



US 20120237078A1

(19) **United States**(12) **Patent Application Publication**
Watson et al.(10) **Pub. No.: US 2012/0237078 A1**(43) **Pub. Date: Sep. 20, 2012**(54) **WATERMARKING AND FINGERPRINTING
DIGITAL CONTENT USING ALTERNATIVE
BLOCKS TO EMBED INFORMATION**

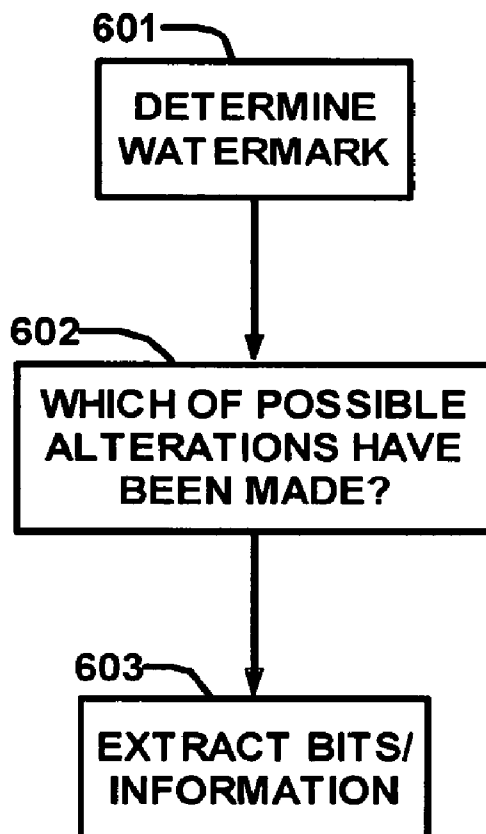
(60) Provisional application No. 60/394,630, filed on Jul. 9, 2002, provisional application No. 60/394,922, filed on Jul. 9, 2002, provisional application No. 60/394,588, filed on Jul. 9, 2002.

(75) Inventors: **Stephen Watson**, Toronto (CA);
Daniel A. Collens, Waterloo (CA);
Kevin Hui, Sunnyvale, CA (US);
Michael A. Malcolm, Aspen, CO
(US)**Publication Classification**(51) **Int. Cl.**
G06K 9/00 (2006.01)
(52) **U.S. Cl.** **382/100**(57) **ABSTRACT**(73) Assignee: **KALEIDESCAPE, INC.**,
Sunnyvale, CA (US)(21) Appl. No.: **13/482,137**(22) Filed: **May 29, 2012**

A method of embedding information in digital content representing media streams. The method includes (1) selecting a set of locations within that digital content representing the media stream to embed information, (2) selecting a set of possible alterations to make at those locations, and (3) making a subset of the possible alterations. The set of locations and possible alterations is herein sometimes called a "watermark." The subset of actual alterations that are made is herein sometimes called a "fingerprint." The method determines a set of locations at which there are alternative versions of digital content representing the same media stream, such as one being the original and one being an alternative version of the same digital content, herein sometimes called the "original movie" and the "alt-movie," or herein sometimes called the "original block" and the "alt-block" for a particular block in the digital content representing the media stream.

Related U.S. Application Data

(63) Continuation of application No. 11/707,634, filed on Feb. 16, 2007, now Pat. No. 8,189,854, which is a continuation of application No. 11/261,442, filed on Oct. 28, 2005, now Pat. No. 7,181,044, which is a continuation of application No. 10/356,322, filed on Jan. 31, 2003, now Pat. No. 7,003,131.



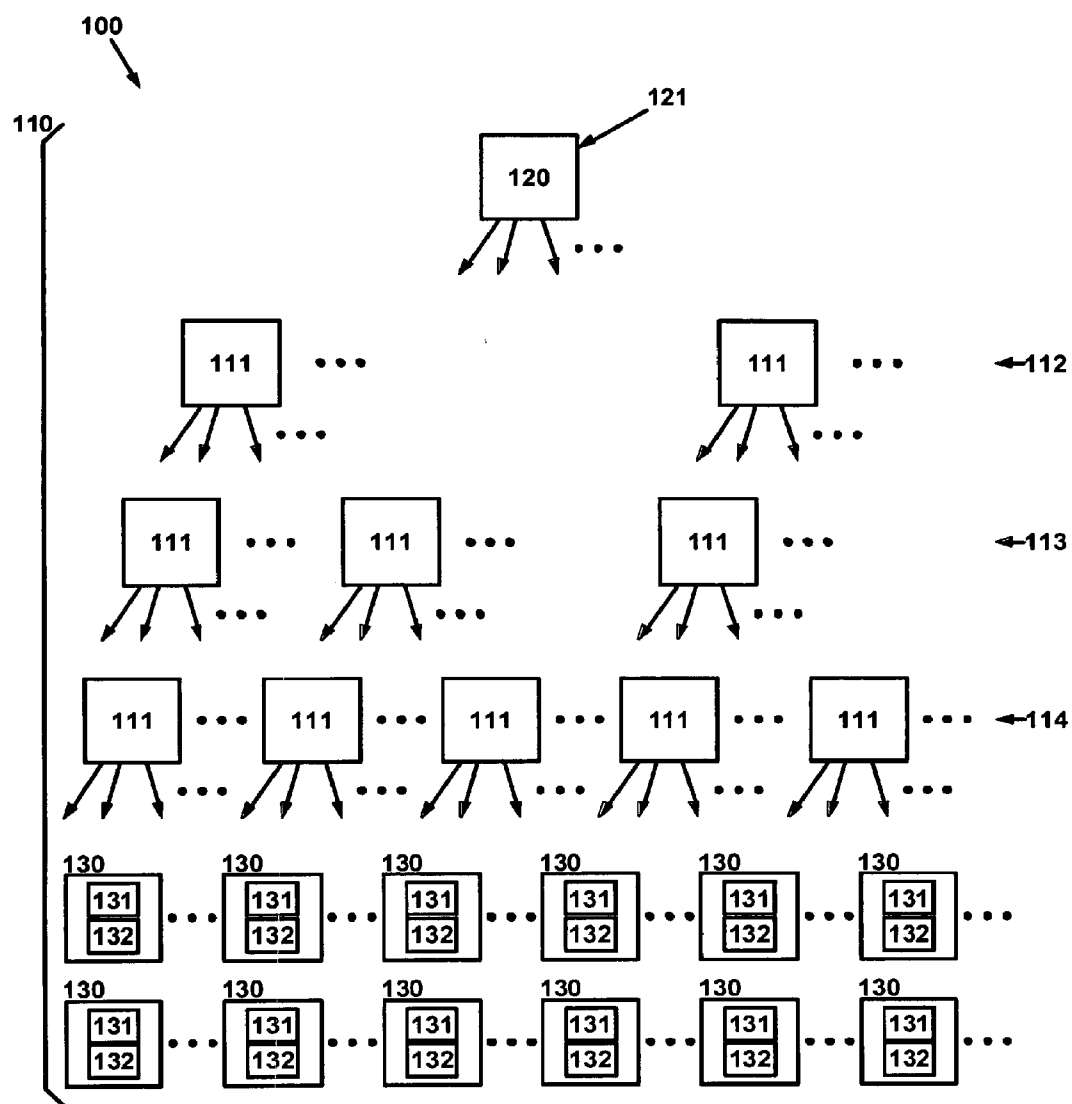


Fig. 1

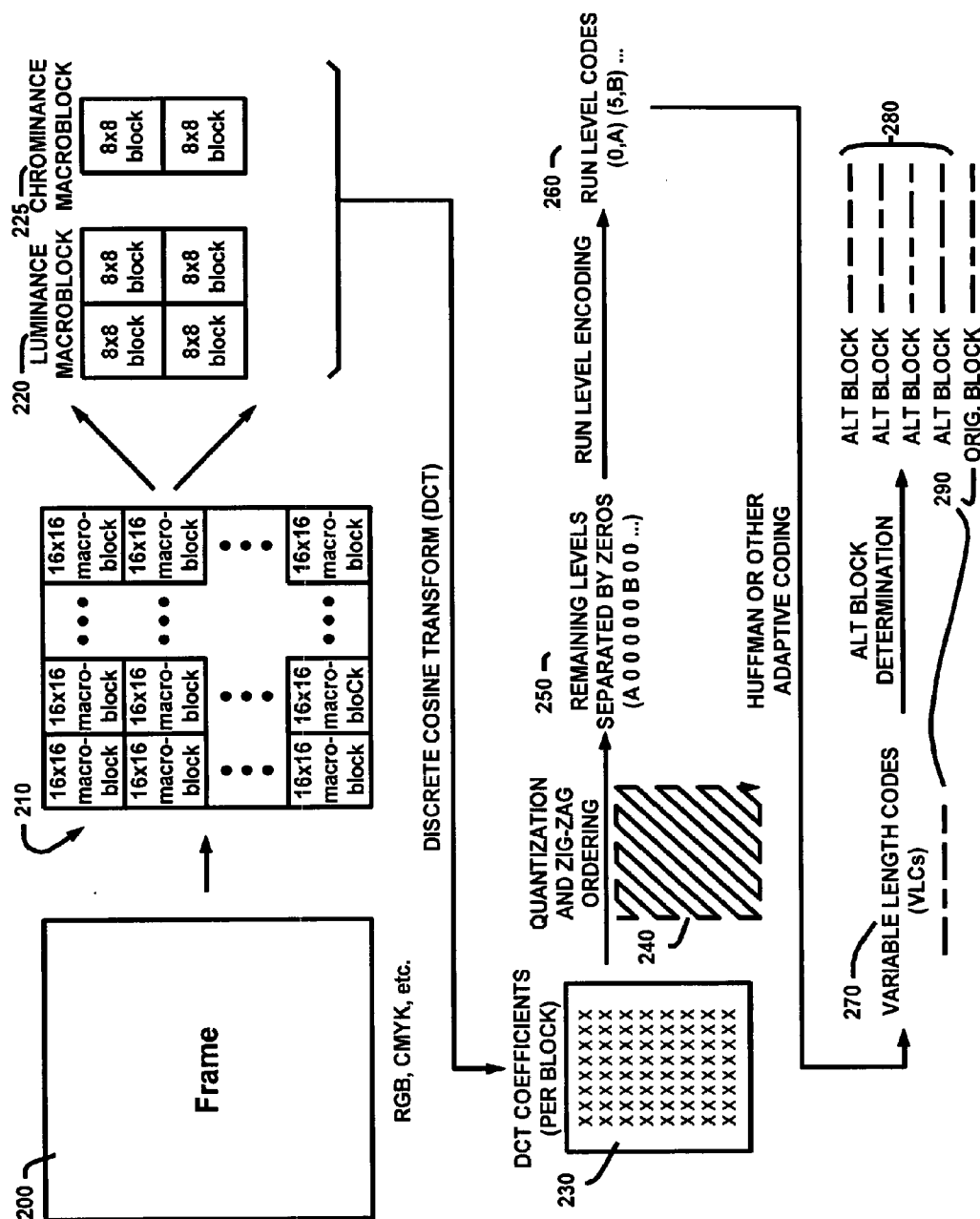


Fig. 2

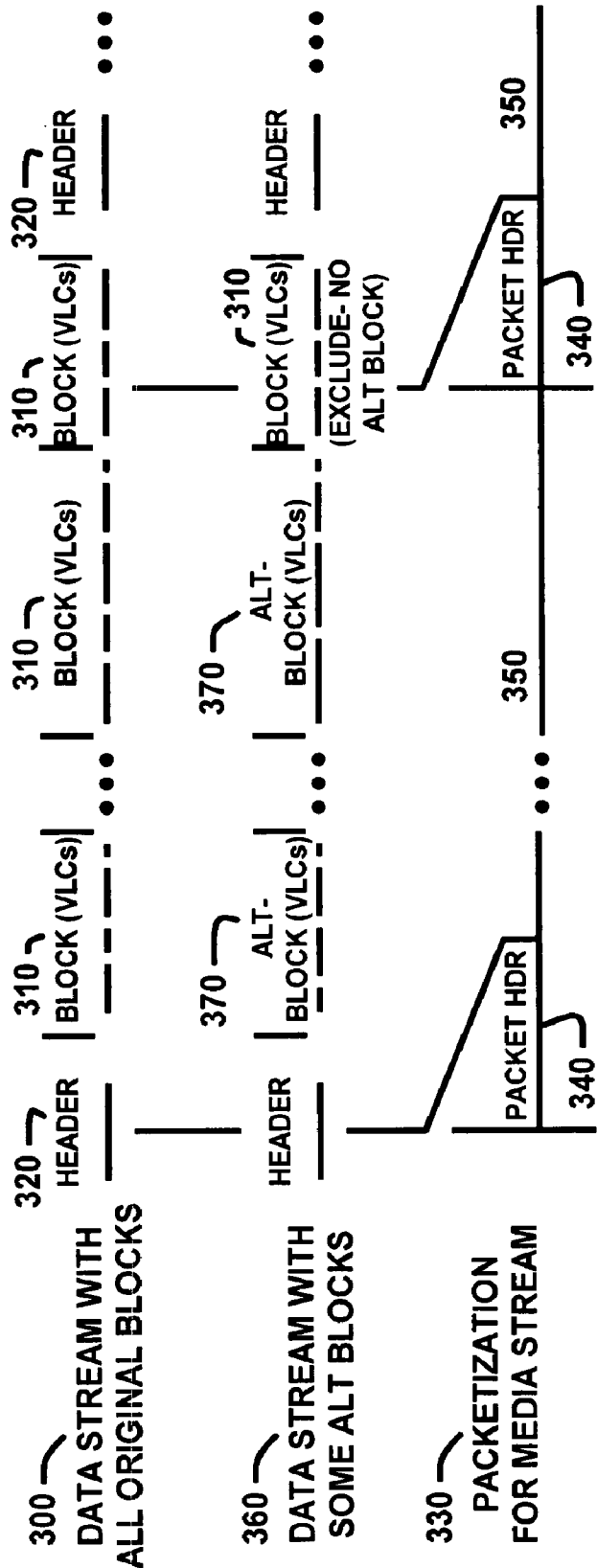
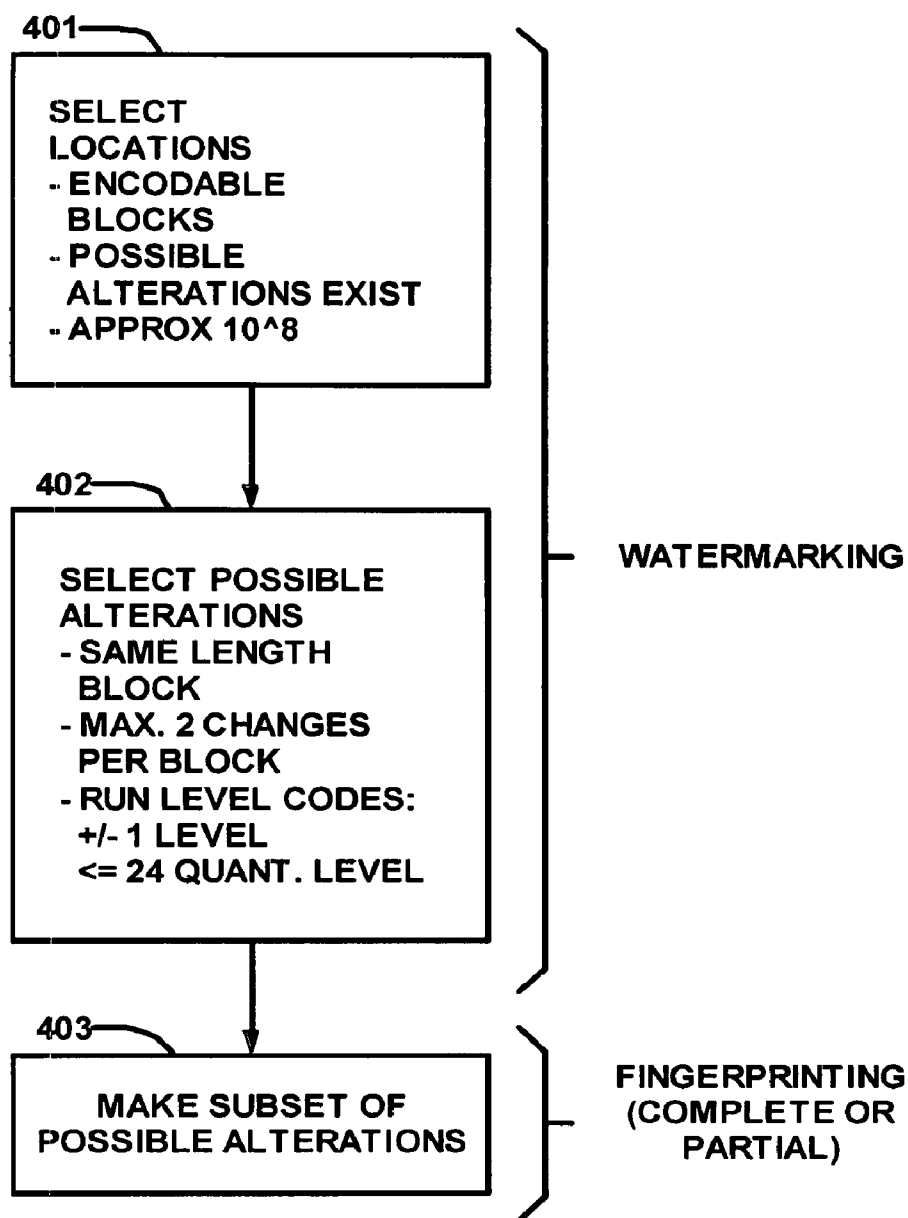
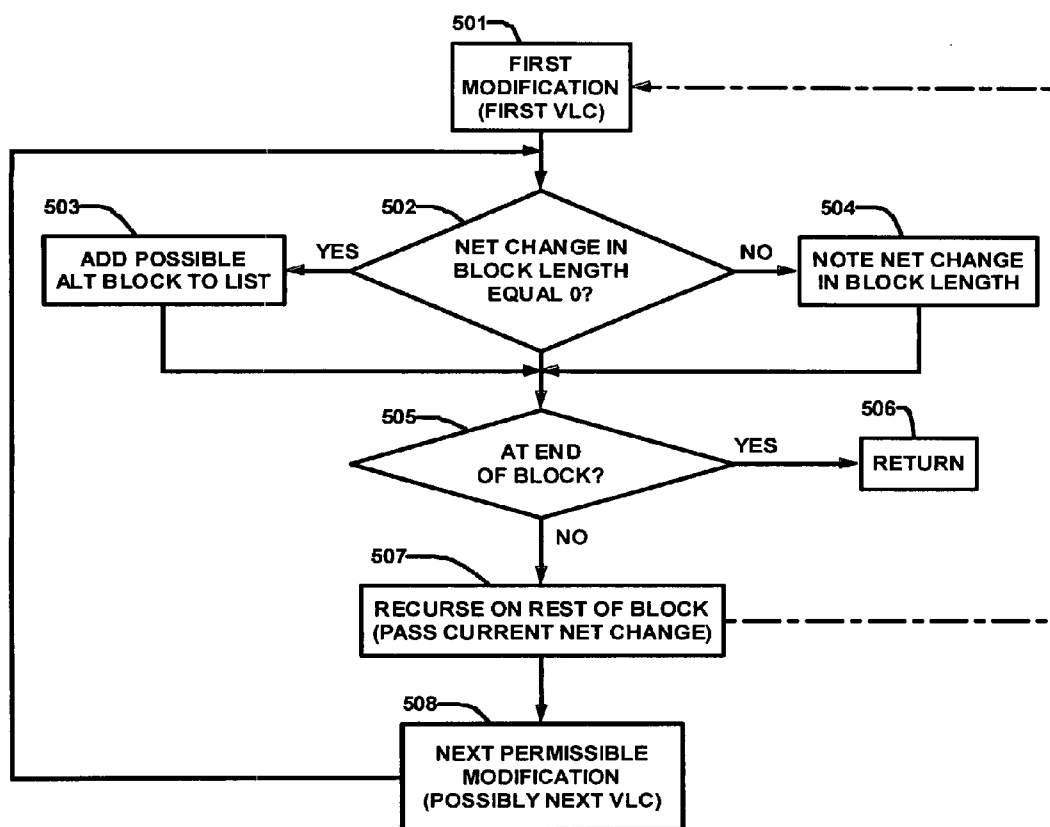


Fig. 3

**Fig. 4**

**Fig. 5**

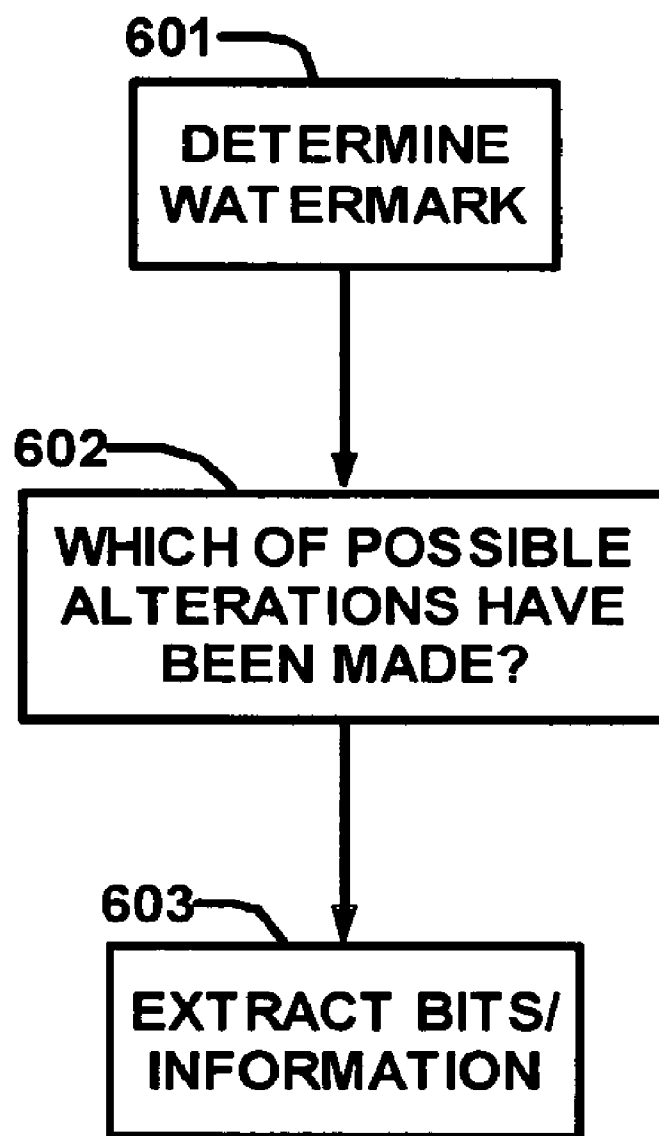


Fig. 6

WATERMARKING AND FINGERPRINTING DIGITAL CONTENT USING ALTERNATIVE BLOCKS TO EMBED INFORMATION

CROSS REFERENCE TO RELATED APPLICATIONS

[0001] This application claims priority of the following documents, each of which is hereby incorporated by reference as if fully set forth herein.

[0002] U.S. provisional application 60/394,630, filed Jul. 9, 2002, in the name of inventors Michael A Malcolm, Stephen Watson, Daniel A Collens, and Kevin Hui, attorney docket number 217.1001.01, titled “Watermarking and Fingerprinting a Movie for Secure Distribution.”

[0003] U.S. provisional application 60/394,922, filed Jul. 9, 2002, in the name of inventors Michael A Malcolm, Stephen Watson, and Daniel A Collens, attorney docket number 217.1002.01, titled “System Architecture of a System for Secure Distribution of Media.”

[0004] U.S. provisional application 60/394,588, filed Jul. 9, 2002, in the name of inventors Michael A Malcolm and Daniel A Collens, attorney docket number 217.1003.01, titled “Topology of Caching Nodes in a System for Secure Delivery of Media Content.”

[0005] U.S. application Ser. No. 10/356,322, filed Jan. 31, 2003, PN 7,003,131, in the name of inventors Stephen Watson, Daniel A. Collens, Kevin Hui, and Michael A. Malcolm, attorney docket number 217.1005.01, titled “Watermarking and Fingerprinting Digital Content Using Alternative Blocks to Embed Information.”

[0006] U.S. application Ser. No. 11/261,442, filed Oct. 28, 2005, now allowed, in the name of inventors Stephen Watson, Daniel A. Collens, Kevin Hui, and Michael A. Malcolm, attorney docket number 217.1005.05, titled “Watermarking and Fingerprinting Digital Content Using Alternative Blocks to Embed Information.”

[0007] This application is submitted in the name of the following inventors:

Inventor	Citizenship	Residence City and State
Stephen WATSON	Canada	Toronto, Ontario Canada
Daniel COLLENS	Canada	Waterloo, Ontario Canada
Kevin HUI	Canada	Kitchener, Ontario Canada
Michael MALCOLM	United States	Aspen, Colorado

BACKGROUND OF THE INVENTION

[0008] 1. Field of the Invention

[0009] The invention relates to distribution of digital content.

[0010] 2. Related Art

[0011] Distribution of digital content for media streams, such as for example movies, is subject to several problems. One problem is that it is easy to make exact copies of digital content, thus allowing any recipient of that content to redistribute it, whether or not authorized to do so. It would be advantageous to be able to distribute digital content, particularly digital content for media streams, without fear of its unauthorized distribution. This would be particularly advantageous when it is desired to distribute digital content using a communication link, such as for example a computer network

or other technique for distribution to end viewers (for example, either on demand, in anticipation of future demand, or in response to something else).

[0012] One known solution is to mark the digital content with a “fingerprint,” so that an unauthorized redistributor of the content can be identified, thus hopefully deterring potential unauthorized redistributors. However, fingerprinting of digital content is subject to several known problems, including (1) that presentation of the media stream might be degraded by altering the original content, (2) that recipients might attack the fingerprint, either by altering it or erasing it, or (3) that it might be difficult to determine the unauthorized redistributor with sufficient certainty, particularly if multiple unauthorized redistributors collude to make copies in which the fingerprint has been altered or erased using information available to those multiple recipients.

[0013] Another problem is that the fingerprint might interfere with distribution, decoding, or presentation of the original media stream. In particular, when the original media stream is encoded using a known format for movies, such as for example the MPEG-2 format, the amount of data included in even a single movie can be quite large. It would be advantageous for any fingerprinting method to retain the structure of the original MPEG encoding (including packetization of the original media stream), so that the particular fingerprinted digital content is not changed for distribution purposes by the fingerprint. In particular, it would be advantageous to assure that (1) the length of the fingerprinted digital content is the same as the length of the original digital content, and (2) sending the fingerprinted digital content can be interrupted and restarted, such as when using network communication techniques, without having to recompute the fingerprinted digital content and without having to maintain large amounts of intermediate state information about the fingerprinted digital content.

SUMMARY OF THE INVENTION

[0014] One aspect of the invention is a method of embedding information in a media stream. The method includes (1) selecting a set of locations within that media stream to embed information, (2) selecting a set of possible alterations to make at those locations, and (3) making a subset of the possible alterations. The set of locations and possible alterations is herein sometimes called a “watermark.” The subset of actual alterations that are made is herein sometimes called a “fingerprint.”

[0015] The method determines a set of locations at which there are alternative versions of the same media stream, such as one being the original and one being an alternative version of the same media stream, herein sometimes called the “original movie” and the “alt-movie” (“alternative movie”), or sometimes called the “original block” and the “alt-block” (“alternative block”) for a particular block in the media stream. More than one alt-movie or alt-block can be defined for each location in order to permit more than one bit of information to be embedded at each location. Thus, each such location can embed one or more bits of information, the embedded bits being responsive to whether the original movie or the alt-movie (or one of plural alt-movies) is selected for that location.

[0016] An aspect of the method includes selecting the alterations so that there is no change in distribution of the media stream, such as for example (1) packetization of the digital content representing that media stream, or (2) synchroniza-

tion of audio with video portions of the media stream. In a preferred embodiment, unchanged distribution can be accomplished by making no changes in lengths of portions of the digital content representing that media stream, such as for example individual blocks of an MPEG-encoded movie.

[0017] In a preferred embodiment, the method includes determining a set of intra-coded blocks in an MPEG-2 encoding of the digital content for that media stream. Each intra-coded block has a set of run-level encoded values for DCT coefficients for that block. The method determines if there is an alternative set of values which differ only a little from the original set of values, and which do not change the bit-length of the encoded block. Each such block thus provides both a location to embed information, and an alteration for that location, and thus provides at least one bit worth of embeddable information. In alternative embodiments, macroblocks may be used instead of blocks.

[0018] This preferred embodiment would include the choice of (1) the number of run-level encoded values to be changed in any individual block, such as ≤ 2 values; (2) the amount of alteration, such as ± 1 level, for any run-level encoded values to be changed; and (3) the amount of quantization allowed for any run-level encoded values to be changed, such as a quantization scale ≤ 24 .

[0019] In a preferred embodiment, the method includes noting those blocks at which an alt-block can be selected, and selecting the particular alt-block at each block in response to a random or pseudo-random effect. This type of effect may help a fingerprint resist attacks that attempt to study the run-level codes in order to “undo” the fingerprint. It may also help to spread the watermarking over a relatively large range of spatial frequencies of the content, further diminishing visible effects while also helping to resist attacks. Thus, for each movie that is watermarked, the particular alt-movie by which it is watermarked is resistant to attacks that might involve attempting to reverse the embedding of information by re-encoding alt-blocks into original blocks or re-encoding blocks into alt-blocks, because the selection of those alt-blocks or those original blocks is not easily known to the attacker.

[0020] The method of the preferred embodiment also excludes blocks at locations that span packet boundaries within a packetized data stream for the digital content representing the media stream. Alt-blocks preferably are not selected for such spanning blocks because accessing those blocks would involve parsing of the packetized digital content, possibly involving non-trivial look-ahead and analysis of the digital content representing the media stream. Thus, this optimization simplifies implementation of the preferred embodiment of the invention.

[0021] The invention is not restricted to movies, but is also applicable to other digital content and other media streams, such as for example animation or sound, as well as to still media, such as for example pictures or illustrations, and to databases and other collections of information.

BRIEF DESCRIPTION OF THE DRAWINGS

[0022] FIG. 1 shows a block diagram of a system for watermarking and fingerprinting digital content.

[0023] FIG. 2 illustrates MPEG encoding and generation of alt-blocks according to the invention.

[0024] FIG. 3 illustrates preservation of packetization according to the invention.

[0025] FIG. 4 shows a flow diagram of a method for watermarking and fingerprinting digital content with a set of locations at which information might be embedded.

[0026] FIG. 5 shows a flow diagram of a recursive technique that can be used to identify possible alterations in a block for determining alt-blocks according to the invention.

[0027] FIG. 6 shows a flow diagram of a method for detecting a fingerprint that embeds information in digital content.

DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

[0028] In the following description, a preferred embodiment of the invention is described with regard to preferred process steps and data structures. Those skilled in the art would recognize after perusal of this application that embodiment of the invention can be implemented using one or more general-purpose processors or special-purpose processors or other circuits adapted to particular process steps and data structures described herein, and that implementation of particular process steps and data structures would not require undue experimentation or further invention.

[0029] Lexicography

[0030] The following terms refer or relate to aspects of the invention as described below. The descriptions of general meanings of these terms are not intended to be limiting, only illustrative.

[0031] The phrase “digital content” describes data in a digital format, intended to represent media streams or other information for presentation to an end viewer. “Digital content” is distinguished from packaging information, such as for example message header information.

[0032] The phrase “media stream” describes information intended for presentation in a sequence, such as motion pictures including a sequence of frames or fields, or such as audio including a sequence of sounds. As used herein, the phrase “media stream” has a broader meaning than it’s the standard meaning for “streaming media,” of sound and pictures that are transmitted continuously using packets and that start to play before all of the content arrives. Rather, as used herein, there is no particular requirement that “media streams” must be delivered continuously. Also as described herein, media streams can refer to other information for presentation, such as for example animation or sound, as well as to still media, such as for example pictures or illustrations, and also to databases and other collections of information.

[0033] The phrase “embedding information in media streams” describes generating a set of digital content for that media stream, for which the digital content both represents the media stream and also includes the embedded information in a form capable of later detection.

[0034] The term “watermark” describes a schema for digital content by which information can be embedded into that digital content. As described herein, an attacker cannot easily remove the watermark provided by the invention. However, the concept of a watermark as described herein is sufficiently general to include watermarks that are not so resistant to attack. As described herein, the watermark provided by the invention includes within the media stream, both a set of locations at which to embed information, and possible alterations to make at those locations by which information is embedded. However, the concept of a watermark as described herein is sufficiently general to include watermarks using other techniques for embedding information.

[0035] The term “fingerprint” describes a specific set of information sufficient to identify at least one designated recipient of digital content. As described herein, multiple attackers colluding together cannot easily remove the fingerprint provided by the invention, or prevent at least one of them from being detected as unauthorized distributor of the digital content. However, the concept of the fingerprint as described herein is sufficiently general to include fingerprints that are not so resistant to removal, or do not provide such capability for detecting unauthorized distributors of the digital content. As described herein, the fingerprint provided by the invention includes within the media stream, a specific set of alterations to make at the locations identified by the watermark. However, the concept of the fingerprint as described herein is sufficiently general to include fingerprints using other techniques for embedding information, detecting the embedded information, and detecting unauthorized distributors of the digital content.

[0036] The term “adaptation” describes a process in which a sender delivers digital content to a recipient. As described herein, the sender decrypts its copy of the digital content, embeds information in the media stream represented by that digital content (thus partially fingerprinting that digital content), and re-encrypts that partially fingerprinted digital content. The sender delivers the adapted digital content to the recipient.

[0037] The phrase “end viewer” describes a recipient of the media stream for whom decoding of the digital content for the media stream, and presentation of the media stream, is contemplated.

[0038] The term “decoding” describes generating data in a form for presentation of the media stream, in response to the digital content for the media stream in an encoded format. As described herein, the encoded format might include an industry standard encoded format such as MPEG-2.

[0039] However, the concept of decoding as described herein is sufficiently general to include other encoding formats for the media stream.

[0040] The term “presentation” describes generating information in a form for viewing (or other sensing) of the media stream, such as for example audio and visual information for viewing a movie. As described herein, presentation of a movie might include visual display of the frames or fields of motion picture, as well as audio presentation of a soundtrack associated with that motion picture. However, the concept of presentation as described herein is sufficiently general to include a wide variety of other forms of generating information for reception by end viewers, including audio, visual, or otherwise.

[0041] The phrases “original movie” and “alt-movie” describe alternative versions of the same media stream, such as one being an original version of that media stream introduced into a system using aspects of the invention, and another being an alternative version of that same media stream generated in response to the original movie. Similarly, the phrases “original block” and “alt-block” describe alternative versions of the same individual block or macroblock within the original movie or alt-movie. As described herein, a difference between the original movie and the alt-movie is historical, in that the alt-movie can be substituted for the original movie in every respect. Similarly, a difference between any one original block and its associated alt-block is historical, in that the alt-block can be substituted for the original block in every respect.

[0042] The phrase “MPEG” is an acronym for the “Moving Picture Experts Group,” a working group of the ISO/IEC (International Organization for Standardization/International Engineering Consortium). The phrases “MPEG-1,” “MPEG-2,” and “MPEG-4” refer to techniques for encoding media content as set forth in the ISO/IEC 11172, ISO/IEC 13818, and ISO/IEC 14496 documents, respectively. The invention is not limited to use with MPEG, and these terms should be read broadly to encompass other encoding techniques, whether of similar nature or otherwise.

[0043] The term “intra-coded block” refers to a block that is part of an intra-coded macroblock. Intra-coded blocks, and macroblocks are familiar terms in the art of MPEG techniques.

[0044] Other and further applications of the invention, including extensions of these terms and concepts, would be clear to those of ordinary skill in the art after perusing this application. These other and further applications are part of the scope and spirit of the invention, and would be clear to those of ordinary skill in the art without further invention or undue experimentation.

[0045] System Elements

[0046] FIG. 1 shows a block diagram of a system for watermarking and fingerprinting digital content.

[0047] System 100 includes video distribution network 110. The video distribution network includes at least one injection origin 120 and a plurality of end viewer premises 130.

[0048] 1. Distribution from the Injection Origin to the End Viewer Premises.

[0049] Injection origin 120 receives digital content 121 for media streams from sources outside the video distribution network 110. In a preferred embodiment, these sources might include content producers or content aggregators, such as for example movie production studios, television studios, or radio or television network syndicators. If necessary, injection origin 120 formats digital content 121, watermarks it, and encrypts it for storage at injection origin 120. In a preferred embodiment, injection origin 120 uses a method of watermarking and fingerprinting as described herein.

[0050] In a preferred embodiment, injection origin 120 includes at least a processor capable of executing instructions, memory for storing digital content and instructions, and a network interface.

[0051] Video distribution network 110 includes network of caching devices 111, each capable of acting individually or in concert, to receive, store, and distribute digital content 121 from injection origin 120 to end viewer premises 130. In a preferred embodiment, requests from end viewers prompt video distribution network 110 to distribute digital content 121 to end viewer premises 130, thus using a “pull” model for distribution. However, in alternative embodiments, injection origin 120 or another device may prompt video distribution network 110 to distribute digital content 121 to end viewer premises 130, thus alternatively using a “push” model or another model for distribution.

[0052] In a preferred embodiment, caching devices 111 are disposed in a tiered distribution system, including primary caches 112, intermediate caches 113, and leaf caches 114. The primary caches 112 receive digital content 121 directly from injection origin 120. Intermediate caches 113 receive digital content 121 from primary caches 112, or from other intermediate caches 113 closer by the network topology to injection origin 120. Leaf caches 114 receive digital content

121 from intermediate caches **113**, or possibly directly from primary caches **112**, and distribute digital content **121** directly to end viewer premises **130**.

[0053] Preferably (i.e., in a preferred embodiment), each of the caching devices and end viewer premises includes at least a processor capable of executing instructions, memory for storing digital content and instructions, and a network interface.

[0054] In a preferred embodiment, video distribution network **110** includes a redundant communication network, such as the Internet or a secure subnet thereof. However, in the context of the invention there is no particular requirement for video distribution network **110** to use any particular communication technique. In alternative embodiments, any communication technique capable of delivering copies of digital content **121** from injection origin **120**, through video distribution network **110**, and ultimately to end viewer premises **130**, would also be suitable.

[0055] Distribution of digital content **121** using video distribution network **110** in a preferred embodiment provides that copies of digital content **121** might be recorded and maintained at multiple caching devices **111**, and might be delivered using more than one pathway from injection origin **120** to end viewer premises **130**.

[0056] For a first example, copies of the digital content **121** might be delivered from the injection origin **120** to two different intermediate caches **113** (A and B), and from those intermediate caches **113** (A and B) to multiple end viewer premises **130**. In the event that one of those intermediate caches **113** (A) later discards its copy of the digital content **121**, it can receive another copy from the other intermediate cache **113** (B) for further delivery to end viewer premises **130**.

[0057] For a second example, different portions of the digital content **121** might be delivered from the injection origin **120** to different intermediate caches **113** (A and B), and from those intermediate caches **113** (A and B) to the same end viewer premises **130**. This might occur if the act of sending the digital content **121** from the injection origin **120** to the end viewer premises **130** was interrupted, such as for example by a communication link failure within the video distribution network **110** or alternatively by user action, and was later resumed and completed.

[0058] 2. Distribution to each Recipient Using the Video Distribution Network.

[0059] Whenever any sender delivers digital content **121** to any recipient within the video distribution network **110**, the sender performs adaptation of the digital content **121** for that recipient. In adaptation, the sender decrypts its copy of the digital content, embeds information in the media stream represented by that digital content by partially fingerprinting that digital content, and re-encrypts that partially fingerprinted digital content.

[0060] In a preferred embodiment, adaptation is performed for all recipients, including both caching devices **111** and end viewer premises **130**. This would include transfers among caching devices **111**, even those the same or similar distance from the injection origin **120**. However, in the context of the invention there is no particular requirement for adaptation to be performed for all possible recipients, so that in alternative embodiments, some portion of the video distribution network **110** might transmit the digital content **121** through without decrypting or re-encrypting it.

[0061] Preferably, a different key is used for decryption and re-encryption. It is also possible to use different crypto-

graphic schemes for decryption and re-encryption. Alternatively, the same keys, schemes, or both can be used.

[0062] As described above, it is therefore possible as a consequence for individual end viewer premises **130** to receive digital content **121** that has been partially fingerprinted for multiple recipients. However, in a preferred embodiment, the method of fingerprinting (such as for example using a technique described in related applications for detecting collusion among multiple recipients of fingerprinted digital content) provides for detecting individual viewers anyway.

[0063] When individual end viewer premises **130** receives the encrypted, fingerprinted digital content **121**, it records that digital content **121** in local video library **131**. Local video library **131** maintains digital content **121** in its encrypted, fingerprinted form for later distribution to one or more playback elements **132**. In response to a request by an end viewer, local video library **131** distributes digital content **121** to one or more playback elements **132**, at which digital content **121** is substantially simultaneously decrypted and presented to end viewers for viewing.

[0064] Further detail of one possible implementation of system **100** is discussed in a related application, "PARALLEL DISTRIBUTION AND FINGERPRINTING OF DIGITAL CONTENT [1004]."

[0065] Methods of Operation

[0066] FIG. 2 illustrates MPEG encoding and generation of alternative blocks (i.e., alt-blocks) according to the invention. The invention is not limited to use with MPEG encoded digital content. After reading the following discussion of the invention in the MPEG context, one skilled in the art of digital encoding would be able to apply the invention to different encoding schemes and data types without undue experimentation or further invention.

[0067] In FIG. 2, frame **200** of digital content is processed according to the MPEG standard. For illustrative purposes, this frame is shown as an image frame in RGB, CMYK, or some other format. The invention is also applicable to other types of digital content.

[0068] The data in the frame itself can be processed. If the data in the frame itself is processed, the frame is said to be "intra coded."

[0069] Alternatively, the difference of the data from data predicted for the frame can be processed. Prediction of frame data can be based on data in a previous frame or on data in both previous and succeeding frames. In the former case, the frame is said to be a "predictive" frame; in the latter case, the frame is said to be a "bidirectional" frame.

[0070] The preferred embodiment of the invention is applied to intra coded frames only; however, such need not be the case.

[0071] Frame **200** is divided into 16x16 pixel macroblocks **210**. Each macroblock is then decomposed into luminance macroblock **220** and chrominance macroblock **225**. FIG. 2 illustrates a 4:2:0 chrominance format. In this format, the luminance macroblock contains four 8x8 blocks, and the chrominance macroblock contains two 8x8 blocks. Lower resolution can be used for the chrominance data because the human eye is less sensitive to chrominance variations than to luminance variations. The chrominance blocks can be determined through any of various downsampling techniques.

[0072] In other chrominance formats, different size chrominance macroblocks can be used. For example, in a 4:2:2 format, each chrominance macroblock contains four

8×8 blocks, and in a 4:4:4 format, each chrominance macroblock contains eight 8×8 blocks.

[0073] Next, each block of luminance and chrominance data is processed. In order to process a block, a discrete cosine transform (DCT) is applied to the block, resulting in a set of 8×8 DCT coefficients **230**.

[0074] The DCT coefficients are then quantized. Quantization involves dividing all of the DCT coefficients for a block by an integer and discarding any remainders. The process results in a few non-zero coefficients interspersed among coefficients of zero. The integer by which the coefficients are divided is the quantization level for the block. Quantization results in some loss of precision; however, depending on the degree of quantization permitted, the loss of precision will be acceptable to an end viewer (if noticed at all). The benefit of quantization is that it allows for a high degree of data compression.

[0075] The quantized data for a block is then ordered by running through the block in a zig-zag pattern such as pattern **240**. This ordering results in a series of non-zero coefficients, called levels, separated by runs of zeros. In FIG. 2, such a series is shown representationally at reference numeral **250**.

[0076] The series of levels and zeros are converted into a list of pairs of numbers through a process called run level encoding. The pairs of numbers in the list are called run level codes, represented at reference number **260**. The first number in each pair represents a number of zeros in a run preceding a level, and the second number in each pair represents the level. Thus, for example, the series of levels and zeros (A 0 0 0 0 B 0 0 . . .) can be converted to the pairs (0,A) and (5,B), etc., with A and B being values for levels.

[0077] In order to improve compression, the run level codes are then encoded through some adaptive coding scheme such as a Huffman code. This type of coding scheme results in different length binary codes for each run level code. For this reason, the resulting codes are called variable length codes (VLCs). In FIG. 2, different length VLCs **270** are represented by different length dashes.

[0078] VLCs **270** include four dashes representing four variable length codes, which in turn represent four run level codes for quantized DCT coefficients for a single 8×8 pixel block of luminance or chrominance data. A block could be represented by fewer or more such VLCs of shorter or longer length.

[0079] As discussed above, the conversion of a frame into VLCs involves downsampling and quantization; as a result, the VLCs do not represent the exact frame data. The invention takes advantage of this fact by determining one or more alternate sets of VLCs for a frame that represent the frame in almost, but not exactly, the same way. These alternate sets of VLCs form alt-blocks according to the invention. The original set of VLCs is referred to as the original block.

[0080] Some or all of the VLCs for the alt-blocks might have different lengths than the VLCs in the original block. However, according to the invention, the total length of the VLCs for an alt-block should be equal to the total length of the VLCs for the original block. This is shown representationally in FIG. 2, where the total lengths of the VLCs for alt-blocks **280** are equal to the total length of VLCs **270** for original block **290**.

[0081] FIG. 3 illustrates preservation of packetization according to the invention.

[0082] In FIG. 3, data stream **300** includes original blocks **310** of VLCs along with control data and the like in headers

320. The variable number and lengths of VLCs in each block are represented by the dashed lines in blocks **310**.

[0083] Data stream **300** is packetized for presentation as a media stream as packetized data stream **330**. The packetized data stream includes its own packet headers **340** and packets **350** including all data from data stream **300**. The packet boundaries can occur at any place in data stream **300**, as shown in FIG. 3 by vertical lines between packetized data stream **330** and data stream **300**. Thus, the packet boundaries can occur in blocks **310** and headers **320**.

[0084] Data stream **360** includes alt-blocks **370** for some of the blocks in data stream **300**. These alt-blocks can be inserted into the data stream in place of the corresponding original blocks in order to embed data in the data stream.

[0085] As discussed with respect to FIG. 2, the total length of the VLCs for an alt-block equals the total length of the VLCs for the corresponding original block. However, the number, size, or both of the individual VLCs can vary from those in the original blocks, as long as the overall block lengths are unchanged. These variations are represented by the dashed lines in blocks **370**.

[0086] Because the length of an alt-block matches the length of its corresponding original block, an alt-block can be substituted into packetized data stream **330** by substituting a packet with the alt-block for the packet with the original block.

[0087] However, if an alt-block spans two packets, substitution of the alt-block would require non-trivial look-ahead and analysis of the packetized data stream. Therefore, the preferred embodiment of the invention excludes blocks which span packet boundaries from the possible locations for embedding data. In other words, alt-blocks preferably are not permitted for blocks that span packet boundaries in the packetized data stream.

[0088] Specific details of a preferred technique for selecting locations and alt-blocks for those locations are discussed next. The set of possible locations and alt-blocks for a particular item of digital content forms a watermark for that digital content. A copy of the content in which some or all of those possible alt-blocks have been inserted is said to be wholly or partially fingerprinted.

[0089] FIG. 4 shows a flow diagram of a method for watermarking and fingerprinting digital content with a set of locations at which information might be embedded.

[0090] 1. Watermarking

[0091] A set of block locations and alt-blocks at those locations are a specific example of a set of locations and possible alterations in the context of MPEG. In general, a set of such locations and possible alterations at those locations forms a watermark according to the invention. Step **401** and **402** are the steps for creating this watermark. Preferably, these steps are performed at injection origin **120**.

[0092] In step **401**, locations for embedding information are selected in digital content. In the preferred embodiment, this digital content can be an MPEG-1, MPEG-2, or MPEG-4 (collectively referred to as simply MPEG hereinafter) encoded digital movie. The following steps are described in the context of an encoded digital movie. However, the invention is equally applicable to other digital content, and application of these steps would not require further invention or undue experimentation.

[0093] The locations are preferably 8×8 blocks of either luminance and chrominance DCT coefficients, but could also be 16×16 macroblocks of such coefficients. Preferably, the

locations are blocks of intra coded macroblocks, although the invention can also be used with locations that are complete intra coded macroblocks. Blocks and intra coded macroblocks are well known in the art of MPEG encoding.

[0094] The invention also can be applied to other blocks that contain coefficients from transforms other than DCT, for example wavelets or any other transform in which luminance or chrominance information is presented in some transformed domain (e.g., in a non-MPEG encoding scheme), or to transforms of RGB data, CMYK data, YUV data, and more generally, to any transform in which information useful for presentation of the media stream is represented in the digital content. Those skilled in the art, after perusal of this application, would recognize that essentially any combination of color space and basis functions would be workable, is within the scope and spirit of the invention, and would not require undue experimentation or further invention.

[0095] In the case of packetized digital content, blocks that span packet boundaries preferably are excluded as possible locations for embedding information.

[0096] The locations are also selected such that alternative versions of the blocks exist that meet the criteria discussed in step 402 for selecting possible alterations for the locations. Thus, step 401 preferably occurs in conjunction with step 402.

[0097] In step 402, possible alterations to the block are selected. In order to maintain packetization and synchronization of the digital content, these alterations preferably do not involve any change to the length of the digital content at the locations (i.e., blocks) where information is embedded.

[0098] In the MPEG context, each block has a set of run-level encoded values for discrete cosine transform (DCT) coefficients for that block. The invention determines if there is an alternative set of values which differ only a little from the original set of values, and which do not change the bit-length of the encoded block. Each such block thus provides both a location to embed information and an alteration for that location, and thus provides at least one bit worth of embeddable information. In an alternative embodiment, macroblocks are used instead of blocks.

[0099] In more detail, in MPEG, chrominance and luminance blocks are encoded using variable length codes (VLCs) corresponding to run level codes that represent discrete cosine transforms of pixel data values. These VLCs are Huffman codes that provide an extremely efficient way to compress data. However, the resulting data for different blocks can be different lengths.

[0100] Thus, in order to maintain constant block length at a location for embedding information, any changes to the VLCs for the block must result in a net length difference of zero. This can be accomplished in several ways.

[0101] First, one VLC could be substituted for another VLC that has the same length. Second, more than one VLC could be substituted for an equal number of VLCs, with the sums of the lengths of the original and substituted VLCs being equal. For example, two VLCs with length 5 and 6 could be substituted for VLCs with lengths 4 and 7. Third, one or more VLCs could be added or deleted. In order to reduce visible impact, additions and deletions preferably are restricted to VLCs with a level of one. Combinations of these three techniques, as well as other techniques, can be utilized.

[0102] If more than two VLCs for a block are changed, artifacts can result that might be seen by viewers, albeit at

possibly a very low level of perception. Therefore, alt-blocks preferably are limited to blocks resulting from two changes to VLCs.

[0103] In order to limit the visible impact on the presentation of the digital content, changes to the data at the identified locations preferably are increases or decreases by a value of one level in the run level codes. In addition, MPEG involves quantization of data represented by the run level codes. If the quantization scale (QS) is higher than 24, even a level change of one can result in unacceptable distortion of the presentation. Thus, only blocks with a quantization scale of less than or equal to 24 preferably are used to form alt-blocks.

[0104] In sum, in the preferred embodiment, the following criteria are used to identify a possible alteration (i.e., alt-block) for an original block:

[0105] the block is part of an intra coded macroblock

[0106] the block includes one or two run level codes that can be changed by a value of plus or minus one level, with the change(s) in run level(s) resulting in VLC(s) that have a same length as the VLC(s) for the unchanged levels (if two run level codes are changed, only the sums of the lengths of the VLCs need to be equal)

[0107] the quantization scale of the block is less than or equal to 24

[0108] Experimentally, a typical MPEG-encoded digital movie has been found to include approximately one hundred million suitable locations that meet these criteria.

[0109] While use of the foregoing criteria is the preferred embodiment, the invention is not limited to these criteria. Thus, alternative embodiments of the invention can create alt-blocks from any types of blocks including blocks contained within macroblocks which are not intra coded, can change, add, or delete more than two VLCs in a block, can use changes in levels that are greater than one level, and can create alt-blocks from blocks with quantization scales greater than 24. Other variations are possible without departing from the scope of the invention.

[0110] FIG. 5 shows a flow diagram of a recursive technique that can be used to identify possible alterations in a block in step 402 for determining alt-blocks. Other different techniques, including non-recursive techniques, can be used in performing step 402 without departing from the invention.

[0111] In a recursive technique, an initial process is started that in turn calls another instance of itself. The called instances of the process can then also call other instances of the process, etc. In FIG. 5, the recursive call is shown as a dashed line.

[0112] The initial process makes a first permissible modification of a VLC for a block in step 501. A modification of a VLC is permissible if it meets the criteria for quantization level and any other requirements established for modifications to VLCs. Then, in step 502, the process checks to see if the net change in length of the modified VLCs for the block is zero. If the net change (including changes from modifications in any calling recursive processes) is zero, a possible alt-block has been found. The possible alt-block is added to a list of possible alt-blocks in step 503. If the net change is not zero, the change is noted in step 504.

[0113] The process recursively calls another instance of itself in step 507, passing on the net change up to that point. The recursively called process starts from the next possible modification of a VLC for the block. This next modification might be another modification of the first or current VLC or a modification of the next VLC.

[0114] The processes continue to make recursive calls until the end of the block is reached. When the end of the block is reached by one of the processes, flow for that process is diverted by step 505 to step 506, where the recursive process returns. At this point, the process that called the returning process continues at step 508, where a next permissible modification of the VLCs in the block is made. This entire recursive process continues until the initial process reaches the end of the block.

[0115] An example is useful for understanding the foregoing recursive process. In this example, only two changes are tried for each of three VLCs for a block. In order to simplify the example, all modifications are assumed to be permissible. These changes are denoted A+1, A-1, B+1, B-1, C+1, and C-1. In this example, the following orders of VLC modifications are checked for net length changes of zero: (A+1), (A+1, B+1), (A+1, B+1, C+1), (A+1, B+1, C-1), (A+1, B-1), (A+1, B-1, C+1), (A+1, B-1, C-1), (A+1, C+1), (A+1, C-1), (A-1), (A-1, B+1), (A-1, B+1, C+1), (A-1, B+1, C-1), (A-1, B-1), (A-1, B-1, C+1), (A-1, B-1, C-1), (A-1, C+1), (A-1, C-1), (B+1), (B+1, C+1), (B+1, C-1), (B-1), (B-1, C+1), (B-1, C-1), (C+1), and (C-1).

[0116] The recursive technique of FIG. 5 can be used to find all possible alt-blocks for a given block. However, in alternative embodiments, the technique could be stopped once a certain number of possible alt-blocks have been found, or even once a single alt-block has been found. If more than one possible alt-block has been found, one or more alt-blocks could be selected from the possible alt-blocks, for example pseudorandomly. Other variations are possible and remain within the scope of the invention.

[0117] 2. Fingerprinting

[0118] Returning to FIG. 4, fingerprinting is performed in step 403. Fingerprinting is the process of actually making some of the alterations at the selected locations in order to embed information in the digital content. In the MPEG context, alterations are made by using alt-blocks in place of some original blocks.

[0119] If one alt-block is found for a block, that alt-block can be used to embed one bit at that location. For example, once the set of locations and possible alterations are defined, a "0" can be embedded at a location by using an original block at that location, and a "1" can be embedded by using an alt-block at the location. Other schemes for embedding the data also can be used.

[0120] Furthermore, if more than one alt-block is found for a block at a selected location, those alt-blocks can be used to embed more than one bit at that location. For example, the original block could represent "00," a first alt-block could represent "01," a second alt-block could represent "10," and a third alt-block could represent "11." Again, other schemes for using multiple alt-blocks are possible.

[0121] In step 403, information (i.e., bits) are embedded in the digital content by substituting alt-blocks for original blocks at some of the selected locations in the digital content. Preferably, only a subset of the locations are subject to change at each of plural different points in distribution of the digital content. For example, a first subset can be subject to change at primary caches 112, a second subset can be subject to change at intermediate caches 113, a third subset can be subject to change at leaf caches 114, etc. Typically, not all of the locations in each subset will be altered because at least some "0s" (or other values depending on the coding scheme) will be embedded at the available locations.

[0122] 3. Extracting Fingerprint Information

[0123] Fingerprinting is only meaningful if the embedded information can be extracted. FIG. 6 shows a flow diagram of a method for extracting embedded information from a fingerprint in digital content. The data can be extracted at computing device that can perform the steps shown in FIG. 6. Such a computing device preferably includes at least a processor and a memory for storing the digital content and for storing instructions for performing the steps.

[0124] In step 601, a watermark for a specific item of digital content is determined. This watermark includes a set of locations and possible alterations (e.g., alt-blocks) at those locations for the specific item of digital content.

[0125] The watermark itself preferably is not included with digital content that is distributed to end users. Therefore, the watermark preferably is retrieved from injection point 120 based on identifying information about the digital content. Examples of such identifying information include the content's title, revision number, serial number, and the like.

[0126] The identifying information preferably is itself embedded in the digital content in some robust fashion or is self-evident from the digital content. For example, in the case of an MPEG encoded movie, the identifying information could be the title of the movie, which would be self-evident from the content of the movie. Other identifying information can be utilized.

[0127] Once the watermark is retrieved, the selected locations for embedding information defined by the watermark can be examined in step 602. The locations are examined so as to determine which of the locations have been altered in accordance with the possible alterations specified by the watermark.

[0128] Next, in step 603, the embedded information can be extracted from an examination of which alterations (e.g., alt-blocks) are or are not present. For example, alterations that are present can represent digital "1s," and alterations that are not present can represent digital "0s." Other encoding schemes can be used without departing from the invention.

[0129] Preferably, each embedded bit of information is embedded many times in the digital content. Thus, loss or corruption of the alterations at some of the locations will not result in loss of embedded information.

[0130] In addition, the order of the locations in the digital content preferably is related to the order of bits in the embedded information in some known but random (or pseudorandom) fashion. This scrambling of the embedded information helps prevent unauthorized access to or corruption of the embedded information.

[0131] The digital content that is being examined might have been altered, either intentionally or unintentionally. As a result, any given block in the digital content might not exactly match either an original block or an alt-block from the content's watermark. In order to address this issue, the distance of each block from the corresponding original block in some vector space, for example a vector space of DCT coefficients derived from VLCs, could be calculated. Then, blocks that are within some distance of an original block or an alt-block could be deemed to match those blocks. If each bit of embedded data is embedded multiple times, enough bits are likely to be extracted in order to calculate the embedded data.

[0132] The following other related applications discuss various techniques for utilizing the watermarking and fingerprinting techniques discussed herein, including further details on how embedded information is organized in the

digital content. Each of these applications also is hereby incorporated by reference as if fully set forth herein:

[0133] U.S. provisional application 60/394,630, filed Jul. 9, 2002, in the name of inventors Michael A Malcolm, Stephen Watson, Daniel A Collens, and Kevin Hui, attorney docket number 217.1001.01, titled “Watermarking and Fingerprinting a Movie for Secure Distribution.”

[0134] U.S. provisional application 60/394,922, filed Jul. 9, 2002, in the name of inventors Michael A Malcolm, Stephen Watson, and Daniel A Collens, attorney docket number 217.1002.01, titled “System Architecture of a System for Secure Distribution of Media.”

[0135] U.S. provisional application 60/394,588, filed Jul. 9, 2002, in the name of inventors Michael A Malcolm and Daniel A Collens, attorney docket number 217.1003.01, titled “Topology of Caching Nodes in a System for Secure Delivery of Media Content.”

[0136] U.S. provisional patent application 60/444,012, filed Jan. 31, 2003, in the name of Michael Malcolm, Stephen Watson, and Daniel Collens, attorney docket number 217.1015.01, titled “Watermarking and Fingerprinting a Movie for Secure Distribution.”

[0137] U.S. patent application Ser. No. 10/356,692, filed Jan. 31, 2003, in the name of inventors Daniel Collens, Stephen Watson, and Michael Malcom, attorney docket number 217.1004.01, titled “Parallel Distribution and Fingerprinting of Digital Content.”

[0138] Generality of the Invention

[0139] The generation of alt-blocks is not dependent upon the type of encoding used for the digital content. In a general sense, the watermarking and fingerprinting techniques of the invention can be applied to any digital data that models a continuous or analog physical process. The invention can be applied to digitized audio data, measurement data, video data, other multimedia data, and the like, whether encoded by MPEG, some variation of MPEG that may or may not use Huffman coding, or some other entirely different encoding scheme. With any of this digitized data, the techniques of the invention can be used to select locations in the digital content and to select possible alterations to make at the selected locations so as to embed data, all while preserving packetization of the data.

[0140] Furthermore, the invention is useful for, and has sufficient generality for, applications other than distribution of media streams, and other than distribution of digital content. For example, the invention is also generally useful for applications in which security of datasets or identifying recipients of those datasets is desired.

[0141] Thus, although preferred embodiments are disclosed herein, many variations are possible which remain within the concept, scope, and spirit of the invention. These variations would become clear to those skilled in the art after perusal of this application.

What is claimed is:

1. A computer-implemented method, comprising:

determining, for digital content, a watermark including locations and alternate blocks, at the locations for embedding data, wherein replacement of an original block with an alternate block embeds more than zero bits of the data in the digital content;

based at least in part on the alternate blocks, determining actual alterations in the digital content; and

based at least in part on the actual alterations in the digital content, extracting bits from the digital content,

wherein the alternate blocks contain two or more alterations, wherein the alterations if made individually result in a changed block length for the original block, but each alternate block has the same block length as the corresponding original block.

2. The method of claim 1, wherein the alternate blocks preserve packetization of the digital content.

3. The method of claim 1, wherein the determining actual alterations in the digital content includes identifying at least one alteration that individually would change the length of a packet.

4. A device, comprising:

a network interface over which digital content can be injected into a network;

a processor;

a memory storing the digital content and storing instructions executable by the processor, the instructions when executed cause the processor to:

(a) select locations in the digital content for embedding data; and

(b) select alternate blocks to replace original blocks at the selected locations, wherein replacement of an original block with an alternate block embeds more than zero bits of the data in the digital content, and wherein the locations and the alternate blocks together form a watermark for the digital content,

wherein the alternate blocks contain two or more alterations, wherein the alterations if made individually result in a changed block length for the original block, but each alternate block has the same block length as the corresponding original block.

5. The device of claim 4, wherein the alternate blocks preserve packetization of the digital content.

6. The device of claim 4, wherein the digital content is encoded using variable length codes, and wherein at least one alternate block uses different variable length codes than the corresponding original block.

7. The device of claim 4, wherein each alternate block does not change the presentation of the corresponding original block by more than a predefined amount.

8. The device of claim 7, wherein the predefined amount is based at least in part on a maximum level change and a maximum quantization scale.

9. The device of claim 8, wherein the maximum level change is plus or minus one, and wherein the maximum quantization scale is twenty-four.

10. A computer readable medium storing instructions executable by a processor, the instructions when executed cause to the processor to:

accept data corresponding to digital content;

accept watermark data, wherein the watermark data includes locations within the digital content, and wherein the watermark data includes alternate blocks at the locations of the digital content; and

based on at least a portion of the watermark data, alter the digital content,

wherein the alternate blocks contain two or more alterations, wherein the alterations if made individually result in a changed block length for the original block, but each alternate block has the same block length as the corresponding original block.

* * * * *