a teaching, suggestion, or motivation to combine;
- Market demand, rather than scientific literature, can drive design trends and may show obviousness;
- In determining whether the subject matter of a patent claim would have been obvious, neither the particular motivation nor the avowed purpose of the named inventor controls;
- One of the ways in which a patent's subject can be proved obvious is by noting that there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims;

- Any need or problem known in the field of endeavor at the time of invention and addressed by the patent can provide a reason for combining the elements in the manner claimed;
- “Common sense” teaches that familiar items may have obvious uses beyond their primary purposes, and in many cases a person of ordinary skill will be able to fit the teachings of multiple patents together like pieces of a puzzle;
- A person of ordinary skill in the art is also a person of ordinary creativity, and is not an automaton;
- A patent claim can be proved obvious by showing that the claimed combination of elements was “obvious to try,” particularly when there is a design need or market pressure to solve a problem and there are a finite number of identified, predictable solutions such that a person of ordinary skill in the art would have had good reason to pursue the known options within his or her technical grasp; and
- One should be cautious of using hindsight in evaluating whether an alleged invention would have been obvious.

38. I have further been informed that, in making a determination as to whether or not the alleged invention would have been obvious to a person of ordinary skill, the Board may consider certain objective factors if they are present, such as: commercial success of products practicing the alleged invention; long-felt but

unsolved need; teaching away; unexpected results; copying; and praise by others in the field. These factors are generally referred to as “secondary considerations” or “objective indicia” of nonobviousness. I have been informed, however, that for such objective evidence to be relevant to the obviousness of a claim, there must be a causal relationship (called a “nexus”) between the claim and the evidence and that this nexus must be based on what is claimed and novel in the claim rather than something in the prior art. I also have been informed that even when they are present, secondary considerations may be unable to overcome primary evidence of obviousness (e.g., motivation to combine with predictable results) that is sufficiently strong.

39. I have been asked to consider the patentability of Claims 1 and 2 (the “Challenged Claims”) of the ’603 patent that are challenged in the Petition. I have been informed that for *inter partes* reviews, unpatentability must be shown under a preponderance of the evidence standard. I have been informed that to establish something by a preponderance of the evidence one needs to prove it is more likely true than not true. I have concluded that each of the Challenged Claims is unpatentable under 35 U.S.C. § 103 based on **Griswold**, or under 35 U.S.C. § 103 based on **England**, as described below, under both the preponderance of the evidence standard as well as the higher standard of clear and convincing evidence.

3. Claim Construction

40. I have been informed that patent claims are construed from the viewpoint of a person of ordinary skill in the art at the time of the alleged invention. I have been informed that patent claims generally should be interpreted consistent with their plain and ordinary meaning as understood by a person of ordinary skill in the art in the relevant time period (*i.e.*, at the time of the purported invention, or the so called “effective filing date” of the patent application), after reviewing the patent claim language, the specification and the prosecution history (*i.e.*, the intrinsic record).

41. I have further been informed that a person of ordinary skill in the art must read the claim terms in the context of the claim itself, as well as in the context of the entire patent specification. I understand that in the specification and prosecution history, the patentee may specifically define a claim term in a way that differs from the plain and ordinary meaning. I understand that the prosecution history of the patent is a record of the proceedings before the U.S. Patent and Trademark Office, and may contain explicit representations or definitions made during prosecution that affect the scope of the patent claims. I understand that an applicant may, during the course of prosecuting the patent application, limit the scope of the claims to overcome prior art or to overcome an examiner’s rejection, by clearly and unambiguously arguing to overcome or distinguish a prior art reference, or to clearly and unambiguously disavow claim coverage.

42. In interpreting the meaning of the claim language, I understand that a person of ordinary skill in the art may also consider “extrinsic” evidence, including expert testimony, inventor testimony, dictionaries, technical treatises, other patents, and scholarly publications. I understand this evidence is considered to ensure that a claim is construed in a way that is consistent with the understanding of those of skill in the art at the time of the alleged invention. This can be useful for technical terms whose meaning may differ from its ordinary English meaning. I understand that extrinsic evidence may not be relied on if it contradicts or varies the meaning of claim language provided by the intrinsic evidence, particularly if the applicant has explicitly defined a term in the intrinsic record.

II. DESCRIPTION OF THE RELEVANT FIELD AND THE RELEVANT TIMEFRAME

43. I have carefully reviewed the '603 patent and its prosecution history.

44. I understand that the '603 patent issued from U.S. Patent Application 09/653,517, filed on August 31, 2000, and claims the benefit of U.S. Provisional Application No. 60/151,790 filed on August 31, 1999.

45. I have been instructed by counsel to assume the relevant timeframe for my analysis in this declaration to be on or before August 31, 1999.

46. Based on my review of this material, I believe that the relevant general fields for the purposes of the '603 patent are electronic data protection and digital rights management.

III. THE PERSON OF ORDINARY SKILL IN THE RELEVANT FIELD IN THE RELEVANT TIMEFRAME

47. My opinions are provided based on what a person of ordinary skill in the art in the technical field of the invention would have understood at the time of the invention of the Challenged Claims. As I explained above, the relevant timeframe in this Declaration is on or before August 31, 1999. I have been informed and understand that the content of a patent and prior art should be interpreted the way a person of ordinary skill in the art (“POSITA”) would have interpreted those references at the time of the invention of the patent using the ordinary and customary meanings of the claim terms. I understand that the POSITA is a hypothetical concept referring to one who thinks along the lines of conventional wisdom at the time.

48. I was asked to provide an opinion as to the level of a POSITA pertinent to the subject matter set forth in the Challenged Claims of the ’603 patent at the time of the priority date. I have been informed that the level of one of ordinary skill in the art is evidenced by prior art references. In the relevant time period, it is my opinion that a POSITA in the field of the Challenged Claims would have been someone with a good working knowledge of data protection, electronic content protection, and/or digital rights management. A POSITA to whom the patent is addressed would have a Bachelor of Science in computer science, electrical engineering, mathematics, or a related field, and approximately two years of

professional experience or equivalent study in electronic data protection or digital rights management. Additional graduate education could substitute for professional experience, or significant experience in the field could substitute for formal education. The basis for my familiarity with the level of ordinary skill is my own technical experience and my own interaction with large numbers of students and my employees in the computing field who were at this level of skill. In reaching this opinion as to the hypothetical POSITA, I have considered the types of problems encountered in the art, the prior art solutions to those problems, the rapidity with which innovations are made, the sophistication of the technology, and the educational level and professional capabilities of workers in the field.

IV. TECHNICAL BACKGROUND AND STATE OF THE ART

49. The '603 patent describes "data protection systems and methods." (Ex. 1001, Title). While the listed inventors seem to believe they have described and claimed a novel technique, the method of processing a portion of electronic media content using a software module and evaluating whether the software module processes the portion of the electronic media content in an authorized manner has been previously practiced, and in the same manner as claimed in Claims 1 and 2 of the '603 patent:

1. A method for protecting electronic media content from unauthorized use by a user of a computer system, the method including:
receiving a request from a user of the computer system to use a piece of electronic media content;

identifying one or more software modules responsible for processing the piece of electronic media content and enabling use of the piece of electronic media content by the user;

processing at least a portion of said piece of electronic media content using at least one of the one or more software modules;

evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner, the evaluating including at least one action selected from the group consisting of:

- evaluating whether the at least one of the one or more software modules make calls to certain system interfaces;

- evaluating whether the at least one of the one or more software modules direct data to certain channels;

- analyzing dynamic timing characteristics of the at least one of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity;

denying the request to use the piece of electronic media content if the evaluation indicates that the at least one of the one or more software modules fail to satisfy a set of predefined criteria.

2. A method as in claim 1, further including: using the predefined criteria to evaluate the at least one of the one or more software modules according to a predefined policy, and basing a decision to deny the request on the outcome of this evaluation.

Below I provide some background information related to Claims 1 and 2 of the '603 patent.

50. The '603 patent is directed to digital rights management ("DRM") systems and methods for protecting electronic content and recognizes the need to "provide enhanced resistance to attempts to circumvent content protection." (Ex. 1001, Abstract, 1:23-30, 3:2-3.) Such need has been recognized in the prior art well before

1999. For example, **England** discloses that for digital content “the publisher (or reseller) gives or sells the content to a client, but continues to restrict rights to use the content even after the content is under the sole physical control of the client,” and thus “the legitimate user of a computer can be an adversary of the data or content provider.” (Ex. 1005, 1:61-2:8.) Accordingly, **England** recognizes that “there is a need in the art for a digital rights management operating system that enforces digital rights on content downloaded from a provider while operating on a general purpose personal computer without the need of specialized or additional hardware.” (Ex. 1005, 3:57-61.) Similarly, **Griswold** explains that “licensed products may be easily copied or ‘pirated’ and used without the licensor’s knowledge” and recognizes the need to “ensure that a licensed product is used only on machines under which it is licensed.” (Ex. 1006, 1:29-33, 3:30-34.)

51. One well-known way of protecting digital content was allowing use of the content only by “trusted” software. For example, Peinado et al. in U.S. Patent No. 7,319,759 (Ex. 1008), based on an application filed March 15, 2000 and claiming the benefit of a provisional application filed March 27, 1999, described “trusted” elements and explained that “to be ‘trusted’ means that the license server 24 (or any other trusting element) is satisfied that the trusted element will carry out the wishes of the owner of the digital content 12 according to the rights description in the license 16, and that a user cannot easily alter such trusted element for any purpose,

nefarious or otherwise.” (Ex. 1008, 15:48-56.) When content is accessed, it may flow in a path from the rendering application to its ultimate destination, and there may be multiple software “modules” that define such a path. (Ex. 1008, 33:53-34:25.) Software or program “modules” include routines, programs, objects, components, data structures and the like that perform particular tasks or implement particular abstract data types. (Ex. 1008, 5:46-49.) Thus, preferably the DRM system would “authenticate[] such path 58 to ensure that each constituent module 62 in the path 58 is to be trusted by the DRM system 32. Otherwise, the potential exists that one or modules 62 in the path can be employed by a nefarious entity to obtain the naked digital content 12 as such naked digital content 12 leaves the rendering application 34.” (Ex. 1008, 34:26-32.) **England** similarly described a DRM system that “must load and execute only OS components that are authenticated as respecting digital rights (‘trusted’), and must allow access to the downloaded content by only similarly trusted applications.” (Ex. 1005, 8:45-50.) Thus, as a first line of defense, DRM systems provided access to content only by modules that are deemed trusted.

52. However, software modules that are used to process content—even “trusted” modules—may be vulnerable to exploitation to circumvent content protection systems, or may otherwise be used in a manner that violates license limitations. Thus, it was recognized that in addition to providing access controls, it was desirable

to continually monitor the processing of content by software modules. For example, **England** discloses that “[t]he use the entity makes of the content is monitored and terminated if the entity violates the license limitations” (Ex. 1005, Abstract, 4:7-13) and as another example discloses monitoring for attempts to load a kernel debugger into memory, and renouncing the trusted identity if an attempt is detected (Ex. 1005, 15:54-58). Similarly, Kobata et al. in U.S. Patent No. 6,591,367 (Ex. 1009), based on an application filed March 31, 1999, described a system for preventing unauthorized copying and distribution of electronic messages wherein the system “monitor[s] the computer system for process changes that occur on the computer system while the message is being output at the output device.” (Ex. 1009, Abstract, 1:9-14, 2:55-60.) And **Griswold** described a license check system that made use of request and reply datagrams sent at regular intervals during processing to set an “authorization code” depending on detected events. (Ex. 1006, Abstract, 3:62-4:5, 5:38-52, 6:59-61.)

53. A robust DRM system needs to monitor for a wide range of events or activities to address the many possible approaches and tools that may be employed to circumvent protections. Thus, it was known to configure DRM systems to monitor various types of events or criteria that indicate a violation of license limitations or may indicate nefarious activity, such as copying. For example, **England** discloses that “the use the entity makes of the content can be monitored and terminated if the

entity violates the license limitations” which may include “the number of times the content can be accessed or what derivative use can be made of the content.” (Ex. 1005, Abstract, 4:7-13, 10:7-10.) The license limitations may also include sublicense rights, which permit a trusted application to validate other client computers and share content with them. (Ex. 1005, 19:32-55.) As another example, **England** discloses monitoring for whether there is an attempt to load a kernel debugger, which would allow the user to make a copy of the content loaded in memory. (Ex. 1005, 15:54-58.) If an attempt to load a kernel debugger was detected, the DRM system would renounced the trusted identity and terminated the trusted application that was accessing the content before loading the debugger. (Ex. 1005, 15:54-58.) Other known limitations related to timing. **Griswold’s** DRM system, which used request and reply datagrams to set an “authorization code,” allowed the licensed product to be used for a duration of time without a reply datagram from the licensor, and would terminate use of the licensed product if the time exceeded the disconnect allowed interval, which indicated that the product was being used without the required connection to a communication network. (Ex. 1006, 6:24-36, 5:38-52, 6:59-61, 8:48-9:4, Figs. 5-6.)

54. After an event is detected indicating a violation of license limitations or nefarious activity, the DRM system may take any number of potential responses. For example, it was known to (1) terminate the trusted identity, (2) terminate the

application that was accessing the content, or (3) prevent the application from performing the desired processing. (Ex. 1005, 15:54-58, Abstract, 4:7-13.)

V. THE '603 PATENT

A. Overview

55. The '603 patent is directed to a system and method for protecting electronic media content. (Ex. 1001, Abstract.) Figure 6, reproduced and color-annotated below, illustrates an embodiment of the disclosed system.

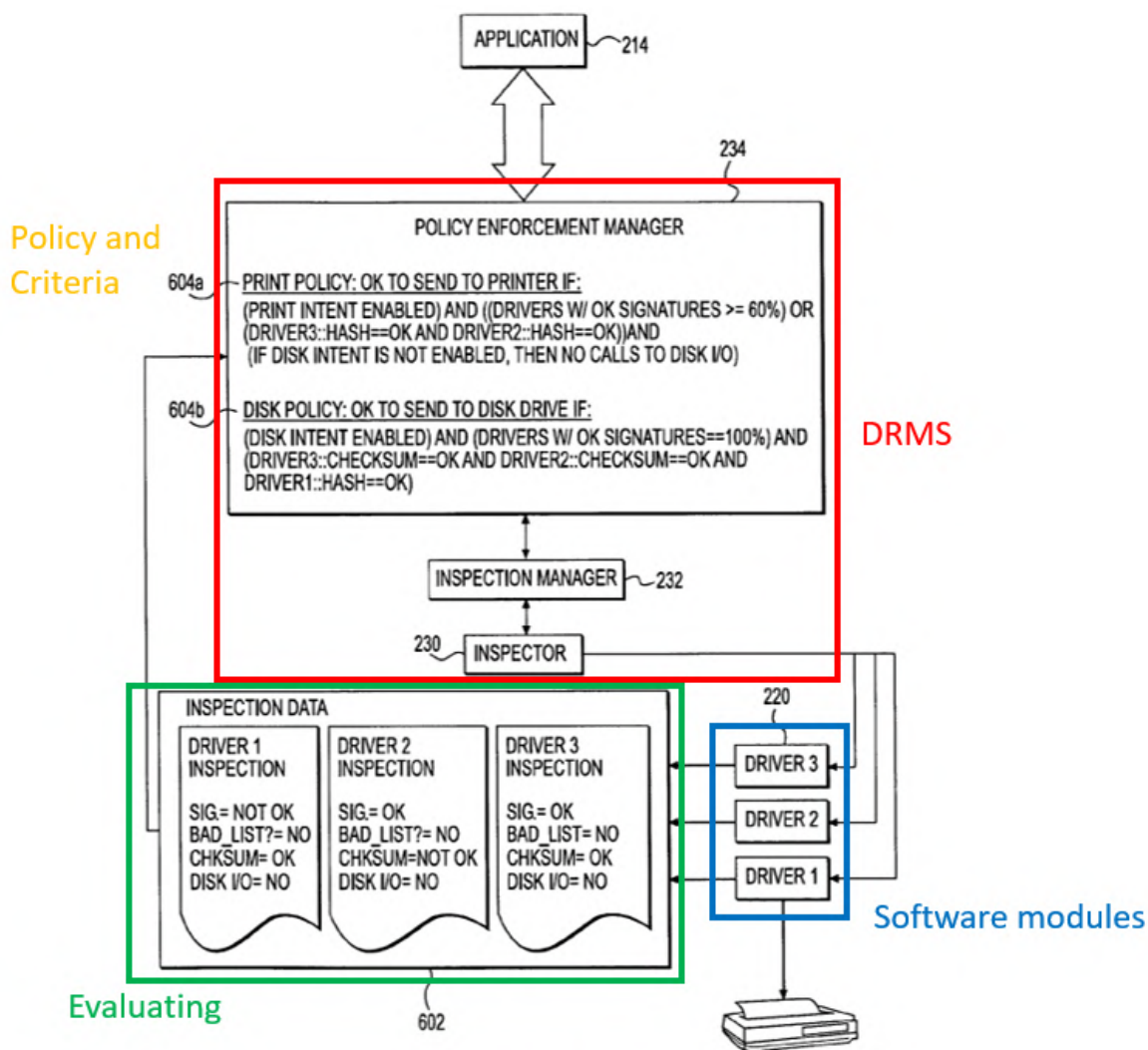


FIG. 6

56. When application program 214 (*e.g.*, music or video player) seeks to implement processing for user activities (*e.g.*, playing a song or a movie) (Ex. 1001, 7:38-41), a digital rights management system (“DRMS”) (highlighted in red) is responsible for protecting the content according to a set of rules or policies (Ex. 1001, 3:18-29).

57. In operation, the DRMS identifies software modules that are involved in processing content (Ex. 1001, drivers, plug-ins, and/or components) (highlighted in blue), and evaluates the modules to determine whether they behave in a satisfactory manner. (Ex. 1001, 15:15-23.) The ’603 patent discloses a number of methods for evaluating software modules. For example, the system can scan for the use of certain “system interfaces” that indicate undesirable behavior or that are maintained in a list of interfaces known to be undesirable. (Ex. 1001, 18:3-19.) Another approach is to “monitor and analyze the dynamic timing operations performed by the module to identify anomalous timing characteristics indicative of invalid and/or malicious activities.” (Ex. 1001, 18:34-37.) In another example, the system determines whether content is being directed through an unapproved streaming channel. (Ex. 1001, 19:16-29.)

58. When an unauthorized module is detected during processing of protected content, the system can respond in an appropriate manner, for example by (1) returning an error and denying the operation; (2) removing or disabling the offending

module and denying the operation; or (3) damaging the content, but permitting the operation to continue. (Ex. 1001, 22:2-9.) A set of “rules” or policy controls are used to determine whether the system will allow, modify, or disallow downstream processing operations on protected content. (Ex. 1001, 2:56-24.)

B. Prosecution History

59. I have reviewed the file history for the ’603 patent (Ex. 1003).

60. The ’603 patent issued from U.S. Application No. 09/653,517 (the “’603 application”), which was filed on August 31, 2000. Ex. 1003 at 1-105.

61. In a Non-Final Rejection of August 4, 2004, the Examiner rejected claims 1-2 (issued as the Challenged Claims, after amendments) as obvious over U.S. Patent No. 6,064,739 (“Davis”) in view of U.S. Patent No. 6,088,801 (“Grecsek”). Ex. 1003 at 132-34. In response, the Applicant amended claim 1 to recite that the request to access a piece of electronic content is received “from a user of the computer system” and argued that “Grecsek is concerned with protecting the user’s system from external attackers, not from misuse by the user himself. Ex. 1003 at 153, 160.

62. In a Final Rejection of April 28, 2005, the Examiner rejected claims 1-2 as obvious over the same references. Ex. 1003 at 170-72. In response, the Applicant argued that the Examiner’s rejection was conclusory and that a person of ordinary skill in the art would not have any motivation to combine the cited references. Ex.

1003 at 191-95. Applicant filed a Request for Continued Examination. Ex. 1003 at 211.

63. In Non-Final and Final Rejections of November 28, 2005 and June 1, 2006, the Examiner rejected claims 1-2 as anticipated by Grecsek. Ex. 1003 at 216-18, 251-53. In response to the Non-Final Rejection, the Applicant amended the “evaluating” step in claim 1 to require that the evaluating step include at least one of six “protection mechanisms” added to the claims, and in response to the Final Rejection, the Applicant filed a Request for Continued Examination and further amended claim 1 to recite that the software module are “authorized to execute on the computer system.” Ex. 1003 at 235-36, 278-81.

64. In a Non-Final Rejection of September 6, 2007, the Examiner again rejected claims 1-2 as anticipated by Grecsek. Ex. 1003 at 297-300. In response, the Applicant amended claim 1 to require “processing at least a portion of said piece of electronic media content using at least one of the one or more software modules” before the “evaluating” step, and substantially amended the “evaluating step” including by removing three of the six actions that the claim requires selecting from and amending the others. Ex. 1003 at 314-15. In its remarks, Applicant argued:

Claim 1 in the application recites ‘processing at least a portion of said piece of electronic media content using at least one of the one or more software modules,’ and ‘evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an unauthorized manner.’ **In Grecsek,**

the evaluation determines whether the process (110) is allowed to execute on the computer system. Before the evaluation, the process (110) should not be allowed to process protected resource. In contrast, the amended claim 1 requires processing a portion of the electronic media content, and evaluating whether the processing is in an authorized manner.

Ex. 1003 at 322.

65. The Examiner issued a Notice of Allowance on April 3, 2008, which stated that claim 1 was allowed because the prior art presented during prosecution does not explicitly disclose “processing at least a portion of said piece of electronic media content using at least one of the one or more software modules and evaluate whether the at least one or more software modules process the portion of the electronic media content in an authorized manner.” Ex. 1003 at 337.

66. Thus, the '603 patent was apparently allowed because the prior art of record failed to disclose processing a portion of the electronic media content, and evaluating whether that processing is in an unauthorized manner (*i.e.*, processing before evaluating). Nevertheless, as explained herein, this feature was well-known in the art before the earliest possible priority date.

VI. CLAIM INTERPRETATION

67. I have been informed that for purposes of this *Inter Partes* Review, the standard for claim construction is the same as the standard used in the federal district courts: claim terms should generally be given their ordinary and customary meaning

as understood by one of ordinary skill in the art at the time of the invention and after reading the patent and its prosecution history.

68. I have also been informed that only terms necessary to resolve the controversy need to be construed. For the purposes of the present declaration, I have applied the legal principles outlined above. I offer an opinion regarding the meaning of two claim terms at this time, and have been instructed by counsel to apply Patent Owner's interpretation from District Court for a third term, as set forth below. I reserve the right to offer opinions on claim construction in response to arguments that may be made by Patent Owner.

A. "predefined criteria"

69. Claim 1 recites denying the request to use the piece of electronic media content if the evaluation indicates that the at least one of the one or more software modules fail to satisfy a set of "predefined criteria." The term "predefined criteria" should be construed as "conditions or characteristics determined in advance against which to check the structure and/or behavior of one or more software modules."

70. The '603 patent discloses inspector modules that "are operable to check the structure and/or behavior of drivers, software, and/or hardware against predefined criteria." (Ex. 1001, 15:36-62.) For example, there may be "one or more lists of criteria 510 against which to check driver modules 530." (Ex. 1001, 16:25-34.) An example criteria is public keys. (Ex. 1001, 16:25-34.)

71. Claim 1 additionally recites that the “evaluating” includes at least one action selected from the group consisting of (1) “evaluating whether the at least one of the one or more software modules make calls to certain system interfaces,” (2) “evaluating whether the at least one of the one or more software modules direct data to certain channels,” and (3) “analyzing dynamic timing characteristics of the at least one of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity.” Thus, “predefined criteria” encompasses conditions or characteristics against which to check or evaluate whether call are made to certain system interfaces, whether data is directed to certain channels, and whether certain timing characteristics are present (*i.e.*, certain behaviors of the claimed software module).

72. Thus, the term “predefined criteria” should be construed as “conditions or characteristics determined in advance against which to check the structure and/or behavior of one or more software modules.”

B. “predefined policy”

73. Dependent Claim 2 recites using the predefined criteria to evaluate the at least one of the one or more software modules according to a “predefined policy,” and basing a decision to deny the request on the outcome of this evaluation. The term “predefined policy” should be construed as “one or more rules determined in advance governing the processing of content.”

74. The '603 patent discloses that use of the electronic media content by a software module is in accordance with “a set of ‘rules’ or policy controls” governing “whether it will allow, modify, or disallow downstream processing operations on protected content.” (Ex. 1001, 2:56-64.) Policies may comprise logical expressions containing a variety of conditions. (Ex. 1001, 20:56-57.) As an example, the '603 patent describes “print policy 604” which sets forth a rule governing printing of a content file. The print policy 604 provides that “the content file can be sent to the printer as long as (a) the rules (e.g., rules 514 in FIG. 5) associated with the content indicate that it is ok to print the content (i.e., if the print intent is enabled); and (b) the drivers responsible for handling the content on its way to the printer satisfy certain conditions (e.g., a certain percentage have valid signatures, certain drivers’ hash values are found on the list of known ‘good’ drivers, etc.).” (Ex. 1001, 20:57-65.) Thus, consistent with the specification, “predefined policy” means “one or more rules determined in advance governing the processing of content.”

C. “evaluating whether the at least one of the one or more software modules direct data to certain channels”

75. Claim 1 recites “evaluating whether the at least one of the one or more software modules direct data to certain channels” as one element of a Markush group. I understand that in District Court, Patent Owner asserts that the following activity is within the scope of the this limitation: “determin[ing] whether...downstream [devices] are authenticated and their certificates are deemed

to be trusted by the Trusted Device List (TDL) of the KDM associated with the content to be played.” (Ex. 1007, 15-17.) I have been instructed by counsel to include in my analysis Patent Owner’s interpretation of “evaluating whether the at least one of the one or more software modules direct data to certain channels” as at least encompassing evaluating a particular output channel device. I have applied this interpretation with respect to one alternative read of Ground 2 (**England**). Ground 1 (**Griswold**) and the other alternative read of Ground 2 (**England**) are not based on this element of the Markush group.

VII. DISCUSSION OF RELEVANT PRIOR ART

A. Ground 1: Claims 1 and 2 are Rendered Obvious by Griswold

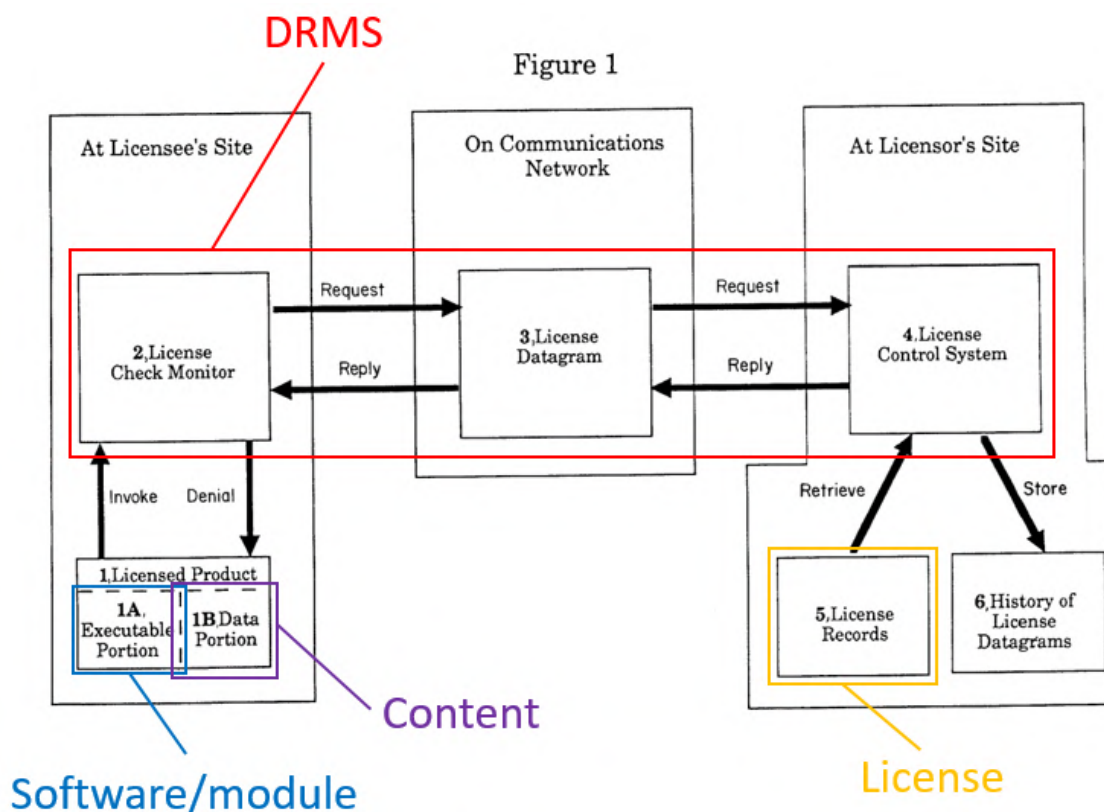
76. It is my opinion that the Challenged Claims 1 and 2 are rendered obvious by **Griswold**. Below, I provide an overview of **Griswold**. I further provide an analysis of claim 1, followed by claim 2, and a claim chart of relevant prior art disclosures to explain how the limitations of claim 1 and 2 are met.

1. Overview of Griswold

77. **Griswold**, entitled “Licensing management system and method in which datagrams including an address of a licensee and indicative of use of a licensed product are sent from the licensee’s site, is directed to a license management system and method for controlling the use of a licensed product in accordance with the terms of the license. (Ex. 1006, Abstract.) Licensed products include computer software,

video games, CD-ROM information, movies and other video products, music and other audio products, and multimedia products. (Ex. 1006, 1:16-22.)

78. Figure 1 shows a system level overview of **Griswold's** license management system. As shown in Figure 1, a licensed product 1 on the licensee's site includes a data portion 1B and a functional portion 1A:



Data portion 1B of the licensed product includes, for example, video information if the licensed product is a movie or other video product, *i.e.* electronic media content. (Ex. 1006, 5:19-33.) **Functional portion or executable portion 1A** of the licensed product is a computer software product or any other kind of information product used to control use of data portion 1B. (Ex. 1006, 5:19-33.)

The functional portion, or software, is executable to control, *e.g.*, the display of video information. (Ex. 1006, 5:19-36.) A POSITA would have understood that the functional portion is either a module or a collection of modules, and thus is “one or more software modules.”

79. Although the software is depicted in Figure 1 as part of the licensed product, **Griswold** also discloses that the software that controls or processes the content may be on the licensee’s computer separate from the content:

Although only a few exemplary embodiments of this invention have been described in detail above, those skilled in the art will readily appreciate that many modifications are possible in the preferred embodiments without materially departing from the novel teachings and advantages of this invention. For example, **product 1 was described as sometimes consisting of information as well as software which controls the information. This approach provides the greatest flexibility, but it is also possible to include the software which controls the information in the networked machine at the licensee’s *site*. In this case, product 1 is split, with part of it on media and part on the licensee’s machine. By doing this, some space can be saved on the media containing product 1, but the capabilities of these products will be limited by the standard functions available on these machines.**

(Ex. 1006, 11:28-43.) In this embodiment, the software is not limited to software provided by the licensor.

80. A license check system is employed to approve or deny use of the content by licensed product 1. (Ex. 1006, 5:38-52.) A POSITA would have understood that in

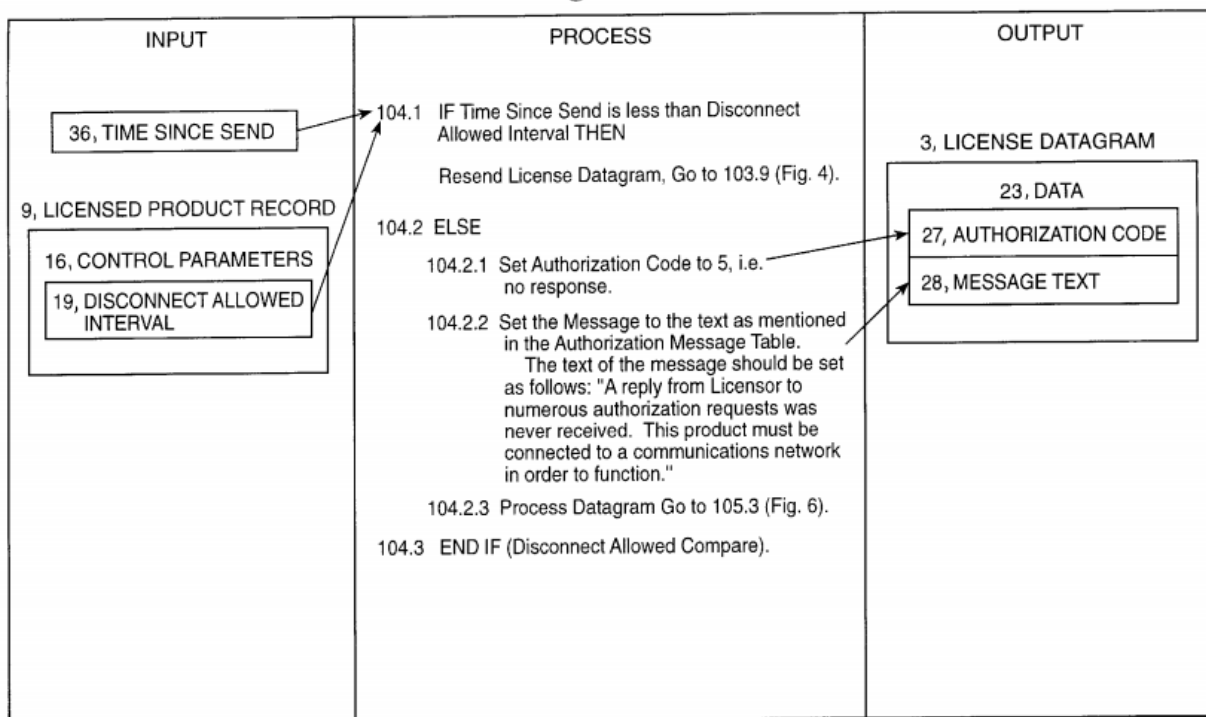
the embodiment where the software is separate from the content, the approval or denial is for use of the content by the separate software. A monitor on the licensee's site is invoked, for example when the user pushes a play button, and is invoked at regular time intervals. (Ex. 1006, Abstract, 7:35-36, 12:9-14.) The monitor on the licensee's site then sends a "request datagram" (license datagram 3 in Fig. 1) to the licensor's site in order to obtain approval to use the licensed product. (Ex. 1006, 3:62-4:5, 5:44-52.) The request datagram is received by a license control system at the licensor's site. (Ex. 1006, Abstract, Fig. 1.) For a duration of time, the licensed product can be used without a reply datagram from the licensor. (Ex. 1006, 6:24-36.) Thus, the licensed product processes at least a portion of the content before the monitor and license control system evaluates the request.

81. The license datagram 3 describes information related to the use of licensed product 1, including an identification of product 1 (*i.e.*, the software). (Ex. 1006, 5:44-45, 6:37-51.) A POSITA would have understood that the monitor at the licensee's site must first identify the software in order for the software to be used together with the content as contemplated, and further so that information identifying the software can be transmitted in the license datagram for evaluation at the licensor's site as taught by **Griswold**.

82. The monitor at the licensee's site receives a reply datagram containing an approval or denial, and prevents further use of the product if the datagram contains

a denial. (Ex. 1006, 5:38-52.) An “authorization code” is used to indicate the type of denial and to control which message will be displayed to the user upon a denial. (Ex. 1006, 6:59-61.) The monitor on the licensee’s site also evaluates whether a reply datagram is overdue. (Ex. 1006, 8:48-9:4.) The monitor compares the time since send to the disconnect allowed interval in the licensed product record to determine whether the elapsed time exceeds the permitted time interval for operating the product without receiving a reply. (Ex. 1006, 8:48-9:4.)

Figure 5



(Ex. 1006, Fig 5.) If the time since send is greater than the disconnect allowed interval, the authorization code is set to “5” which results in a denial and termination of the use of the licensed product. (Ex. 1006, Fig 5.)

2. Claim 1

a) [1pre] “A method for protecting electronic media content from unauthorized use by a user of a computer system, the method including:”

83. To the extent the preamble is limiting, **Griswold** discloses **a method for protecting electronic media content from unauthorized use by a user of a computer system.**

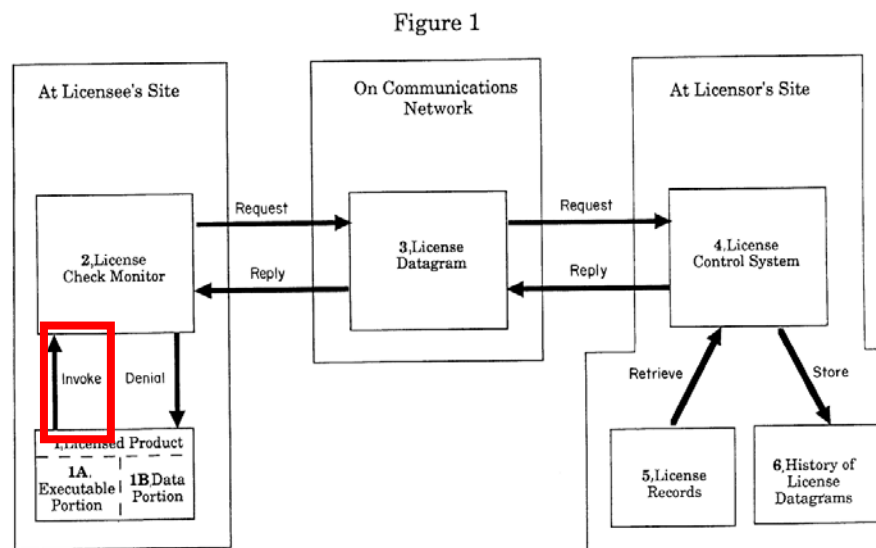
84. For example, **Griswold** discloses a method for controlling use of a licensed product, such as computer software, video games, movies, videos, or music (*i.e.*, electronic media content). **Griswold** discloses “[a] license management system and method for recording the use of a licensed product, and for controlling its use in accordance with the terms of the license.” (Ex. 1006, Abstract.) **Griswold** discloses that “The license control system maintains a record of the received datagrams, and compares the received datagrams to data stored in its licensee database.” (Ex. 1006, Abstract.) **Griswold** further discloses that the system manages licenses of “products such as computer software, video games, CD-ROM information, movies and other video products, music and other audio products, multimedia products.” (Ex. 1006, 1:16-22.)

b) [1a] “receiving a request from a user of the computer system to use a piece of electronic media content”

85. **Griswold** discloses **receiving a request** (*e.g.*, “monitor 2 is invoked”; “request datagram”) **from a user of the computer system** (*e.g.*, “licensee” at

“licensee’s site”) to use a piece of electronic media content (e.g., “data portion” of “licensed product”).

86. For example, **Griswold** discloses that a monitor on the licensee’s site is invoked, for example when the user pushes a play button (i.e., the monitor receives a request from the user to use the licensed product). **Griswold** discloses that “monitor 2 is invoked by the licensee’s action of pushing the ‘play’ or similar button, and in a broadcast music application or similar system, the monitor may be invoked simply by turning the device on.” (Ex. 1006, 12:9-14.)



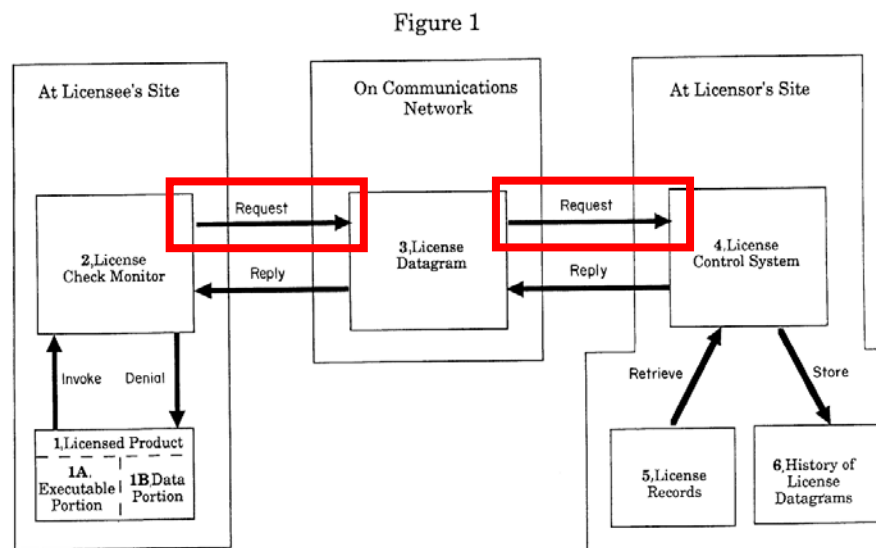
(Ex. 1006, Fig. 1.)

87. **Griswold** discloses that the monitor on the licensee’s site then periodically sends a “request datagram” in order to obtain approval to continue using a licensed product, and the request is received by a license control system at the licensor’s site. For example, **Griswold** discloses that “[a] licensed product invokes a license check

monitor at regular time intervals. The monitor generates request datagrams which identify the licensee and the product and sends the request datagrams over a communications facility to a license control system.” (Ex. 1006, Abstract)

Griswold discloses that “a licensed product generates request “datagrams,” messages transmitted over a communications network.” (Ex. 1006, 3:62-4:5.)

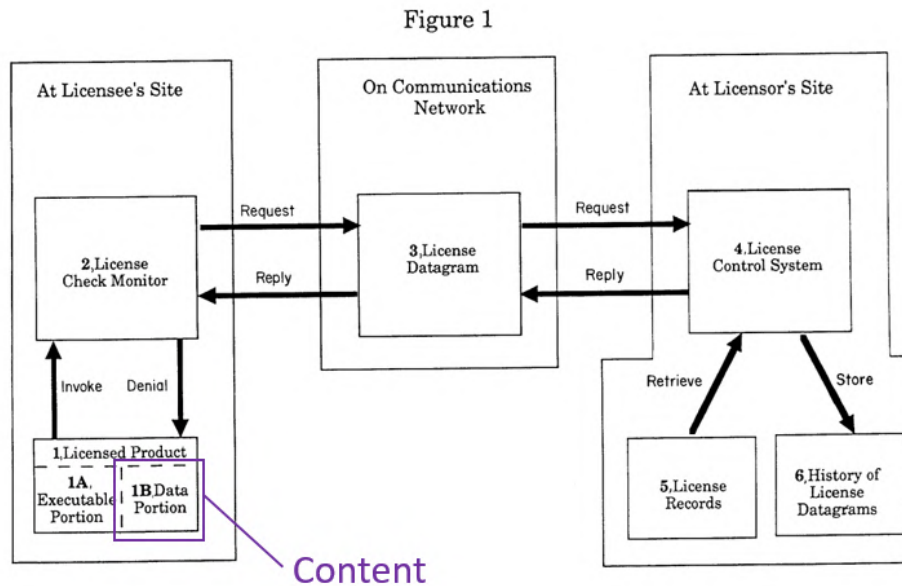
Griswold discloses that “the licensee sends a request datagram 3 over the network to the licensor. The licensor then returns a reply datagram containing either an approval or denial.” (Ex. 1006, 5:44-52.)



(Ex. 1006, Fig. 1.)

88. Griswold discloses that the licensed product includes a “data portion,” which is electronic media content. For example, **Griswold** discloses that the system manages licenses of “products such as computer software, video games, CD-ROM information, movies and other video products, music and other audio products,

multimedia products.” (Ex. 1006, 1:16-22.) **Griswold** discloses that “a licensed product 1 is located at a licensee’s site. Product 1 may include a data portion 1B.” (Ex. 1006, 5:19-33.) As an example, **Griswold** discloses that “data portion 1B is video information.” (Ex. 1006, 5:19-33.)



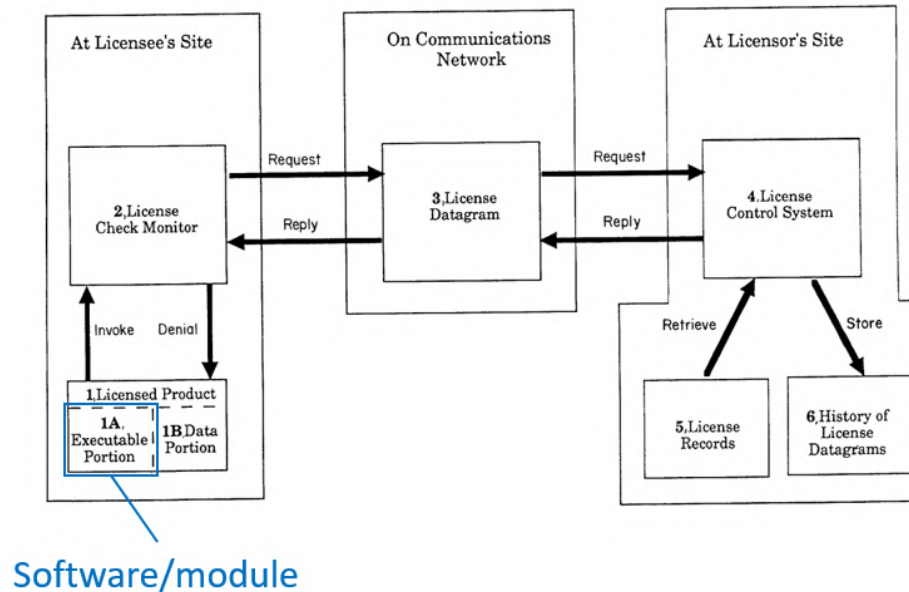
(Ex. 1006, Fig. 1.)

c) [1b] “identifying one or more software modules responsible for processing the piece of electronic media content and enabling use of the piece of electronic media content by the user”

89. **Griswold** discloses **identifying one or more software modules** (*e.g.*, “identify” the “executable portion” or “functional portion” of “licensed product 1”) **responsible for processing the piece of electronic media content** (*e.g.*, “used to control use of data portion 1B”) **and enabling use of the piece of electronic media content by the user** (*e.g.*, “control the display of the video information”).

90. For example, **Griswold** discloses a functional portion of the licensed product. **Griswold** discloses that “a licensed product 1 is located at a licensee’s site. Product 1 may include ... a functional portion 1A such as computer software product or any other kind of information product used to control use of data portion 1B. (Ex. 1006, 5:19-33.) **Griswold** further discloses that the functional portion may be separate software on the licensee’s computer. For example, **Griswold** discloses that while “product 1 was described as sometimes consisting of information as well as software which controls the information ... it is also possible to include the software which controls the information in the networked machine at the licensee’s site” in which case “the capabilities ... will be limited by the standard functions available on these machines.” (Ex. 1006, 11:28-43.) As explained in Section VII.A.1, A POSITA would have understood that this software is either a module or a collection of modules, and thus is “one or more software modules.”

Figure 1



(Ex. 1006, Fig. 1.)

91. Griswold discloses that the functional portion of the licensed product (which as described above may be separate software on the licensee’s computer) is executable to control, *e.g.*, the display of video information. For example, **Griswold** discloses “a functional portion 1A ... used to control use of data portion 1B” and that “[i]f data portion 1B is video information, functional portion 1A should control the display of the video information.” (Ex. 1006, 5:19-33.) A POSITA would have recognized that display of information from the data portion, such as video information, enables use of the content by the user.

92. Griswold discloses that license datagram 3 (the request datagram) describes information related to the use of licensed product 1, including an identification of product 1. For example, **Griswold** discloses that “[l]icense datagrams 3 are

messages that describe information related to the use of licensed product 1.” (Ex. 1006, 5:44-45.) **Griswold** further discloses: “Data 23, a part of datagram 3, conveys a message, and contains a number of fields. Product model number 24 and datagram number 25 identify product 1 and datagram 3, respectively.” (Ex. 1006, 6:37-51.)

93. As explained in Section VII.A.1, to the extent that Patent Owner argues that this claim element is not expressly disclosed, a POSITA would have understood that in the embodiment where the software is separate from the content the monitor at the licensee’s site must first identify the software in order for the software to be used together with the content, and further so that information identifying the software can be transmitted in the license datagram for evaluation at the licensor’s site as taught by **Griswold**.

d) [1c] “processing at least a portion of said piece of electronic media content using at least one of the one or more software modules”

94. **Griswold** discloses **processing at least a portion of said piece of electronic media content using at least one of the one or more software modules** (*e.g.*, “use of data portion 1B” by “functional portion 1A”; “use the licensed product”).

95. For example, **Griswold** discloses that “[a]fter a request datagram has been sent out, a user may be permitted to use the licensed product for a limited duration.” (Ex. 1006, 4:23-29.) **Griswold** discloses that use of the product is by the “functional portion” of the licensed product, which as explained with respect to [1b] can be

separate software from the content. For example, **Griswold** discloses “a functional portion 1A ... used to control use of data portion 1B” and that “[i]f data portion 1B is video information, functional portion 1A should control the display of the video information.” (Ex. 1006, 5:19-33.)

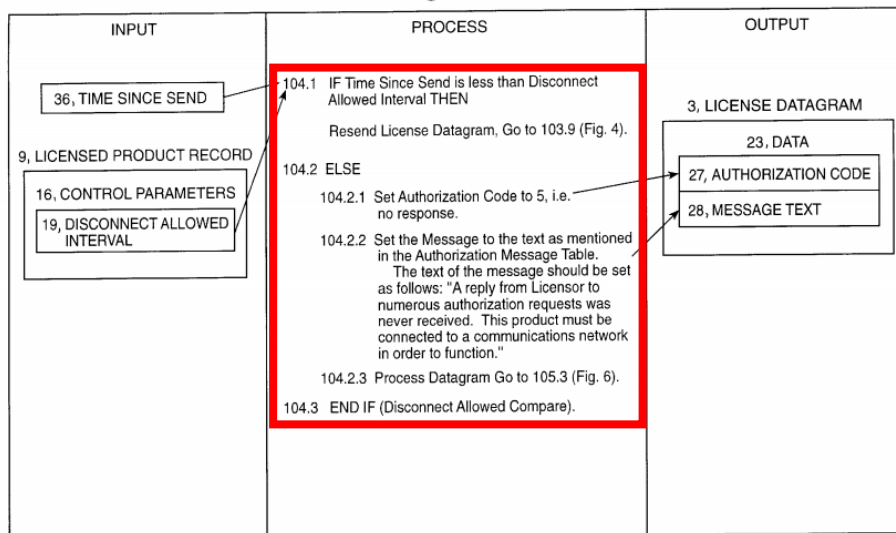
e) [1d] “evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner”

96. **Griswold** discloses **evaluating whether the at least one of the one or more software modules** (*e.g.*, “functional portion” of “licensed product”) **process the portion of the electronic media content in an authorized manner** (*e.g.*, “compares time since the last datagram was sent 36 to disconnect allowed interval 19” and sets an “authorization code” depending on the result).

97. For example, **Griswold** discloses that processing the content involves sending and receiving datagrams with certain timing frequencies. The monitor compares the time since the last datagram was sent to a disconnect allowed interval in the licensed product record to determine if the product has been processing the content for too long without the required reply datagram (*i.e.*, evaluates whether the product is processing the content in an authorized manner). **Griswold** discloses that “FIG. 5 shows the operation of the ‘Reply Datagram is Overdue’ procedure. Step 104.1 compares time since the last datagram was sent 36 to disconnect allowed interval

19.... Step 104.2 ‘disconnects’ product 1 from further service, if time since send 36 is greater than disconnect allowed interval 19.” (Ex. 1006, 8:48-67.)

Figure 5



(Ex. 1006, Fig. 5.)

98. Griswold discloses that if the time exceeds the disconnect allowed interval, then the monitor sets an “authorization code” to “5” which indicates a denial. **Griswold** discloses that “[s]tep 104.2.1 assigns number 5 to authorization code 27” which is “interpreted by monitor 2 as a denial.” (Ex. 1006, 8:48-67.) **Griswold** further discloses that “[t]he denial Step 104.2.2 sets message text 28 to the following: ‘A reply from licensor to numerous authorization requests was never received. This product must be connected to a communications network in order to function.’” (Ex. 1006, 8:48-67.)

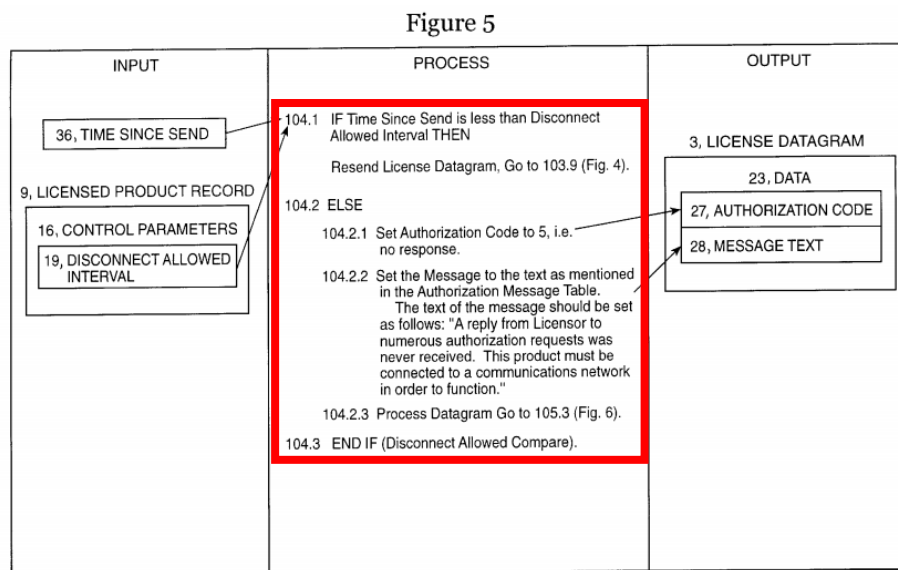
f) [1e] “the evaluating including at least one action selected from the group consisting of: evaluating whether the at least one of the one or more software modules make calls to certain system interfaces; evaluating whether the at least one of the one or more software modules direct data to certain channels; analyzing dynamic timing characteristics of the at least one of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity”

99. I have been instructed by counsel that for a “Markush” claim element, the entire element is disclosed by the prior art if one alternative in the Markush group is in the prior art.

100. **Griswold** discloses the evaluating including at least one action selected from the group consisting of:...analyzing dynamic timing characteristics of the at least one of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity (*e.g.*, “compares time since the last datagram was sent 36 to disconnect allowed interval 19” and “if time since send 36 is greater than disconnect allowed interval 19” this indicates the invalid activity of operating the product without a “reply from licensor” and/or “connect[ion] to a communications network”).

101. For example, **Griswold** discloses that the monitor permits use of a licensed product for a set period of time without receiving a reply datagram, and repeatedly compares the time since the last datagram was sent to the disconnect allowed interval in the licensed product record to determine whether the elapsed time exceeds the

permitted time interval for operating the product without receiving a reply. **Griswold** discloses that “FIG. 5 shows the operation of the ‘Reply Datagram is Overdue’ procedure. Step 104.1 compares time since the last datagram was sent 36 to disconnect allowed interval 19.... Step 104.2 ‘disconnects’ product 1 from further service, if time since send 36 is greater than disconnect allowed interval 19.” (Ex. 1006, 8:48-67.)



(Ex. 1006, Fig. 5.) A POSITA would have understood that when the elapsed time exceeds the permitted time interval that is an “anomalous timing characteristic” because the timing deviates from what is normal and expected.

102. Griswold further teaches that continued processing without a reply, such as when operating without a network connection, is unauthorized (*i.e.*, indicates invalid activity) and results in setting an “authorization code” to “5” which acts as a denial. For example, **Griswold** discloses that “[s]tep 104.2.1 assigns number 5 to

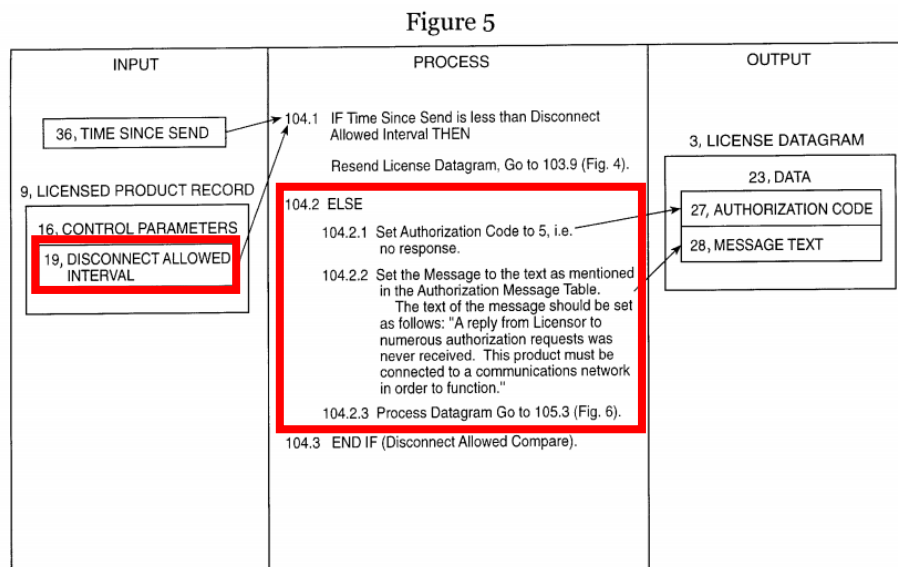
authorization code 27” which is “interpreted by monitor 2 as a denial.” (Ex. 1006, 8:48-67.) **Griswold** further discloses that “[t]he denial Step 104.2.2 sets message text 28 to the following: ‘A reply from licensor to numerous authorization requests was never received. This product must be connected to a communications network in order to function.’” (Ex. 1006, 8:48-67.)

g) [1f] “denying the request to use the piece of electronic media content if the evaluation indicates that the at least one of the one or more software modules fail to satisfy a set of predefined criteria”

103. Griswold discloses denying the request to use the piece of electronic media content (e.g., “generates a denial”) if the evaluation indicates that the at least one of the one or more software modules fail to satisfy a set of predefined criteria (e.g., “if time since send 36 is greater than disconnect allowed interval 19”).

104. For example, as explained in [1d] and [1e], **Griswold** discloses comparing the time since the last datagram was sent to the disconnect allowed interval in the licensed product record to determine whether the elapsed time exceeds the permitted time interval for operating the product without receiving a reply. The disconnect allowed interval and other restrictions in the licensed product record are a set of conditions or characteristics determined in advance for checking the behavior of the

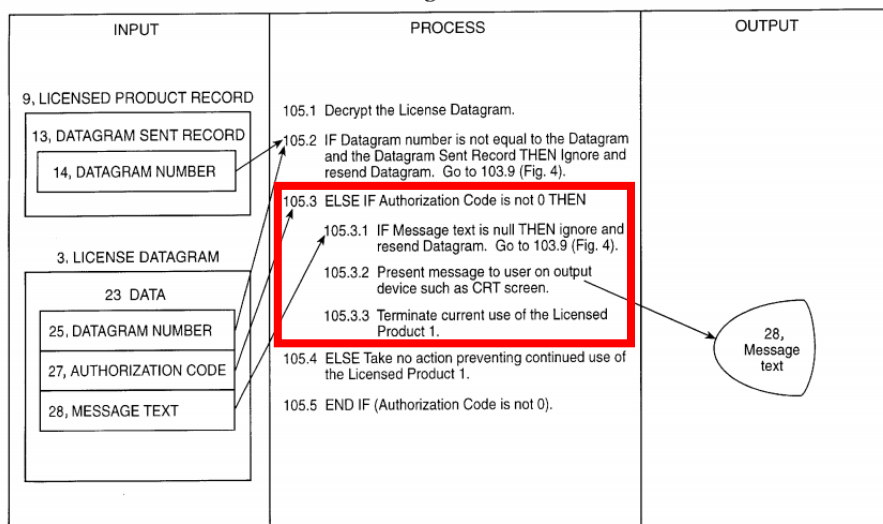
software (*i.e.*, predefined criteria).¹ If the time since send exceeds the disconnect allowed interval for the licensed product (*i.e.*, fail to satisfy the predefined criteria), then the request is denied. For example, **Griswold** discloses that “Step 104.2 ‘disconnects’ product 1 from further service, if time since send 36 is greater than disconnect allowed interval 19.” (Ex. 1006, 8:48-67.) **Griswold** discloses that “when a denial message is received or generated, monitor 2 must be able to switch ‘play’ to ‘off’.” (Ex. 1006, 12:16-18.) Figures 5-6 of **Griswold** illustrate the process that results in termination of the use of the licensed product if the disconnect allowed interval is exceeded:



(Ex. 1006, Fig. 5.)

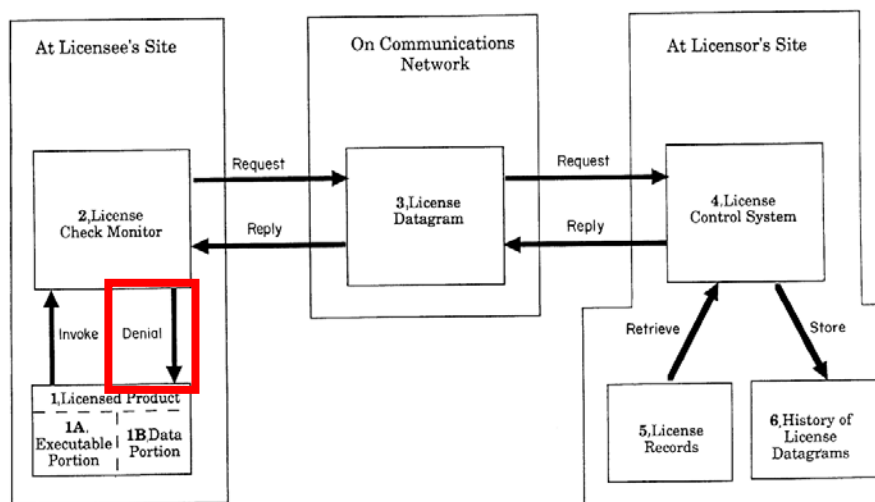
¹ As discussed in Section VI.A, the term “predefined criteria” means “conditions or characteristics determined in advance against which to check the structure and/or behavior of one or more software modules.”

Figure 6



(Ex. 1006, Fig. 6.) Figure 1 shows the issuance of a “denial” by the monitor:

Figure 1



(Ex. 1006, Fig. 1.)

3. Claim 2

a) [2] “A method as in claim 1, further including: using the predefined criteria to evaluate the at least one of the one or more software modules according to a predefined policy, and basing a decision to deny the request on the outcome of this evaluation”

105. Griswold discloses using the predefined criteria (*e.g.*, “disconnect allowed interval” in the “licensed product record”) to evaluate the at least one of the one or more software modules according to a predefined policy (*e.g.*, “permit[] the use of product 1 for a prescribed period of time”), and basing a decision to deny the request on the outcome of this evaluation (*e.g.*, “generates a denial” “if time since send 36 is greater than disconnect allowed interval 19”).

106. For example, as explained in [1d]-[1f], Griswold discloses comparing the time since the last datagram was sent to the disconnect allowed interval in the licensed product record (*i.e.*, predefined criteria) to implement a rule that permits the use of the licensed product for a prescribed period of time (*i.e.*, a predefined policy).² If the time since send exceeds the disconnect allowed interval for the licensed product, then the request is denied. For example, Griswold discloses that “Step 104.2 ‘disconnects’ product 1 from further service, if time since send 36 is greater than disconnect allowed interval 19.” (Ex. 1006, 8:48-67.) Griswold discloses that

² As discussed in Section VI.B, the term “predefined policy” means “one or more rules determined in advance governing the processing of content.”

“the present system permits the use of product 1 for a prescribed period of time. After the prescribed period of time has elapsed, the present system generates a denial.” (Ex. 1006, 9:1-4.)

4. Claim Charts

107. I have reviewed, had input to, and endorse, attached as Appendix C, the claim charts of the accompanying Petition showing that each element of Challenged Claims 1 and 2 of the '603 patent are met by **Griswold**. Any similarities between the claim charts below and those in the accompanying Petition are intentional.

B. Ground 2: Claims 1 and 2 are Rendered Obvious by England

108. It is my opinion that the Challenged Claims 1 and 2 are rendered obvious by **England**. Below, I provide an overview of **England** and an explanation on Ground 2. I further provide an analysis of claim 1, followed by claim 2, and a claim chart of relevant prior art disclosures to explain how the limitations of claim 1 and 2 are met.

1. Overview of England

109. **England**, entitled “Controlling access to content based on certificates and access predicates,” is directed to a method and system for enforcing digital rights on content from a provider. (Ex. 1005, Abstract.) Content may include media content such as video or audio, *i.e.* electronic media content. (Ex. 1005, 18:18-20.)

110. Like the '603 patent, **England** recognizes the need to prevent unauthorized access and unauthorized use of protected content. (Ex. 1005, Abstract, 9:1-17.)

Figure 2 illustrates a system level overview:

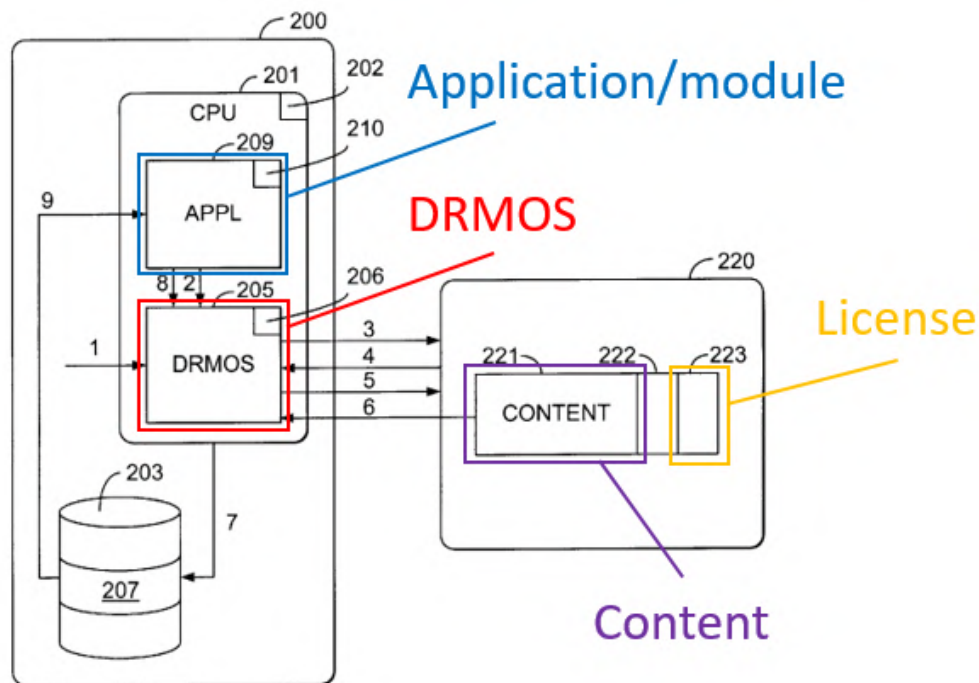


Fig. 2

A subscriber computer 200, such as a client computer, connects to a content provider server computer 220 through a wide-area network to download **content 221** at the request of application 209. (Ex. 1005, 8:24-32, 9:26-28.) A **digital rights management operating system 205 (“DRMOS”)** operates to allow access to the content by trusted applications. (Ex. 1005, 8:41-50.) An access predicate 222 may specify applications or families of applications that are allowed to process the

content. (Ex. 1005, 10:5-7.) The content is made available to such applications subject to use restrictions defined by a **license 223**. (Ex. 1005, 10:7-10.)

111. The subscriber computer contains “[a] number of **program modules** ... including an operating system 35, one or more application programs 36, other program modules 37, and program data 38.”³ (Ex. 1005, 6:24-28.) Such modules/applications are “identified” by the DRMOS as either trusted or non-trusted. (Ex. 1005, 8:63-67.) For example, the DRMOS “identifies” trusted application 209 through a rights manager certificate 210 that is compared against information in the access predicate 222, such as a list of applications or families of applications that are allowed to process the content. (Ex. 1005, 9:1-14, 8:63-67, 10:5-7.) Trusted application 209 accesses and handles (*i.e.*, is responsible for processing) certain types of content. (Ex. 1005, 9:1-14, 8:41-50, 18:20-22.)

112. **England’s** identification of modules by comparing a rights manager certificate 210 against a list of applications or families in the access predicate 222 is consistent with the ’603 patent’s disclosure that identification is carried out using “a library of identification and validation information ... maintained for use in the identification and validation process.” (Ex. 1001, 15:25-27.) The ’603 patent

³ **England** further discloses that “[g]enerally, program modules include routines, programs, objects, components, data structures, etc. that perform particular tasks or implement particular abstract data types.” (Ex. 1005, 5:30-37.) This is consistent with the ’603 patent’s disclosure of “modules ... involved in handling content (e.g., drivers, plug-ins, and/or components).” (Ex. 1001, 15:15-18.)

broadly explains that modules “can be identified or validated in a number of ways, including without limitation by their file names; by cryptographic signatures contained in the [modules]; by distinctive code patterns and/or behavior patterns contained in, or exhibited by, the [modules]; by the size of the [module] files; by the memory (and/or hardware) addresses at which the [modules] are located; or by any other suitable technique, including a combination of some or all of the aforementioned identification techniques.” (Ex. 1001, 15:27-35.)

113. England discloses monitoring the operation of modules that are processing the content. For example, **England** discloses prohibiting the loading of a kernel debugger because it would allow the user to make a copy of the content loaded in memory. (Ex. 1005, 15:51-54.) The DRMOS monitors trusted applications for attempts to load a kernel debugger into memory, and if an attempt is detected then the DRMOS renounces the trusted application’s trusted identity and terminates the trusted application that was accessing the content before loading the debugger. (Ex. 1005, 15:54-58.) In this example where the trusted application “was accessing the content” before the DRMOS terminates the application, the trusted application processes at least a portion of the content before the DRMOS evaluates whether the trusted application processed the portion of content in an authorized manner, as required by the claims.

114. As another example, **England** discloses that the license 223 places restrictions on the use of content 221 by the trusted application on the subscriber computer, and that the DRMOS monitors the use of the content for violations of the license limitations. (Ex. 1005, 10:7-10, 19:23-52, 4:9-11, Abstract.) For example, the license can specify sublicense rights 1107 that specify whether or not the trusted application on the subscriber computer is permitted to validate other computers and share content with them. (Ex. 1005, 19:32-52, Fig. 11.) **England** further discloses that the use of content by the trusted application on the subscriber computer is terminated if it violates the license limitations placed on the content. (Ex. 1005, 4:9-11, Abstract.) In this example where the “use of the content” by the trusted application is “monitored” for violations of the license limitations and terminated if a violation is detected, the trusted application processes at least a portion of the content before the DRMOS evaluates whether the trusted application processed the portion of content in an authorized manner, as required by the claims.

2. Claim 1

a) [1pre] “A method for protecting electronic media content from unauthorized use by a user of a computer system, the method including:”

115. To the extent the preamble is limiting, **England** discloses **a method for protecting electronic media content from unauthorized use by a user of a computer system.**

116. For example, **England** discloses monitoring the use of content by a user on a computer and terminating that use if the user violates certain license limitations (*i.e.*, if the use is unauthorized). **England** discloses that “[a] license that specifies limitations on the use of the content can also be associated with the content and provided to the entity. The use the entity makes of the content is monitored and terminated if the entity violates the license limitations. (Ex. 1005, Abstract; *see also* 4:1-11.)

b) [1a] “receiving a request from a user of the computer system to use a piece of electronic media content”

117. **England** discloses **receiving a request** (*e.g.*, “request 2”) **from a user of the computer system** (*e.g.*, from “application 209” of “subscriber computer 200”) **to use a piece of electronic media content** (*e.g.*, “content 221”).

118. For example, **England** discloses that application 209 on subscriber computer 200 requests the download of content from a content provider. **England** discloses a “subscriber computer 200” with an application 209 and that “application 209 requests 2 the download of content 221 from provider 220.” (Ex. 1005, 8:29-31, 9:26-36.)

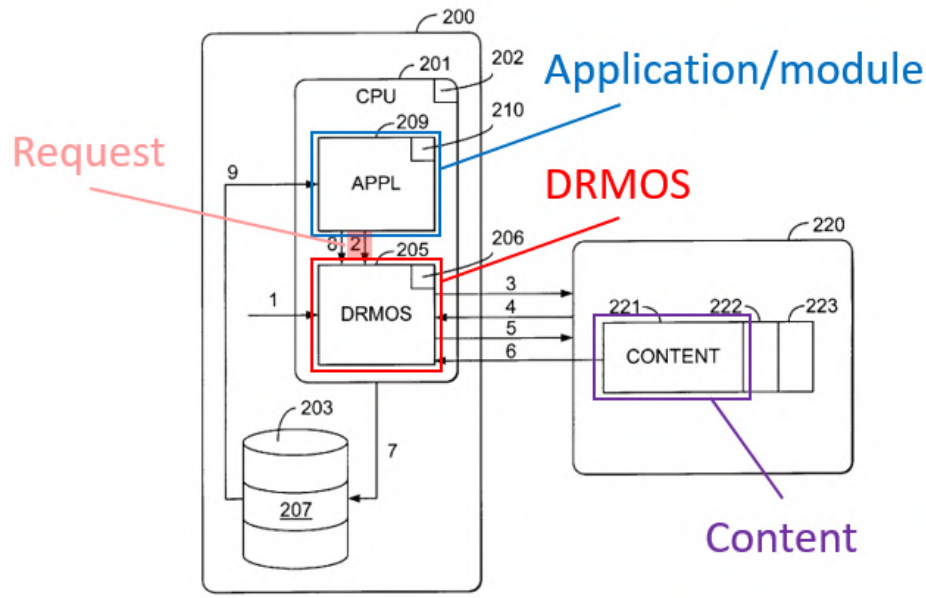


Fig. 2

(Ex. 1005, Fig. 2.)

119. A POSITA would have recognized that the request to use content originates from a user of the computer system (controlling application 209), or at minimum it would have been obvious for the user to initiate the request. For example, **England** discloses that “[a] user may enter commands and information into the personal computer 20 through input devices such as a keyboard 40 and pointing device 42.”

(Ex. 1005, 6:28-30.)

c) [1b] “identifying one or more software modules responsible for processing the piece of electronic media content and enabling use of the piece of electronic media content by the user”

120. **England** discloses identifying one or more software modules (*e.g.*, “trusted application 209 is identified”) **responsible for processing the piece of electronic**

media content (*e.g.*, “content type handled”) **and enabling use of the piece of electronic media content by the user** (*e.g.*, “allow access to the downloaded content by...trusted applications”)

121. For example, **England** discloses that the subscriber computer contains “program modules” (*i.e.*, software modules) including “one or more application programs.” **England** discloses “[a] number of program modules may be stored on the hard disk, magnetic disk 29, optical disk 31, ROM 24, or RAM 25, including ... one or more application programs 36...” (Ex. 1005, 6:24-28.)

122. **England** discloses that “trusted application 209” is one such application program. (Ex. 1005, 9:1-14.) As discussed above in Section VII.B.1, to the extent it is argued that trusted application 209 is not a software module despite **England**’s express definition, at minimum a POSITA would have recognized that programs such as trusted application 209 are nonetheless formed of “one or more software modules” as claimed.

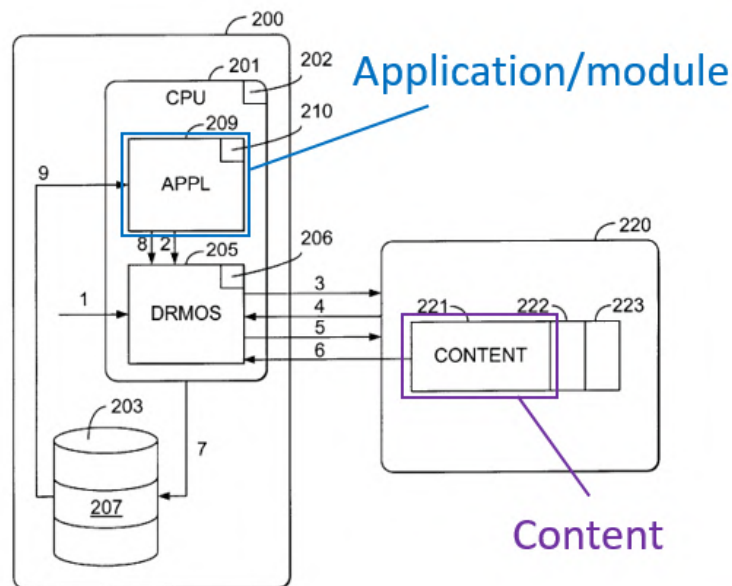


Fig. 2

(Ex. 1005, Fig. 2.)

123. England discloses that trusted application 209 is “identified” by rights manager certificate 210. For example, **England** discloses that “trusted applications must be identified in some fashion.” (Ex. 1005, 8:63-67.) **England** discloses that “[t]he trusted application 209 is identified through a “rights manager” certificate 210” and “the certificate 210 also identifies the trusted application.” (Ex. 1005, 9:1-14.)

124. England discloses identifying the software module responsible for processing the content. For example, **England** discloses that a content provider must trust “the application that will process the content.” (Ex. 1005, 18:20-22) **England** further discloses that the rights manager certificate 210 includes a list of content type

handled by the trusted application (*i.e.*, identifying the software responsible for processing the content). For example, **England** discloses that the rights manager certificate 210 adds “a list of services, or properties, provided by the application, *i.e.*, content type handled.” (Ex. 1005, 9:1-14.)

125. England discloses that the trusted application is used to access the content. For example, **England** discloses that “a digital rights management operating system (DRMOS) must ... must allow access to the downloaded content by only similarly trusted applications. (8:41-50.) A POSITA would have recognized that accessing content by the trusted application enables use of the content by the user.

d) [1c] “processing at least a portion of said piece of electronic media content using at least one of the one or more software modules”

126. England discloses **processing at least a portion of said piece of electronic media content** (*e.g.*, “use the entity makes of the content”; “accessing the content”) **using at least one of the one or more software modules** (*e.g.*, “trusted application”).

127. For example, **England** discloses “[t]he use the entity makes of the content is monitored and terminated if the entity violates the license limitations.” (Ex. 1005, Abstract; 4:7-13.) **England** further discloses that “[a] DRMOS must also protect the content once it is loaded into the client computer’s memory by a trusted application.” (Ex. 1005, 15:45-50.) For example, **England** discloses that “[i]f the

user of the subscriber computer attempts to load a kernel debugger into memory, the DRMos can either 1) refuse to load the debugger, or 2) renounce its trusted identity and terminate the trusted application that was accessing the content before loading the debugger. (Ex. 1005, 15:54-58.)

e) [1d] “evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner”

128. England discloses **evaluating whether the at least one of the one or more software modules** (*e.g.*, “trusted application 209”) **process the portion of the electronic media content in an authorized manner** (*e.g.*, “[t]he use the entity makes of the content is monitored and terminated if the entity violates the license limitations”).

129. For example, **England** discloses a digital rights management operating system (DRMos) that places restrictions on the use or processing of content by the application through the use of license limitations defined by license 223. **England** discloses “[t]he content license (FIG. 11) imposes additional restrictions on what kind of processing can be performed on the content once an application has access to the content. (Ex. 1005, 19:22-31.)

130. England further discloses that the use or processing of the content is monitored for violations of the license limitations (*i.e.*, processing in an unauthorized manner). For example, **England** discloses that “[t]he use the entity makes of the

content is monitored and terminated if the entity violates the license limitations. (Ex. 1005, Abstract; 4:9-12.) As another example, **England** discloses that “[i]f the user of the subscriber computer attempts to load a kernel debugger into memory, the DRMOs can either 1) refuse to load the debugger, or 2) renounce its trusted identity and terminate the trusted application that was accessing the content before loading the debugger. (Ex. 1005, 15:54-58.)

f) [1e] “the evaluating including at least one action selected from the group consisting of: evaluating whether the at least one of the one or more software modules make calls to certain system interfaces; evaluating whether the at least one of the one or more software modules direct data to certain channels; analyzing dynamic timing characteristics of the at least one of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity”

131. I have been instructed by counsel that for a “Markush” claim element, the entire element is disclosed by the prior art if one alternative in the Markush group is in the prior art.

132. **Engand** discloses the evaluating including at least one action selected from the group consisting of:... evaluating whether the at least one of the one or more software modules make calls to certain system interfaces...(e.g., “[i]f the user of the subscriber computer attempts to load a kernel debugger into memory”)

133. For example, **England** discloses detecting whether the user of the subscriber computer attempts to load a kernel debugger into memory, and terminating the trusted application and renouncing its trusted identity if this procedure is detected. **England** discloses that “[i]f the user of the subscriber computer attempts to load a kernel debugger into memory, the DRMOS can either 1) refuse to load the debugger, or 2) renounce its trusted identity and terminate the trusted application that was accessing the content before loading the debugger. (Ex. 1005, 15:54-58.) A POSITA would have recognized that loading a kernel debugger or portions of a kernel debugger for copying content stored in memory, as taught by **England**, involves making a call to certain system interfaces, for example the “ptrace” and “/proc” interfaces in UNIX systems. The “ptrace” interface was a well-known debugger interface. (Ex. 1010 (U.S. Patent No. 5,915,114 to McKee), 4:4-11 (“Process control interface 67 may be any variety of interfaces that accomplish this function. For instance, process control interface 67 may be a ptrace interface of the type used in UNIX systems.”); Ex. 1011 (U.S. Patent No. 5,978,902 to Mann), 16:23-25 (“Operating systems have supported debuggers via privileged system calls such a ptrace() call for some time.”).) The “ptrace” interface allowed one process to control another, and to gain access to the memory of the controlled process. (Ex. 1012 (UK Patent Application GB2236202A to Itzkowitz), 14 (“In the UNIX operating system environment, the system call ‘PTRACE’ enables a first process to attach to a second

process whereby the first process attains access to the header and symbolic information of the second process.”); Ex. 1013 (U.S. Patent No. 5,603,032 to Attal), 5:11-20 (“The agent can then, using a system call ‘PTRACE’, trace the execution and monitor the processing operation of the application. It is then possible for it to access the memory zone where the implantation is listed in the symbols table of the application and to run the proper processing operation (reading, modification, etc.)....”).) The “/proc” interface was another well-known debugger interface. (Ex. 1014 (Faulkner), 243; Ex. 1018 (Certified Translation of European Patent Specification EP0611210B1), 3; Ex. 1017.) It provided detailed process information and control mechanisms (Ex. 1014 (Faulkner), 243), and was used to read data from the memory of a running process (Ex 1018 (EP0611210B1), 3; Ex. 1017.). Thus, in order to determine whether the user attempts to load a kernel debugger for copying content stored in memory, as taught by **England**, a POSITA would have understood to evaluate whether the trusted application makes calls to certain system interfaces, such as the “ptrace” and “/proc” interfaces in UNIX systems.

134. Alternatively, England discloses the evaluating including at least one action selected from the group consisting of:...evaluating whether the at least one of the one or more software modules direct data to certain channels... (e.g., monitoring and enforcing the trusted application’s “sublicense rights”).

135. For example, **England** discloses that the license can specify sublicense rights 1107 that specify whether or not the trusted application on the subscriber computer is permitted to validate other computers (downstream computers) and share content with them. **England** discloses that “[t]he license can also specify whether or not a trusted application is permitted to validate other client computers and share the content with them (sublicense rights 1107), in effect having the subscriber computer act as a secondary content provider.” (Ex. 1005, 19:32-55.) Sharing content is “directing data to” sublicensed computers and the data paths to those sublicensed computers are “channels” in accordance with the claim.

136. **England** further discloses that the use of content by the trusted application on the subscriber computer (the upstream computer) is terminated if it violates the license limitations placed on the content. For example, England discloses that “[t]he use the entity makes of the content is monitored and terminated if the entity violates the license limitations. (Ex. 1005, Abstract; 4:9-12.) In the sublicense context, the use of content by the trusted application on the subscriber computer would be terminated if it violates the sublicense rights by sharing content with non-validated computers, which involves determining whether the downstream computers are validated.⁴

⁴ As discussed in Section VI.C, I have been instructed to apply Patent Owner’s interpretation of “evaluating whether the at least one of the one or more software

137. To the extent it is argued that terminating the “use” in the sublicense context would not terminate use of the content by the upstream subscriber, only the ability to sublicense, it would have been obvious to terminate the underlying use of the content by the upstream subscriber. For example, in other examples, **England** describes that the DRMOs may renounce the trusted application’s trusted status (Ex. 1005, 15:54-58) where a kernel debugger is loaded, evidencing an intent of the user in making unauthorized copies of the content executing in memory. Thus, it would have been obvious to a POSITA in view of **England**’s disclosures to terminate the trusted application on the upstream subscriber computer (and renounce the trusted application’s trusted status) if the application is used to share content with non-validated computers in violation of sublicense rights 1107, which involves determining whether the downstream computers are validated. This is because, like the kernel debugger example, there is a heightened interest of content providers to protect against unauthorized copying, and shutting down users exhibiting this type of behavior is critical to ensuring unauthorized content is not propagated over networks.

modules direct data to certain channels” as at least encompassing evaluating a particular output channel device.

g) [1f] “denying the request to use the piece of electronic media content if the evaluation indicates that the at least one of the one or more software modules fail to satisfy a set of predefined criteria”

138. England discloses **denying the request to use the piece of electronic media content** (*e.g.*, “terminate the trusted application that was accessing the content”) **if the evaluation indicates that the at least one of the one or more software modules fail to satisfy a set of predefined criteria** (*e.g.*, “[i]f the user of the subscriber computer attempts to load a kernel debugger into memory”).

139. For example, as discussed above with respect to “evaluating whether the at least one of the one or more software modules make calls to certain system interfaces” in [1e], **England** discloses that detecting whether the user of the subscriber computer attempts to load a kernel debugger into memory, and terminating the trusted application if this procedure is detected. For example, **England** discloses that “[i]f the user of the subscriber computer attempts to load a kernel debugger into memory, the DRMOS can either 1) refuse to load the debugger, or 2) renounce its trusted identity and terminate the trusted application that was accessing the content before loading the debugger. (Ex. 1005, 15:54-58.)

140. Terminating the trusted application which terminates use of the content is “denying the request” to use the content as recited in Claim 1 of the ’603 patent. The claim requires receiving a request to use the content, identifying a module that enables use of the content, and processing at least a portion of the content before

evaluating that processing. “Processing” before “evaluating” that processing was the alleged point of novelty argued during prosecution in order to secure allowance. Thus, “denying” the request cannot mean access gating and must encompass stopping any further processing of the content by the software module (*e.g.*, terminating the trusted application as taught by **England**).

141. As further discussed with respect to [1e], in order to determine whether the user attempts to load a kernel debugger into memory, as taught by **England**, it would have been obvious to a POSITA to evaluate whether the trusted application makes calls to certain system interfaces for loading a kernel debugger. Calls to such known system interfaces for loading a kernel debugger are a set of conditions or characteristics determined in advance for checking the behavior of the trusted application (*i.e.*, predefined criteria).⁵

142. Alternatively, **England** discloses denying the request to use the piece of **electronic media content** (*e.g.*, “[t]he use the entity makes of the content is monitored and terminated”) **if the evaluation indicates that the at least one of the one or more software modules fail to satisfy a set of predefined criteria** (*e.g.*, “if the entity violates the license limitations” such as “sublicense rights”).

⁵ As discussed in Section VI.A, the term “predefined criteria” means “conditions or characteristics determined in advance against which to check the structure and/or behavior of one or more software modules.”

143. For example, as discussed above with respect to “evaluating whether the at least one of the one or more software modules direct data to certain channels” in [1e], **England** discloses that the use of the content is monitored and terminated if the entity violates the license limitations, and that the license limitations that are monitored include sublicense limitations. For example, **England** discloses that “[t]he license can also specify whether or not a trusted application is permitted to validate other client computers and share the content with them (sublicense rights 1107), in effect having the subscriber computer act as a secondary content provider.” (Ex. 1005, 19:32-55.) **England** further discloses that “[t]he use the entity makes of the content is monitored and terminated if the entity violates the license limitations. (Ex. 1005, Abstract; 4:9-12.)

144. As further discussed with respect to [1e], it would have been obvious to a POSITA in view of **England**’s disclosures to terminate the trusted application on the subscriber computer (and renounce the trusted application’s trusted status) if the application is used to share content with non-validated computers in violation of sublicense rights 1107, which involves determining whether the downstream computers are validated. The information against which to check whether the downstream computers are validated is a set of conditions or characteristics determined in advance for evaluating the behavior of the trusted application (*i.e.*, predefined criteria).

3. Claim 2

a) [2] “A method as in claim 1, further including: using the predefined criteria to evaluate the at least one of the one or more software modules according to a predefined policy, and basing a decision to deny the request on the outcome of this evaluation”

145. **England** discloses using the predefined criteria (*e.g.*, criteria as set forth in “license 223”) to evaluate the at least one of the one or more software modules according to a predefined policy, and basing a decision to deny the request on the outcome of this evaluation (*e.g.*, “[i]f the user of the subscriber computer attempts to load a kernel debugger into memory, ...terminate the trusted application that was accessing the content before loading the debugger”).

146. For example, as explained above in [1e] and [1f], **England** renders obvious evaluating whether the trusted application makes calls to certain system interfaces for loading a kernel debugger (*i.e.*, predefined criteria), and discloses terminating the trusted application if that behavior is detected (*i.e.*, a predefined policy).⁶ For example, **England** discloses that “[i]f the user of the subscriber computer attempts to load a kernel debugger into memory, the DRMOS can either 1) refuse to load the debugger, or 2) renounce its trusted identity and terminate the trusted application that was accessing the content before loading the debugger. (Ex. 1005, 15:54-58.)

⁶ As discussed in Section VI.B, the term “predefined policy” means “one or more rules determined in advance governing the processing of content.”

147. Alternatively, England discloses using the predefined criteria (*e.g.*, criteria as set forth in “license 223”) **to evaluate the at least one of the one or more software modules according to a predefined policy, and basing a decision to deny the request on the outcome of this evaluation** (*e.g.*, “[t]he use the entity makes of the content is...terminated if the entity violates the license limitations” such as “sublicense rights”).

148. For example, as explained above in [1e] and [1f], **England** discloses that the use of the content is monitored and terminated if the entity violates the license limitations, and that the license limitations that are monitored include sublicense limitations. For example, **England** discloses that “[t]he license can also specify whether or not a trusted application is permitted to validate other client computers and share the content with them (sublicense rights 1107), in effect having the subscriber computer act as a secondary content provider.” (Ex. 1005, 19:32-55.) **England** further discloses that “[t]he use the entity makes of the content is monitored and terminated if the entity violates the license limitations. (Ex. 1005, Abstract; 4:9-12.)

149. As further discussed with respect to [1e] and [1f], it would have been obvious to a POSITA in view of **England**’s disclosures to evaluate whether the trusted application is used to share content with non-validated computers in violation of sublicense rights 1107 by applying predefined criteria, and to terminate the trusted

application on the subscriber computer (and renounce the trusted application's trusted status) if a violation is found. Thus, the use of the content is monitored and terminated if the entity violates the limitations on sublicense rights, *i.e.* a rule determined in advance governing the processing of content (a predefined policy).

4. Claim Charts

150. I have reviewed, had input to, and endorse, attached as Appendix D, the claim charts of the accompanying Petition showing that each element of the Challenged Claims 1 and 2 of the '603 patent are met by **England**. Any similarities between the claim charts below and those in the accompanying Petition are intentional.

VIII. SECONDARY CONSIDERATIONS

151. Prior to working on this declaration, I have no recollection of hearing of the inventors on the '603 patent or of the '603 patent. I have never heard anyone offer praise for the '603 patent, nor am I aware of any commercial success attributable to the '603 patent. I am also unaware of any copying of the alleged invention of the '603 patent.

152. I have found no evidence of secondary considerations or objective factors of non-obviousness, and it is my opinion that Challenged Claims of the '603 patent are obvious over the prior art. To the extent Patent Owner alleges secondary considerations in this proceeding, it is my opinion that they would not outweigh the strong evidence of obviousness of the '603 patent Claims, as set forth herein.

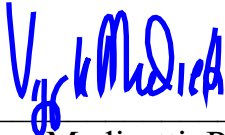
IX. CONCLUSION

153. As explained above, the Challenged Claims 1 and 2 of the '603 patent are disclosed and/or rendered obvious by the grounds set forth therein, and the Challenged Claims 1 and 2 are unpatentable under 35 U.S.C. § 103.

154. In signing this declaration, I understand that the declaration will be filed as evidence in a review proceeding before the Patent Trial and Appeal Board of the U.S. Patent and Trademark Office. I acknowledge that I may be subject to cross examination in the case and that cross examination will take place within the United States. If cross examination is required of me, I will appear for cross examination within the United States during the time allotted for cross examination.

155. 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 the Title 18 of the United States Code and that such willful false statements may jeopardize the results of these proceedings.

Executed on: May 27, 2020



Vijay Madisetti, Ph.D.

APPENDIX

A

Dr. Vijay K. Madiseti

Fellow, IEEE

vkm@madiseti.com

Cell: 770-527-0177

Address:

**56 Creekside Park Drive
Johns Creek, GA 30022**

Employment:

- 1984-1989: Post Graduate Researcher (UC Berkeley),
- 1989-present: Full Professor of Electrical & Computer Engineering (**Georgia Tech, Atlanta, GA 30332**).

Areas of Technical Interest – Wireless & Mobile Communications, Computer Engineering, Circuit Design (Analog/Digital), Software Engineering, Digital Signal Processing, Wireline & Wireless Computer Networks, Software Systems, Control Systems, Cloud Computing.

Startup Companies:

Director, **VP Technologies, Inc.** (1995-): A startup commercialized through Georgia Tech's Advanced Technology Development Corporation (ATDC) focusing on digital software and hardware design services for military market. <http://www.vptinc.net>

Director, **Soft Networks, LLC** (2001-2007): A startup commercialized through Georgia Tech support focusing on software development tools and compilers for Cellular/WiFi/VOIP/telecommunication products. <http://www.soft-networks.com>

Director, **Elastic Video Inc.** (2007- 2009): A startup commercialized through Georgia Tech's VentureLab (<http://venturelab.gatech.edu>) development image and video processing software for wireless & IP networking.

Litigation Experience (2011-2019) With Testimony

(Note: There may be multiple cases between the parties, e.g., District Court v. ITC, US versus Foreign Cases)

Case Name: HTC v. IPCOM

Case No: 1:2008-cv-01897 (District of Columbia)

Expert for IPCOM

(3G Standards: 2009 – 2012)

Testified by deposition

Case Name: Apple v. Kodak

Case No. ITC 337-TA-717 (ITC)

Expert for Kodak

(Digital Image Processing & UI: 2008-2011)

Testified at trial

Case Name: Harkabi v. Sandisk,

Case No: 1:08-cv-08203-WHP (SDNY)

Expert for Harkabi

(Digital Rights Management for Flash Devices: 2010-2012)

Testified at trial

Case Name: Yangaroo Inc. v. Destiny Media Technologies, Inc.

Case No: 09-C-0462 (ED Wisconsin)

Expert for Yangaroo.

(Digital Rights Management Streaming: 2010-2011)

Testified by deposition

Case Name: Motorola v. Microsoft,

Case No: ITC 337-TA-752

Expert for Motorola

(Peer to Peer Gaming: 2011-2013)

Testified at trial

Case Name: Motorola v. Apple,

Case No: ITC 337-TA-745 (ITC)

Expert for Motorola

(Mobile Applications & UI: 2011-2012)

Testified at trial

Case Name: Innovative Sonic Ltd. vs. RIM

Case No: 3:11-cv-00706-K-BF (ND Dallas)

Expert for Innovative Sonic Ltd

(3G Standards – Encryption, HSDPA: 2010-2013)

Testified at trial

Case Name: Interdigital v. ZTE et al (JDA)

Case No: ITC 337-TA-800

Expert for JDA

(3G Standards – HSDPA: 2012-2013)

Testified at trial

Case Name: Kodak v. Apple, HTC

Case No: ITC 337-TA-831

Expert for Kodak

(Digital Image Processing & UIs: 2011-2012)

Submitted reports

Case Name: Calypso v. T-Mobile

Case No: 2:08-CV-441-JRG-RSP [ED Texas]

Expert for T-Mobile

(Unified Communications: 2012-2013)

Testified by deposition

Case Name: TracBeam v. AT&T

Case No: 6:11-cv-00096-LED [ED Texas]

Expert for AT&T

(GPS Services: 2011-2012)

Testified by deposition

Case Name: BT v. Cox/Comcast

Case No: 10-658 (SLR) (District of Delaware)

Expert for Cox and Comcast

(VOIP, Network Management: 2012-2014)

Testified by deposition

Case Name: Ericsson v. Samsung

Case No: 337-TA-862 (ITC)

Expert for Ericsson

(RF Receivers, EDGE Standards: 2012- 2013)

Testified at trial

Case Name: IPR – ContentGuard v. ZTE

Case No: (PTAB)

Expert for ZTE

(DRM for Digital Devices: 2012-2014)

Testified by deposition

Case Name: Emblaze v. Apple

Case No: 5:11-cv-01079-PSG (ND Cal)

Expert for Emblaze

(Digital Video/Audio Streaming: 2012-2014)

Testified at trial

Case Name: Emblaze v. Microsoft

Case No: 3:12-cv-05422-JST (ND Cal)

Expert for Emblaze

(Digital Video/Audio Streaming: 2012 - Present)

Ongoing

Case Name: MMI v. RIM

Case No: 2:10-cv-00113-TJW-CE (ED Texas)

Expert for MMI

(Area: Mobile Devices/User Interfaces: 2012- 2013)

Testified by deposition

Case Name: Wi-LAN v. Apple

Case No: 13-cv-0790 DMS (ED Texas)

Case No: 3:14-cv-010507-DMS-BLM

Expert for Wi-LAN

(Area: 4G/3G Wireless Communications: 2013 –2018)

Testified by Deposition

Case Name: Sentius LLC v. Microsoft

Case No: 5:13-cv-00825-PSG (ND Cal)

Expert for Sentius

(Area: Enterprise Software Systems: 2014-2015)

Testified by deposition

Case Name: Medius Eagle Harbor v. Ford

Case No: 3:1-cv-05503-BHS (WD Washington)

Expert for Medius Tech

(Area: Automotive Multimedia Systems: 2014-2016)

Testified at Trial

Genband US LLC v. Metaswitch Networks

No 2:14-cv-33 (E.D. Texas)

Expert for Metaswitch Networks

Technology: Voice & Data Over IP Networks (2014-2015)

Submitted declarations & deposition

Enterprise - Systems Technologies S.a.r.l v. Samsung Electronics Co. Ltd

Case No: 6:14-cv-555-MHS (ED Texas) and ITC Inv. No. 337-TA-925

Expert for Samsung

Technology: Android Operating System (2014-2015)

Testified by deposition

Ericsson Inc. v. Apple Inc.

Case No: 2:15-cv-287 (ED Texas) and ITC-337-952/953

Expert for Ericsson

Technology: 4G Wireless Systems (2015 – present)

Testified by deposition & Trial

Intellectual Ventures LLC v. Motorola Mobility LLC (Google)

Case No: 13-cv-61358-RST (S.D. Florida)

Expert for Google

Technology: Wireless Systems (2013- present)

Testified by deposition (IPR)

Intellectual Ventures LLC v. Nikon Corp

C.A No. 11-1025-SLR (District of Delaware)

Expert for Nikon

Technology: Wireless Systems (WiFi) (2014-2015)

Submitted declarations

Masimo v. Mindray Biomedical Electronics Co. / Philips

Case No: SACV-12-02206 CJC (JPRx) (C.D. California)

8:12-cv-02206-CJC-JPR

Expert for Masimo

Technology: Pulse Oximetry (2014 – 2016)

Submitted reports, testified by deposition

Samsung v. Nvidia

Case No: 3:14-cv-757-REP ED Virginia

Expert for Samsung

Technology: Microprocessors & Memories (2014 – 2016)

Submitted reports & Deposition & Trial

Chrimar v. HP/Cisco/Alcatel/Dell/Adtran/AeroHive/D-Link/TP-Link/TrendNet/Juniper Networks/CoStar/Accton/AMX

Case No: 4:13-cv-1300-JSW, Case 6:15-cv-163 (ED Texas)

Case No: 6:15-cv-00618-JRG-JDL (ED Texas)

Expert for Chrimar

Technology: Power over Ethernet (2015-2017)

Submitted reports & Deposition & Trial

Chamberlain v. Ryobi/TTI

Case No: 1:16-cv-06097 (ND Illinois)

Expert for Ryobi

Technology: Wireless/IoT/Barrier Movement (2016 – present)

Submitted reports & deposition & trial testimony

IOEngine v. IMC/Imation

Case No: cv-14-1572-GMS (US Delaware)

Expert for IMC/Imation

Technology: Networked Storage Device (2016-2017)

Submitted reports & deposition & trial testimony

Huawei v. Samsung

Case No: 3:16-cv-2787-WHO (ND Cal)

Expert for Samsung

Technology: 4G/LTE Random Access Protocols (2016-present)

Submitted reports & deposition

Hitachi Maxell v. ZTE/Huawei

Case No: 5:16-cv-00178-RWS (ED Texas)

Expert for Hitachi Maxell

Technology: Digital Cameras

Submitted reports & deposition (2017 – 2018)

Qualcomm v. Apple

Case No: 17-ccv-0108-GPC-MDD (SD Cal) Also, Related ITC/FTC Matters

Expert for Qualcomm

Technology: 4G/Wireless Communications/Smartphones (2017-2019)

Submitted Reports and Deposition

Qualcomm v. Apple

Case No: 3:17-cv-01375-DMS-MDD (SD Cal)

Expert for Qualcomm

Technology: 4G/Wireless Communications/Smartphones (2017-2019)

Submitted Reports and Deposition

Optis v. Huawei

Case No: 2:17-cv-123 (E.D. Texas)

Expert for Optis Wireless

Technology: 4G/Video (2017-2019)

Submitted reports & deposition

Broadcom v. Sony

Case No: 8:16-cv-1052 (PTAB and Central Cal)

Expert for Broadcom

Technology: Wi Fi

No activity - settled (2017 – 2017)

Ameranth v. Hyatt Corporation

Case No: 3:11-cv-1810 (SD Cal)

Expert for Hyatt

Technology: Wireless eCommerce Applications (2017-2018)

Expert Technical consulting

Beckman Coulter v. Sysmex

Case No: 1:17-cv-24049-DPG (ND Illinois)

Expert for Sysmex

Technology: Medical Instrumentation Automation (2017-present)

Testifying Expert

TQ Delta

Expert for TQ Delta

Technology: DSL Technologies (2018-present)

Testifying Expert

3GL/KPN v. LG, Blackberry, HTC

Expert for 3GL/KPN

Technology: 4G/LTE Protocols (2018-present)

Reports and Deposition / Testifying Expert

Cirba/Densify v. VMWare

Case No: 1:19-cv-00742-LPS

Expert for Cirba/Densify

Technology: Virtualization (2019-present)

Reports Deposition/PI Hearing / Testifying Expert

Power Integrations v. On Semiconductor

Case No: 17-cv-03189-BLF

Expert for On Semiconductor

Technology: Power Electronics (2018-present)

Reports & Deposition/Testifying Expert.

Wilan v. Apple

Case No: 3:14-cv-2235

Expert for WiLan

Technology: Voice over LTE/LTE Protocols

Reports and Testified through Deposition/Trials

Additional matters include declarations supporting IPRs at the PTAB for Google (US Patent 8,601,154), On Semiconductor (US Patent 6,212,079), Ubisoft (US Patent 5,490,216), Broadcom (WiFi), Sony (US Patent 6,101,534), Kia, (US Patent 5,530,431), Qualcomm, Fortinet (US patent 6,195,587), and ZTE (US Patent 7,523,072), and Ericsson, Amazon, Ring, Digital Ally, On Semiconductor, United Patents, Lenovo, BMC Software.

Earned Degrees

- 1. B. Tech (Hons), Electronics & Electrical Comm. Engineering**
Indian Institute of Technology (IIT), Kharagpur, India
1984.
- 2. Ph.D., Electrical Engineering & Computer Sciences (EECS)**
University of California (UC), Berkeley. CA
1989.

Books

- 1. VLSI Digital Signal Processors**
Madiseti, V.K.;
Boston: MA, IEEE Press: Butterworth Heinemann, 1995, 525 pp.
- 2. Quick-Turnaround ASIC Design in VHDL**
Romdhane, M., Madiseti, V.K., Hines, J.
Boston: MA, Kluwer Academic Press, 1996, 190 pp.
- 3. The Digital Signal Processing Handbook (First Edition)**
Madiseti, V. K., Williams, D. (Editors)
CRC Press, Boca Raton, Fla, 1998, 2500 pp.
- 4. VHDL: Electronics Systems Design Methodologies.**
Madiseti, V. K. (Editor)
Boston: MA, IEEE Standards Press, 2000, ISBN 0-7381-1878-8.
- 5. Platform-Centric Approach to System-on-Chip (SoC) Design.**
Madiseti, V. K., Arpnikanondt, A.
Springer, Boston: MA, Springer, 2004, 280 pp.

6. The Digital Signal Processing Handbook – Second Edition.

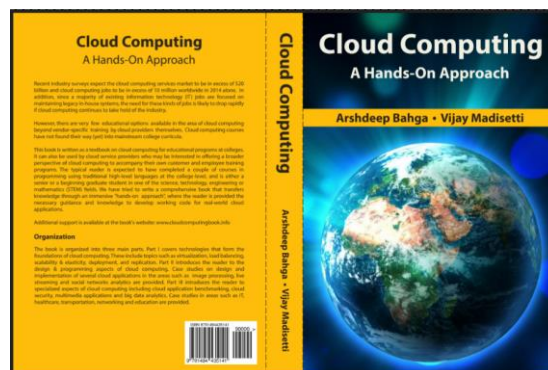
Madiseti, V. K. (2009)
CRC Press, Boca Raton, Fla.

7. Cloud Computing: A Hands-On Approach

A Bahga, V. Madiseti (2013)
Amazon CreateSpace Publishing, 2013, 454 pp.

8. Internet of Things: A Hands-On Approach

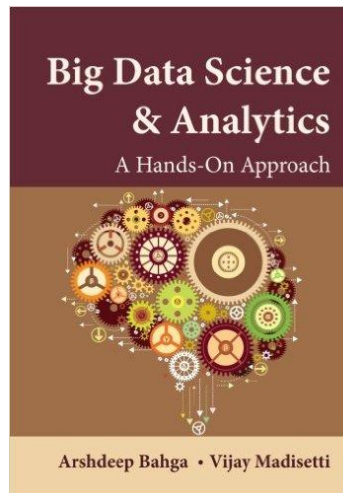
A Bahga, V. Madiseti (2014)
Amazon CreateSpace Publishing, 2014, 450 pp.



9. Big Data Science & Analytics: A Hands-On Approach

A Bahga, V. Madiseti (2016)

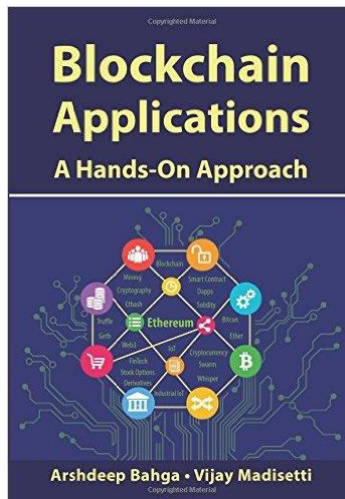
Amazon CreateSpace Publishing, 2016, 542 pp.



10. Blockchain Applications: A Hands-On Approach

A Bahga, V. Madiseti (2017)

Amazon CreateSpace Publishing, 2017, 380 pp.



Edited Books & Collection of Papers

1. Advances in Parallel & Distributed Simulation

Madiseti, V.K.; Nicol, D., Fujimoto, R. (Editors)

San Diego, CA: SCS Press, 1991, 200 pp.

2. Modeling, Analysis, Simulation of Computer & Telecommunications Systems

Madiseti, V., Gelenbe, E., Walrand, J. W. (Editors)

Los Alamitos: CA, IEEE Computer Society Press, 1994, 425 pp.

3. Modeling & Simulations on Microcomputers

Madiseti, V.K. (Editor)

San Diego, CA: SCS Press, 138 pp. 1990.

Editorship of Journals & Transactions

1. IEEE Design & Test of Computers

Special Issue: Reengineering Digital Systems

April – June 1999 (Vol 16, No 2)

Madiseti, V.K (Editor)

Los Alamitos: CA, IEEE Computer Society Press, 1999.

2. IEEE Design & Test of Computers

Special Issue: Rapid Prototyping of Digital Systems

Fall 1996 (Vol 13, No 3)

Madiseti, V., Richards, M. (Editors)

Los Alamitos: CA, IEEE Computer Society Press, 1994, 425 pp.

3. IEEE Transactions on Circuits & Systems II

Associate Editor: 1993-1995.

4. International Journal in Computer Simulation

Associate Editor: 1990-1993

5. International Journal in VLSI Signal Processing

Editorial Board: 1995 - Present

Issued US Patents

[1] [10,503,927](#) [Method and system for securing cloud storage and databases from insider threats and optimizing performance](#), Issued Dec 10, 2019

[2]. [10,460,283](#) [Smart contract optimization for multiparty service or product ordering](#)

- system, Issued Oct 29, 2019
- [3]. [10,459,946](#) [Method and system for tuning blockchain scalability, decentralization, and security for fast and low-cost payment and transaction processing](#), Issued Oct 29, 2019
 - [4]. [10,402,589](#) [Method and system for securing cloud storage and databases from insider threats and optimizing performance](#), Issued Sep 3, 2019
 - [5]. [10,394,845](#) [Method and system for tuning blockchain scalability for fast and low-cost payment and transaction processing](#), Issued Aug 27, 2019
 - [6]. [10,289,631](#) [Method and system for tuning blockchain scalability for fast and low-cost payment and transaction processing](#), Issued May 24, 2019
 - [7]. [10,255,342](#) [Method and system for tuning blockchain scalability, decentralization, and security for fast and low-cost payment and transaction processing](#), Issued April 9, 2019
 - [8]. [10,243,743](#) [Tokens or crypto currency using smart contracts and blockchains](#), Issued March 26, 2019
 - [9]. [10,204,339](#) [Method and system for blockchain-based combined identity, ownership, integrity and custody management](#), Issued February 12, 2019
 - [10]. [10,204,148](#) [Method and system for tuning blockchain scalability, decentralization, and security for fast and low-cost payment and transaction processing](#), Issued Feb 12, 2019
 - [11]. [10,121,143](#) [Method and system for blockchain-based combined identity, ownership, integrity and custody management](#), Issued Nov 6, 2018
 - [12]. [10,102,526](#) [Method and system for blockchain-based combined identity, ownership, integrity and custody management](#), October 16, 2018
 - [13]. [10,102,265](#) [Method and system for tuning blockchain scalability for fast and low-cost payment and transaction processing](#), October 16, 2018
 - [14]. [9,935,772](#) [Methods and systems for operating secure digital management aware applications](#), April 3, 2018
 - [15]. [9,769,213](#) [Method and system for secure digital object management](#), Issued Sep 19, 2017

Refereed Journal Publications

1. Trends in the Electronic Control of Mine Hoists

*Madiseti, V. and Ramlu, M.,
IEEE Transactions on Industry Applications, Vol IA-22, No. 6,
November/December 1986. Pages 1105-1112*

- 2. Multilevel range/NEXT performance in digital subscriber loops**
Brand, G.; Madisetti, V.; Messerschmitt, D.G.;
Communications, Speech and Vision, IEE Proceedings I [see also IEE Proceedings-Communications] ,Volume: 136 , Issue: 2 , April 1989
Pages:169 – 174
- 3. Seismic migration algorithms on parallel computers**
Madisetti, V.K.; Messerschmitt, D.G.;
Signal Processing, IEEE Transactions on [see also Acoustics, Speech, and Signal Processing, IEEE Transactions on] ,Volume: 39 , Issue: 7 , July 1991
Pages:1642 – 1654
- 4. Asynchronous algorithms for the parallel simulation of event-driven dynamical systems**
Madisetti, V.K.; Walrand, J.C.; Messerschmitt, D.G.:
ACM Transactions on Modeling and Computer Simulation, v 1, n 3, July 1991,
Pages: 244-74
- 5. Synchronization mechanisms for distributed event-driven computation**
Madisetti, V.K.; Hardaker, D.:
ACM Transactions on Modeling and Computer Simulation, v 2, n 1, Jan. 1992,
Pages: 12-51
- 6. Efficient VLSI Architectures for the Arithmetic Fourier Transform (AFT)**
Kelley, B.T.; Madisetti, V.K.;
Signal Processing, IEEE Transactions on [see also Acoustics, Speech, and Signal Processing, IEEE Transactions on] ,Volume: 41 , Issue: 1 , January 1993
Pages:365-378
- 7. The fast discrete Radon transform. I. Theory**
Kelley, B.T.; Madisetti, V.K.;
Image Processing, IEEE Transactions on ,Volume: 2 , Issue: 3 , July 1993
Pages:382 – 400
- 8. The Georgia Tech digital signal multiprocessor**
Barnwell, T.P., III; Madisetti, V.K.; McGrath, S.J.A.;
Signal Processing, IEEE Transactions on [see also Acoustics, Speech, and Signal Processing, IEEE Transactions on] ,Volume: 41 , Issue: 7 , July 1993
Pages:2471 – 2487
- 9. The MIMDIX Environment for Parallel Simulation**

Madiseti, V.K.; Hardaker, D.; Fujimoto, R.M.:

Journal of Parallel and Distributed Computing, v18, no. 4, August 1993,
Pages: 473-83.

10.LMSGEN: a prototyping environment for programmable adaptive digital filters in VLSI

Romdhane, M.S.B.; Madiseti, V.K.;

Chapter in VLSI Signal Processing, VII, 1994.,
Pages:33 – 42

11. Fixed-point co-design in DSP

Egolf, T.W.; Famorzadeh, S.; Madiseti, V.K.;

Chapter in VLSI Signal Processing, VII, 1994.,
Pages:113 - 126

12. A fast spotlight-mode synthetic aperture radar imaging system

Madiseti, V.K.;

Communications, IEEE Transactions on ,Volume: 42 , Issue: 234 , February-April 1994

Pages:873 – 876

13. Rapid prototyping on the Georgia Tech digital signal multiprocessor

Curtis, B.A.; Madiseti, V.K.;

Signal Processing, IEEE Transactions on [see also Acoustics, Speech, and Signal Processing, IEEE Transactions on] ,Volume: 42 , Issue: 3 , March 1994

Pages:649 – 662

14.Low-power signaling in asymmetric noisy channels via spectral shaping

Sipitca, M.; Madiseti, V.K.;

Signal Processing Letters, IEEE, Volume: 1 , Issue: 8 , Aug 1994

Pages:117 – 118

15. A quantitative methodology for rapid prototyping and high-level synthesis of signal processing algorithms

Madiseti, V.K.; Curtis, B.A.;

Signal Processing, IEEE Transactions on [see also Acoustics, Speech, and Signal Processing, IEEE Transactions on] ,Volume: 42 , Issue: 11 , Nov. 1994

Pages:3188 – 3208

16. Computer Simulation of Application-Specific Signal Processing Systems

Casinovi, G.; Madiseti, V.K.;

International Journal in Computer Simulation, Vol. 4, No. 4, Nov 1994.

17. System partitioning of MCMs for low power

Khan, S.A.; Madiseti, V.K.;

Design & Test of Computers, IEEE ,Volume: 12 , Issue: 1 , Spring 1995

Pages:41 – 52

18. Error correcting run-length limited codes for magnetic recording

Jaejin Lee; Madiseti, V.K.;

Magnetics, IEEE Transactions on ,Volume: 31 , Issue: 6 , Nov. 1995

Pages:3084 – 3086

19. Virtual prototyping of embedded microcontroller-based DSP systems

Madiseti, V.K.; Egolf, T.W.;

Micro, IEEE ,Volume: 15 , Issue: 5 , Oct. 1995

Pages:9 – 21

20. Constrained multitrack RLL codes for the storage channel

Lee, J.; Madiseti, V.K.;

Magnetics, IEEE Transactions on ,Volume: 31 , Issue: 3 , May 1995

Pages:2355 – 2364

21. Rapid digital system prototyping: current practice, future challenges

Madiseti, V.K.;

Design & Test of Computers, IEEE ,Volume: 13 , Issue: 3 , Fall 1996

Pages:12 – 22

22. Conceptual prototyping of scalable embedded DSP systems

Dung, L.-R.; Madiseti, V.K.;

Design & Test of Computers, IEEE ,Volume: 13 , Issue: 3 , Fall 1996

Pages:54 – 65

23. Advances in rapid prototyping of digital systems

Madiseti, V.K.; Richards, M.A.;

Design & Test of Computers, IEEE ,Volume: 13 , Issue: 3 , Fall 1996

Pages:9

24. Combined modulation and error correction codes for storage channels

Jaejin Lee; Madiseti, V.K.;

Magnetics, IEEE Transactions on ,Volume: 32 , Issue: 2 , March 1996

Pages:509 – 514

25. Model-based architectural design and verification of scalable embedded DSP systems-a RASSP approach

Dung, L.-R.; Madiseti, V.K.; Hines, J.W.;

Chapter in VLSI Signal Processing, IX, 1996.
Pages:147 – 156

26. Low-power digital filter implementations using ternary coefficients

Hezar, R.; Madisetti, V.K.;
Chapter in VLSI Signal Processing, IX, 1996.,
Pages:179 – 188

27. All-digital oversampled front-end sensors

Romdhane, M.S.B.; Madisetti, V.K.;
Signal Processing Letters, IEEE, Volume: 3 , Issue: 2 , Feb. 1996
Pages:38 – 39

28. Modeling COTS components in VHDL

Calhoun, S., Reese, R; Egolf, T., Madisetti, V.K.;
Journal of VLSI Signal Processing, Volume: 14 , Issue: 2 , Nov 1996
Pages: 24 – 31

29. VHDL-Based Rapid Systems Prototyping

Egolf, T.; Madisetti, V.K.;
Journal of VLSI Signal Processing, Volume: 14 , Issue: 2 , Nov 1996
Pages: 40-52

30. Interface design for core-based systems

Madisetti, V.K.; Lan Shen;
Design & Test of Computers, IEEE ,Volume: 14 , Issue: 4 , Oct.-Dec. 1997
Pages:42 - 51

31. Incorporating cost modeling in embedded-system design

Debardelaben, J.A.; Madisetti, V.K.; Gadiant, A.J.;
Design & Test of Computers, IEEE ,Volume: 14 , Issue: 3 , July-Sept. 1997
Pages:24 – 35

32. On homomorphic deconvolution of bandpass signals

Marenco, A.L.; Madisetti, V.K.;
Signal Processing, IEEE Transactions on [see also Acoustics, Speech, and
Signal Processing, IEEE Transactions on] ,Volume: 45 , Issue: 10 , Oct. 1997
Pages:2499 – 2514

**33. A case study in the development of multi-media educational material:
the VHDL interactive tutorial**

Gadiant, A.J.; Stinson, J.A., Jr.; Taylor, T.C.; Aylor, J.H.; Klenke, R.H.;
Salinas, M.H.; Madisetti, V.K.; Egolf, T.; Famorzadeh, S.; Karns, L.N.; Carter,
H.W.;

Education, IEEE Transactions on ,Volume: 40 , Issue: 4 , Nov. 1997
Pages:17 pp.

34. Adaptive mobility management in wireless networks

Jeongwook Kim; Madiseti, V.K.;
Electronics Letters ,Volume: 34 , Issue: 15 , 23 July 1998
Pages:1453 – 1455

35. Efficient implementation of two-band PR-QMF filterbanks

Hezar, R.; Madiseti, V.K.;
Signal Processing Letters, IEEE ,Volume: 5 , Issue: 4 , April 1998
Pages:92 – 94

36. On fast algorithms for computing the inverse modified discrete cosine transform

Yun-Hui Fan; Madiseti, V.K.; Mersereau, R.M.;
Signal Processing Letters, IEEE ,Volume: 6 , Issue: 3 , March 1999
Pages:61 – 64

37. System on chip or system on package?

Tummala, R.R.; Madiseti, V.K.;
Design & Test of Computers, IEEE ,Volume: 16 , Issue: 2 , April-June 1999
Pages:48 – 56

38. Reengineering legacy embedded systems

Madiseti, V.K.; Jung, Y.-K.; Khan, M.H.; Kim, J.; Finnessy, T.;
Design & Test of Computers, IEEE ,Volume: 16 , Issue: 2 , April-June 1999
Pages:38 – 47

39. Reengineering digital systems

Madiseti, V.K.;
Design & Test of Computers, IEEE ,Volume: 16 , Issue: 2 , April-June 1999
Pages:15 – 16

40. Parameter optimization of robust low-bit-rate video coders

Sangyoun Lee; Madiseti, V.K.;
Circuits and Systems for Video Technology, IEEE Transactions on, Volume: 9
Issue: 6 , Sept. 1999
Pages:849 – 855

41. Closed-form for infinite sum in bandlimited CDMA

Jatunov, L.A.; Madiseti, V.K.;
Communications Letters, IEEE ,Volume: 8 , Issue: 3 , March 2004
Pages:138 – 140

- 42. A new protocol to enhance path reliability and load balancing in mobile ad hoc networks**
Argyriou, A.; Madisetti, V.K.;
Journal of Ad Hoc Networks, Elsevier Press, 2004
- 43. Closed-form analysis of CDMA systems using Nyquist pulse**
Jatunov, L.A.; Madisetti, V. K.;
Communications Letters, IEEE (Under Revision), 2005.
- 44. Systematic Design of End-to-End Wireless Mobility Management Protocols,**
Argyriou, A.; Madisetti, V. K.;
ACM/Springer Wireless Networks (WINET), Accepted 2005.
- 45. A Novel End-to-End Approach for Video Streaming Over the Internet,**
Argyriou, A.; Madisetti, V. K.;
Kluwer Telecommunications Systems, Vol. 28, No. 2, Pages 133-150, Jan 2005. *Special Issue on Multimedia Streaming.*
- 46. An Analytical Framework of RD Optimized Video Streaming with TCP,**
Argyriou, A.; Madisetti, V. K.;
IEEE Transactions on Multimedia, Submitted for review in March 2005.
- 47. Modeling the Effect of Handoffs on Transport Protocol Performance,**
Argyriou, A.; Madisetti, V. K.;
IEEE Transactions on Mobile Computing, Submitted for review in March 2005
- 48. Throughput Models for Transport Protocols with CBR and VBR Traffic Workloads",**
Argyriou, A.; Madisetti, V. K.;
ACM Transactions on Multimedia Computing, Communications & Applications, Submitted for review in April 2005.
- 49. "Electronic System, Platform & Package Codesign",**
Madisetti, V. K.
IEEE Design & Test of Computers, Volume 23, Issue 3, June 2006. pages 220-233.
- 50. "The Design of an End-to-End Handoff Management Protocol",**
A. Argyriou, Madisetti, V. K.
Wireless Networks, Springer, May 2006.

51. "A Soft-Handoff Transport Protocol for Media Flows in Heterogeneous Mobile Networks ",

A. Argyriou, Madiseti, V. K.

Computer Networks, Vol 50, Issue 11, Pages 1860-1871, August 2006.

52. "Computationally Efficient SNR Estimation for Bandlimited WCDMA Systems"

L. Jatunov, Madiseti, V. K.

IEEE Transactions on Wireless Communications, Volume 5, Issue 13, December 2006, Pages 3480-3491.

53. "Space-Time Codes for Wireless & Mobile Applications",

M. Sinnokrot, Madiseti, V.K.

DSP Handbook, Second Edition, 2009 (to be published)

54.A. Bahga, V. Madiseti, "Rapid Prototyping of Advanced Cloud-Based Systems", *IEEE Computer*, vol. 46, no. 11, Nov 2013, pp 76-83, 2013

55.A. Bahga, V. Madiseti, "Cloud-Based Information Integration & Informatics Framework for Healthcare Applications", *IEEE Computer*, February 2015.

56.A. Bahga, V. Madiseti, "A Cloud-based Approach for Interoperable EHRs", *IEEE Journal of Biomedical and Health Informatics*, vol. 17, no. 5, Sep 2013, pp. 894-906, 2013

57.A. Bahga, V. Madiseti, "Cloud-Based Information Technology Framework for Data Driven Intelligent Transportation Systems", *Journal of Transportation Technologies*, vol.3 no.2, April 2013

58.A. Bahga, V. Madiseti, "Performance Evaluation Approach for Multi-tier Cloud Applications", *Journal of Software Engineering and Applications*, vol. 6, no. 2, pp. 74-83, Mar 2013.

59.Yusuf, A., V. Madiseti, "Configuration for Predicting Travel Time Using Wavelet Packets and Support Vector Regression", *Journal of Transportation Technologies*, vol 3, no. 3, June 2013.

60.A. Bahga, V. Madiseti, "Analyzing Massive Machine Maintenance Data in a Computing Cloud", *IEEE Transactions on Parallel and Distributed Systems*, vol. 23, no. 10, pp. 1831 - 1843, 2012.

61. N. Radia, Y. Zhang, M. Tatimapula, V. Madiseti, **"Next Generation Applications on Cellular Networks: Trends, Challenges, and Solutions,"** *Proceedings of the IEEE*, Vol 100, Issue 4, pp. 841-854, 2012.
62. A. Bahga, V. Madiseti, **"Rapid Prototyping of Advanced Cloud-Based Systems"**, *IEEE Computer*, vol. 46, no. 11, Nov 2013, pp 76-83, 2013
63. A. Bahga, V. Madiseti, **"A Cloud-based Approach for Interoperable EHRs"**, *IEEE Journal of Biomedical and Health Informatics*, vol. 17, no. 5, Sep 2013, pp. 894-906, 2013
64. A. Bahga, V. Madiseti, **"Cloud-Based Information Integration & Informatics Framework for Healthcare Applications"**, *IEEE Computer*, February 2015.

Peer Reviewed Conference Publications

1. **Dynamically-reduced complexity implementation of echo cancelers**
Madiseti, V.; Messerschmitt, D.; Nordstrom, N.;
Acoustics, Speech, and Signal Processing, IEEE International Conference on ICASSP '86. ,Volume: 11 , Apr 1986
2. **Seismic migration algorithms using the FFT approach on the NCUBE multiprocessor**
Madiseti, V.K.; Messerschmitt, D.G.;
Acoustics, Speech, and Signal Processing, 1988. ICASSP-88., 1988
International Conference on , 11-14 April 1988
3. **Seismic migration algorithms on multiprocessors**
Madiseti, V.K.; Messerschmitt, D.G.;
Acoustics, Speech, and Signal Processing, 1988. ICASSP-88., 1988
International Conference on , 11-14 April 1988
Pages:2124 - 2127 vol.4
4. **WOLF: A rollback algorithm for optimistic distributed simulation systems**
Madiseti, V.; Walrand, J.; Messerschmitt, D.;
Simulation Conference Proceedings, 1988 Winter , December 12-14, 1988
Pages:296 – 305

5. Efficient distributed simulation

Madiseti, V.; Walrand, J.; Messerschmitt, D.;
Simulation Symposium, 1989. The 22nd Annual , March 28-31, 1989
Pages:5 - 6

6. High speed migration of multidimensional seismic data

Kelley, B.; Madiseti, V.;
Acoustics, Speech, and Signal Processing, 1991. ICASSP-91., 1991
International Conference on , 14-17 April 1991
Pages:1117 - 1120 vol.2

7. Performance of a fast analog VLSI implementation of the DFT

Buchanan, B.; Madiseti, V.; Brooke, M.;
Circuits and Systems, 1992., Proceedings of the 35th Midwest Symposium on
, 9-12 Aug. 1992
Pages:1353 - 1356 vol.2

8. Task scheduling in the Georgia Tech digital signal multiprocessor

Curtis, B.A.; Madiseti, V.K.;
Acoustics, Speech, and Signal Processing, 1992. ICASSP-92., 1992 IEEE
International Conference on ,Volume: 5 , 23-26 March 1992
Pages:589 - 592 vol.5

9. The fast discrete Radon transform

Kelley, B.T.; Madiseti, V.K.;
Acoustics, Speech, and Signal Processing, 1992. ICASSP-92., 1992 IEEE
International Conference on ,Volume: 3 , 23-26 March 1992
Pages:409 - 412 vol.3

10.Yield-based system partitioning strategies for MCM and ASEM design

Khan, S.; Madiseti, V.;
Multi-Chip Module Conference, 1994. MCMC-94, Proceedings., 1994 IEEE,15-
17 March 1994
Pages:144 - 149

11. Multitrack RLL codes for the storage channel with immunity to intertrack interference

Lee, J.; Madiseti, V.K.;
Global Telecommunications Conference, 1994. GLOBECOM '94.
'Communications: The Global Bridge', IEEE,Volume: 3 , 28 Nov.-2 Dec. 1994
Pages:1477 - 1481 vol.3

12. A parallel mapping of backpropagation algorithm for mesh signal processor

Khan, S.A.; Madiseti, V.K.;
Neural Networks for Signal Processing [1995] V. Proceedings of the 1995

IEEE Workshop , 31 Aug.-2 Sept. 1995
Pages:561 – 570

13. Virtual prototyping of embedded DSP systems

Madiseti, V.K.; Egolf, T.; Famorzadeh, S.; Dung, L.-R.;
Acoustics, Speech, and Signal Processing, 1995. ICASSP-95., 1995
International Conference on ,Volume: 4 , 9-12 May 1995
Pages:2711 - 2714 vol.4

14. Assessing and improving current practice in the design of application-specific signal processors

Shaw, G.A.; Anderson, J.C.; Madiseti, V.K.;
Acoustics, Speech, and Signal Processing, 1995. ICASSP-95., 1995
International Conference on ,Volume: 4 , 9-12 May 1995
Pages:2707 - 2710 vol.4

15. Introduction to ARPA's RASSP initiative and education/facilitation program

Corley, J.H.; Madiseti, V.K.; Richards, M.A.;
Acoustics, Speech, and Signal Processing, 1995. ICASSP-95., 1995
International Conference on ,Volume: 4 , 9-12 May 1995
Pages:2695 - 2698 vol.4

16. DSP design education at Georgia Tech

Madiseti, V.K.; McClellan, J.H.; Barnwell, T.P., III;
Acoustics, Speech, and Signal Processing, 1995. ICASSP-95., 1995
International Conference on ,Volume: 5 , 9-12 May 1995
Pages:2869 - 2872 vol.5

17. Rapid prototyping of DSP systems via system interface module generation

Famorzadeh, S.; Madiseti, V.K.;
Acoustics, Speech, and Signal Processing, 1996. ICASSP-96. Conference Proceedings., 1996 IEEE International Conference on ,Volume: 2 , 7-10 May 1996
Pages:1256 - 1259 vol. 2

18. Rapid prototyping of DSP chip-sets via functional reuse

Romdhane, M.S.B.; Madiseti, V.K.;
Acoustics, Speech, and Signal Processing, 1996. ICASSP-96. Conference Proceedings., 1996 IEEE International Conference on ,Volume: 2 , 7-10 May 1996
Pages:1236 - 1239 vol. 2

- 19. A constructive deconvolution procedure of bandpass signals by homomorphic analysis**
Marenco, A.L.; Madiseti, V.K.;
Geoscience and Remote Sensing Symposium, 1996. IGARSS '96. 'Remote Sensing for a Sustainable Future.', International ,Volume: 3 , 27-31 May 1996
Pages:1592 - 1596 vol.3
- 20. BEEHIVE: an adaptive, distributed, embedded signal processing environment**
Famorzadeh, S.; Madiseti, V.; Egolf, T.; Nguyen, T.;
Acoustics, Speech, and Signal Processing, 1997. ICASSP-97., 1997 IEEE International Conference on ,Volume: 1 , 21-24 April 1997
Pages:663 - 666 vol.1
- 21. Target detection from coregistered visual-thermal-range images**
Perez-Jacome, J.E.; Madiseti, V.K.;
Acoustics, Speech, and Signal Processing, 1997. ICASSP-97., 1997 IEEE International Conference on ,Volume: 4 , 21-24 April 1997
Pages:2741 - 2744 vol.4
- 22. Variable block size adaptive lapped transform-based image coding**
Klausutis, T.J.; Madiseti, V.K.;
Image Processing, 1997. Proceedings., International Conference on ,Volume: 3 , 26-29 Oct. 1997
Pages:686 - 689 vol.3
- 23. A Rate 8/10 (0, 6) MTR Code And Its Encoder/decoder**
Jaejin Lee; Madiseti, V.K.;
Magnetics Conference, 1997. Digests of INTERMAG '97., 1997 IEEE International , 1-4 April 1997
Pages:BS-15 - BS-15
- 24. VHDL models supporting a system-level design process: a RASSP approach**
DeBardelaben, J.A.; Madiseti, V.K.; Gadiant, A.J.;
VHDL International Users' Forum, 1997. Proceedings , 19-22 Oct. 1997
Pages:183 - 188
- 25. A performance modeling framework applied to real time infrared search and track processing**
Pauer, E.K.; Pettigrew, M.N.; Myers, C.S.; Madiseti, V.K.;
VHDL International Users' Forum, 1997. Proceedings , 19-22 Oct. 1997
Pages:33 - 42

26. System design and re-engineering through virtual prototyping: a temporal model-based approach

Khan, M.H.; Madiseti, V.K.;

Signals, Systems & Computers, 1998. Conference Record of the Thirty-Second Asilomar Conference on , Volume: 2 , 1-4 Nov. 1998

Pages:1720 - 1724 vol.2

27. A debugger RTOS for embedded systems

Akgul, T.; Kuacharoen, P.; Mooney, V.J.; Madiseti, V.K.;

Euromicro Conference, 2001. Proceedings. 27th , 4-6 Sept. 2001

Pages:264 - 269

28. Adaptability, extensibility and flexibility in real-time operating systems

Kuacharoen, P.; Akgul, T.; Mooney, V.J.; Madiseti, V.K.;

Digital Systems, Design, 2001. Proceedings. Euromicro Symposium on , 4-6 Sept. 2001

Pages:400 - 405

29. Effect of handoff delay on the system performance of TDMA cellular systems

Turkboylari, M.; Madiseti, V.K.;

Mobile and Wireless Communications Network, 2002. 4th International Workshop on , 9-11 Sept. 2002

Pages:411 - 415

30. Enforcing interdependencies and executing transactions atomically over autonomous mobile data stores using SyD link technology

Prasad, S.K.; Bourgeois, A.G.; Dogdu, E.; Sunderraman, R.; Yi Pan; Navathe, S.; Madiseti, V.;

Distributed Computing Systems Workshops, 2003. Proceedings. 23rd International Conference on , 19-22 May 2003

Pages:803 - 809

31. Performance evaluation and optimization of SCTP in wireless ad-hoc networks

Argyriou, A.; Madiseti, V.;

Local Computer Networks, 2003. LCN '03. Proceedings. 28th Annual IEEE International Conference on , 20-24 Oct. 2003

Pages:317 - 318

32. Implementation of a calendar application based on SyD coordination links

Prasad, S.K.; Bourgeois, A.G.; Dogdu, E.; Sunderraman, R.; Yi Pan; Navathe, S.; Madiseti, V.;

Parallel and Distributed Processing Symposium, 2003. Proceedings.

International , 22-26 April 2003
Pages:8 pp.

33. Bandwidth aggregation with SCTP

Argyriou, A.; Madiseti, V.;
Global Telecommunications Conference, 2003. GLOBECOM '03. IEEE Volume:
7 , 1-5 Dec. 2003
Pages:3716 - 3721 vol.7

34. Software streaming via block streaming

Kuacharoen, P.; Mooney, V.J.; Madiseti, V.K.;
Design, Automation and Test in Europe Conference and Exhibition, 2003
, 2003
Pages:912 – 917

35. Frequency-dependent space-interleaving for MIMO OFDM systems

Mohajerani, P.; Madiseti, V.K.;
Radio and Wireless Conference, 2003. RAWCON '03. Proceedings , Aug. 10-
13, 2003
Pages:79 - 82

36. A media streaming protocol for heterogeneous wireless networks

Argyriou, A.; Madiseti, V.;
Computer Communications, 2003. CCW 2003. Proceedings. 2003 IEEE 18th
Annual Workshop on , 20-21 Oct. 2003
Pages:30 – 33

37. Realizing load-balancing in ad-hoc networks with a transport layer protocol

Argyriou, A.; Madiseti, V.;
Wireless Communications and Networking Conference, 2004. WCNC. 2004
IEEE ,Volume: 3 , 21-25 March 2004
Pages:1897 - 1902 Vol.3

38.Streaming H.264/AVC video over the Internet

Argyriou, A.; Madiseti, V.;
Consumer Communications and Networking Conference, 2004. CCNC 2004.
First IEEE , 5-8 Jan. 2004
Pages:169 – 174

Other Publications

1. **A Transport Layer Technology for Improving the QoS of Networked Multimedia Applications <draft-madisetti-arguriou-qos-sctp-00.txt>.**
Madisetti, V., Argyriou, A.
IETF Internet-Draft, Jul 25, 2002.
2. **Voice & Video over Mobile IP Networks <draft-madisetti-arguriou-voice-video-mip-00.txt>**
Madisetti, V., Argyriou, A.
IETF Internet-Draft, Nov 20, 2002.
3. **Enhancements to ECRTTP with Applications to Robust Header Compression for Wireless Applications. <draft-madisetti-rao-suresh-rohc-00.txt>**
Madisetti, V.; Rao, S., Suresh, N.
IETF Internet-Draft, June 30, 2003.

Ph.D. Students Graduated

1. **Brian T. Kelley, 1992**
VLSI Computing Architectures for High Speed Signal Processing
Member of Technical Staff, Motorola.

Winner of Dr. Thurgood Marshall Dissertation Fellowship Award
2. **Bryce A. Curtis, 1992**
Special Instruction Set Multiple Chip Computer for DSP
Member of Technical Staff, IBM
3. **Jaejin Lee, 1994**
Robust Multitrack Codes for the Magnetic Channel
Professor, Yonsei University, Korea
4. **Mohamed S. Ben Romdhane, 1995**
Design Synthesis of Application-Specific IC for DSP
Director of IP, Rockwell.
5. **Shoab A. Khan, 1995**
Logic and Algorithm Partitioning on MCMs
Professor, National University of Science & Technology, Pakistan
6. **Lan-Rong Dung, 1997**
VHDL-based Conceptual Prototyping of Embedded DSP Architectures
Professor, National Chaio Tung University, Taiwan.

Winner of VHDL International Best PhD Thesis Award, 1997

7. Thomas W. Egolf, 1997

Virtual Prototyping of Embedded DSP Systems

Distinguished Member of Technical Staff, Agere

8. Alvaro Marenco, 1997

On Homomorphic Deconvolution of Bandpass Signals

Professor, Texas A&M University.

Winner of GIT ECE Outstanding Teaching Assistant Award

9. Shahram Famorzadeh, 1997

BEEHIVE: A Distributed Environment for Adaptive Signal Processing

Member of Technical Staff, Rockwell.

10. Timothy J. Klausutis, 1997

Adaptive Lapped Transforms with Applications to Image Coding.

US Air Force/Univ. of Florida.

11. Lan Shen, 1998

Temporal Design of Core-Based Systems

Member of Technical Staff, IBM

12. James DeBardelaben, 1998

Optimization Based Approach to Cost Effective DSP Design

Research Scientist, Johns Hopkins University

Georgia Tech ECE Faculty Award

13. Sangyoun Lee, 1999

Design of Robust Video Signal Processors

Professor, Yonsei University

US Army Sensors Lab Research Excellence Award, 1999

14. Rahmi Hezar, 2000

Oversampled Digital Filters

Member of Technical Staff, Texas Instruments

15. Yong-kyu Jung, 2001

Model-Based Processor Synthesis

Professor, Texas A&M University

16. Mustafa Turkboylari, 2002

Handoff Algorithms for Wireless Applications

Member of Technical Staff, Texas Instruments

17. Yun-Hui Fan, 2002

A Stereo Audio Coder with Nearly Constant Signal to Noise Ratio

Post-Doctoral Research Associate, Northeastern University

18. Subrato K. De, 2002

Design of a Retargetable Compiler for DSP
Member of Technical Staff, Qualcomm

US Army Sensors Lab Research Excellence Award, 1999

19. Chonlameth Aripnikanondt, 2004

System-on-Chip Design with UML
Professor, King Mongkut's University, Thailand.

US Army Sensors Lab Research Excellence Award, 1999

20. Loran Jatunov, 2004

Performance Analysis of 3G CDMA Systems
Senior Research Scientist, Soft Networks, LLC.

21. Antonios Argyriou, 2005, Serving in Hellenic Army.

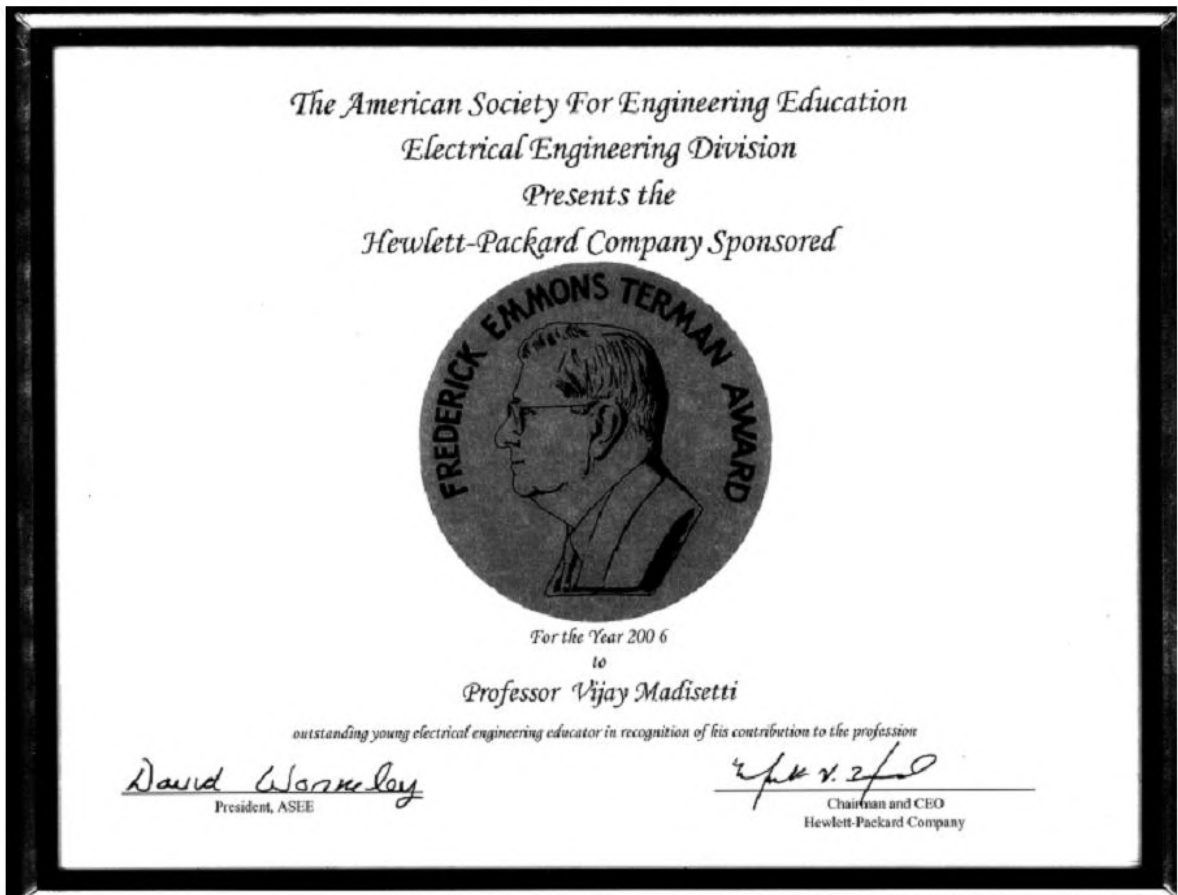
22. Pilho Kim, 2009, Scientist, VP Technologies, Inc.

23. M. Sinnokrot, 2009, Staff Engineer, Qualcomm.

Awards & Honors

1. **Jagasdis Bose National Science Talent Fellowship**, Indian Institute of Technology, Kharagpur, 1980-1984.
2. **General Proficiency Prize**, Indian Institute of Technology, Kharagpur, 1984.
3. **Demetri Angelakos Outstanding Graduate Student Award**, Univ. of California, Berkeley, 1989
4. **Ira Kay IEEE/ACM Best Paper Award** for Best Paper presented at IEEE Annual Simulation Symposium, 1989
5. **IBM Faculty Development Award** 1990
6. **Technical Program Chair**, IEEE Workshop on Parallel and Distributed Simulation. 1990.
7. **Technical Program Chair**, IEEE MASCOTS'94
8. **NSF RI Award**, 1990
9. **VHDL International Best PhD Dissertation Advisor Award**, 1997

10. Georgia Tech Outstanding Doctoral Dissertation Advisor Award, 2001.
11. ASEE 2006 Frederick Emmons Terman Medal, 2006.
12. Fellow of IEEE



Intellectual Property Disclosures (Georgia Tech)

<u>Patent</u>	<u>Date</u>	<u>Description</u>
2843	2004	Method and Apparatus for Improving the Performance of Wireless LANs
2825	2003	Method and Apparatus for Optimal Partitioning and Ordering of Antennas for Layered Space-Time Block Codes in MIMO Communications Systems
2815	2003	How to Rapidly Develop a SyD Application
GSU-023	2003	Rapid Development of SyD Applications

2810	2003	System on Mobile Devices Middleware Design
2718	2003	A Transport Layer Algorithm for Improved Anycast Communication
2717	2003	A Novel Transport Layer Load-Balancing Algorithm
2716	2003	A Transport Layer QoS Algorithm
2715	2003	A Novel Transport Layer Algorithm for MPLS Performance
2659	2002	A New Algorithm and Technology for Implementing Mobile IP with Applications to Voice and Video over Mobile IP
2656	2002	Debugging with Instruction-Level Reverse Execution
2655	2002	Embedded Software Streaming
2539		System of Databases: An Enabling Technology for Programming
2517	2002	A Dynamic Instantiated Real-Time Operating System Debugger
2516	2002	A Dynamic Real-Time Operating System
GSU-009	2001	System of Databases: Architecture,, Global Queries, Triggers and Constraints
2480	2001	Mobile Fleet Application based on SyD Technology
2479	2001	System of Databases: A model with coordination links and a calendar application
1893	1999	Beehive
1726	1995	Very High Scale Integrated Circuit Hardware Description Language Models (VHDL Models)
1401	1995	Self-Compensation Receiver (SCR)

Issued Patents: 9,935,772, 9,769,213

APPENDIX
B

Exhibit ("Ex-")	Description
1001	U.S. Patent No. 7,406,603 (the "'603 patent")
1003	File History of U.S. Application No. 09/653,517, which led to U.S. Patent No. 7,406,603 ("'603 Application")
1004	U.S. Provisional Application No. 60/151,790
1005	U.S. Patent No. 6,820,063 to England ("England")
1006	U.S. Patent No. 5,940,504 to Griswold ("Griswold")
1007	Intertrust's Patent L.R. 3-1 Disclosures: Exhibit 5
1008	U.S. Patent No. 7,319,759 to Peinado ("Peinado")
1009	U.S. Patent No. 6,591,367 to Kobata ("Kobata")
1010	U.S. Patent No. 5,915,114 to McKee ("McKee")
1011	U.S. Patent No. 5,978,902 to Mann ("Mann")
1012	UK Patent Application GB2236202A to Itzkowitz ("Itzkowitz")
1013	U.S. Patent No. 5,603,032 to Attal ("Attal")
1014	Roger Faulkner and Ron Gomes, "The Process File System and Process Model in UNIX System V," USENIX Winter '91 ("Faulkner")
1017	European Patent Specification EP0611210B1
1018	Certified Translation of European Patent Specification EP0611210B1 ("EP0611210B1")
1020	Dolby Laboratories, Inc.'s Preliminary Claim Constructions and Extrinsic Evidence Pursuant to Patent Local Rule 4-2
1021	Intertrust's Claim Constructions and Supporting Evidence

APPENDIX

C

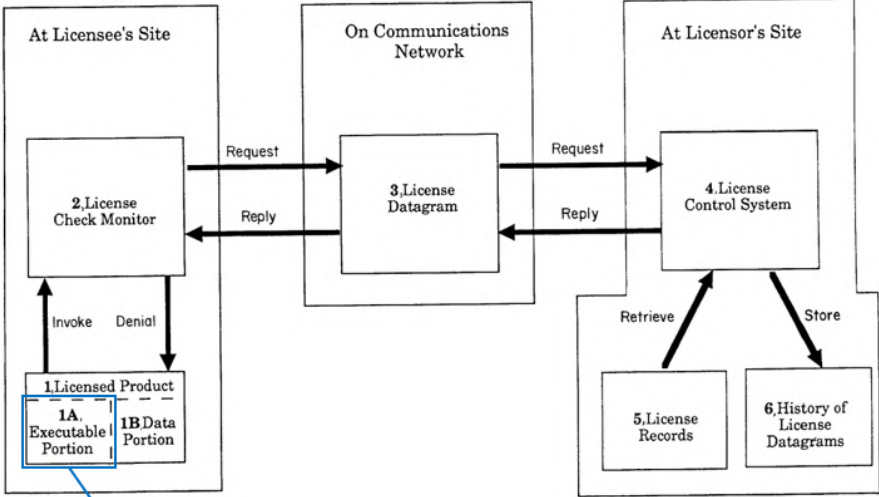
Claim 1	Griswold
<p>[1pre] A method for protecting electronic media content from unauthorized use by a user of a computer system, the method including:</p>	<p>To the extent the preamble is limiting, Griswold discloses a method for protecting electronic media content from unauthorized use by a user of a computer system.</p> <p>For example, Griswold discloses a method for controlling use of a licensed product, such as computer software, video games, movies, videos, or music (<i>i.e.</i>, electronic media content).</p> <ul style="list-style-type: none"> • <u><i>A license management system and method for recording the use of a licensed product, and for controlling its use in accordance with the terms of the license.</i></u> A licensed product invokes a license check monitor at regular time intervals. The monitor generates request datagrams which identify the licensee and the product and sends the request datagrams over a communications facility to a license control system. <u><i>The license control system maintains a record of the received datagrams, and compares the received datagrams to data stored in its licensee database.</i></u> Consequently, the license control system transmits reply datagrams with either a denial or an approval message to the monitor. (Abstract) • The present invention generally relates to systems for managing licenses of <u><i>products such as computer software, video games, CD-ROM information, movies and other video products, music and other audio products, multimedia products,</i></u> and other systems for up-to-date recording of actual usage of such a licensed product to enable efficient billing therefor. (1:16-22)
<p>[1a] receiving a request from a user of the computer system to use a piece of electronic media content;</p>	<p>Griswold discloses receiving a request (<i>e.g.</i>, “monitor 2 is invoked”; “request datagram”) from a user of the computer system (<i>e.g.</i>, “licensee” at “licensee’s site”) to use a piece of electronic media content (<i>e.g.</i>, “data portion” of “licensed product”).</p> <p>For example, Griswold discloses that a monitor on the licensee’s site is invoked, for example when the user pushes a play button (<i>i.e.</i>, the monitor receives a request from the user to use the licensed product). The monitor on the licensee’s</p>

Claim 1	Griswold
	<p>site then periodically sends a “request datagram” in order to obtain approval to continue using a licensed product. The request is received by a license control system at the licensor’s site.</p> <p style="text-align: center;">Figure 1</p> <pre> graph LR subgraph LicenseeSite [At Licensee's Site] LP[1. Licensed Product] subgraph LP_parts [] LP1A[1A. Executable Portion] LP1B[1B. Data Portion] end LCM[2. License Check Monitor] LP -- Invoke --> LCM LCM -- Denial --> LP end subgraph Network [On Communications Network] LD[3. License Datagram] end subgraph LicensorSite [At Licensor's Site] LCS[4. License Control System] LR[5. License Records] HLD[6. History of License Datagrams] LCS -- Retrieve --> LR LCS -- Store --> HLD end LCM -- Request --> LD LD -- Request --> LCS LCS -- Reply --> LD LD -- Reply --> LCM </pre> <ul style="list-style-type: none"> • A license management system and method for recording the use of a licensed product, and for controlling its use in accordance with the terms of the license. <u>A licensed product invokes a license check monitor at regular time intervals. The monitor generates request datagrams which identify the licensee and the product and sends the request datagrams over a communications facility to a license control system.</u> The license control system maintains a record of the received datagrams, and compares the received datagrams to data stored in its licensee database. Consequently, the license control system transmits reply datagrams with either a denial or an approval message to the monitor. (Abstract) • For example, in an alternative hardware embodiment such as a music or video playback device, <u>monitor 2 is invoked by the licensee’s action of pushing the ‘play’ or similar button,</u> and in a broadcast music application or similar system, the monitor may be invoked simply by turning the device on. (12:9-14)

Claim 1	Griswold
	<ul style="list-style-type: none"> <li data-bbox="537 237 1421 787">• In the present invention, <u><i>a licensed product generates request “datagrams,” messages transmitted over a communications network.</i></u> The request datagrams are sent to the licensor’s site. At the licensor’s site the datagram is compared to information stored in a license database. After the comparison, a reply datagram is sent to the licensee. Upon receiving the reply datagram, the licensed product reacts in accordance with the instructions therewithin. For example if a reply datagram contained a “denial,” the licensed product would display an appropriate message to the user and then suspend further execution of its programs. (3:62-4:5) <li data-bbox="537 808 1421 1228">• License datagrams 3 are messages that describe information related to the use of licensed product 1. Datagrams 3 are sent over a communications network between the licensee and licensor. Initially, <u><i>the licensee sends a request datagram 3 over the network to the licensor. The licensor then returns a reply datagram containing either an approval or denial.</i></u> It is also possible to implement the present invention by having the licensor transmit a reply datagram only for approvals. (5:44-52) <p data-bbox="492 1249 1328 1333">The licensed product includes a “data portion,” which is electronic media content.</p> <ul style="list-style-type: none"> <li data-bbox="537 1354 1421 1648">• The present invention generally relates to systems for managing <u><i>licenses of products such as computer software, video games, CD-ROM information, movies and other video products, music and other audio products, multimedia products,</i></u> and other systems for up-to-date recording of actual usage of such a licensed product to enable efficient billing therefor. (1:16-22) <li data-bbox="537 1669 1421 1875">• As shown in FIG. 1, <u><i>a licensed product 1 is located at a licensee’s site. Product 1 may include a data portion 1B</i></u> and a functional portion 1A such as computer software product or any other kind of information product used to control use of data portion 1B. If data

Claim 1	Griswold
	<p>portion 1B is CD-ROM database information, functional portion 1A should enable the licensee to search indexes and display text. <u>If data portion 1B is video information</u>, functional portion 1A should control the display of the video information. For audio information, functional portion 1A should play the audio information. <u>If data portion 1B is an electronic book</u>, functional portion 1A should display and turn pages. The above examples show some of the ways functional portion 1A can control data portion 1B; however, they are hardly exhaustive. (5:19-33)</p> <p style="text-align: center;">Figure 1</p>
<p>[1b] identifying one or more software modules responsible for processing the piece of electronic media content and enabling use of the piece of electronic media</p>	<p>Griswold discloses identifying one or more software modules (e.g., “identify” the “executable portion” or “functional portion” of “licensed product 1”) responsible for processing the piece of electronic media content (e.g., “used to control use of data portion 1B”) and enabling use of the piece of electronic media content by the user (e.g., “control the display of the video information”).</p> <p>For example, Griswold discloses a functional portion of the licensed product, which may be separate software on the licensee’s computer. As explained in Section VII.A.1, A POSITA would have understood that this software is either a</p>

Claim 1	Griswold
content by the user;	<p>module or a collection of modules, and thus is “one or more software modules.”</p> <ul style="list-style-type: none"> As shown in FIG. 1, <u>a licensed product 1 is located at a licensee’s site. Product 1 may include a data portion 1B and a functional portion 1A such as computer software product or any other kind of information product used to control use of data portion 1B.</u> (5:19-33) Although only a few exemplary embodiments of this invention have been described in detail above, those skilled in the art will readily appreciate that many modifications are possible in the preferred embodiments without materially departing from the novel teachings and advantages of this invention. For example, <u>product 1 was described as sometimes consisting of information as well as software which controls the information. This approach provides the greatest flexibility, but it is also possible to include the software which controls the information in the networked machine at the licensee’s site.</u> In this case, product 1 is split, with part of it on media and part on the licensee’s machine. By doing this, some space can be saved on the media containing product 1, but <u>the capabilities of these products will be limited by the standard functions available on these machines.</u> (11:28-43)

Claim 1	Griswold
	<p data-bbox="911 247 1000 275">Figure 1</p>  <p data-bbox="500 842 786 877">Software/module</p> <p data-bbox="488 898 1406 1066">Griswold discloses that the functional portion of the licensed product (which as described above may be separate software on the licensee's computer) is executable to control, <i>e.g.</i>, the display of video information.</p> <ul data-bbox="537 1087 1406 1682" style="list-style-type: none"> As shown in FIG. 1, a licensed product 1 is located at a licensee's site. Product 1 may include a data portion 1B and <u>a functional portion 1A</u> such as computer software product or any other kind of information product <u>used to control use of data portion 1B</u>. If data portion 1B is CD-ROM database information, functional portion 1A should enable the licensee to search indexes and display text. If data portion 1B is video information, <u>functional portion 1A should control the display of the video information</u>. For audio information, functional portion 1A should play the audio information. ... The above examples show some of the ways functional portion 1A can control data portion 1B; however, they are hardly exhaustive. (5:19-33) <p data-bbox="488 1703 1406 1822">A POSITA would have recognized that display of information from the data portion, such as video information, enables use of the content by the user.</p>

Claim 1	Griswold
	<p>Griswold discloses that license datagram 3 (the request datagram) describes information related to the use of licensed product 1, including an identification of product 1.</p> <ul style="list-style-type: none"> • License datagrams 3 are messages that describe information related to the use of licensed product 1. (5:44-45) • Data 23, a part of datagram 3, conveys a message, and contains a number of fields. <u>Product model number 24 and datagram number 25 identify product 1 and datagram 3, respectively.</u> It is noted that retransmitted datagrams have an identical datagram number. Duplicate datagrams must be identified at a licensor's site so that they do not all contribute in billing a licensee. (6:37-51) <p>As explained in Section VII.A.1, a POSITA would have understood that in the embodiment where the software is separate from the content the monitor at the licensee's site must first identify the software in order for the software to be used together with the content, and further so that information identifying the software can be transmitted in the license datagram for evaluation at the licensor's site as taught by Griswold.</p>
[1c] processing at least a portion of said piece of electronic media content using at least one of the one or more software modules;	<p>Griswold discloses processing at least a portion of said piece of electronic media content using at least one of the one or more software modules (e.g., “use of data portion 1B” by “functional portion 1A”; “use the licensed product”).</p> <ul style="list-style-type: none"> • After a request datagram has been sent out, <u>a user may be permitted to use the licensed product for a limited duration.</u> This feature may be necessary because of the delays in network communications. When networks are sufficiently fast, use of a licensed product can be postponed until the reply datagram is received. (4:23-29) • As shown in FIG. 1, <u>a licensed product 1 is located at a licensee's site. Product 1 may include</u> a data portion 1B and <u>a functional portion 1A such as computer</u>

Claim 1	Griswold
	<p><u>software product or any other kind of information product used to control use of data portion 1B.</u> If data portion 1B is CD-ROM database information, functional portion 1A should enable the licensee to search indexes and display text. If data portion 1B is video information, <u>functional portion 1A should control the display of the video information.</u> For audio information, functional portion 1A should play the audio information. If data portion 1B is an electronic book, <u>functional portion 1A should display and turn pages.</u> The above examples show some of the ways functional portion 1A can control data portion 1B; however, they are hardly exhaustive. (5:19-33)</p>
<p>[1d] evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner</p>	<p>Griswold discloses evaluating whether the at least one of the one or more software modules (e.g., “functional portion” of “licensed product”) process the portion of the electronic media content in an authorized manner (e.g., “compares time since the last datagram was sent 36 to disconnect allowed interval 19” and sets an “authorization code” depending on the result).</p> <p>For example, Griswold discloses that processing the content involves sending and receiving datagrams with certain timing frequencies. The monitor compares the time since the last datagram was sent to a disconnect allowed interval in the licensed product record to determine if the product has been processing the content for too long without the required reply datagram (<i>i.e.</i>, evaluates whether the product is processing the content in an authorized manner). If the time exceeds the disconnect allowed interval, then the monitor sets an “authorization code” to “5” which indicates a denial.</p>

Claim 1	Griswold
	<p>Figure 5</p> <pre> graph LR subgraph INPUT 36[36, TIME SINCE SEND] 9[9, LICENSED PRODUCT RECORD] subgraph Box1 [] 16[16, CONTROL PARAMETERS] 19[19, DISCONNECT ALLOWED INTERVAL] end end subgraph PROCESS 1041[104.1 IF Time Since Send is less than Disconnect Allowed Interval THEN Resend License Datagram, Go to 103.9 (Fig. 4).] 1042[104.2 ELSE] 10421[104.2.1 Set Authorization Code to 5, i.e. no response.] 10422[104.2.2 Set the Message to the text as mentioned in the Authorization Message Table. The text of the message should be set as follows: "A reply from Licensor to numerous authorization requests was never received. This product must be connected to a communications network in order to function."] 10423[104.2.3 Process Datagram Go to 105.3 (Fig. 6).] 1043[104.3 END IF (Disconnect Allowed Compare).] end subgraph OUTPUT 3[3, LICENSE DATAGRAM] subgraph Box2 [] 23[23, DATA] subgraph Box3 [] 27[27, AUTHORIZATION CODE] 28[28, MESSAGE TEXT] end end end 36 --> 1041 9 --> 1041 1041 --> 3 1042 --> 10421 10421 --> 27 10422 --> 28 10423 --> 1043 1043 --> 3 </pre> <ul style="list-style-type: none"> • “FIG. 5 shows the operation of the “Reply Datagram is Overdue” procedure. <u>Step 104.1 compares time since the last datagram was sent 36 to disconnect allowed interval 19</u>, which, as described above, is the interval that product 1 is allowed to operate even if a reply is overdue. If time since send 36 is smaller than disconnect allowed interval 19, datagram 3 is retransmitted via executing step 103.9 in FIG. 4. <u>Step 104.2 “disconnects” product 1 from further service, if time since send 36 is greater than disconnect allowed interval 19.</u> • Step 104.2 comprises a sequence of sub-steps 104.2.1-104.2.3. <u>Step 104.2.1 assigns number 5 to authorization code 27</u> in the current datagram being processed. <u>Value 5 is interpreted by monitor 2 as a denial.</u> Step 104.2.2 sets message text 28 to the following: <u>‘A reply from licensor to numerous authorization requests was never received. This product must be connected to a communications network in order to function.’</u> Step 104.2.3 transfers system control to step 105.3 in FIG. 6. Step 105.3 processes the current denial datagram 3 as if it were just received.” (8:48-67)

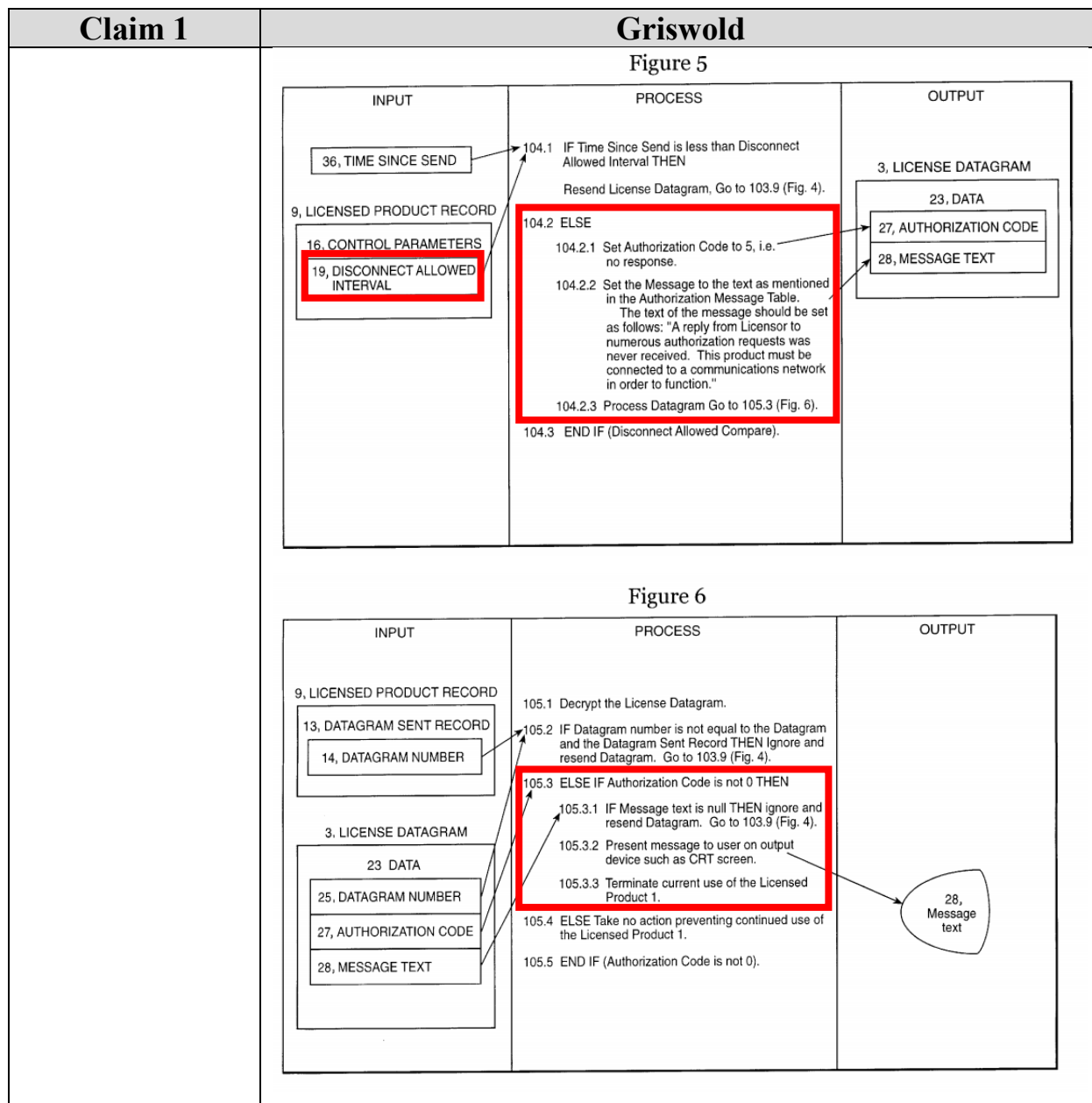
Claim 1	Griswold
	<ul style="list-style-type: none"> “Number of processes running 26 is the number of concurrent uses of product 1 at the time datagram 3 is sent. <u>Authorization code 27 is used on reply datagrams 3 to indicate an approval or a denial.</u> Message text 28 contains a message which will be displayed to the user upon a denial.” (6:57-61)
<p>[1e] the evaluating including at least one action selected from the group consisting of:</p> <p>evaluating whether the at least one of the one or more software modules make calls to certain system interfaces;</p> <p>evaluating whether the at least one of the one or more software modules direct data to certain channels;</p>	<p>Griswold discloses the evaluating including at least one action selected from the group consisting of:...analyzing dynamic timing characteristics of the at least one of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity (e.g., “compares time since the last datagram was sent 36 to disconnect allowed interval 19” and “if time since send 36 is greater than disconnect allowed interval 19” this indicates the invalid activity of operating the product without a “reply from licensor” and/or “connect[ion] to a communications network”).</p> <p>For example, Griswold discloses that the monitor permits use of a licensed product for a period of time without receiving a reply datagram. The monitor repeatedly compares the time since the last datagram was sent to the disconnect allowed interval in the licensed product record to determine whether the elapsed time exceeds the permitted time interval for operating the product without receiving a reply (<i>i.e.</i>, analyzes dynamic timing characteristics for anomalous timing characteristics).⁷ Griswold further teaches that continued processing without a reply, such as when operating without a network connection, is unauthorized (<i>i.e.</i>, indicates invalid activity) and results in setting an “authorization code” to “5” which acts as a denial.</p>

⁷ A POSITA would have understood that when the elapsed time exceeds the permitted time interval that is an “anomalous timing characteristic” because the timing deviates from what is normal and expected.

Claim 1	Griswold
<p>analyzing dynamic timing characteristics of the at least one of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity;</p>	<p style="text-align: center;">Figure 5</p> <pre> graph LR subgraph INPUT 36[36, TIME SINCE SEND] 9[9, LICENSED PRODUCT RECORD] 16[16, CONTROL PARAMETERS] 19[19, DISCONNECT ALLOWED INTERVAL] end subgraph PROCESS 104.1[104.1 IF Time Since Send is less than Disconnect Allowed Interval THEN Resend License Datagram, Go to 103.9 (Fig. 4).] 104.2[104.2 ELSE] 104.2.1[104.2.1 Set Authorization Code to 5, i.e. no response.] 104.2.2[104.2.2 Set the Message to the text as mentioned in the Authorization Message Table. The text of the message should be set as follows: "A reply from Licensor to numerous authorization requests was never received. This product must be connected to a communications network in order to function."] 104.2.3[104.2.3 Process Datagram Go to 105.3 (Fig. 6).] 104.3[104.3 END IF (Disconnect Allowed Compare).] end subgraph OUTPUT 3[3, LICENSE DATAGRAM] 23[23, DATA] 27[27, AUTHORIZATION CODE] 28[28, MESSAGE TEXT] end 36 --> 104.1 19 --> 104.1 104.1 --> 104.2 104.2 --> 104.2.1 104.2.1 --> 104.2.2 104.2.2 --> 104.2.3 104.2.3 --> 104.3 104.3 --> 3 3 --> 23 23 --> 27 23 --> 28 </pre> <ul style="list-style-type: none"> • “FIG. 5 shows the operation of the “Reply Datagram is Overdue” procedure. <u>Step 104.1 compares time since the last datagram was sent 36 to disconnect allowed interval 19</u>, which, as described above, is the interval that product 1 is allowed to operate even if a reply is overdue. If time since send 36 is smaller than disconnect allowed interval 19, datagram 3 is retransmitted via executing step 103.9 in FIG. 4. <u>Step 104.2 “disconnects” product 1 from further service, if time since send 36 is greater than disconnect allowed interval 19.</u> • Step 104.2 comprises a sequence of sub-steps 104.2.1-104.2.3. <u>Step 104.2.1 assigns number 5 to authorization code 27</u> in the current datagram being processed. <u>Value 5 is interpreted by monitor 2 as a denial.</u> Step 104.2.2 sets message text 28 to the following: <u>‘A reply from licensor to numerous authorization requests was never received. This product must be connected to a communications network in order to function.’</u> Step 104.2.3 transfers system control to step 105.3 in FIG. 6. Step 105.3 processes the current denial datagram 3 as if it were just received.” (8:48-67)

Claim 1	Griswold
	<ul style="list-style-type: none"> • “Number of processes running 26 is the number of concurrent uses of product 1 at the time datagram 3 is sent. <u>Authorization code 27 is used on reply datagrams 3 to indicate an approval or a denial.</u> Message text 28 contains a message which will be displayed to the user upon a denial.” (6:57-61) • “Through the execution of steps 104.1-104.3, the present system permits the use of product 1 for a prescribed period of time. <u>After the prescribed period of time has elapsed, the present system generates a denial.</u>” (9:1-4)
<p>[1f] denying the request to use the piece of electronic media content if the evaluation indicates that the at least one of the one or more software modules fail to satisfy a set of predefined criteria.</p>	<p>Griswold discloses denying the request to use the piece of electronic media content (e.g., “generates a denial”) if the evaluation indicates that the at least one of the one or more software modules fail to satisfy a set of predefined criteria (e.g., “if time since send 36 is greater than disconnect allowed interval 19”).</p> <p>For example, as explained in [1d] and [1e], Griswold discloses comparing the time since the last datagram was sent to the disconnect allowed interval in the licensed product record to determine whether the elapsed time exceeds the permitted time interval for operating the product without receiving a reply. The disconnect allowed interval and other restrictions in the licensed product record are a set of conditions or characteristics determined in advance for checking the behavior of the software (<i>i.e.</i>, predefined criteria).⁸ If the time since send exceeds the disconnect allowed interval for the licensed product (<i>i.e.</i>, fail to satisfy the predefined criteria), then the request is denied.</p>

⁸ As discussed in Section VI.A, the term “predefined criteria” means “conditions or characteristics determined in advance against which to check the structure and/or behavior of one or more software modules.”



Claim 1	Griswold
	<p>Figure 1</p> <pre> graph LR subgraph LicenseeSite [At Licensee's Site] LCM[2. License Check Monitor] LP[1. Licensed Product] LP -- Invoke --> LCM LCM -- Denial --> LP end subgraph Network [On Communications Network] LD[3. License Datagram] end subgraph LicensorSite [At Licensor's Site] LCS[4. License Control System] LR[5. License Records] HLD[6. History of License Datagrams] LR -- Retrieve --> LCS LCS -- Store --> HLD end LicenseeSite -- Request --> Network Network -- Reply --> LicenseeSite Network -- Request --> LicensorSite LicensorSite -- Reply --> Network </pre> <ul style="list-style-type: none"> • <u>“Step 104.2 ‘disconnects’ product 1 from further service, if time since send 36 is greater than disconnect allowed interval 19.” (8:48-67)</u> • “Through the execution of steps 104.1-104.3, the present system permits the use of product 1 for a prescribed period of time. <u>After the prescribed period of time has elapsed, the present system generates a denial.</u>” (9:1-4) • The processing of monitor 2 is as described in the presently described embodiment. However, <u>when a denial message is received or generated, monitor 2 must be able to switch “play” to “off”.</u> (12:16-18)

Claim 2	Griswold
[2] A method as in claim 1, further including: using the predefined criteria to evaluate the at least one of the one or more software	<p>Griswold discloses using the predefined criteria (e.g., “disconnect allowed interval” in the “licensed product record”) to evaluate the at least one of the one or more software modules according to a predefined policy (e.g., “permit[] the use of product 1 for a prescribed period of time”), and basing a decision to deny the request on the outcome of this evaluation (e.g., “generates a denial” “if time since send 36 is greater than disconnect allowed interval 19”).</p>

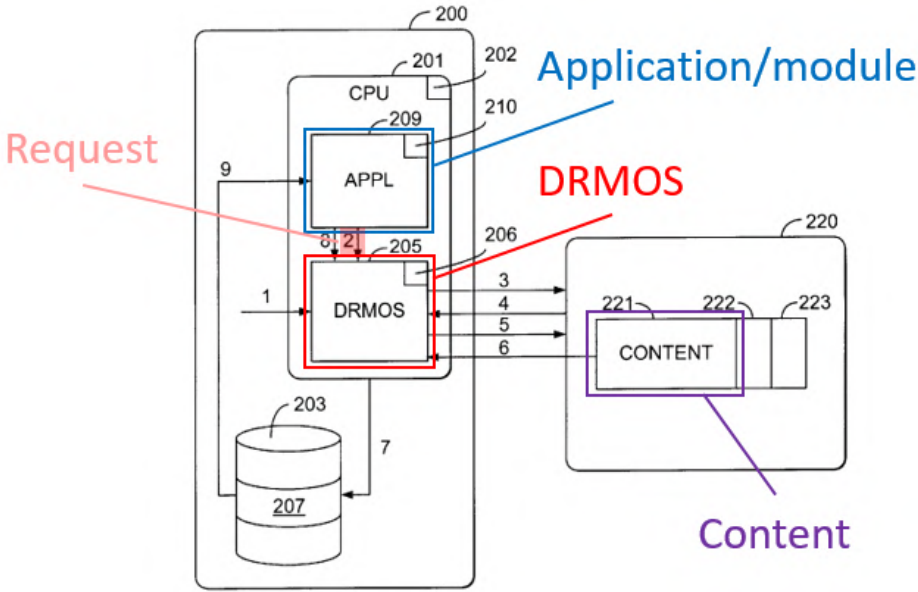
<p>modules according to a predefined policy, and basing a decision to deny the request on the outcome of this evaluation.</p>	<p>For example, as explained in [1d]-[1f], Griswold discloses comparing the time since the last datagram was sent to the disconnect allowed interval in the licensed product record (<i>i.e.</i>, predefined criteria) to implement a rule that permits the use of the licensed product for a prescribed period of time (<i>i.e.</i>, a predefined policy).⁹ If the time since send exceeds the disconnect allowed interval for the licensed product, then the request is denied.</p> <ul style="list-style-type: none"> • “FIG. 5 shows the operation of the ‘Reply Datagram is Overdue’ procedure. Step 104.1 compares time since the last datagram was sent 36 to disconnect allowed interval 19, which, as described above, is the interval that product 1 is allowed to operate even if a reply is overdue. If time since send 36 is smaller than disconnect allowed interval 19, datagram 3 is retransmitted via executing step 103.9 in FIG. 4. <u>Step 104.2 ‘disconnects’ product 1 from further service, if time since send 36 is greater than disconnect allowed interval 19.</u>” (8:48-67) • “Through the execution of steps 104.1-104.3, <u>the present system permits the use of product 1 for a prescribed period of time. After the prescribed period of time has elapsed, the present system generates a denial.</u>” (9:1-4)
---	---

⁹ As discussed in Section VI.B, the term “predefined policy” means “one or more rules determined in advance governing the processing of content.”

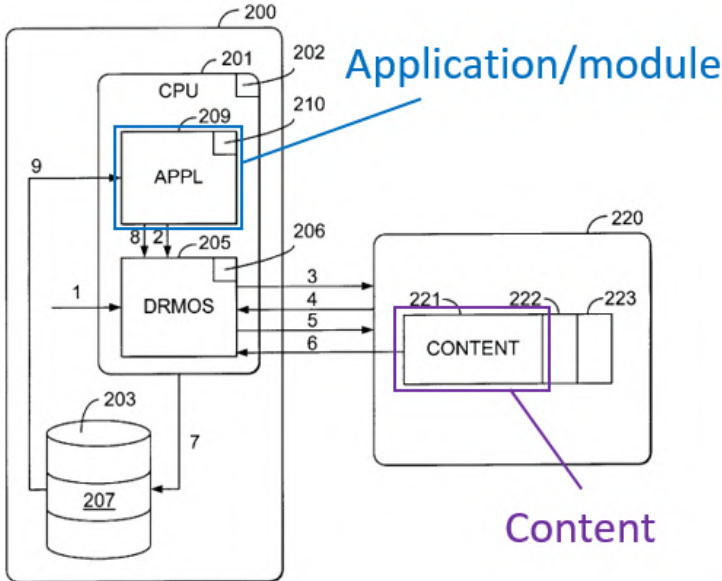
APPENDIX

D

Claim 1	England
<p>[1pre] A method for protecting electronic media content from unauthorized use by a user of a computer system, the method including:</p>	<p>To the extent the preamble is limiting, England discloses a method for protecting electronic media content from unauthorized use by a user of a computer system.</p> <p>For example, England discloses monitoring the use of content by a user on a computer and terminating that use if the user violates certain license limitations (<i>i.e.</i>, if the use is unauthorized).</p> <ul style="list-style-type: none"> • Digital rights for content downloaded to a subscriber computer from a provider are specified in an access predicate. The access predicate is compared with a rights manager certificate associated with an entity, such as an application, that wants access to the content. If the rights manager certificate satisfies the access predicate, the entity is allowed access to the content. <u>A license that specifies limitations on the use of the content</u> can also be associated with the content and provided to the entity. <u>The use the entity makes of the content is monitored and terminated if the entity violates the license limitations</u>. (Abstract; <i>see also</i> 4:1-11)
<p>[1a] receiving a request from a user of the computer system to use a piece of electronic media content;</p>	<p>England discloses receiving a request (<i>e.g.</i>, “request 2”) from a user of the computer system (<i>e.g.</i>, from “application 209” of “subscriber computer 200”) to use a piece of electronic media content (<i>e.g.</i>, “content 221”).</p> <p>For example, England discloses that application 209 on subscriber computer 200 requests the download of content from a content provider.</p> <ul style="list-style-type: none"> • Processes performed by the components of <u>the subscriber computer 200</u> and the content provider 220 are illustrated by arrows in FIG. 2. (8:29-31) • Turning now to the remainder of the processes depicted in FIG. 2, <u>application 209 requests 2 the download of content 221 from provider 220</u>. The DRMOS 205 sends a message 3 to the provider 220 requesting the content 221. The content provider 220 transmits a

Claim 1	England
	<p>challenge message 4 to the DRMOS 205 asking for the identity of the CPU 201, the DRMOS 205, and the application 209. The DRMOS 205 transmits a response message 5 containing a certificate 202 for the CPU 201, its own identity 206, and the rights manager certificate 210 for the application 209. (9:26-36)</p>  <p style="text-align: center;"><i>Fig. 2</i></p> <p>A POSITA would have recognized that the request to use content originates from a user of the computer system (controlling application 209), or at minimum it would have been obvious for the user to initiate the request. For example, England discloses that “[a] user may enter commands and information into the personal computer 20 through input devices such as a keyboard 40 and pointing device 42.” (6:28-30)</p>
[1b] identifying one or more software modules responsible for processing the	<p>England discloses identifying one or more software modules (e.g., “trusted application 209 is identified”) responsible for processing the piece of electronic media content (e.g., “content type handled”) and enabling use of the piece of electronic media content by the user (e.g.,</p>

Claim 1	England
<p>piece of electronic media content and enabling use of the piece of electronic media content by the user;</p>	<p>“allow access to the downloaded content by...trusted applications”).</p> <p>For example, England discloses that the subscriber computer contains “program modules” (<i>i.e.</i>, software modules) including “one or more application programs.”</p> <ul style="list-style-type: none"> • <u><i>A number of program modules</i></u> may be stored on the hard disk, magnetic disk 29, optical disk 31, ROM 24, or RAM 25, <u><i>including</i></u> an operating system 35, <u><i>one or more application programs 36</i></u>, other program modules 37, and program data 38. (6:24-28) <p>England discloses that trusted application 209 is one such application program. As discussed above in Section VIII.B.1, to the extent it is argued that trusted application 209 is not a software module despite England’s express definition, at minimum a POSITA would have recognized that programs such as trusted application 209 are nonetheless formed of “one or more software modules” as claimed.</p> <ul style="list-style-type: none"> • In the exemplary embodiment shown in FIG. 2, <u><i>a trusted application 209</i></u> has agreed to operate in accordance with the limitations placed on content by a provider. (9:1-14) <p>England discloses that trusted application 209 is “identified” by rights manager certificate 210. The rights manager certificate 210 includes a list of content type handled by the trusted application (<i>i.e.</i>, identifying the software responsible for processing the content).</p> <ul style="list-style-type: none"> • <u><i>The trusted application 209 is identified through a “rights manager” certificate 210.</i></u> In one embodiment, the rights manager certificate 210 extends a standard digital certificate...by adding <u><i>a list of services, or properties, provided by the application, i.e., content type handled</i></u>, version of the application, whether it saves content to disk, etc. For purposes of the exemplary embodiment shown in FIG. 2, <u><i>the certificate 210 also identifies the trusted application;</i></u> alternate mechanisms for identifying a trusted

Claim 1	England
	<p>application are described later in the methods section. (9:1-14)</p> <ul style="list-style-type: none"> First, <u>trusted applications must be identified in some fashion</u>, and, second, the DRMOS must prevent non-trusted applications from gaining access to the content when it is stored, either permanently or temporarily, on the subscriber computer. (8:63-67) Therefore, a content provider must not only trust the operating system but must also trust <u>the application that will process the content</u>. (18:20-22)  <p>The diagram, labeled Fig. 2, illustrates a system architecture. A large box labeled 200 contains a CPU (201) and a DRMOS (205). Inside the CPU is an APPL (209). A blue box labeled 210 encompasses the CPU and DRMOS, with a blue arrow pointing to it from the text 'Application/module'. Below the CPU is a database (203) containing data 207. A line labeled 7 connects the database to the DRMOS. A line labeled 1 enters the DRMOS from the left. A line labeled 9 enters the APPL from the left. Inside the APPL, there are lines labeled 8 and 2. A line labeled 202 connects the CPU to the DRMOS. A line labeled 206 connects the DRMOS to a CONTENT box (220). Inside the CONTENT box, there are three sub-components: 221, 222, and 223. Lines labeled 3, 4, 5, and 6 connect the DRMOS to these sub-components. A purple arrow points from the text 'Content' to the CONTENT box.</p> <p style="text-align: center;"><i>Fig. 2</i></p> <p>England discloses that the trusted application is used to access the content. A POSITA would have recognized that accessing content by the trusted application enables use of the content by the user.</p> <ul style="list-style-type: none"> To prevent their content from being stolen or misused, content providers will download content only to known software, and therefore only to subscriber computers that can prove that their operating systems will enforce the limitations the provider places on the content. Such a digital rights management operating system

Claim 1	England
	<p>(DRMOS) must load and execute only OS components that are authenticated as respecting digital rights (“trusted”), and <u>must allow access to the downloaded content by only similarly trusted applications.</u> (8:41-50)</p>
<p>[1c] processing at least a portion of said piece of electronic media content using at least one of the one or more software modules;</p>	<p>England discloses processing at least a portion of said piece of electronic media content (e.g., “use the entity makes of the content”; “accessing the content”) using at least one of the one or more software modules (e.g., “trusted application”).</p> <ul style="list-style-type: none"> • <u>The use the entity makes of the content</u> is monitored and terminated if the entity violates the license limitations. (Abstract; 4:7-13) • <u>A DRMOS must also protect the content once it is loaded into the client computer’s memory by a trusted application.</u> In particular, the DRMOS must prohibit the use of certain types of programs and refrain from performing certain common operating system procedures when content is in memory. (15:45-50) • If the user of the subscriber computer attempts to load a kernel debugger into memory, the DRMOS can either 1) refuse to load the debugger, or <u>2) renounce its trusted identity and terminate the trusted application that was accessing the content</u> before loading the debugger. (15:54-58)
<p>[1d] evaluating whether the at least one of the one or more software modules process the portion of the electronic media content in an authorized manner</p>	<p>England discloses evaluating whether the at least one of the one or more software modules (e.g., “trusted application 209”) process the portion of the electronic media content in an authorized manner (e.g., “[t]he use the entity makes of the content is monitored and terminated if the entity violates the license limitations”).</p> <p>For example, England discloses a digital rights management operating system (DRMOS) that places restrictions on the use or processing of content by the application through the use of license limitations defined by license 223.</p>

Claim 1	England
	<ul style="list-style-type: none"> The content license (FIG. 11) imposes additional restrictions on <u>what kind of processing can be performed on the content once an application has access to the content.</u> (19:22-31) <p>England discloses that the use or processing of the content is monitored for violations of the license limitations (<i>i.e.</i>, processing in an unauthorized manner).</p> <ul style="list-style-type: none"> <u>The use the entity makes of the content is monitored and terminated if the entity violates the license limitations.</u> (Abstract; 4:9-12) An example of one kind of procedure that must be prohibited is loading a kernel debugger because it would allow the user to make a copy of the content loaded in memory. <u>If the user of the subscriber computer attempts to load a kernel debugger into memory, the DRMos can</u> either 1) refuse to load the debugger, or 2) <u>renounce its trusted identity and terminate the trusted application that was accessing the content before loading the debugger.</u> (15:51-64)
<p>[1e] the evaluating including at least one action selected from the group consisting of:</p> <p>evaluating whether the at least one of the one or more software modules make calls to certain system interfaces;</p>	<p>England discloses the evaluating including at least one action selected from the group consisting of:... evaluating whether the at least one of the one or more software modules make calls to certain system interfaces...(e.g., “[i]f the user of the subscriber computer attempts to load a kernel debugger into memory”).</p> <p>For example, England discloses detecting whether the user of the subscriber computer attempts to load a kernel debugger into memory, and terminating the trusted application and renouncing its trusted identity if this procedure is detected.</p> <ul style="list-style-type: none"> An example of one kind of procedure that must be prohibited is loading a kernel debugger because it would allow the user to make a copy of the content loaded in memory. <u>If the user of the subscriber computer attempts to load a kernel debugger into memory, the DRMos can</u> either 1) refuse to load the debugger, or 2) <u>renounce its trusted identity and</u>

Claim 1	England
<p>evaluating whether the at least one of the one or more software modules direct data to certain channels;</p> <p>analyzing dynamic timing characteristics of the at least one of the one or more software modules for anomalous timing characteristics indicative of invalid or malicious activity;</p>	<p><u>terminate the trusted application that was accessing the content before loading the debugger.</u> (15:51-64)</p> <p>A POSITA would have recognized that loading a kernel debugger or portions of a kernel debugger for copying content stored in memory, as taught by England, involves making a call to certain system interfaces, for example the “ptrace” and “/proc” interfaces in UNIX systems. The “ptrace” interface was a well-known debugger interface. (Ex. 1010, 4:4-11; Ex. 1011, 16:23-25.) The “ptrace” interface allowed one process to control another, and to gain access to the memory of the controlled process. (Ex. 1012, 14; Ex. 1013, 5:11-20; Ex. 1017.) The “/proc” interface was another well-known debugger interface. (Ex. 1014, 243; Ex. 1018, 3.) It provided detailed process information and control mechanisms (Ex. 1014, 243), and was used to read data from the memory of a running process (Ex 1018, 3; Ex. 1017.). Thus, in order to determine whether the user attempts to load a kernel debugger for copying content stored in memory, as taught by England, a POSITA would have understood to evaluate whether the trusted application makes calls to certain system interfaces, such as the “ptrace” and “/proc” interfaces in UNIX systems.</p> <p>Alternatively, England discloses the evaluating including at least one action selected from the group consisting of:...evaluating whether the at least one of the one or more software modules direct data to certain channels... (e.g., monitoring and enforcing the trusted application’s “sublicense rights”).</p> <p>For example, England discloses that the license can specify sublicense rights 1107 that specify whether or not the trusted application on the subscriber computer is permitted to validate other computers (downstream computers) and share content with them. Sharing content is “directing data to” sublicensed computers and the data paths to those sublicensed computers are “channels” in accordance with the claim.</p> <ul style="list-style-type: none"> • The license can also specify whether or not <u>a trusted application is permitted to validate other client computers and share the content with them</u>

Claim 1	England
	<p><u>(sublicense rights 1107)</u>, in effect having the subscriber computer act as a secondary content provider. (19:32-55)</p> <p>England further discloses that the use of content by the trusted application on the subscriber computer (the upstream computer) is terminated if it violates the license limitations placed on the content. For example, in the sublicense context, the use of content by the trusted application on the subscriber computer would be terminated if it violates the sublicense rights by sharing content with non-validated computers, which involves determining whether the downstream computers are validated.¹⁰</p> <ul style="list-style-type: none"> • <u>The use the entity makes of the content is monitored and terminated if the entity violates the license limitations.</u> (Abstract; 4:9-12) <p>As explained above in Section VIII.B.1, to the extent it is argued that terminating the “use” in the sublicense context would not terminate use of the content by the upstream subscriber, only the ability to sublicense, it would have been obvious to terminate the underlying use of the content by the upstream subscriber. or example, in other examples, England describes that the DRMOS may renounce the trusted application’s trusted status (15:54-58) where a kernel debugger is loaded, evidencing an intent of the user in making unauthorized copies of the content executing in memory. Thus, it would have been obvious to a POSITA in view of England’s disclosures to terminate the trusted application on the upstream subscriber computer (and renounce the trusted application’s trusted status) if the application is used to share content with non-validated computers in violation of sublicense rights 1107, which involves determining whether the downstream computers are validated. This is because, like the kernel debugger example, there is a heightened</p>

¹⁰ As discussed in Section VI.C, I have been instructed to apply Patent Owner’s construction of “evaluating whether the at least one of the one or more software modules direct data to certain channels” as at least encompassing evaluating a particular output channel device.

Claim 1	England
	<p>interest of content providers to protect against unauthorized copying, and shutting down users exhibiting this type of behavior is critical to ensuring unauthorized content is not propagated over networks.</p>
<p>[1f] denying the request to use the piece of electronic media content if the evaluation indicates that the at least one of the one or more software modules fail to satisfy a set of predefined criteria.</p>	<p>England discloses denying the request to use the piece of electronic media content (e.g., “terminate the trusted application that was accessing the content”) if the evaluation indicates that the at least one of the one or more software modules fail to satisfy a set of predefined criteria (e.g., “[i]f the user of the subscriber computer attempts to load a kernel debugger into memory”).</p> <p>As discussed above with respect to “evaluating whether the at least one of the one or more software modules make calls to certain system interfaces” in [1e], England discloses that detecting whether the user of the subscriber computer attempts to load a kernel debugger into memory, and terminating the trusted application if this procedure is detected.</p> <ul style="list-style-type: none"> • An example of one kind of procedure that must be prohibited is loading a kernel debugger because it would allow the user to make a copy of the content loaded in memory. <u>If the user of the subscriber computer attempts to load a kernel debugger into memory, the DRMOS can</u> either 1) refuse to load the debugger, or 2) <u>renounce its trusted identity and terminate the trusted application that was accessing the content before loading the debugger.</u> (15:51-64) <p>Terminating the trusted application which terminates use of the content is “denying the request” to use the content as recited in Claim 1. The claim requires receiving a request to use the content, identifying a module that enables use of the content, and processing at least a portion of the content before evaluating that processing. “Processing” before “evaluating” that processing was the alleged point of novelty argued during prosecution in order to secure allowance. Thus, “denying” the request cannot mean access gating and must encompass stopping any further processing of the content by the software</p>

Claim 1	England
	<p>module (e.g., terminating the trusted application as taught by England).</p> <p>As further discussed with respect to [1e], in order to determine whether the user attempts to load a kernel debugger into memory, as taught by England, it would have been obvious to a POSITA to evaluate whether the trusted application makes calls to certain system interfaces for loading a kernel debugger. Calls to such known system interfaces for loading a kernel debugger are a set of conditions or characteristics determined in advance for checking the behavior of the trusted application (i.e., predefined criteria).¹¹</p> <p>Alternatively, England discloses denying the request to use the piece of electronic media content (e.g., “[t]he use the entity makes of the content is monitored and terminated”) if the evaluation indicates that the at least one of the one or more software modules fail to satisfy a set of predefined criteria (e.g., “if the entity violates the license limitations” such as “sublicense rights”).</p> <p>As discussed above with respect to “evaluating whether the at least one of the one or more software modules direct data to certain channels” in [1e], England discloses that the use of the content is monitored and terminated if the entity violates the license limitations, and that the license limitations that are monitored include sublicense limitations.</p> <ul style="list-style-type: none"> • <u>The use the entity makes of the content is monitored and terminated if the entity violates the license limitations.</u> (Abstract; 4:9-12) • The license can also specify whether or not <u>a trusted application is permitted to validate other client computers and share the content with them (sublicense rights 1107), in effect having the</u>

¹¹ As discussed in Section VI.A, the term “predefined criteria” means “conditions or characteristics determined in advance against which to check the structure and/or behavior of one or more software modules.”

Claim 1	England
	<p><u>subscriber computer act as a secondary content provider.</u> (19:32-55)</p> <p>As further discussed with respect to [1e], it would have been obvious to a POSITA in view of England's disclosures to terminate the trusted application on the subscriber computer (and renounce the trusted application's trusted status) if the application is used to share content with non-validated computers in violation of sublicense rights 1107, which involves determining whether the downstream computers are validated. The information against which to check whether the downstream computers are validated is a set of conditions or characteristics determined in advance for evaluating the behavior of the trusted application (<i>i.e.</i>, predefined criteria).</p>

Claim 2	England
<p>[2] A method as in claim 1, further including: using the predefined criteria to evaluate the at least one of the one or more software modules according to a predefined policy, and basing a decision to deny the request on the outcome of this evaluation.</p>	<p>England discloses using the predefined criteria (<i>e.g.</i>, criteria as set forth in "license 223") to evaluate the at least one of the one or more software modules according to a predefined policy, and basing a decision to deny the request on the outcome of this evaluation (<i>e.g.</i>, "[i]f the user of the subscriber computer attempts to load a kernel debugger into memory, ...terminate the trusted application that was accessing the content before loading the debugger").</p> <p>As explained above in [1e] and [1f], England renders obvious evaluating whether the trusted application makes calls to certain system interfaces for loading a kernel debugger (<i>i.e.</i>, predefined criteria), and discloses terminating the trusted application if that behavior is detected (<i>i.e.</i>, a predefined policy).¹²</p> <ul style="list-style-type: none"> • An example of one kind of procedure that must be prohibited is loading a kernel debugger because it would allow the user to make a copy of the content loaded in memory. <u>If the user of the subscriber computer attempts to load a kernel debugger into</u>

¹² As discussed in Section VI.B, the term "predefined policy" means "one or more rules determined in advance governing the processing of content."

memory, the DRMOs can either 1) refuse to load the debugger, or 2) **renounce its trusted identity and terminate the trusted application that was accessing the content before loading the debugger.** (15:51-64)

Alternatively, England discloses using the predefined criteria (e.g., criteria as set forth in “license 223”) to evaluate the at least one of the one or more software modules according to a predefined policy, and basing a decision to deny the request on the outcome of this evaluation (e.g., “[t]he use the entity makes of the content is...terminated if the entity violates the license limitations” such as “sublicense rights”).

As explained above in [1e] and [1f], England discloses that the use of the content is monitored and terminated if the entity violates the license limitations, and that the license limitations that are monitored include sublicense limitations.

- **The use the entity makes of the content is monitored and terminated if the entity violates the license limitations.** (Abstract; 4:9-12)
- **The license 223 places restrictions on the use of the content 221 by an approved application...** (9:66-10:10)
- The license can also specify whether or not **a trusted application is permitted to validate other client computers and share the content with them (sublicense rights 1107), in effect having the subscriber computer act as a secondary content provider.** (19:32-55)

As further discussed with respect to [1e] and [1f], it would have been obvious to a POSITA in view of England’s disclosures to evaluate whether the trusted application is used to share content with non-validated computers in violation of sublicense rights 1107 by applying predefined criteria, and to terminate the trusted application on the subscriber computer (and renounce the trusted application’s trusted status) if a violation is found. Thus, the use of the content is monitored and terminated if the entity violates the limitations on

	sublicense rights, <i>i.e.</i> a rule determined in advance and governing the processing of content (a predefined policy).
--	--