PCT WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 7 : H04N 7/167 — A1

(11) International Publication Number: **WO 00/57643**

(43) International Publication Date: 28 September 2000 (28.09.00)

(21) International Application Number: PCT/US00/06522

(22) International Filing Date: 14 March 2000 (14.03.00)

(30) Priority Data:
60/125,990 24 March 1999 (24.03.99) US

(71) Applicant *(for all designated States except US)*: BLUE SPIKE, INC. [US/US]; 16711 Collins Avenue, Miami, FL 33160 (US).

(72) Inventors; and
(75) Inventors/Applicants *(for US only)*: MOSKOWITZ, Scott, A. [US/US]; 16711 Collins Avenue, Miami, FL 33160 (US). BERRY, Michael [US/US]; 12401 Princess Jeanne, Albuquerque, NM 87112 (US).

(74) Agents: CHAPMAN, Floyd, B. et al.; Baker Botts, L.L.P., 1299 Pennsylvania Avenue, N.W., Washington, DC 20004 (US).

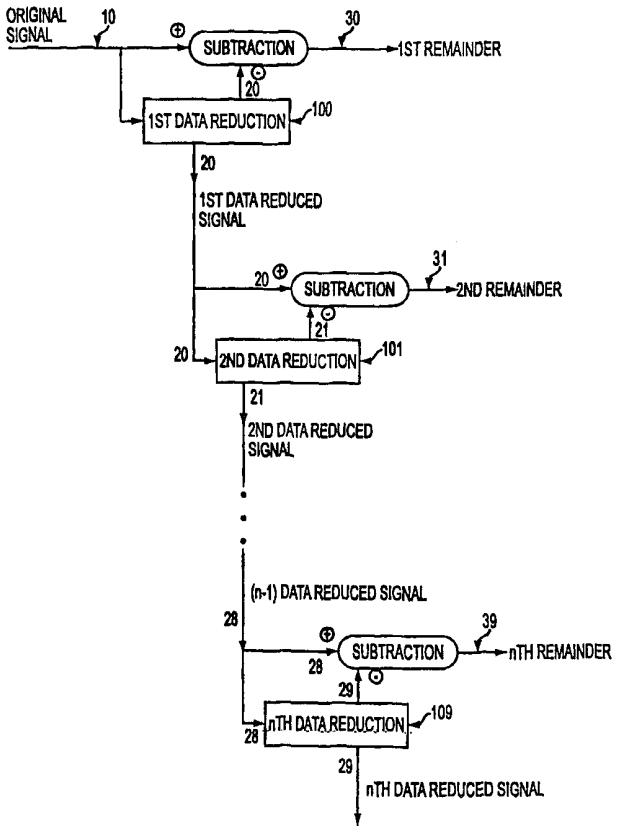
(81) Designated States: JP, US, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.
Before the expiration of the time limit for amending the claims and to be republished in the event of the receipt of amendments.

(54) Title: UTILIZING DATA REDUCTION IN STEGANOGRAPHIC AND CRYPTOGRAPHIC SYSTEMS

(57) Abstract

The present invention is a method for protecting a data signal where the method comprises the following steps: applying a data reduction technique (200) to the signal to produce a reduced signal, subtracting (60) the reduced data signal from the original signal to produce a remainder signal (39), embedding (300) a first watermark into the reduced data signal to produce a watermarked redued data signal, and adding (50) the watermarked reduced signal to the remainder signal to produce an output signal (90). A second watermark (301) may be embedded into the remainder signal (39) before the final addition (50) step. Cryptographic techniques may be employed to encrypt the remainder signal and/or the reduced signal prior to the addition step (50).



FOR THE PURPOSES OF INFORMATION ONLY

Codes used to identify States party to the PCT on the front pages of pamphlets publishing international applications under the PCT.

AL	Albania	**ES**	Spain	**LS**	Lesotho	**SI**	Slovenia
AM	Armenia	**FI**	Finland	**LT**	Lithuania	**SK**	Slovakia
AT	Austria	**FR**	France	**LU**	Luxembourg	**SN**	Senegal
AU	Australia	**GA**	Gabon	**LV**	Latvia	**SZ**	Swaziland
AZ	Azerbaijan	**GB**	United Kingdom	**MC**	Monaco	**TD**	Chad
BA	Bosnia and Herzegovina	**GE**	Georgia	**MD**	Republic of Moldova	**TG**	Togo
BB	Barbados	**GH**	Ghana	**MG**	Madagascar	**TJ**	Tajikistan
BE	Belgium	**GN**	Guinea	**MK**	The former Yugoslav Republic of Macedonia	**TM**	Turkmenistan
BF	Burkina Faso	**GR**	Greece			**TR**	Turkey
BG	Bulgaria	**HU**	Hungary	**ML**	Mali	**TT**	Trinidad and Tobago
BJ	Benin	**IE**	Ireland	**MN**	Mongolia	**UA**	Ukraine
BR	Brazil	**IL**	Israel	**MR**	Mauritania	**UG**	Uganda
BY	Belarus	**IS**	Iceland	**MW**	Malawi	**US**	United States of America
CA	Canada	**IT**	Italy	**MX**	Mexico	**UZ**	Uzbekistan
CF	Central African Republic	**JP**	Japan	**NE**	Niger	**VN**	Viet Nam
CG	Congo	**KE**	Kenya	**NL**	Netherlands	**YU**	Yugoslavia
CH	Switzerland	**KG**	Kyrgyzstan	**NO**	Norway	**ZW**	Zimbabwe
CI	Côte d'Ivoire	**KP**	Democratic People's Republic of Korea	**NZ**	New Zealand		
CM	Cameroon			**PL**	Poland		
CN	China	**KR**	Republic of Korea	**PT**	Portugal		
CU	Cuba	**KZ**	Kazakstan	**RO**	Romania		
CZ	Czech Republic	**LC**	Saint Lucia	**RU**	Russian Federation		
DE	Germany	**LI**	Liechtenstein	**SD**	Sudan		
DK	Denmark	**LK**	Sri Lanka	**SE**	Sweden		
EE	Estonia	**LR**	Liberia	**SG**	Singapore		

UTILIZING DATA REDUCTION IN STEGANOGRAPHIC AND CRYPTOGRAPHIC SYSTEMS

FIELD OF INVENTION

This invention relates to digital signal processing, and more particularly to a method and a system for encoding at least one digital watermark into a signal as a means of conveying information relating to the signal and also protecting against unauthorized manipulation of the signal.

BACKGROUND OF INVENTION

Digital watermarks help to authenticate the content of digitized multimedia information, and can also discourage piracy. Because piracy is clearly a disincentive to the digital distribution of copyrighted content, establishment of responsibility for copies and derivative copies of such works is invaluable. In considering the various forms of multimedia content, whether "master," stereo, NTSC video, audio tape or compact disc, tolerance of quality will vary with individuals and affect the underlying commercial and aesthetic value of the content. It is desirable to tie copyrights, ownership rights, purchaser information or some combination of these and related data into the content in such a manner that the content must undergo damage, and therefore reduction of its value, with subsequent, unauthorized distribution, commercial or otherwise. Digital watermarks address many of these concerns.

A matter of general weakness in digital watermark technology relates directly to the manner of implementation of the watermark. Many approaches to digital watermarking leave detection and decode control with the implementing party of the digital watermark, not the creator of the work to be protected. This weakness removes proper economic incentives for improvement of the technology. One specific form of exploitation mostly regards efforts to obscure subsequent watermark detection. Others regard successful over encoding using the same watermarking process at a subsequent time. Yet another way to perform secure digital watermark implementation is through "key-based" approaches.

This paper draws a distinction between a "forensic watermark," based on provably-secure methods, and a "copy control" or "universal" watermark which is intended to be low cost and easily implemented into any general computing or consumer electronic device. A watermark can be forensic if it can identify the source of the data from which a copy was made. For example, assume that digital data are stored on a disk and provided to "Company A" (the "A disk"). Company A makes an unauthorized copy and delivers the copy to "Company B" (the "B disk"). A forensic watermark, if present in the digital data stored on the "A disk," would identify the "B disk" as having been copied from the "A disk."

On the other hand, a copy control or universal watermark is an embedded signal which is governed by a "key" which may be changed (a "session key") to increase security, or one that is easily accessible to devices that may offer less than strict cryptographic security. The "universal" nature of the watermark is the computationally inexpensive means for accessing or other associating the watermark with operations that can include playback, recording or manipulations of the media in which it is embedded.

A fundamental difference is that the universality of a copy control mechanism, which must be redundant enough to survive many signal manipulations to eliminate most casual piracy, is at odds with the far greater problem of establishing responsibility for a given instance of a suspected copying of a copyrighted media work. The more dedicated pirates must be dealt with by encouraging 3rd party authentication with "forensic watermarks" or those that constitute "transactional watermarks" (which are encoded in a given copy of said content to be watermarked as per the given transaction).

The goal of a digital watermark system is to insert a given information signal or signals in such a manner as to leave little or no evidence of the presence of the information signal in the underlying content signal. A separate but equal goal is maximizing the digital watermark's encoding level and "location sensitivity" in the underlying content signal such that the watermark cannot be removed without damage to the content signal.

One means of implementing a digital watermark is to use key-based security. A predetermined or random key can be generated as a map to access the hidden information signal. A key pair may also be used. With a typical key pair, a party possesses a public and a private key. The private key is maintained in confidence by the owner of the key, while the owner's public key is disseminated to those persons in the public with whom the owner would regularly communicate. Messages being communicated, for example by the owner to another, are encrypted with the private key and can only be read by another person who possesses the corresponding public key. Similarly, a message encrypted with the person's public key can only be decrypted with the corresponding private key. Of course, the keys or key pairs may be processed in separate software or hardware devices handling the watermarked data.

SUMMARY OF THE INVENTION

A method of securing a data signal comprises the steps of: applying a data reduction technique to reduce the data signal into a reduced data signal; subtracting said reduced data signal from the data signal to produce a remainder signal; using a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal; using a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal; and adding said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal.

A system for securing a data signal comprises: means to apply a data reduction technique to reduce the data signal into a reduced data signal; means to subtract said reduced data signal from the data signal to produce a remainder signal; means to apply a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal; means to apply a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal; and means to add said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal.

A method of securing a data signal comprises the steps of: applying a data reduction technique to reduce the data signal into a reduced data signal; subtracting said reduced data signal from the data signal to produce a remainder signal; embedding a first watermark into said reduced data signal to produce a watermarked, reduced data signal; embedding a second watermark into said remainder signal to produce a watermarked remainder signal; and adding said watermarked, reduced data signal to said watermarked remainder signal to produce an output signal.

A method of protecting a data signal comprises: applying a data reduction technique to reduce the data signal into a reduced data signal; subtracting said reduced data signal from the data signal to produce a remainder signal; using a first scrambling technique to scramble said reduced data signal to produce a scrambled, reduced data signal; using a second scrambling technique to scramble said remainder signal to produce a scrambled remainder signal; and adding said scrambled, reduced data signal to said scrambled remainder signal to produce an output signal.

There are two design goals in an overall digital watermarking system's low cost, and universality. Ideally, a method for encoding and decoding digital watermarks in digitized media for copy control purposes should be inexpensive and universal. This is essential in preventing casual piracy. On the other hand, a more secure form of protection, such as a "forensic watermarks," can afford to be computationally intensive to decode, but must be unaffected by repeated re-encoding of a copy control watermark. An ideal method for achieving these results would separate the signal into different areas, each of which can be accessed independently. The embedded signal or may simply be "watermark bits" or "executable binary code," depending on the application and type of security sought. Improvements to separation have been made possible by enhancing more of the underlying design to meet a number of clearly problematic issues. The present invention interprets the signal as a stream which may be split into separate streams of digitized samples or may undergo data reduction (including both lossy and lossless compression, such as MPEG lossy compression and Meridian's lossless compression, down sampling, common to many studio operations, or any

related data reduction process). The stream of data can be digital in nature, or may also be an analog waveform (such as an image, audio, video, or multimedia content). One example of digital data is executable binary code. When applied to computer code, the present invention allows for more efficient, secure, copyright protection when handling functionality and associations with predetermined keys and key pairs in software applications or the machine readable versions of such code in microchips and hardware devices. Text may also be a candidate for authentication or higher levels of security when coupled with secure key exchange or asymmetric key generation between parties. The subsets of the data stream combine meaningful and meaningless bits of data which may be mapped or transferred depending on the application intended by the implementing party.

The present invention utilizes data reduction to allow better performance in watermarking as well as cryptographic methods concerning binary executable code, its machine readable form, text and other functionality-based or communication-related applications. Some differences may simply be in the structure of the key itself, a pseudo random or random number string or one which also includes additional security with special one way functions or signatures saved to the key. The key may also be made into key pairs, as is discussed in other disclosures and patents referenced herein. The present invention contemplates watermarks as a plurality of digitized sample streams, even if the digitized streams originate from the analog waveform itself. The present invention also contemplates that the methods disclosed herein can be applied to non-digitized content. Universally, data reduction adheres to some means of "understanding "the reduction. This disclosure looks at data reduction which may include down sampling, lossy compression, summarization or any means of data reduction as a novel means to speed up watermarking encode and decode operations. Essentially a lossy method for data reduction yields the best results for encode and decode operations.

It is desirable to have both copy control and forensic watermarks in the same signal to address the needs of the hardware, computer, and software industries while

also providing for appropriate security to the owners of the copyrights. This will become clearer with further explanation of the sample embodiments discussed herein.

The present invention also contemplates the use of data reduction for purposes of speedier and more tiered forms of security, including combinations of these methods with transfer function functions. In many applications, transfer functions (e.g., scrambling), rather than mapping functions (e.g., watermarking), are preferable or can be used in conjunction with mapping. With "scrambling," predetermined keys are associated with transfer functions instead of mapping functions, although those skilled in the art may recognize that a transfer function is simply a subset of mask sets encompassing mapping functions. It is possible that tiered scrambling with data reduction or combinations of tiered data reduction with watermarking and scrambling may indeed increase overall security to many applications.

The use of data reduction can improve the security of both scrambling and watermarking applications. All data reduction methods include coefficients which affect the reduction process. For example, when a digital signal with a time or space component is down sampled, the coefficient would be the ratio of the new sample rate to the original sample rate. Any coefficients that are used in the data reduction can be randomized using the key, or key pair, making the system more resistant to analysis. Association to a predetermined key or key pair and additional measure of security may include biometric devices, tamper proofing of any device utilizing the invention, or other security measures.

Tests have shown that the use of data reduction in connection with digital watermarking schemes significantly reduces the time required to decode the watermarks, permitting increases in operational efficiency.

Particular implementations of the present invention, which have yielded incredibly fast and inexpensive digital watermarking systems, will now be described. These systems may be easily adapted to consumer electronic devices, general purpose computers, software and hardware. The exchange of predetermined keys or key pairs may facilitate a given level of security. Additionally, the complementary increase in

security for those implementations where transfer functions are used to "scramble" data, is also disclosed.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the invention and some advantages thereof, reference is now made to the following descriptions taken in connection with the accompanying drawings in which:

FIG. 1 is a functional block diagram that shows a signal processing system that generates "n" remainder signals and "n" data reduced signals.

FIG. 2 is a functional block diagram for an embodiment of the present invention which illustrates the generation of an output signal comprised of a data-reduced, watermarked signal and a first remainder signal.

FIG. 3 is a functional block diagram for an embodiment of the present invention which illustrates the generation of an output signal comprised of a data-reduced, watermarked signal and a watermarked, first remainder signal.

FIG. 4 is a functional block diagram for decoding the output signal generated by the system illustrated in FIG. 2.

FIG. 5 is a functional block diagram for decoding the output signal generated by the system illustrated in FIG. 3.

FIG. 6 is a functional block diagram for an embodiment of the present invention which illustrates the generation of an output signal comprised of a data-reduced, scrambled signal and a first remainder signal.

FIG. 7 is a functional block diagram for an embodiment of the present invention which illustrates the generation of an output signal comprised of a data--reduced, scrambled signal and a scrambled, first remainder signal.

FIG. 8 is a functional block diagram for decoding the output signal generated by the system illustrated in FIG. 6.

FIG. 9 is a functional block diagram for decoding the output signal generated by the system illustrated in FIG. 7.

DETAILED DESCRIPTION

The embodiments of the present invention and its advantages are best understood by referring to the drawings, like numerals being used for like and corresponding parts of the various drawings.

An Overview

A system for achieving multiple levels of data reduction is illustrated in FIG. 1. An input signal 10 (for example, instructional text, executable binary computer code, images, audio, video, multimedia or even virtual reality imaging) is subjected to a first data reduction technique 100 to generate a first data reduced signal 20. First data reduced signal 20 is then subtracted from input signal 10 to generate a first remainder signal 30.

First data reduced signal 20 is subjected to a second data reduction technique 101 to generate a second data reduced signal 21. Second data reduced signal 21 is then subtracted from first data reduced signal 20 to generate a second remainder signal 31.

Each of the successive data reduced signals is, in turn, subjected to data reduction techniques to generate a further data reduced signal, which, in turn, is subtracted from its respective parent signal to generate another remainder signal. This process is generically described as follows. An (n-1) data reduced signal 28 (i.e, a signal that has been data reduced n-1 times) is subjected to an nth data reduction technique 109 to generate an nth data reduced signal 29. The nth data reduced signal 29 is then subtracted from the (n-1) data reduced signal 28 to produce an n^{th} remainder signal 39.

An output signal can be generated from the system illustrated in FIG. 1 in numerous ways. For example, each of the n remainder signals (which, through represented by reference numerals 30-39, are not intended to be limited to 10 signals) and the n^{th} data signal may optionally subjected to a watermarking technique, or even optionally subjected to a encryption technique, and each of the (n+1) signals (whether

watermarked or encrypted, or otherwise untouched) may then be added together to form an output signal. By way of more particular examples, each of the (n+1) signals (i.e., the n remainder signals and the n^{th} data reduced signal) can be added together without any encryption or watermarking to form an output signal; or one or more of the (n+1) signals may be watermarked and then all (n+1) signals may be added together; or one or more of the (n+1) signals may be encrypted and then all (n+1) signals may be added together. It is anticipated that between these three extremes lie numerous hybrid combinations involving one or more encryptions and one or more watermarkings.

Each level may be used to represent a particular data density. E.g., if the reduction method is down-sampling, for a DVD audio signal the first row would represent data sampled at 96 kHz, the second at 44.1 kHz., the third at 6 kHz., etc. There is only an issue of deciding what performance or security needs are contemplated when undertaking the data reduction process and choice of which types of keys or key pairs should be associated with the signal or data to be reduced. Further security can be increased by including block ciphers, special one way functions, one time stamps or even biometric devices in the software or hardware devices that can be embodied. Passwords or biometric data are able to assist in the determination of the identity of the user or owner of the data, or some relevant identifying information.

An example of a real world application is helpful here. Given the predominant concern, at present, of MPEG 1 Layer 3, or MP3, a perceptual lossy compression audio data format, which has contributed to a dramatic re-evaluation of the distribution of music, a digital watermark system must be able to handle casual and more dedicated piracy in a consistent manner. The present invention contemplates compatibility with MP3, as well as any perceptual coding technique that is technically similar. One issue, is to enable a universal copy control "key" detect a watermark as quickly as possible from a huge range of perceptual quality measures. For instance, DVD 24 bit 96 kHz, encoded watermarks, should be detected in at least "real time," even after the signal has been down sampled, to say 12 kHz of the 96 kHz originally referenced. By delineating and starting with less data, since the data-reduced signal is obviously smaller though

still related perceptually to the original DVD signal, dramatic increases in the speed and survival of the universal copy control bits can be achieved. The present invention also permits the ability to separate any other bits which may be associated with other more secure predetermined keys or key pairs.

Where the data stream is executable computer code, the present invention contemplates breaking the code into objects or similar units of functionality and allowing for determination of what is functionally important. This may be more apparent to the developer or users of the software or related hardware device. Data reduction through the use of a subset of the functional objects related to the overall functionality of the software or executable code in hardware or microchips, increase the copyright protection or security sought, based on reducing the overall data to be associated with predetermined keys or key pairs. Similarly, instead of mapping functions, transfer functions, so-called "scrambling," appear better candidates for this type of security although both mapping and transferring may be used in the same system. By layering the security, the associated keys and key pairs can be used to substantially improve the security and to offer easier methods for changing which functional "pieces" of executable computer code are associated with which predetermined keys. These keys may take the form of time-sensitive session keys, as with transactions or identification cards, or more sophisticated asymmetric public key pairs which may be changed periodically to ensure the security of the parties' private keys. These keys may also be associated with passwords or biometric applications to further increase the overall security of any potential implementation.

An example for text message exchange is less sophisticated but, if it is a time sensitive event, e.g., a secure communication between two persons, benefits may also be encountered here. Security may also be sought in military communications. The ability to associate the securely exchanged keys or key pairs while performing data reduction to enhance the detection or decoding performance, while not compromising the level of security, is important. Though a steganographic approach to security, the present invention more particularly addresses the ability to have data reduction to

increase speed, security, and performance of a given steganographic system. Additionally, data reduction affords a more layered approach when associating individual keys or key pairs with individual watermark bits, or digital signature bits, which may not be possible without reduction because of considerations of time or the payload of what can be carried by the overall data "covertext" being transmitted.

Layering through data reduction offers many advantages to those who seek privacy and copyright protection. Serialization of the detection chips or software would allow for more secure and less "universal" keys, but the interests of the copyright owners are not always aligned with those of hardware or software providers. Similarly, privacy concerns limit the amount of watermarking that can be achieved for any given application. The addition of a pre-determined and cryptographic key-based "forensic" watermark, in software or hardware, allows for 3rd party authentication and provides protection against more sophisticated attacks on the copy control bits. Creating a "key pair" from the "predetermined" key is also possible.

Separation of the watermarks also relates to separate design goals. A copy control mechanism should ideally be inexpensive and easily implemented, for example, a form of "streamed watermark detection." Separating the watermark also may assist more consistent application in broadcast monitoring efforts which are time-sensitive and ideally optimized for quick detection of watermarks. In some methods, the structure of the key itself, in addition to the design of the "copy control" watermark, will allow for few false positive results when seeking to monitor radio, television, or other streamed broadcasts (including, for example, Internet) of copyrighted material. As well, inadvertent tampering with the embedded signal proposed by others in the field can be avoided more satisfactorily. Simply, a universal copy control watermark may be universal in consumer electronic and general computing software and hardware implementations, but less universal when the key structure is changed to assist in being able to log streaming, performance, or downloads, of copyrighted content. The embedded bits may actually be paired with keys in a decode device to assure accurate broadcast monitoring and tamper proofing, while not requiring a watermark to exceed

the payload available in an inaudible embedding process. E.g., A full identification of the song, versus time-based digital signature bits, embedded into a broadcast signal, may not be recovered or may be easily over encoded without the use of block ciphers, special one way functions or one time pads, during the encoding process, prior to broadcast. Data reduction as herein disclosed makes this operation more efficient at higher speeds.

A forensic watermark is not time sensitive, is file-based, and does not require the same speed demands as a streamed or broadcast-based detection mechanism for copy control use. Indeed, a forensic watermark detection process may require additional tools to aid in ensuring that the signal to be analyzed is in appropriate scale or size, ensuring signal characteristics and heuristic methods help in appropriate recovery of the digital watermark. Simply, all aspects of the underlying content signal should be considered in the embedding process because the watermarking process must take into account all such aspects, including for example, any dimensional or size of the underlying content signal. The dimensions of the content signal may be saved with the key or key pair, without enabling reproduction of the unwatermarked signal. Heuristic methods may be used to ensure the signal is in proper dimensions for a thorough and accurate detection authentication and retrieval of the embedded watermark bits. Data reduction can assist in increasing operations of this nature as well, since the data reduction process may include information about the original signal, for example, signal characteristics, signal abstracts, differences between samples, signal patterns, and related work in restoring any given analog waveform.

The present invention provides benefits, not only because of the key-based approach to the watermarking, but the vast increase in performance and security afforded the implementations of the present invention over the performance of other systems.

The architecture of key and key-pair based watermarking is superior to statistical approaches for watermark detection because the first method meets an evidentiary level of quality and are mathematically provable. By incorporating a level

of data reduction, key and key paired based watermarking is further improved. Such levels of security are plainly necessary if digital watermarks are expected to establish responsibility for copies of copyrighted works in evidentiary proceedings. More sophisticated measures of trust are necessary for use in areas which exceed the scope of copyright but are more factually based in legal proceedings. These areas may include text authentication or software protection (extending into the realm of securing microchip designs and compiled hardware as well) in the examples provided above and are not contemplated by any disclosure or work in the art.

The present invention may be implemented with a variety of cryptographic protocols to increase both confidence and security in the underlying system. A predetermined key is described as a set of masks: a plurality of mask sets. These masks may include primary, convolution and message delimiters but may extend into additional domains. In previous disclosures, the functionality of these masks is defined solely for mapping. Public and private keys may be used as key pairs to further increase the unlikeliness that a key may be compromised. Examples of public key cryptosystems may be found in the following U.S. Patents Nos: 4,200,770; 4,218,582; 4,405,829; and 4,424,414, which examples are incorporated herein by reference. Prior to encoding, the masks described above are generated by a cryptographically secure random generation process. Mask sets may be limited only by the number of dimensions and amount of error correction or concealment sought, as has been previously disclosed.

A block cipher, such as DES, in combination with a sufficiently random seed value emulates a cryptographically secure random bit generator. These keys, or key pairs, will be saved along with information matching them to the sample stream in question in a database for use in subsequent detection or decode operation. These same cryptographic protocols may be combined with the embodiments of the present invention in administering streamed content that requires authorized keys to correctly display or play said streamed content in an unscrambled manner. As with digital watermarking, symmetric or asymmetric public key pairs may be used in a variety of

implementations. Additionally, the need for certification authorities to maintain authentic key-pairs becomes a consideration for greater security beyond symmetric key implementations, where transmission security is a concern.

Signal Processing in a Multi-watermark System (A Plurality of Streams May Be Watermarked)

FIG. 2 illustrates a system and method of implementing a multiple-watermark system. An input signal 11 (e.g., binary executable code, instruction text. or other data), is first processed by a lossy data-reduction scheme 200 (e.g., down-sampling, bit-rate reduction, or compression method) to produced a data-reduced signal 40. Data-reduced signal 40 is then embedded with a watermark (process step 300) to generate a watermarked, data-reduced signal 50, while a copy of the unmarked, data-reduced signal 40 is saved.

The saved, unwatermarked data-reduced signal (signal 40) is subtracted from the original input signal 11, yielding a remainder signal 60 composed only of the data that was lost during the data-reduction. A second watermark is then applied (process step 301) to remainder signal 60 to generate a watermarked remainder signal 70. Finally, the watermarked remainder 70 and the watermarked, data-reduced signal 50 are added to form an output signal 80, which is the final, full-bandwidth, output signal.

The two watermarking techniques (process steps 300 and 301) may be identical (i.e., be functionally the same), or they may be different.

To decode the signal, a specific watermark is targeted. Duplicating the data-reduction processes that created the watermark in some cases can be used to recover the signal that was watermarked. Depending upon the data-reduction method, it may or may not be necessary to duplicate the data-reduction process in order to read a watermark embedded in a remainder signal. Because of the data-reduction, the decoding search can occur much faster than it would in a full-bandwidth signal. Detection speed of the remainder watermark remains the same as if there were no other watermark present.

FIG. 4 illustrates a functional block diagram for one means of decoding the output signal generated by the system illustrated in FIG. 2. A signal to be analyzed 80 (e.g., the same output from FIG. 2) is processed by a data-reduction scheme 200. Data reduced signal 41 can then be decoded to remove the message that was watermarked in the original data reduced signal. Further, data reduced signal 41 can be subtracted from signal to be analyzed 80 to form a differential signal 61 which can then be decoded to remove the message that was watermarked in the original remainder signal. A decoder may only be able to perform one of the two decodings. Differential access and/or different keys may be necessary for each decoding.

Additionally, the watermarking described in connection with this embodiment above may be done with a plurality of predetermined keys or key pairs associated with a single watermark "message bit," code object, or text.

Signal Processing in a Single Watermark System

FIG. 3 illustrates a system and method of implementing a single watermark system. The process and system contemplated here is identical to process described in connection to FIG. 2, above, except that no watermark is embedded in the remainder signal. Hence, the watermarked, data-reduced signal 50 is added directly to the remainder signal 60 to generate an output signal 90. Additionally, the watermarking described in connection with this embodiment above may be done with a plurality of predetermined keys or key pairs associated with a single watermark "message bit," code object, or text.

In either process, an external key can be used to control the insertion location of either watermark. In a copy-control system, a key is not generally used, whereas in a forensic system, a key must be used. The key can also control the parameters of the data-reduction scheme. The dual scheme can allow a combination of copy-control and forensic watermarks in the same signal. A significant feature is that the copy-control watermark can be read and rewritten without affecting the forensic mark or compromising its security.

FIG. 5 illustrates a functional block diagram for one means of decoding the output signal generated by the system illustrated in FIG. 3. A signal to be analyzed 90 (e.g., the same output from FIG. 3) is processed by a data-reduction scheme 200. Data reduced signal 41 can then be decoded to remove the message that was watermarked in the original data reduced signal.

Signal Processing in a Multi-scrambler System (A Plurality of Streams May Be Scrambled)

FIG. 6 illustrates a system and method of implementing a multi-scrambler system. An input signal 12 (e.g., binary executable code, instruction text. or other data), is first processed by a lossy data-reduction scheme 400 (e.g., down-sampling, bit-rate reduction, or compression method) to produced a data-reduced signal 45. Data-reduced signal 45 is then scrambled using a first scrambling technique (process step 500) to generate a scrambled, data-reduced signal 55, while a copy of the unscrambled, data-reduced signal 45 is saved.

The saved, unscrambled data-reduced signal (signal 45) is subtracted from the original input signal 12, yielding a remainder signal 65 composed only of the data that was lost during the data-reduction. A second scrambling technique is then applied (process step 501) to remainder signal 65 to generate a scrambled remainder signal 75. Finally, the scrambled remainder signal 75 and the scrambled data-reduced signal 55 are added to form an output signal 85, which is the final, full-bandwidth, output signal.

The two scrambling techniques (process steps 500 and 501) may be identical (i.e., be functionally the same), or they may be different.

Additionally the scrambling described in connection with this embodiment may be done with a plurality of predetermined keys or key pairs associated with a single scrambling operation containing only a "message bit," code object, or text.

To decode the signal, unscrambling follows the exact pattern of the scrambling process except that the inverse of the scrambling transfer function is applied to each portion of the data, thus returning it to its pre-scrambled state.

FIG. 8 illustrates a functional block diagram for one means of decoding the output signal generated by the system illustrated in FIG. 6. A signal to be analyzed 85 (e.g., the same output from FIG. 6) is processed by a data-reduction scheme 200. Data reduced signal 46 can be subtracted from signal to be analyzed 85 to form a differential signal 66, which signal can then be descrambled in process 551 using the inverse transfer function of the process that scrambled the original remainder signal (e.g., the inverse of scrambling process 501). Descrambling process 551 generates an descrambled signal 76. Data reduced signal 46 may further be descrambled in process 550 using the inverse transfer function of the process that scrambled the original data reduced signal (e.g., the inverse of scrambling process 500). Descrambling process 550 generates an descrambled signal 56, which may then be added to descrambled signal 76 to form an output signal 98.

Signal Processing in a Single Scrambling Operation

FIG. 7 illustrates a system and method of implementing a single scrambling system. The process and system contemplated here is identical to process described in connection to FIG. 6, above, except that no scrambling is applied to the remainder signal. Hence, the scrambled data-reduced signal 55 is added directly to the remainder signal 65 to generate an output signal 95.

Additionally the scrambling described in connection with this embodiment may be done with a plurality of predetermined keys or key pairs associated with a single scrambling operation containing only a "message bit," code object, or text.

FIG. 9 illustrates a functional block diagram for one means of decoding the output signal generated by the system illustrated in FIG. 7. A signal to be analyzed 95 (e.g., the same output from FIG. 7) is processed by a data-reduction scheme 200. Data reduced signal 46 can be subtracted from signal to be analyzed 95 to form a differential

signal 66. Data reduced signal 46 may further be descrambled in process 550 using the inverse transfer function of the process that scrambled the original data reduced signal (e.g., the inverse of scrambling process 500). Descrambling process 550 generates an descrambled signal 56, which may then be added to differential signal 66 to form an output signal 99.

Sample Embodiment: Combinations

Another embodiment may combine both watermarking and scrambling with data reduction. Speed, performance and computing power may influence the selection of which techniques are to be used. Decisions between data reduction schemes ultimately must be measured against the types of keys or key pairs to use, the way any pseudo random or random number generation is done (chaotic, quantum or other means), and the amount of scrambling or watermarking that is necessary given the needs of the system.

It is quite possible that some derived systems would yield a fairly large decision tree, but the present invention offers many benefits to applications in security that are not disclosed in the art.

Conclusions

Data signals fall into two categories: those which can undergo lossy data reduction and remain functional and those which cannot. Audio, images, video are examples of the first. Computer code is an example of the second. In general, all members of the first category contain an aesthetic component, which may be reduced and/or manipulated during a data reduction, in addition to a functional component which serves to identify the signal. For example, an audio signal may have noise added while still remaining recognizably identifiable as a particular song. However, beyond a certain point, the addition of more noise will cause the signal to become unidentifiable, thus impairing the functional character of the signal. In the absence of

an aesthetic component, as with computer code where every bit of data is necessary, lossy compression that retains functionality is not possible.

Signals in the first category are the only candidates for watermarking. A watermark is a distortion of the aesthetic component, generally of an imperceptible nature. This category will gain speed benefits during the watermark decoding process when a lossy data-reduction method is used as described above.

Scrambling, on the other hand, may be applied to any signal, regardless of its aesthetic component, since it allows for perfect reconstruction of the original signal. A scrambling system can be made more secure by applying a data reduction method prior to scrambling, even if this data reduction makes the intermediate signals non-functional, as is the case with signals in category two.

Data reduction can make both watermarking and scrambling more secure. Data reduction can also speed the decoding process for watermarks. Finally, data reduction can allow natural channelization of watermarks for different purposes.

While the invention has been particularly shown and described in the foregoing detailed description, it will be understood by those skilled in the art that various other changes in form and detail may be made without departing from the spirit and scope of the invention.

WHAT IS CLAIMED IS:

1. A method of securing a data signal comprising:

applying a data reduction technique to reduce the data signal into a reduced data signal;

subtracting said reduced data signal from the data signal to produce a remainder signal;

embedding a first watermark into said reduced data signal to produce a watermarked, reduced data signal;

embedding a second watermark into said remainder signal to produce a watermarked remainder signal; and

adding said watermarked, reduced data signal to said watermarked remainder signal to produce an output signal.

2. The method of claim 1 wherein the step of subtracting is comprised of

storing a copy of the data signal; and

subtracting said reduced data signal from the copy of the data signal to produce a remainder signal.

3. The method of claim 1, wherein at least one of the watermarks is embedded using at least one key.

4. The method of claim 1, wherein at least one of the watermarks is embedded using a key pair.

5. The method of claim 4, wherein one key of the key pair is publicly available while the other key of the key pair is secret.

6. A method of protecting a data signal comprising:

applying a data reduction technique to reduce the data signal into a reduced data signal;

subtracting said reduced data signal from the data signal to produce a remainder signal;

embedding a first watermark into said reduced data signal to produce a watermarked, reduced data signal; and

adding said watermarked, reduced data signal to said remainder signal to produce an output signal.

7. The method of claim 6 wherein the step of adding said watermarked, reduced data signal to said remainder signal comprises:

embedding a second watermark into said remainder signal to produce a watermarked remainder signal; and

adding said watermarked, reduced data signal to said watermarked remainder signal to produce an output signal.

8. The method of claim 7, wherein at least one of the watermarks is embedded using at least one key.

9. The method of claim 7, wherein at least one of the watermarks is embedded using a key pair.

10. The method of claim 9, wherein one key of the key pair is publicly available while the other key of the key pair is secret.

11. A method of protecting a data signal:

applying a data reduction technique to reduce the data signal into a reduced data signal;

subtracting said reduced data signal from the data signal to produce a remainder signal;

using a first scrambling technique to scramble said reduced data signal to produce a scrambled, reduced data signal;

using a second scrambling technique to scramble said remainder signal to produce a scrambled remainder signal; and

adding said scrambled, reduced data signal to said scrambled remainder signal to produce an output signal.

12. The method of claim 11 wherein said first and second scrambling techniques are identical.

13. A method of securing a data signal comprising:

applying a data reduction technique to reduce the data signal into a reduced data signal;

subtracting said reduced data signal from the data signal to produce a remainder signal;

using a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal;

using a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal; and

adding said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal.

14. The method of claim 13 wherein said first and second cryptographic techniques are identical.

15. The method of claim 13 wherein at least one of said first and second cryptographic techniques is a watermarking technique.

16. The method of claim 15, wherein at least one of the watermarks is embedded using at least one key.

17. The method of claim 15, wherein at least one of the watermarks is embedded using a key pair.

18. The method of claim 13 wherein at least one of said first and second cryptographic techniques is a scrambling technique.

19. The method of claim 13 wherein one of said first and second cryptographic techniques is a watermarking technique and the other is a scrambling technique.

20. The method of claim 13 wherein said first and second cryptographic techniques are identical.

21. A system for securing a data signal comprising:

means to apply a data reduction technique to reduce the data signal into a reduced data signal;

means to subtract said reduced data signal from the data signal to produce a remainder signal;

means to apply a first cryptographic technique to encrypt the reduced data signal to produce an encrypted, reduced data signal;

means to apply a second cryptographic technique to encrypt the remainder signal to produce an encrypted remainder signal; and

means to add said encrypted, reduced data signal to said encrypted remainder signal to produce an output signal.

22. The system of claim 21 wherein said first and second cryptographic techniques are identical.

23. The system of claim 21 wherein at least one of said means to apply a first and second cryptographic technique utilizes a watermarking technique.

24. The system of claim 21 wherein at least one of said means to apply a first and second cryptographic technique utilizes a scrambling technique.

25. The system of claim 13 wherein said means to apply a first cryptographic technique is a means to apply a watermarking technique and said means to apply a second cryptographic technique is a means to apply a scrambling technique.

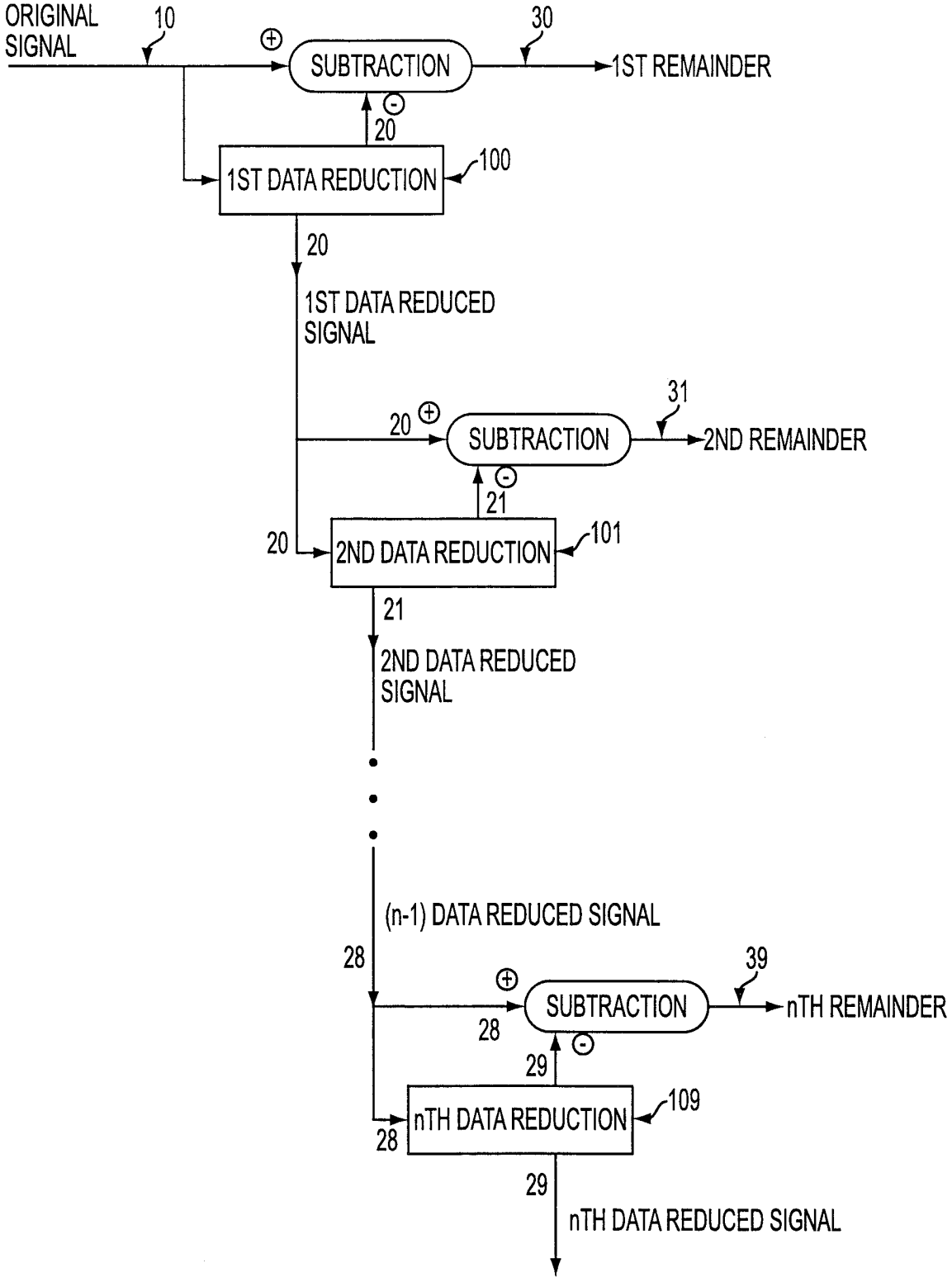

ORIGINAL SIGNAL
10
SUBTRACTION
30
1ST REMAINDER
20
1ST DATA REDUCTION
100
20
1ST DATA REDUCED SIGNAL
20
31
SUBTRACTION
2ND REMAINDER
21
20
2ND DATA REDUCTION
101
21
2ND DATA REDUCED SIGNAL
(n-1) DATA REDUCED SIGNAL
28
39
SUBTRACTION
nTH REMAINDER
28
29
nTH DATA REDUCTION
109
28
29
nTH DATA REDUCED SIGNAL

FIG. 1

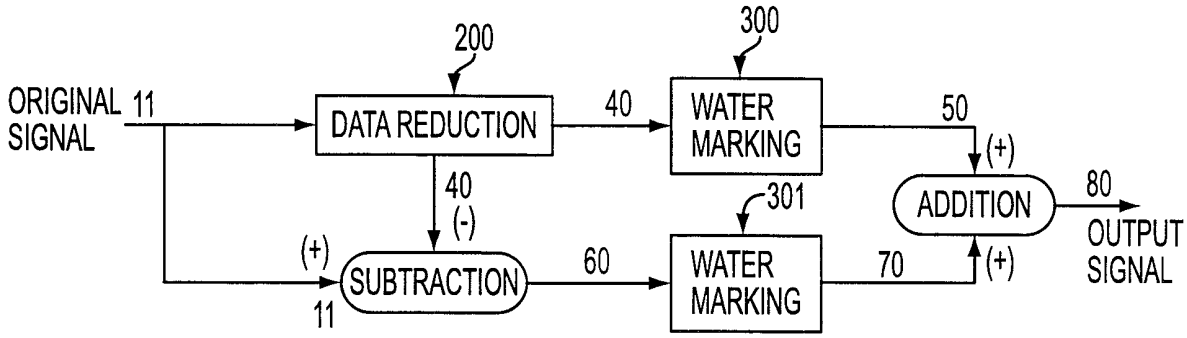

ORIGINAL SIGNAL
11
200
DATA REDUCTION
40
300
WATER MARKING
50
(+)
ADDITION
80
OUTPUT SIGNAL
40
(-)
301
(+)
SUBTRACTION
60
WATER MARKING
70
(+)
11

FIG. 2

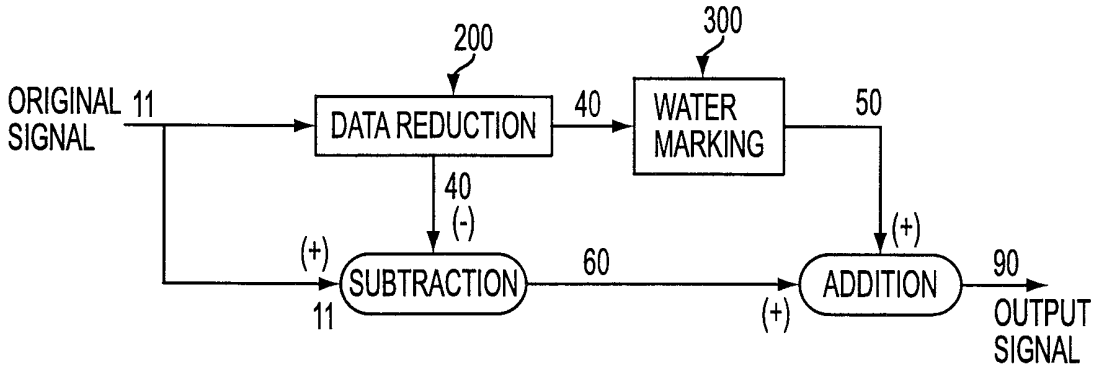

ORIGINAL SIGNAL
11
200
DATA REDUCTION
40
300
WATER MARKING
50
40
(-)
(+)
(+)
SUBTRACTION
60
ADDITION
90
OUTPUT SIGNAL
11
(+)

FIG. 3

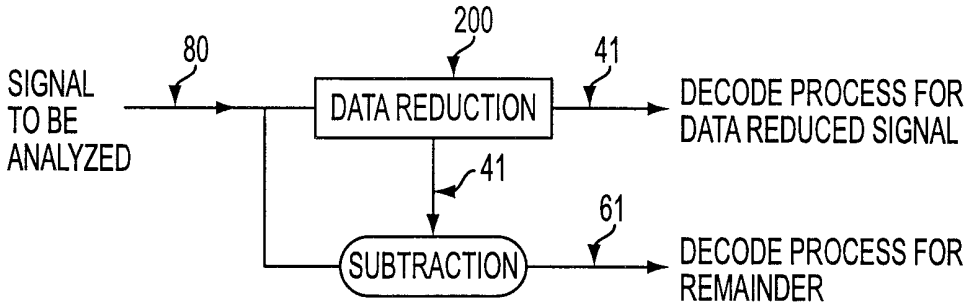

200
80
41
SIGNAL
TO BE
ANALYZED
DATA REDUCTION
DECODE PROCESS FOR
DATA REDUCED SIGNAL
41
61
SUBTRACTION
DECODE PROCESS FOR
REMAINDER

FIG. 4

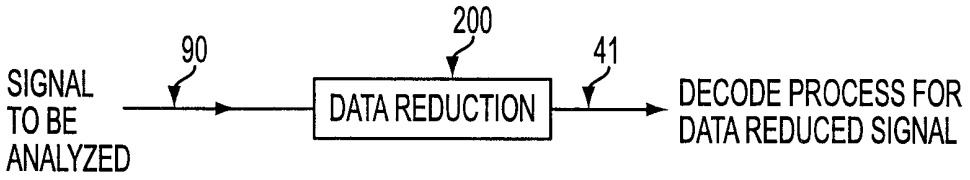

200
90
41
SIGNAL
TO BE
ANALYZED
DATA REDUCTION
DECODE PROCESS FOR
DATA REDUCED SIGNAL

FIG. 5

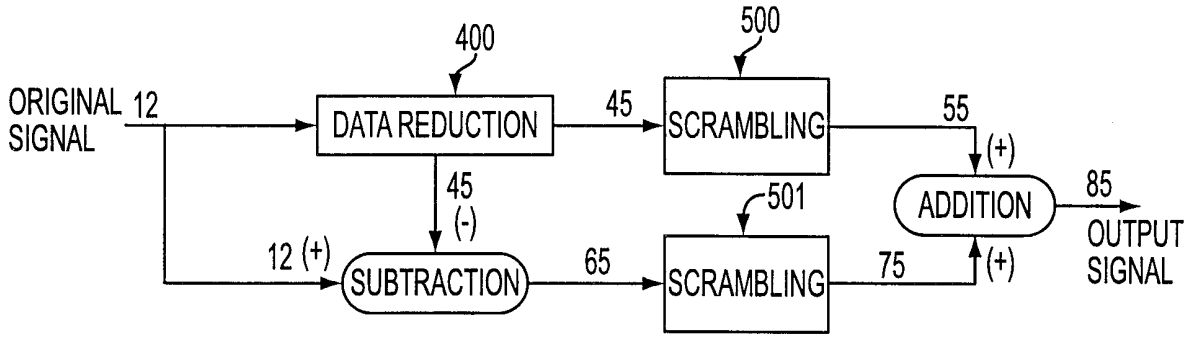

ORIGINAL SIGNAL
12
400
DATA REDUCTION
45
500
SCRAMBLING
55
(+)
45
(-)
501
ADDITION
85
OUTPUT SIGNAL
12 (+)
SUBTRACTION
65
SCRAMBLING
75
(+)

FIG. 6

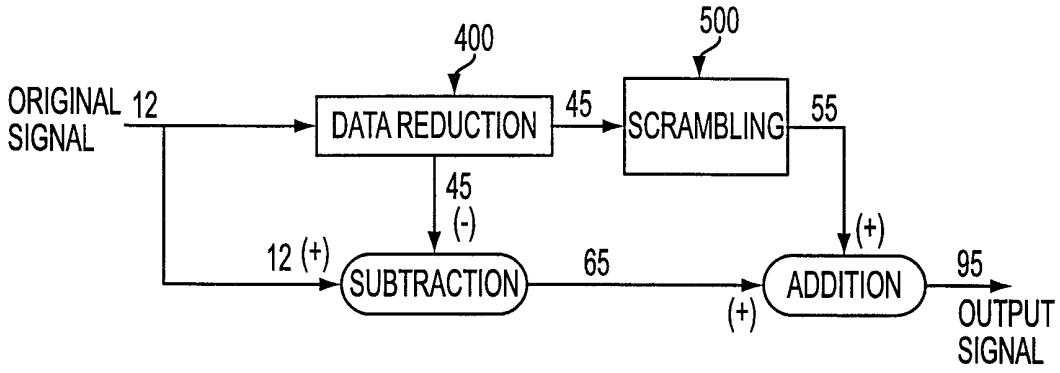

ORIGINAL SIGNAL
12
400
DATA REDUCTION
45
500
SCRAMBLING
55
45
(-)
(+)
12 (+)
SUBTRACTION
65
ADDITION
95
(+)
OUTPUT SIGNAL

FIG. 7

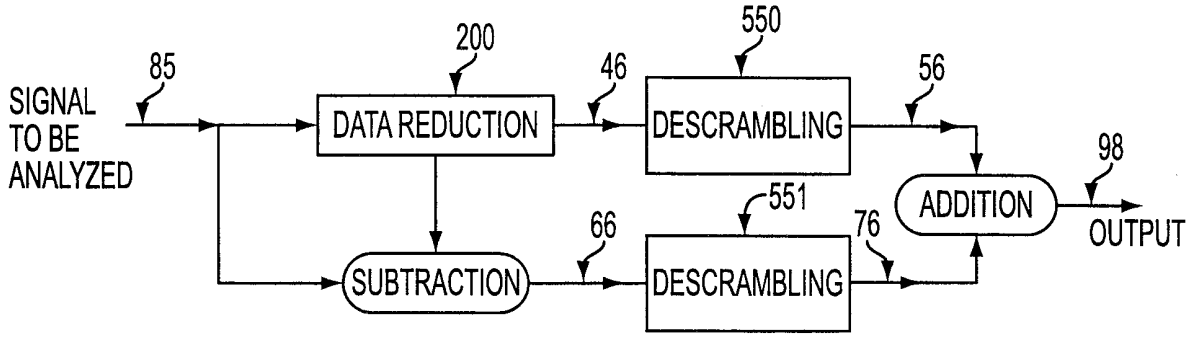

SIGNAL TO BE ANALYZED
85
200
DATA REDUCTION
46
550
DESCRAMBLING
56
98
ADDITION
OUTPUT
551
DESCRAMBLING
76
66
SUBTRACTION

FIG. 8

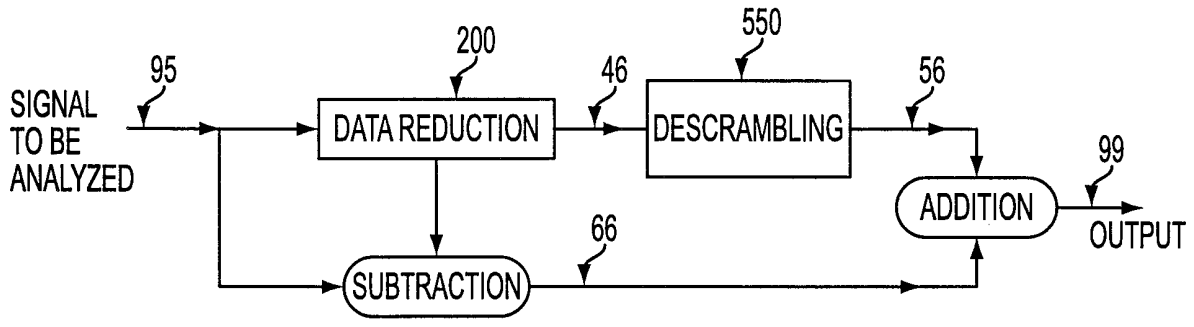

SIGNAL TO BE ANALYZED
95
200
DATA REDUCTION
46
550
DESCRAMBLING
56
99
ADDITION
OUTPUT
66
SUBTRACTION

FIG. 9

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/06522

A. CLASSIFICATION OF SUBJECT MATTER
IPC(7) : HO4N 7/167
US CL : 713/176
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

U.S. : 380/200,206,207,237,238; 705/54; 704/216-218, 226-228, 500, 501, 503,504; 713/176; 360/49; 348/461, 462

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched

Watermark Digest: Art Unit 2767

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

IEEE, EAST, Internet, Dialog

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X,E	US 6,061,793 A [TEWFIK et al.] 09 MAY 2000, Entire Document	1-25
X	US 5,809,139 A [GIROD et al.] 15 SEPTMBER 1998, Entire Document	1-25
X	US 5,848,155 A [COX] 08 DECEMBER 1998, Entire Document	1-25
A,P	US 5,889,868 A [MOSKOWITZ et al.] 30 MARCH 1999, Entire Document	1-25
A,P	US 5,915,027 A [COX et al.] 22 JUNE 1999, Entire Document	1-25
A,P	US 5,940,134 A [WIRTZ] 17 AUGUST 1999, Entire Document	1-25

[X] Further documents are listed in the continuation of Box C. [ ] See patent family annex.

*	Special categories of cited documents:	"T"	later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"A"	document defining the general state of the art which is not considered to be of particular relevance	"X"	document of particular relevance, the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"E"	earlier document published on or after the international filing date	"Y"	document of particular relevance, the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"L"	document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)	"&"	document member of the same patent family
"O"	document referring to an oral disclosure, use, exhibition or other means		
"P"	document published prior to the international filing date but later than the priority date claimed		

Date of the actual completion of the international search	Date of mailing of the international search report
30 JUNE 2000	18 AUG 2000
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231 Facsimile No. (703) 305-3230	Authorized officer PAUL E. CALLAHAN Telephone No. (703) 305-1338

Form PCT/ISA/210 (second sheet) (July 1998)★

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/06522

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A,P	US 5,991,426 A [COX et al.] 23 NOVEMBER 1999, Entire Document	1-25
A,E	US 6,069,914 A [COX] 30 MAY 2000, Entire Document	1-25
A,P	US 5,943,422 A [VAN WIE et al.] 24 AUGUST 1999, Entire Document	1-25