DOLBY'S INVALIDITY CONTENTIONS – '815 PATENT
Exhibit C-04: U.S. Patent No. 6,009,176 ("Gennaro")

As demonstrated in the claim chart below, the Asserted Claims of the '815 patent are invalid (a) under one or more sections of 35 U.S.C. § 102 as anticipated by Gennaro and (b) under 35 U.S.C. § 103(a) as obvious over Gennaro standing alone and as set forth herein, and/or combined with the knowledge of a person of ordinary skill in the art, admitted prior art, and/or the additional prior art references identified in the '815 patent section of Dolby's Invalidity Contentions, the contents of which are hereby incorporated by reference into this chart. Although the following charts illustrate where Gennaro discloses the preambles of the asserted claims, Dolby does not imply by these contentions that the preambles are claim limitations.

'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
[42.pre]	A method for managing at least one use of a file of electronic data, the method including:	Gennaro discloses a method for managing at least one use of a file of electronic data. For example, Gennaro discloses: Abstract ("A method of signing digital streams so that a receiver of the stream can authenticate and consume the stream at the same rate which the stream is being sent to the receiver. More specifically, this invention involves computing and verifying a single digital signature on at least a portion of the stream. The properties of this single signature will propagate to the rest of the stream through ancillary information embedded in the rest of the stream.") 2:30-33 ("It is therefore an object of this invention to reduce computation time necessary to sign and authenticate a stream of data by reducing the number of digital signatures required for one to authenticate the data stream.") 2:50-54 ("Finally we assume that the receiver has processing power or hardware that can compute a small number of fast cryptographic c[h]ecksums [sic] faster than the incoming stream rate while still being able to play the stream in real-time.") 2:64-67 ("In the first scenario the stream is finite and is known in its entirety to the signer in advance. This is not a very limiting requirement since it covers most of the internet applications (digital movies, digital sounds, applets).") 3:66-4:1 ("The preferred embodiment for authenticating streams known in advance to the sender has been designed to work for MPEG video streams.")

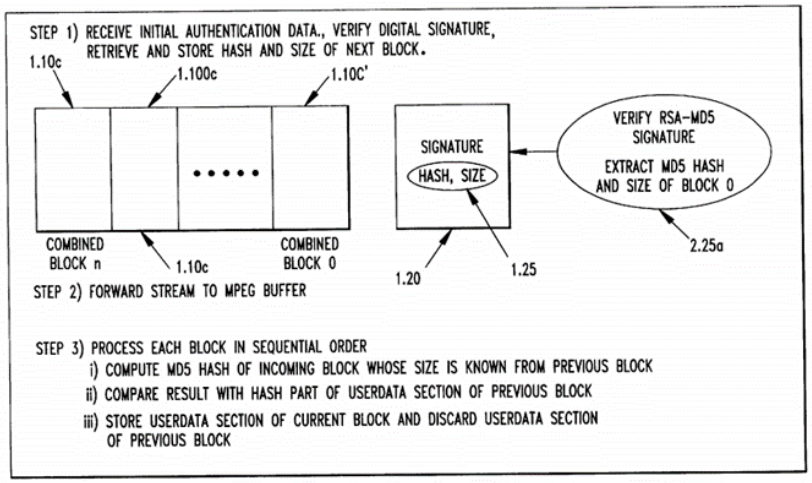
'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		5:54-63 ("The MD5 hash of the recently arrived block is compared against what it should be according to the authentication chain emanating from the Digital Signature from (1.20). If it is different, then tampering has been detected and processing halted. Otherwise, the MPEG software/hardware is informed that a block of bits of a certain size representing a frame has arrived and it can proceed to process the incoming original block that was authenticated.") 5:3-14 ("FIG. 2 graphically illustrates how the combined stream previously created is authenticated. The invention requires additional authentication software to be added to any existing MPEG software (2.200) or hardware both of which currently do not do any authentication. The function of this authentication software is to authenticate blocks from the incoming combined stream before passing them on to the MPEG processing software (2.200) to be converted back to video using the MPEG standard. In what follows, the functioning of the additional authentication software is described.") 5:15-20 ("The authentication software shares with the MPEG processing hardware/software 2.200, a bit buffer which is at least 1.8 M-bits in size. In addition this authentication software now controls how the MPEG processing software/hardware is informed of incoming data.") 12:44-51 ("As described earlier, the main applications of the present invention are for audio, video and data streams as well as applets in an internet/interactive TV environment. We briefly describe the specifics of how these techniques are applicable for MPEG audio/video and java applets. Later we also describe how our construction carries over to a broadcast environment and how in could be useful in non-stream settings.") To the extent Intertrust alleges that Gennaro does not explicitly disclose this claim limitation, this limitation is inherent and/or it would have been obvious in view of the knowledge of one of ordinary skill in the art, and/or in view of the references identified in the '815 patent section of Dolby's Invalidity Contentions.

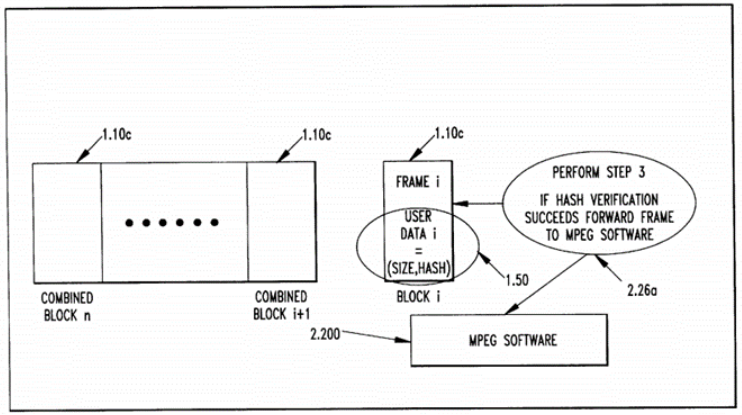
'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
[42.a]	receiving a request to use the file in a predefined manner;	Gennaro discloses receiving a request to use the file in a predefined manner. For example, Gennaro discloses: 1:28-30 ("When the receiver asks for the authenticated stream, the sender first sends the signed table followed by the stream.") 3:64-4:10 ("Preferred Embodiment for Signing Streams Known in Advance The preferred embodiment for authenticating streams known in advance to the sender has been designed to work for MPEG video streams. The following is with reference to FIG. 1. In the MPEG video encoding format, each picture frame allows for a USER-DATA section which can act as a placeholder to hold ancillary information. Moreover MPEG standards define that no frame can be more than 1.8 M-bits in size. The original MPEG video stream (1.100) is generated such that there is a 20-byte USER DATA 1.5 section in each picture frame which will act as a placeholder for ancillary information. All these bytes are initialized to the value of 0.") 2:43-54 ("The present solution makes some reasonable/practical assumptions about the nature of the streams being authenticated. First of all we assume that it is possible for the sender to embed authentication information in the stream. This is usually the case (e.g., USER DATA section in MPEG Video elementary Stream etc.) We also assume that the receiver has a "small" buffer in which it can first authenticate the received bits before consuming them. Finally we assume that the receiver has processing power or hardware that can compute a small number of fast cryptographic ckecksums [sic] faster than the incoming stream rate while still being able to play the stream in real-time.") 3:66-4:1 ("The preferred embodiment for authenticating streams known in advance to the sender has been designed to work for MPEG video streams.") 5:3-14 ("FIG. 2 graphically illustrates how the combined stream previously created is authenticated. The invention requires additional authentication software to be

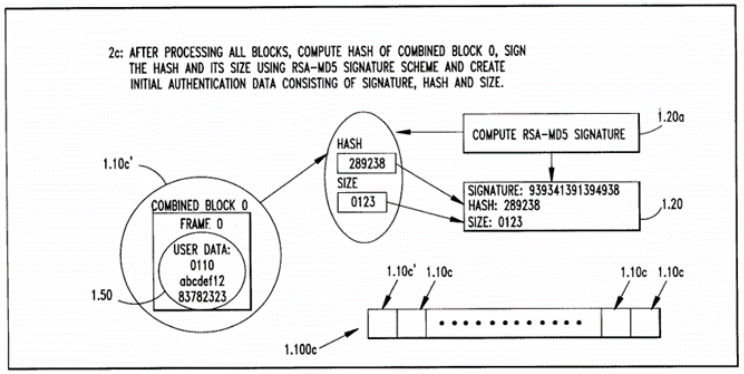
'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		added to any existing MPEG software (2.200) or hardware both of which currently do not do any authentication. The function of this authentication software is to authenticate blocks from the incoming combined stream before passing them on to the MPEG processing software (2.200) to be converted back to video using the MPEG standard. In what follows, the functioning of the additional authentication software is described.") 5:15-20 ("The authentication software shares with the MPEG processing hardware/software 2.200, a bit buffer which is at least 1.8 M-bits in size. In addition this authentication software now controls how the MPEG processing software/hardware is informed of incoming data.") 9:63-67 ("The authentication software shares with the MPEG processing hardware/software, a bit buffer which is at least 1.8 M-bits in size. In addition this authentication Software now controls how the MPEG processing software/hardware is informed of incoming data.") 13:44-46 ("Accommodating classes or data resources which are generated on the fly by the application server based on a client request.") 13:53-67 ("Our schemes (both the off-line and the on-line one) can be easily modified to fit in a broadcast scenario. Assume that the stream is being sent to a broadcast channel with multiple receivers who dynamically join or leave the channel. In this case a receiver who joins when the transmission is already started will not be able to authenticate the stream since she missed the first block that contained the signature. Both schemes however can be modified so that every once in a while apart from the regular chaining information, there will also be a regular digital signature on a block embedded in the stream. Receivers who are already verifying the stream via the chaining mechanism can ignore this signature whereas receivers tuned in at various time will rely on the first such signature they encounter to start their authentication chain.") 12:52-13:20 ("MPEG VIDEO AND AUDIO. In the case of MPEG video and audio, there are several methods for embedding authentication data. Firstly the Video

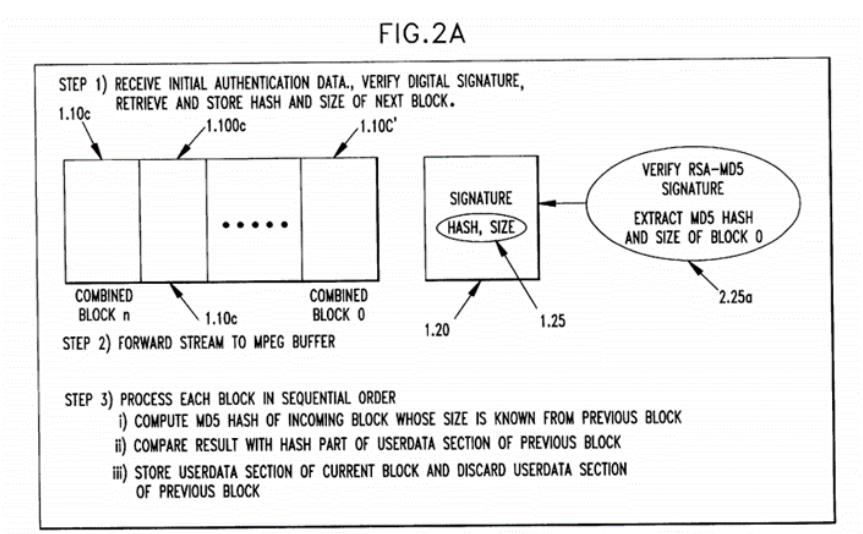
'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		Elementary stream has a USER-DATA section for putting arbitrary user defined information and this section could be embedded in each frame (or field). Secondly, the MPEG system layer allows for an elementary data stream to be multiplexed synchronously with the packetized audio and video streams. One such elementary stream could carry the authentication information. Thirdly, techniques borrowed from digital watermarking can be used to embed information in the audio and video itself at the cost of slight quality degradation. In the case of MPEG video since each frame is fairly large, (hundreds of kilobits) and the receiver is required to have a buffer of at least 1.8 Mbits, both the off-line as well as the on-line solutions can be deployed without compromising picture quality. In the case of audio however, in the extreme case the bit rate could be fairly small (e.g., 32 Kbits/s) and each audio frame can also be small (a few hundred kilobytes) and therefore the receiver's audio buffer could also be very small (3-4 Kbytes). In such extreme cases a direct application of the on-line method, which requires around 1000 bytes of authentication information per block, where a block is limited by the size of the receiver's audio buffer would seriously cut into the audio quality. For these extreme cases, the best on-line strategy would be either to send the authentication information via a separate but multiplexed MPEG data stream. If the receiver has a good sized buffer (say 32 K) then by having a large audio block (say 20 K) our method yields a scheme which has a server-introduced delay of approximately 5-6 seconds and a 5% quality degradation. If the receiver buffer is really tiny (say 2-3 K) a hybrid scheme is required: as an example of a scheme that can be built one could use groups of 33 hash-chained blocks of length 1000 bytes each; this has a 5% degradation and a server initial delay in the 20second range.") 13:20-51 ("JAVA. In the original version of java (JDK 1.0), for a applet coming from the network, first the startup class was loaded and then additional classes were (down) loaded by the class loader in a lazy fashion as and when the running applet first attempted to access them. Since our ideas apply not only to streams which are a linear sequence of blocks but in general to trees as well (where one block can invoke any of its children), based on our model, one way to sign java applets would

'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		be to sign the startup class and each downloaded class would have embedded in it the hashes of the additional classes that it downloads directly. However for code signing, Javasoft has adopted the multiple signature and hash table based approach in JDK1.1, where each applet is composed of one or several Java archives, each of which contains a signed table of hashes (the manifest) of its components. It is our belief that once java applets become really large and complex the shortcomings of this approach will become apparent: ("Large size of the hash table in relation to the classes actually invoked during a run. This table has to fully extracted and authenticated before any class gets authenticated. The computational cost of signing each of the manifests if an applet is composed of several archives. Accommodating classes or data resources which are generated on the fly by the application server based on a client request. These could be addressed by using some of our techniques. Also the problem of how to sign audio/video streams will have to be considered in the future evolution of Java, since putting the hash of a large audio/video file is not an acceptable solution.") 13:52-14:2 ("Broadcast Applications Our schemes (both the off-line and the on-line one) can be easily modified to fit in a broadcast scenario. Assume that the stream is being sent to a broadcast channel with multiple receivers who dynamically join or leave the channel. In this case a receiver who joins when the transmission is already started will not be able to authenticate the stream since she missed the first block that contained the signature. Both schemes however can be modified so that every once in a while apart from the regular chaining information, there will also be a regular digital signature on a block embedded in the stream. Receivers who are already verifying the stream via the chaining mechanism can ignore this signature whereas receivers tuned in at various

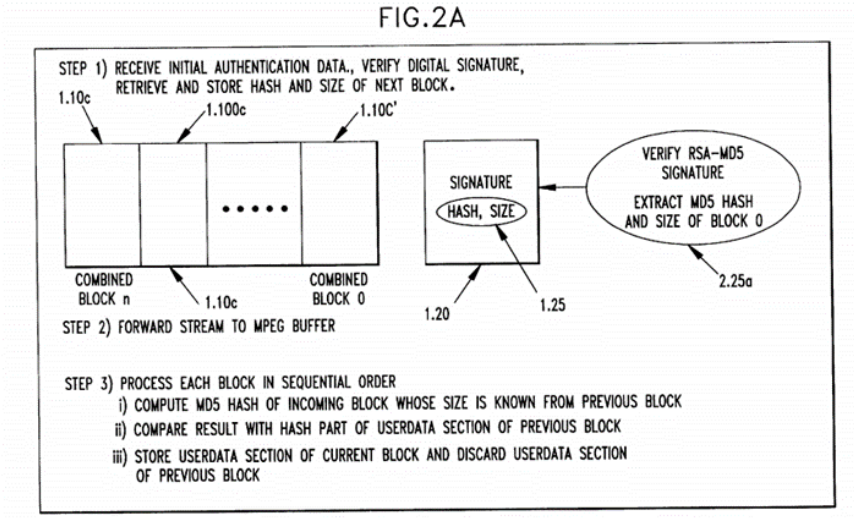
'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		time will rely on the first such signature they encounter to start their authentication chain. A different method to authenticate broadcasted streams, with weaker non-repudiation properties than ours, was proposed in [8].") 14:3-15 ("Long Files When Communication is at Cost Our solution can be used also to authenticate long files in a way to reduce communication cost in case of tampering. Suppose that a receiver is downloading a long file from the Web. There is no "stream requirement" to consume the file as it is downloaded, so the receiver could easily receive the whole file and then check a signature at the end. However if the file has been tampered with, the user will be able to detect this fact only at the end. Since communication is at a cost (time spent online, bandwidth wasted etc) this is not a satisfactory solution. Using our solution the receiver can interrupt the transmission as soon as tampering is detected thus saving precious communication resources.") FIG.2A  Figure 2A (" ")

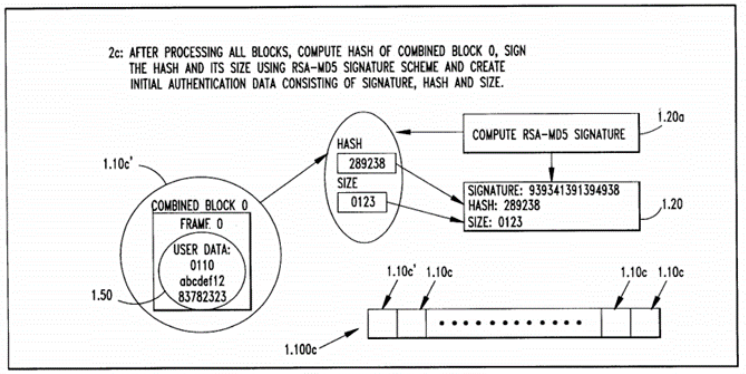
'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		 FIG.2B FIG.2 FIG.2A FIG.2B Figures 2 and 2B (" ") To the extent Intertrust alleges that Gennaro does not explicitly disclose this claim limitation, this limitation is inherent and/or it would have been obvious in view of the knowledge of one of ordinary skill in the art, and/or in view of the references identified in the '815 patent section of Dolby's Invalidity Contentions.
[42.b]	retrieving at least one digital signature and at least one check value associated with the file;	Gennaro discloses retrieving at least one digital signature and at least one check value associated with the file. For example, Gennaro discloses: 4:59-5:2 ("The hash 1.25 and the size of the combined distinguished block, which is the first of the combined blocks, in the stream (1.10c') is calculated, and the said hash value together with the size of said block is signed using a RSA-MD5 signature scheme (1.20a). The signature, the hash and the size are combined to form initial authentication data (1.20). The combined blocks (1.10c) in sequence now constitute the combined stream (1.100c). The initial authentication data (1.20) will be sent to the receiver before the combined stream (1.100c) is sent.")

'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		5:21-34 ("The following constitute the steps that the authentication software follows. Step 1) Before receiving the combined stream (1.100c) the receiver receives the initial authentication data (1.20) consisting of a digital signature on the hash of the first combined block (1.10c) and the size of first combined block, together with the purported values of the hash and size. The authentication software at this stage does the following (2.25a): It verifies the signature. If the provided signature verifies, then the purported hash and size values of the first combined block (1.10c) are authentic, and the hash and size values 1.25 are extracted out for use in authenticating the combined stream (1.100c).")  FIG.1B FIG.1 FIG.1A FIG.1B Figures 1 and 1B (" ")

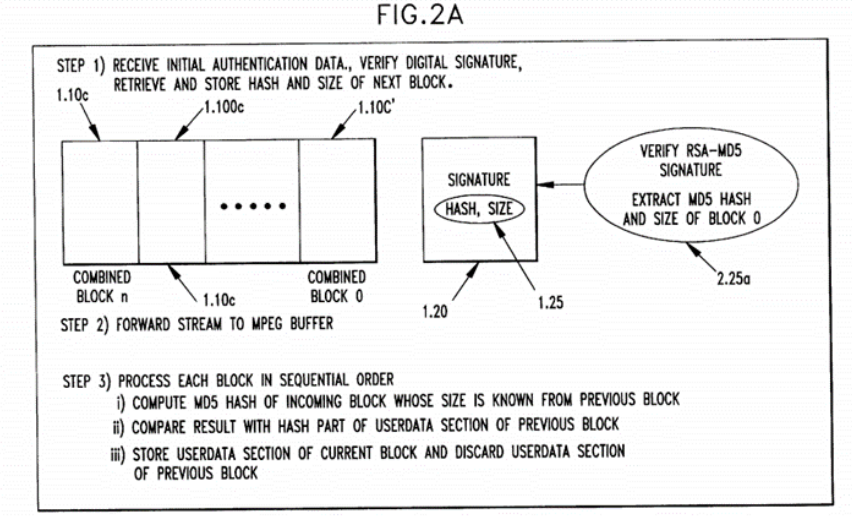
'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		 Figure 2A (" ") To the extent Intertrust alleges that Gennaro does not explicitly disclose this claim limitation, this limitation is inherent and/or it would have been obvious in view of the knowledge of one of ordinary skill in the art, and/or in view of the references identified in the '815 patent section of Dolby's Invalidity Contentions.
[42.c]	verifying the authenticity of the at least one check value using the digital signature;	Gennaro discloses verifying the authenticity of the at least one check value using the digital signature. For example, Gennaro discloses: 3:5-7 ("In this first scenario, verification of the find [sic] stream is performed by verifying the signature of the first block and subsequently verifying hashes of the following blocks.") 5:21-34 ("The following constitute the steps that the authentication software follows.

'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		Step 1) Before receiving the combined stream (1.100c) the receiver receives the initial authentication data (1.20) consisting of a digital signature on the hash of the first combined block (1.10c) and the size of first combined block, together with the purported values of the hash and size. The authentication software at this stage does the following (2.25a): It verifies the signature. If the provided signature verifies, then the purported hash and size values of the first combined block (1.10c) are authentic, and the hash and size values 1.25 are extracted out for use in authenticating the combined stream (1.100c).") 5:40-67 ("Step 3) The incoming combined stream is split into blocks by the authentication software shown in FIG. 2. This splitting is facilitated by the software always knowing in advance the authenticated size of the next incoming combined block long before the incoming block is fully received. The following algorithm or step (2.26a), which is repeated for all the blocks in the stream, is now applied: i) Compute the MD5 hash of the incoming bytes as they are transferred into the buffer of the receiver. As soon as a block comes in, its MD5 hash gets computed, and computation of the MD5 hash of the next incoming block is started (although its length is not immediately known). ii) The MD5 hash of the recently arrived block is compared against what it should be according to the authentication chain emanating from the Digital Signature from (1.20). If it is different, then tampering has been detected and processing halted. Otherwise, the MPEG software/hardware is informed that a block of bits of a certain size representing a frame has arrived and it can proceed to process the incoming original block that was authenticated. iii) Concurrently with the above, the now authenticated size and hash of the next block stored in the ancillary part of the processed block (1.50) is extracted for use to authenticate the next block.") 16:1-9 ("8. A method of authenticating a combined stream of data, comprising:

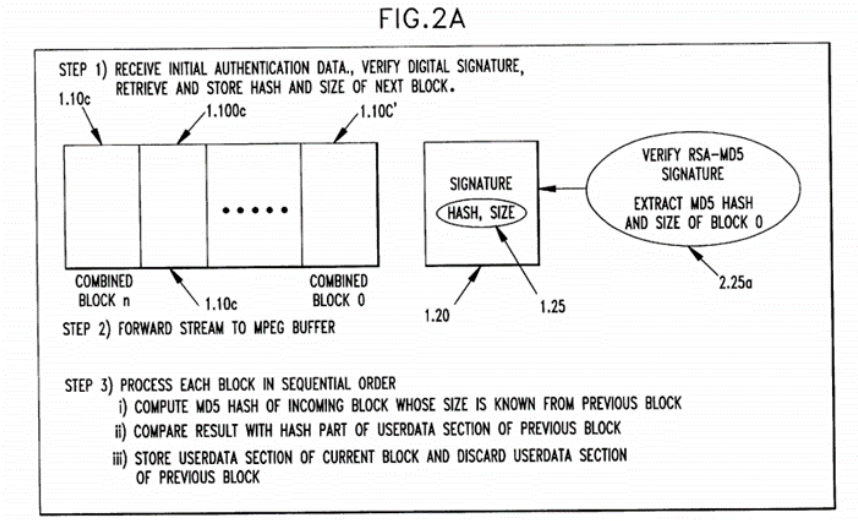
'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		decomposing said stream into a plurality of combined blocks, each of said combined blocks comprising consumable information and ancillary information; establishing non-repudiably the sender of said stream by verifying a digital signature on one of said combined blocks, and authenticating some of said combined blocks by using ancillary information extracted from said authenticated combined blocks.") FIG.2A  Figure 2A (" ")

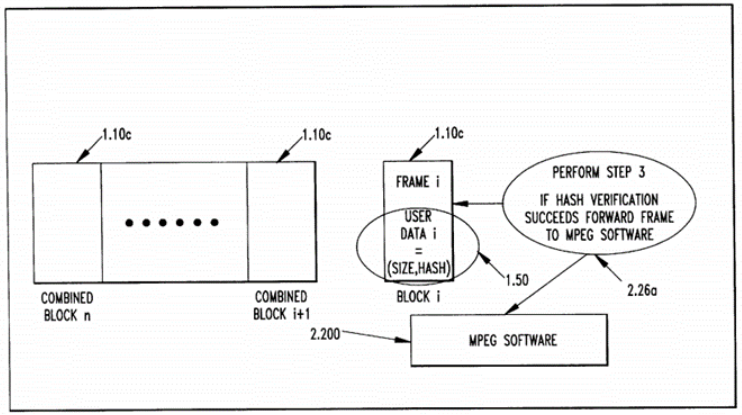
'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		 FIG.1B FIG.1 FIG.1A FIG.1B Figures 1 and 1B (" ") To the extent Intertrust alleges that Gennaro does not explicitly disclose this claim limitation, this limitation is inherent and/or it would have been obvious in view of the knowledge of one of ordinary skill in the art, and/or in view of the references identified in the '815 patent section of Dolby's Invalidity Contentions.
[42.d]	verifying the authenticity of at least a portion of the file using the at least one check value; and	Gennaro discloses verifying the authenticity of at least a portion of the file using the at least one check value. For example, Gennaro discloses: 5:8-12 ("The function of this authentication software is to authenticate blocks from the incoming combined stream before passing them on to the MPEG processing software (2.200) to be converted back to video using the MPEG standard.") 2:67-3:4 ("In this case we will show that a single hash computation will suffice to authenticate the internal blocks. The idea is to embed in the current block the hash of the following block (which in turns includes the hash of the following one and so on . . .).")

'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		4:44-48 ("The next sixteen bytes of the 20 byte ancillary information placeholder is updated to hold the MD5 cryptographic hash of the successor block. This information can be used to authenticate the the [sic] successor block which already has its ancillary information in place.") 5:29-34 ("The authentication software at this stage does the following (2.25a): It verifies the signature. If the provided signature verifies, then the purported hash and size values of the first combined block (1.10c') are authentic, and the hash and size values 1.25 are extracted out for use in authenticating the combined stream (1.100c).") 5:40-67 ("Step 3) The incoming combined stream is split into blocks by the authentication software shown in FIG. 2. This splitting is facilitated by the software always knowing in advance the authenticated size of the next incoming combined block long before the incoming block is fully received. The following algorithm or step (2.26a), which is repeated for all the blocks in the stream, is now applied: i) Compute the MD5 hash of the incoming bytes as they are transferred into the buffer of the receiver. As soon as a block comes in, its MD5 hash gets computed, and computation of the MD5 hash of the next incoming block is started (although its length is not immediately known). ii) The MD5 hash of the recently arrived block is compared against what it should be according to the authentication chain emanating from the Digital Signature from (1.20). If it is different, then tampering has been detected and processing halted. Otherwise, the MPEG software/hardware is informed that a block of bits of a certain size representing a frame has arrived and it can proceed to process the incoming original block that was authenticated. iii) Concurrently with the above, the now authenticated size and hash of the next block stored in the ancillary part of the processed block (1.50) is extracted for use to authenticate the next block.") 16:1-9 ("8. A method of authenticating a combined stream of data, comprising:

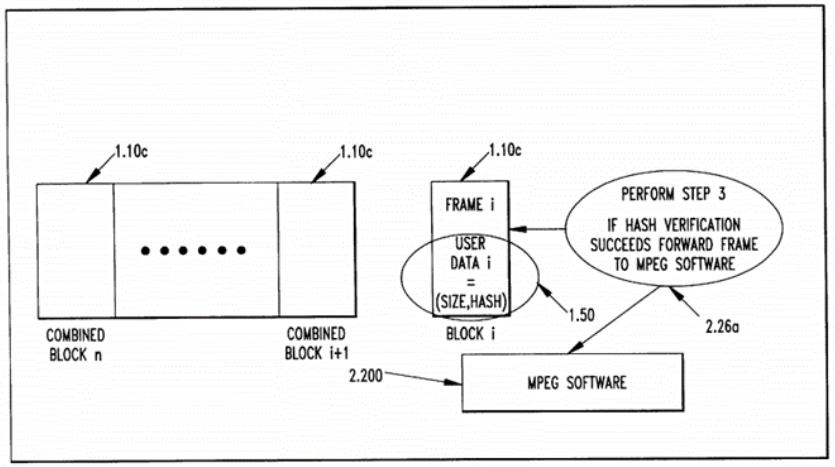
'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		decomposing said stream into a plurality of combined blocks, each of said combined blocks comprising consumable information and ancillary information; establishing non-repudiably the sender of said stream by verifying a digital signature on one of said combined blocks, and authenticating some of said combined blocks by using ancillary information extracted from said authenticated combined blocks.") 16:13-16 ("9. A method as recited in claim 8, wherein said ancillary information is a hash of some of said combined blocks and said combined blocks are authenticated by verifying the value of said hash.") FIG.2A  Figure 2A (" ") To the extent Intertrust alleges that Gennaro does not explicitly disclose this claim limitation, this limitation is inherent and/or it would have been obvious in view of the knowledge of one of ordinary skill in the art, and/or in view of the references identified in the '815 patent section of Dolby's Invalidity Contentions.

'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
[42.e]	granting the request to use the file in the predefined manner.	Gennaro discloses granting the request to use the file in the predefined manner. For example, Gennaro discloses: 2:39-42 ("As a consequence, the receiver can consume authenticated data from the stream at the same rate he receives such data from the stream.") 2:43-54 ("The present solution makes some reasonable/practical assumptions about the nature of the streams being authenticated. First of all we assume that it is possible for the sender to embed authentication information in the stream. This is usually the case (e.g., USER DATA section in MPEG Video elementary Stream etc.) We also assume that the receiver has a "small" buffer in which it can first authenticate the received bits before consuming them. Finally we assume that the receiver has processing power or hardware that can compute a small number of fast cryptographic ckecksums [sic] faster than the incoming stream rate while still being able to play the stream in real-time.") 5:8-12 ("The function of this authentication software is to authenticate blocks from the incoming combined stream before passing them on to the MPEG processing software (2.200) to be converted back to video using the MPEG standard.") 5:35-39 ("Step 2) The receiver then receives the combined stream which is forwarded into the MPEG bit-buffer. However the MPEG software is not informed of incoming data before it is authenticated. This prevents the MPEG software to consuming unauthenticated data.") 5:54-63 ("The MD5 hash of the recently arrived block is compared against what it should be according to the authentication chain emanating from the Digital Signature from (1.20). If it is different, then tampering has been detected and processing halted. Otherwise, the MPEG software/hardware is informed that a block of bits of a certain size representing a frame has arrived and it can proceed to process the incoming original block that was authenticated.") 12:44-51 ("As described earlier, the main applications of the present invention are for audio, video and data streams as well as applets in an internet/interactive TV

'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		environment. We briefly describe the specifics of how these techniques are applicable for MPEG audio/video and java applets. Later we also describe how our construction carries over to a broadcast environment and how in could be useful in non-stream settings.")  Figure 2A (" ")

'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		 FIG.2B FIG.2 FIG.2A FIG.2B Figures 2 and 2B (" ") To the extent Intertrust alleges that Gennaro does not explicitly disclose this claim limitation, this limitation is inherent and/or it would have been obvious in view of the knowledge of one of ordinary skill in the art, and/or in view of the references identified in the '815 patent section of Dolby's Invalidity Contentions.
[43]	A method as in claim 42, in which the at least one check value comprises one or more hash values, and in which verifying the authenticity of at least a portion of the file using the at least one check value includes: hashing at least a portion of the file to obtain a first hash value; and comparing the first hash value to at least	Gennaro discloses the at least one check value comprises one or more hash values, and in which verifying the authenticity of at least a portion of the file using the at least one check value includes: hashing at least a portion of the file to obtain a first hash value; and comparing the first hash value to at least one of the one or more hash values. For example, Gennaro discloses: *See* [42.d]; *see also* 5:40-67 ("Step 3) The incoming combined stream is split into blocks by the authentication software shown in FIG. 2. This splitting is facilitated by the software always knowing in advance the authenticated size of the next incoming combined

'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
	one of the one or more hash values.	block long before the incoming block is fully received. The following algorithm or step (2.26a), which is repeated for all the blocks in the stream, is now applied: i) Compute the MD5 hash of the incoming bytes as they are transferred into the buffer of the receiver. As soon as a block comes in, its MD5 hash gets computed, and computation of the MD5 hash of the next incoming block is started (although its length is not immediately known). ii) The MD5 hash of the recently arrived block is compared against what it should be according to the authentication chain emanating from the Digital Signature from (1.20). If it is different, then tampering has been detected and processing halted. Otherwise, the MPEG software/hardware is informed that a block of bits of a certain size representing a frame has arrived and it can proceed to process the incoming original block that was authenticated. iii) Concurrently with the above, the now authenticated size and hash of the next block stored in the ancillary part of the processed block (1.50) is extracted for use to authenticate the next block.")

'815 Claim	Claim Element	U.S. Patent No. 6,009,176 ("Gennaro")
		 Figure 2 (" ") To the extent Intertrust alleges that Gennaro does not explicitly disclose this claim limitation, this limitation is inherent and/or it would have been obvious in view of the knowledge of one of ordinary skill in the art, and/or in view of the references identified in the '815 patent section of Dolby's Invalidity Contentions.