DOLBY'S INVALIDITY CONTENTIONS – '815 PATENT
Exhibit C-03: International Patent No. WO1999040702 ("Hanna")

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 Hanna and (b) under 35 U.S.C. § 103(a) as obvious over Hanna 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 Hanna discloses the preambles of the asserted claims, Dolby does not imply by these contentions that the preambles are claim limitations.

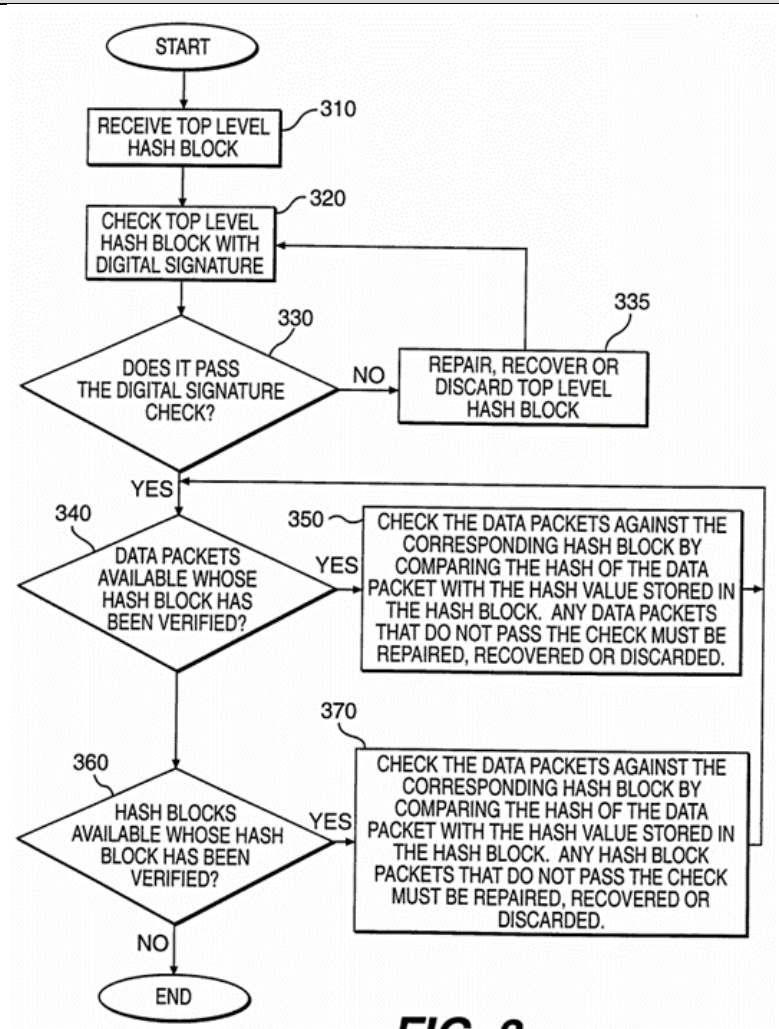
'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
[42.pre]	A method for managing at least one use of a file of electronic data, the method including:	Hanna discloses a method for managing at least one use of a file of electronic data. For example, Hanna discloses: 1:6-8 ("This invention generally relates to data corruption detection and, more particularly, to a method and apparatus for efficient authentication and integrity checking in data processing using hierarchical hashing.") 3:14-22 ("In accordance with the present invention, as embodied and broadly described herein, a computer-implemented data processing method comprises the steps of dividing a data set into packets, hashing the data within each of the packets to produce a hash block including hash values and applying a signature to the hash block. In accordance with another aspect of the present invention, as embodied and broadly described herein, a computer-implemented data processing method comprises the steps of receiving a packet including data, a hash block and a digital signature, verifying the digital signature, hashing the data to produce hash values and comparing the hash values to values in the hash block.") 1:8-3:4 ("B. Description of the Related Art Certain types of business activities create the need to transfer information in a secure manner. For instance, banks periodically "backup" their computer files to a remote central database and need to know that these files were successfully copied to the remote database without having been changed or corrupted during the

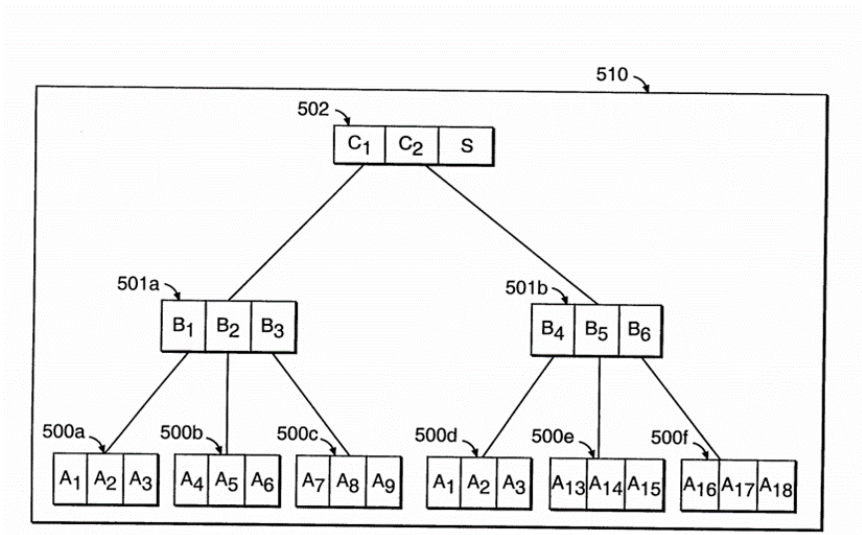
'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		process. Video conferencing is another example of an application that demands the secure transmission of information (video/voice/data). Open networks such as the Internet provide simple and effective means for digital communication. However, such communication can be unintentionally corrupted by network transmission errors or altered by malicious acts. Several conventional techniques guard against these communication problems. These techniques require applying checksums or digital signatures to data before transmission and verifying the checksum or digital signature upon receipt. Checksums, values derived from the data, are typically easy to compute. After computing the checksum, a transmitting machine sends the checksum with the data itself. A receiving machine then recalculates the checksum from the received data and compares the calculated checksum with the received checksum. However, a hacker with the ability to modify data likely also has the ability to replace the original checksum with a recalculated checksum that corresponds to the modified data. Digital signatures protect against malicious acts intended to corrupt data but are more expensive than checksums to compute. The protection provided by digital signatures becomes increasingly important in networked environments where data must pass through unguarded points. Digital signatures are often used in a bulk signature format in which a digital signature is applied to a complete data set. However, the bulk signature format has several drawbacks. The process of confirming the digital signature operates on the whole data set. Bulk signature algorithms cannot identify the portion of the data that was corrupted. This leads to increased cost since the data, if corrupted, must all be sent again. If the data is communicated in discrete packets signed with a bulk signature, detecting corruption or invalid packets inserted by a hacker also carries a high cost. It requires waiting for the receipt of at least one copy of each sequence number of packets. At this point, the signature can be checked. The integrity of the bulk

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		signature cannot be checked until all of the packets are received. This aspect creates a time delay relative to the size of the data set. If several packets with the same sequence number and different contents are received, one is a forgery. Then, to detect which one is the valid copy of any given sequence number if a forgery is inserted, each copy of that sequence number would have to be compared with all the valid packets of the sequence. A method called packet-level signature addresses this problem. The packet-level signature method assigns a digital signature to each individual packet. Although allowing the verification to begin as the individual packets are received making it easy to identify individual corrupted packets, this method requires additional computation and repeated checking of the digital signatures, which is quite time-consuming. A conventional hierarchical hashing technique for neighboring databases on a local area network (LAN) allows a database management system to check if the databases are identical by hashing pieces of the database. The hashes are then hashed, and the final value is broadcast periodically to confirm that all neighbors on the LAN have identical databases. If they do not, the next hash level is compared until the area of the database that differs is located, at which time it can be updated accordingly. However, this system does not deal with the application of a single digital signature to protect an arbitrary amount of data against both malicious errors and unintentional errors. Currently, there is no system that allows a single digital signature to apply to an arbitrary amount of data and allows the data to be verified as it is received. There is, therefore, a need for a system that protects against unintentional data corruption and malicious acts that cause errors in data processing and allows data to be checked as it is received. Additionally, the need exists for a system that provides information regarding which section of data was corrupted while keeping a low computational overhead.")

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		14:24-28 ("10. A computer implemented data processing method comprising the steps of: receiving a packet including data, a hash block and a digital signature; verifying the digital signature; hashing the data to produce hash values; and comparing the hash values to values in the hash block.") 15:1-6 ("11. A computer implemented data processing method comprising the steps of: signing, with a digital signature, a hash block corresponding to a data set; sending the data and the hash block from a source to a destination; upon receipt at the destination, checking the digital signature on the hash block; applying the hash function to the received data set; and comparing the hashes of the received data with the hash values stored in the hash block.") *See also* 1:10-13, Abstract, 3:6-17, 4:15, 8:9-11, Figs. 2-5. To the extent Intertrust alleges that Hanna 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.a]	receiving a request to use the file in a predefined manner;	Hanna discloses receiving a request to use the file in a predefined manner. For example, Hanna discloses: 5:23-28 ("The invention is related to the use of computer system 100 for signing data and verifying data. According to one embodiment of the invention, signed or verified data is provided by computer system 100 in response to processor 104

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		executing one or more sequences of one or more instructions contained in main memory 106. Such instructions may be read into main memory 106 from another computer-readable medium, such as storage device 110. Execution of the sequences of instructions contained in main memory 106 causes processor 104 to perform the process steps described herein.") 4:19-21 ("The top level hash block, the smallest one, is signed with a digital signature. The hash blocks and data are then transmitted to an intended destination such as a network node.") 11:12-13 ("Data verification begins with checking the digital signature on the top level hash block 502. If the top level hash block 502 passes this check, the next level hash block 501 is verified.")

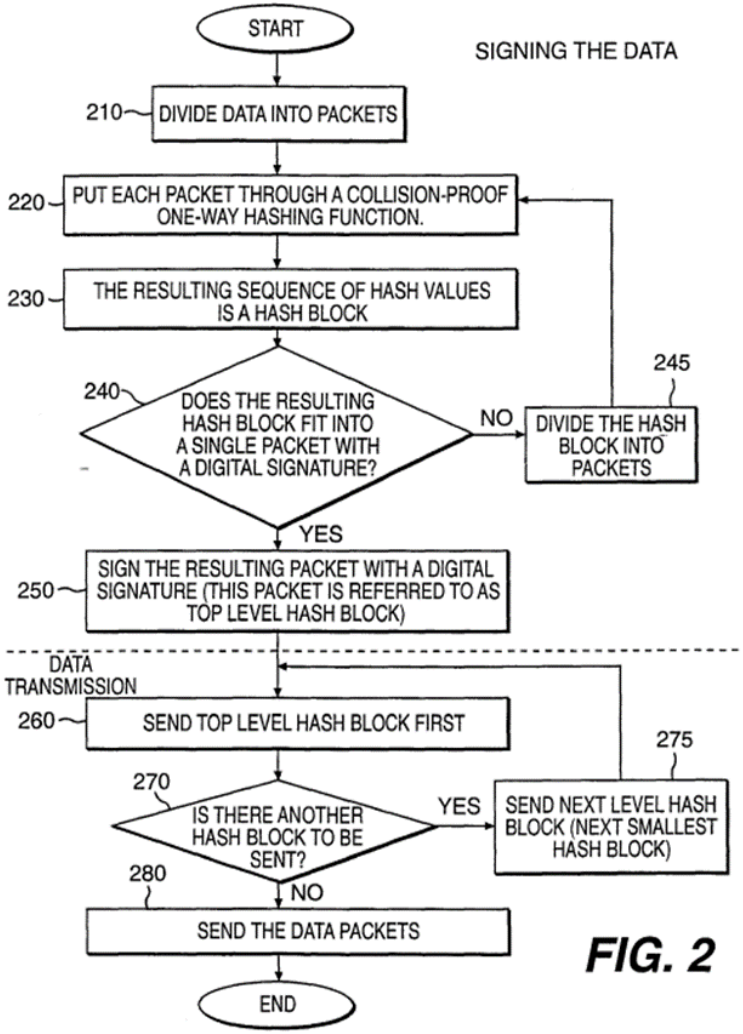
'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		 Figure 3 (" ")

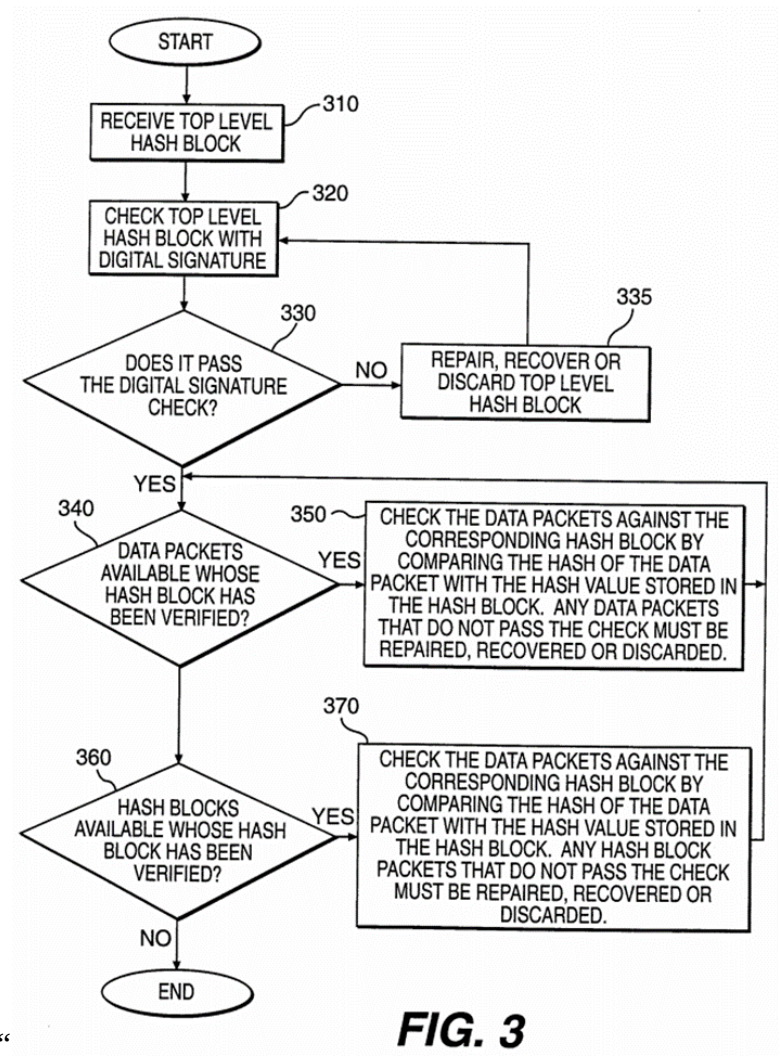
'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		 FIG. 5 Figure 5 (" ") 14:24-28 ("10. A computer implemented data processing method comprising the steps of: receiving a packet including data, a hash block and a digital signature; verifying the digital signature; hashing the data to produce hash values; and comparing the hash values to values in the hash block.") 15:1-6 ("11. A computer implemented data processing method comprising the steps of: signing, with a digital signature, a hash block corresponding to a data set;

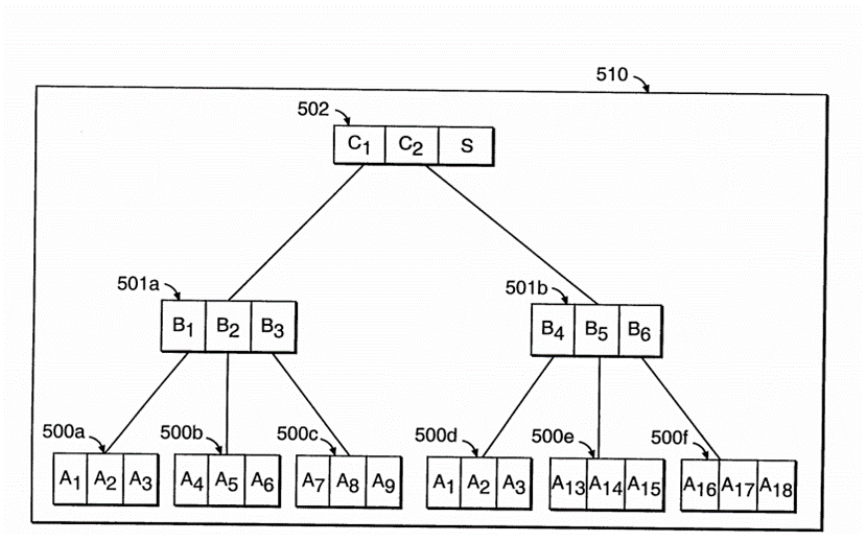
'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		sending the data and the hash block from a source to a destination; upon receipt at the destination, checking the digital signature on the hash block; applying the hash function to the received data set; and comparing the hashes of the received data with the hash values stored in the hash block.") *See also* 5:2-5, 5:22-28, 6:26-7:7:23. To the extent Intertrust alleges that Hanna 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;	Hanna discloses retrieving at least one digital signature and at least one check value associated with the file. For example, Hanna discloses: 3:19-22 ("In accordance with another aspect of the present invention, as embodied and broadly described herein, a computer-implemented data processing method comprises the steps of receiving a packet including data, a hash block and a digital signature, verifying the digital signature, hashing the data to produce hash values and comparing the hash values to values in the hash block.") 4:22-25 ("Systems consistent with the present invention generally verify the data set by checking the digital signature on the top level hash block. Once the top level hash block is verified, the next lower level hash block can be verified by comparing the hash of the packets of that hash block against the hashes stored in the top level block.") 11:12-13 ("Data verification begins with checking the digital signature on the top level hash block 502. If the top level hash block 502 passes this check, the next level hash block 501 is verified.")

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		9:22-28 ("Fig. 3 is a flowchart of the steps used in the data receiving and verification procedure for systems consistent with the present invention. To verify data, the digital signature on the top level packet must be verified first (step 320). If the signature fails this verification step or it is determined that the packet was corrupted during transmission, the top level packet must be repaired or recovered before checking the other packets (steps 330, 335). If lower level hash blocks were signed for extraordinary redundancy, their signatures may be checked in this case to allow verification to proceed.") 8:14-17 ("Once the data is broken into packets, a collision-proof, one-way hash function is applied to each packet (step 220). Each application of the hash function will produce a single hash value. The application of the hash function to each of the data packets will produce a sequence of hash values. This sequence is called a hash block (step 230).") 9:1-4 ("If, however, the hash block originally created by the hashing of the data packets (step 230) is small enough to fit in a single packet with the digital signature, there is no need to go through the steps of breaking down the hash block and creating another higher level hash block and the top level hash block remains the only hash block.") 9:5-8 ("Systems consistent with the present invention apply a digital signature to the top level hash block packet (step 250). No signature need be applied to any of the other hash blocks or data packets. The single digital signature applied to the top level packet is sufficient to verify all of the data.") 9:18-20 ("In accordance with the data signing procedure, the top level hash block packet with the single digital signature, the hierarchy of lower level hash blocks, and the data are sent to a receiver.") 14:24-28 ("10. A computer implemented data processing method comprising the steps of: receiving a packet including data, a hash block and a digital signature;

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		verifying the digital signature; hashing the data to produce hash values; and comparing the hash values to values in the hash block.") 15:1-6 ("11. A computer implemented data processing method comprising the steps of: signing, with a digital signature, a hash block corresponding to a data set; sending the data and the hash block from a source to a destination; upon receipt at the destination, checking the digital signature on the hash block; applying the hash function to the received data set; and comparing the hashes of the received data with the hash values stored in the hash block.")

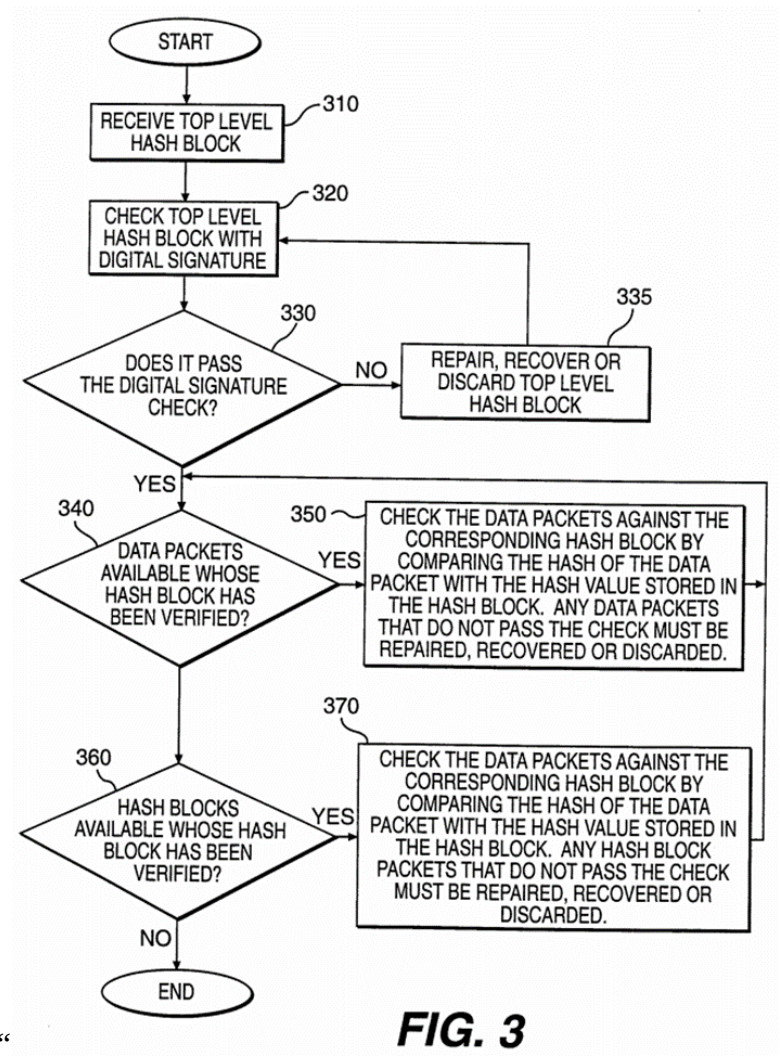
'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		 Figure 2 (" ")

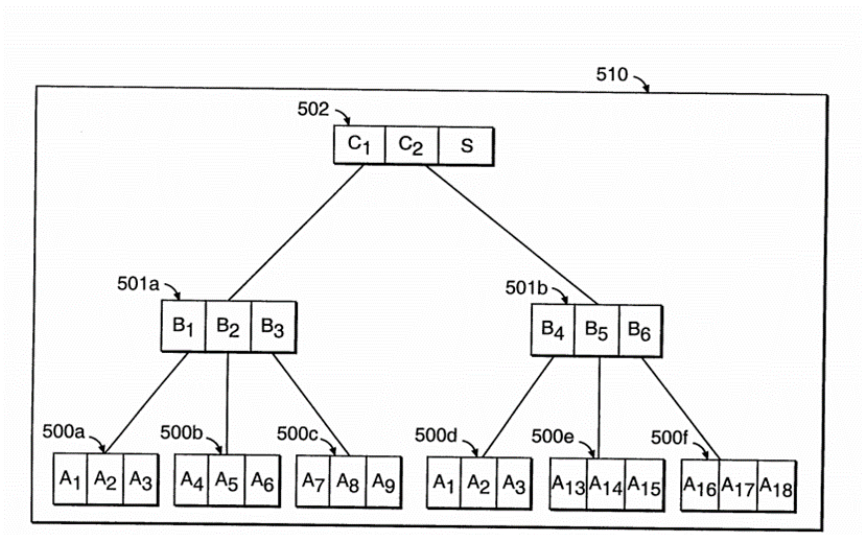
'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		 Figure 3 (" ")

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		 FIG. 5 Figure 5 (" ") To the extent Intertrust alleges that Hanna 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;	Hanna discloses verifying the authenticity of the at least one check value using the digital signature. For example, Hanna discloses: 4:22-28 ("Systems consistent with the present invention generally verify the data set by checking the digital signature on the top level hash block. Once the top level hash block is verified, the next lower level hash block can be verified by comparing the hash of the packets of that hash block against the hashes stored in the top level block. All lower level hash blocks are checked against the next higher level hash

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		blocks in the same manner. Finally, the data is checked against the hash block containing the hashes of the data set. Any given data packet can be checked once all hash blocks above it are received.") 9:22-28 ("Fig. 3 is a flowchart of the steps used in the data receiving and verification procedure for systems consistent with the present invention. To verify data, the digital signature on the top level packet must be verified first (step 320). If the signature fails this verification step or it is determined that the packet was corrupted during transmission, the top level packet must be repaired or recovered before checking the other packets (steps 330, 335). If lower level hash blocks were signed for extraordinary redundancy, their signatures may be checked in this case to allow verification to proceed.") 11:12-19 ("Data verification begins with checking the digital signature on the top level hash block 502. If the top level hash block 502 passes this check, the next level hash block 501 is verified. A hash function (not shown) is applied to each packet and compared with the corresponding hash value in the hash block in the level above it. For example, the packets 501a and b of the hash block 501, B1 through B6, are checked with the values stored in the other hash block 502, C1 and C2. In the sample in Fig. 5, the hash of the packet B1, B2, B3 would be compared with the value C1. If the check fails, the packet B1, B2, B3 is corrupt and must be repaired or replaced before any packets that depend on it can be verified, in this case, data values A1 through A9, 500a-c.") 14:24-28 ("10. A computer implemented data processing method comprising the steps of: receiving a packet including data, a hash block and a digital signature; verifying the digital signature; hashing the data to produce hash values; and comparing the hash values to values in the hash block.")

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		15:1-6 ("11. A computer implemented data processing method comprising the steps of: signing, with a digital signature, a hash block corresponding to a data set; sending the data and the hash block from a source to a destination; upon receipt at the destination, checking the digital signature on the hash block; applying the hash function to the received data set; and comparing the hashes of the received data with the hash values stored in the hash block.")

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		 Figure 3 (" ")

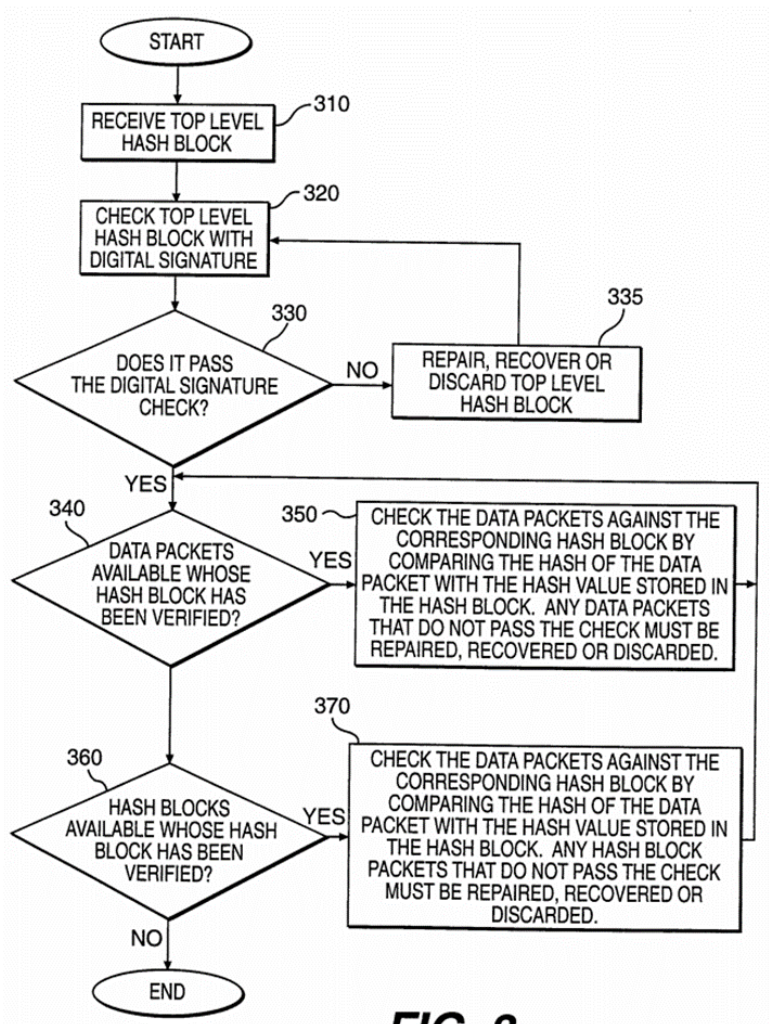
'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		 FIG. 5 Figure 5 (" ") To the extent Intertrust alleges that Hanna does not explicitly disclose this claim limitation, this limitation is inherent and/or it would have been obvious in view of the knowledge of one of ordinary skill 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	Hanna discloses verifying the authenticity of at least a portion of the file using the at least one check value. For example, Hanna discloses: 4:22-28 ("Systems consistent with the present invention generally verify the data set by checking the digital signature on the top level hash block. Once the top level hash block is verified, the next lower level hash block can be verified by comparing the hash of the packets of that hash block against the hashes stored in the top level block. All lower level hash blocks are checked against the next higher level hash

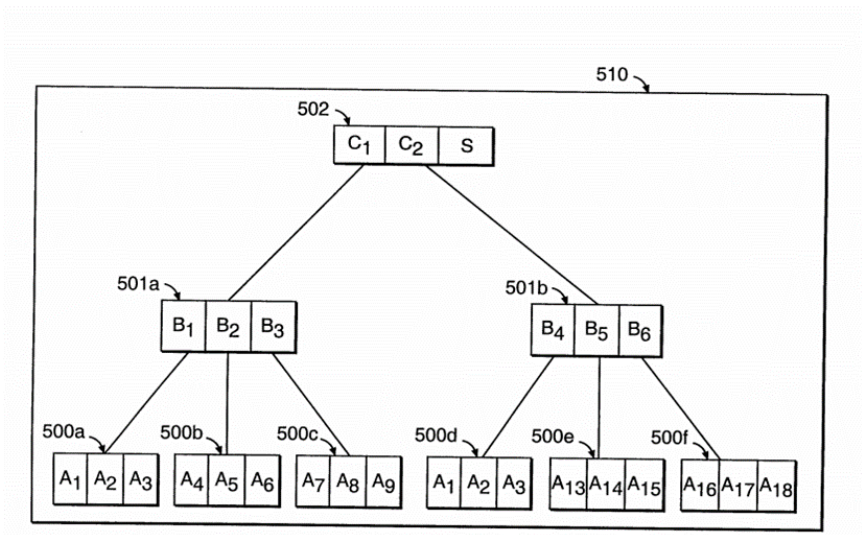
'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		blocks in the same manner. Finally, the data is checked against the hash block containing the hashes of the data set. Any given data packet can be checked once all hash blocks above it are received.") 3:10-11 ("The hierarchical structure used in the method cryptographically protects individual portions of the data and makes it easier to recognize corruption.") 3:19-22 ("In accordance with another aspect of the present invention, as embodied and broadly described herein, a computer-implemented data processing method comprises the steps of receiving a packet including data, a hash block and a digital signature, verifying the digital signature, hashing the data to produce hash values and comparing the hash values to values in the hash block.") 4:26-28 ("Finally, the data is checked against the hash block containing the hashes of the data set. Any given data packet can be checked once all hash blocks above it are received.") 10:1-5 ("Once a hash block is received and verified, data packets that depend on it may be verified (step 340) by computing the hash of the packet and comparing it with the hash value stored in the hash block (step 350). If this check fails, the data packet is corrupt and should be repaired or recovered (step 350). Of course the verification process must use the same hash function used to sign the data.") 10:6-11 ("If it is determined that additional hash blocks are expected (step 360), the packets of these hash blocks are then received and verified (step 370). The hash function is applied to each packet to derive its hash value. The hash value derived from the received hash block packet is compared with the one stored in the received top level hash block. If the comparison fails, the packet is corrupt and must be repaired or replaced before any packets that depend on this hash block can be verified (step 370).") 11:12-19 ("Data verification begins with checking the digital signature on the top level hash block 502. If the top level hash block 502 passes this check, the next level hash block 501 is verified. A hash function (not shown) is applied to each packet

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		and compared with the corresponding hash value in the hash block in the level above it. For example, the packets 501a and b of the hash block 501, B1 through B6, are checked with the values stored in the other hash block 502, C1 and C2. In the sample in Fig. 5, the hash of the packet B1, B2, B3 would be compared with the value C1. If the check fails, the packet B1, B2, B3 is corrupt and must be repaired or replaced before any packets that depend on it can be verified, in this case, data values A1 through A9, 500a-c.") 11:24-12:2 ("The data packets are checked in the same manner. For example, the data packet A10, A11, A12 would be checked by comparing the hash of the data packet 500d with the value B4. If this check fails, the data packet A10, A11, A12, is corrupt. However, the other data packets can still be verified. For an arbitrary example, in Fig. 5, even if the fourth packet 500d in the data, A10, A11, A12, was corrupt, the fifth packet 500e in the data A13, A14, A15 could still be checked by comparison of the hash of the data packet with the value B5. In this manner, the data receiving 12 and verification procedure (Fig. 3) is applied to the top level hash block 502 to verify data set 500. According to the present invention, data packets may be verified even if the data is sent, received or retrieved out of order. Systems consistent with the present invention need not wait for all of the packets to be delivered to verify a data packet. Any packet can be verified as long as the hash block for that packet has been received and verified. This effectively reduces the delay time to the amount of time required to compute the hash and compare it to the value stored in its corresponding hash block. This delay time is much less than bulk signature's delay time in which all packets must be received before any can be verified. The computational overhead is less than packet-level signature.") 12:3-10 ("According to the present invention, data packets may be verified even if the data is sent, received or retrieved out of order. Systems consistent with the present invention need not wait for all of the packets to be delivered to verify a data packet. Any packet can be verified as long as the hash block for that packet has been received and verified. This effectively reduces the delay time to the amount of time

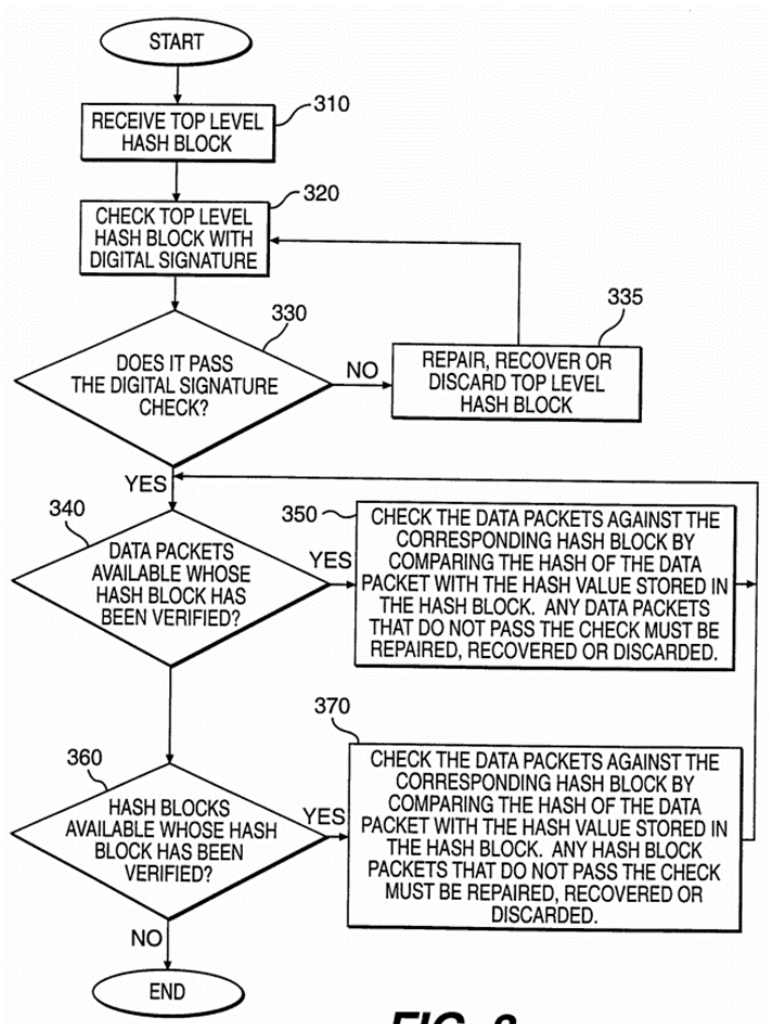
'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		required to compute the hash and compare it to the value stored in its corresponding hash block. This delay time is much less than bulk signature's delay time in which all packets must be received before any can be verified. The computational overhead is less than packet-level signature.") 12:11-13:6 ("The choice of when to send a hash block can save time. For instance, the second packet in a hash block need not be sent until after the packets that depend on the first packet in the hash block. This implementation can save the delay time of sending all of the hash blocks first. Conclusion Hierarchical hashing consistent with the present invention protects against malicious modification of data, while checksums do not. It also allows a single digital signature to apply to an arbitrary amount of data, which packet-level signature does not. The structure permits verification of data as it is received, thus eliminating the delay time of waiting for all of the data to be received as in bulk signature methods. Although the data can be verified as it is received, systems consistent with the present invention do not have the high computational overhead associated with individual packet signing. Additionally, the data need not be received or sent in any particular order for verification to begin. The hierarchical structure allows for recognition of corrupt individual packets or sections of data. The other packets that are not corrupt can be used and are unaffected by the corrupt packets. Additionally, other packets that are unverified can be verified even though some packets may be corrupt. Corrupt packets can be repaired or recovered while other packets are being checked. Total replacement of the data is not needed as in bulk signature methods, thus creating greater efficiency and reducing time expended. In summary, systems consistent with the present invention thus allow a single digital signature to protect an arbitrary amount of data, while cryptographically protecting individual portions of the data. To accomplish this, a hierarchy of hash values representing the data is built, and the top level of hashes

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		are signed and sent. After receipt, the digital signature on the hash values is checked. The data, upon receipt, is checked against the hash values that corresponded to the data.") 14:24-28 ("10. A computer implemented data processing method comprising the steps of: receiving a packet including data, a hash block and a digital signature; verifying the digital signature; hashing the data to produce hash values; and comparing the hash values to values in the hash block.") 15:1-6 ("11. A computer implemented data processing method comprising the steps of: signing, with a digital signature, a hash block corresponding to a data set; sending the data and the hash block from a source to a destination; upon receipt at the destination, checking the digital signature on the hash block; applying the hash function to the received data set; and comparing the hashes of the received data with the hash values stored in the hash block.")

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		 Figure 3 (" ")

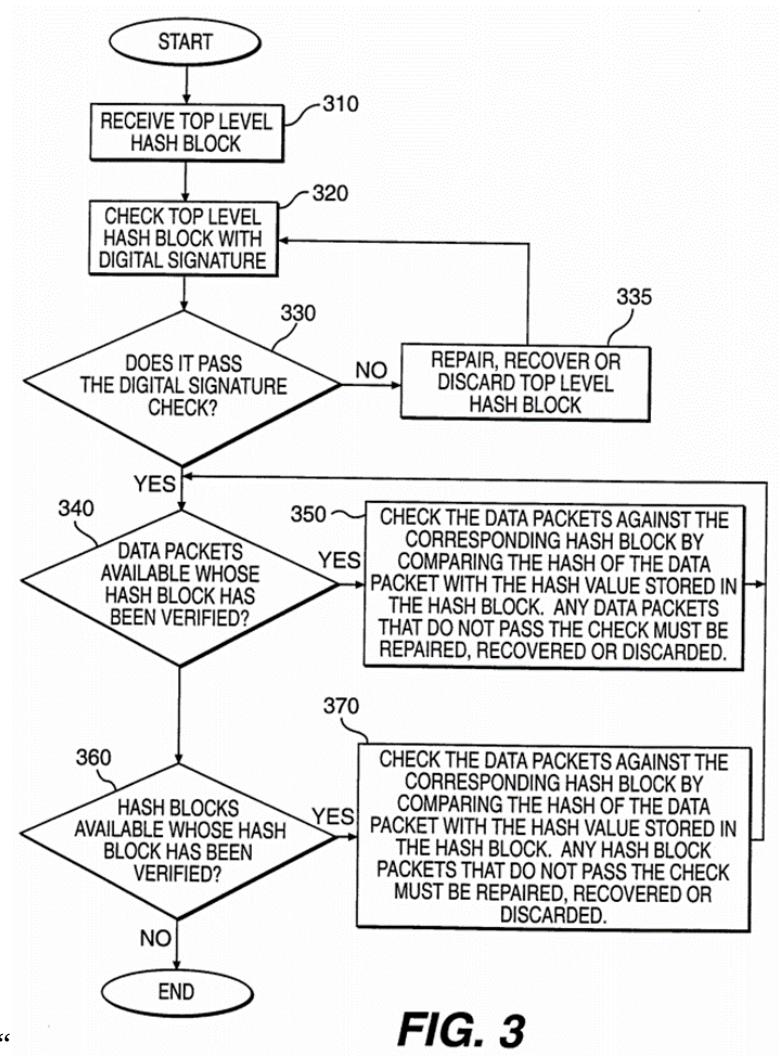
'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		 **FIG. 5** Figure 5 (" ") *See also* Abstract, 3:6-17, 4:15, 8:9-11, 9:1-4, 11:27-12:2. To the extent Intertrust alleges that Hanna does not explicitly disclose this claim limitation, this limitation is inherent and/or it would 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.e]	granting the request to use the file in the predefined manner.	Hanna discloses granting the request to use the file in the predefined manner. For example, Hanna discloses: 10:1-5 ("Once a hash block is received and verified, data packets that depend on it may be verified (step 340) by computing the hash of the packet and comparing it with the hash value stored in the hash block (step 350). If this check fails, the data

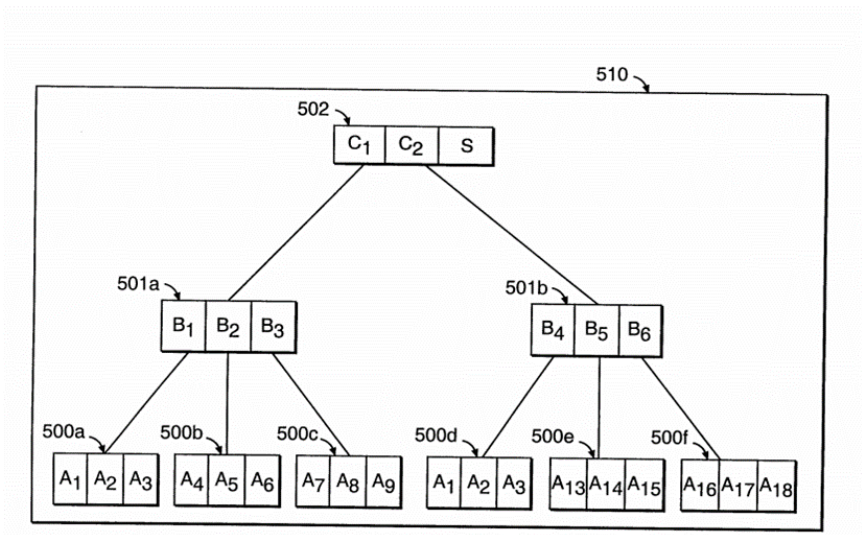
'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		packet is corrupt and should be repaired or recovered (step 350). Of course the verification process must use the same hash function used to sign the data.") 10:12-16 ("If other hash blocks are expected, the hashes of the packets of each lower level hash block are compared with the values stored in the hash block in the level above. If this verification step fails, the packet is corrupt and must be repaired or recovered before any packets that depend on this packet can be verified. However, other packets in the hash block can be verified.") 11:24-26 ("The data packets are checked in the same manner. For example, the data packet A10, A11, A12 would be checked by comparing the hash of the data packet 500d with the value B4. If this check fails, the data packet A10, A11, A12, is corrupt.") 12:23-27 ("The hierarchical structure allows for recognition of corrupt individual packets or sections of data. The other packets that are not corrupt can be used and are unaffected by the corrupt packets. Additionally, other packets that are unverified can be verified even though some packets may be corrupt. Corrupt packets can be repaired or recovered while other packets are being checked.")

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		 Figure 3 (" ") *See also* 1:6-8, 3:6-13.

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		To the extent Intertrust alleges that Hanna 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 one of the one or more hash values.	Hanna 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, Hanna discloses: *See* [42.d]; *see also*: 3:10-11 ("The hierarchical structure used in the method cryptographically protects individual portions of the data and makes it easier to recognize corruption.") 8:14-17 ("Once the data is broken into packets, a collision-proof, one-way hash function is applied to each packet (step 220). Each application of the hash function will produce a single hash value. The application of the hash function to each of the data packets will produce a sequence of hash values. This sequence is called a hash block (step 230).") 10:1-4 ("Once a hash block is received and verified, data packets that depend on it may be verified (step 340) by computing the hash of the packet and comparing it with the hash value stored in the hash block (step 350). If this check fails, the data packet is corrupt and should be repaired or recovered (step 350).") 10:26-30 ("Given an initial data sequence of data values 401, the data values are divided into data packets 402a-f. The present example shows 18 data values, A1 though A18, divided into six packets with three data values in each packet. A one-way, collision-proof hash function 403 is applied to the data packets 403. The

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		hashing of each data packet results in a single hash value. For instance, the hashing of the data packet A1, A2, A3 in this case yields value B1.") 4:26-28 ("Finally, the data is checked against the hash block containing the hashes of the data set. Any given data packet can be checked once all hash blocks above it are received.") 10:1-5 ("Once a hash block is received and verified, data packets that depend on it may be verified (step 340) by computing the hash of the packet and comparing it with the hash value stored in the hash block (step 350). If this check fails, the data packet is corrupt and should be repaired or recovered (step 350). Of course the verification process must use the same hash function used to sign the data.") 10:6-11 ("If it is determined that additional hash blocks are expected (step 360), the packets of these hash blocks are then received and verified (step 370). The hash function is applied to each packet to derive its hash value. The hash value derived from the received hash block packet is compared with the one stored in the received top level hash block. If the comparison fails, the packet is corrupt and must be repaired or replaced before any packets that depend on this hash block can be verified (step 370).") 11:14-15 ("A hash function (not shown) is applied to each packet and compared with the corresponding hash value in the hash block in the level above it.") 11:24-26 ("The data packets are checked in the same manner. For example, the data packet A10, A11, A12 would be checked by comparing the hash of the data packet 500d with the value B4. If this check fails, the data packet A10, A11, A12, is corrupt.")

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		 Figure 3 (" ")

'815 Claim	Claim Element	International Patent No. WO1999040702 ("Hanna")
		 ***FIG. 5*** Figure 5 (" ") *See also* Abstract, 3:6-17, 4:15, 8:9-11, 9:1-4, 11:27-12:2. To the extent Intertrust alleges that Hanna 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.