Fig. 5. *A standard* 500 × 480 *image of a mandrill.*

Fig. 6. *A log polar map of the image of a mandrill. The log-polar map employs bilinear interpolation and the log-polar grid is 600 × 600 samples.*

6 Conclusion

This paper has outlined the theory of integral transform invariants and showed that this can be used to produce watermarks that are resistant to translation,

Fig. 7. *The image of a mandrill reconstructed from a log polar map of size 100 × 100 samples. This reconstruction uses nearest neighbour interpolation.*

Fig. 8. *A watermarked image of a mandrill that has been rotated by 143 degrees and scaled by 75%. The embedded mark was recovered from this image.*

rotation and scaling. The importance of invertibility of the invariant representation was emphasised. One of the significant points is the novel application of the Fourier-Mellin transform to digital image watermarking.

There are several advantages in using integral transform domain marks. The main advantage is that the transforms can be computed very quickly (although in practice it has been found that the inverse log-polar mapping is a computational bottleneck). In addition, transform space contains a large number of samples which can be used to hide a spread spectrum signal.

An example of a rotation and scale invariant watermark was presented. As one might expect, this proved to be robust to changes in scale and rotation. It was also found to be weakly resistant to lossy image compression and cropping. The robustness of the embedded mark to these attacks will be greatly improved with future work.

On its own, the invariant watermark discussed in this paper cannot resist changes in aspect ratio or shear transformations. There is no obvious means of constructing an integral transform-based operator that is invariant to these transformations. However, work is currently in progress to find a means of searching for the most likely values of aspect ratio and shear factor, and then to apply the necessary corrections during watermark extraction.

In addition to the above, we intend to investigate the possible use of phase-based complete invariants. This would have some advantage over only marking strong invariants, since a complete invariant presents a maximal number of potential communications channels through which watermark information may be transmitted.

Acknowledgement

We wish to thank Dr David McG. Squire, Sergei Starchik and Dr Feng-Lin for their extremely helpful advice on the theory of invariants and Dr A. Z. Tirkel for many stimulating conversations and for exchanging many ideas. We are also grateful to Dr Alexander Herrigel and Adrian Perrig for their useful comments.

References

[1] R. E. Blahut. *The theory and practice of error control codes*. Addison-Wesley, 1983.

[2] R. D. Brandt and F. Lin. Representations that uniquely characterize images modulo translation, rotation and scaling. *Pattern Recognition Letters*, 17:1001–1015, August 1996.

[3] G. Caronni. Assuring Ownership Rights for Digital Images. In H. H. Brueggemann and W. Gerhardt-Haeckl, editors, *Reliable IT Systems VIS '95*. Vieweg Publishing Company, Germany, 1995.

[4] W. G. Chambers. *Basics of Communications and Coding*. Oxford Science Publications. Clarendon Press Oxford, 1985.

[5] I. Cox, J. Killian, T. Leighton, and T. Shamoon. Secure spread spectrum communication for multimedia. Technical report, N.E.C. Research Institute, 1995. ftp://ftp.nj.nec.com/pub/ingemar/papers/watermark.ps.Z.

[6] I. Cox, J. Killian, T. Leighton, and T. Shamoon. Secure spread spectrum watermarking for images, audio and video. In *Proceedings of the IEEE Int. Conf. on Image Processing ICIP-96*, pages 243–246, Lausanne, Switzerland, September 16-19 1996.

[7] I. Cox, S. Roy, and S. L. Hingorani. Dynamic histogram warping of image pairs for constant image brightness. In *Proceedings of the IEEE Int. Conf. on Image Processing ICIP-95*, Austin, Texas, 1995.

[8] S. Craver, N. Memon, B. Yeo, and M. Yeung. Can invisible marks resolve rightful ownerships? In *IS&T/SPIE Electronic Imaging '97: Storage and Retrieval of Image and Video Databases*, 1997.

[9] P. Davern and M. Scott. Fractal based image steganography. In Ross Anderson, editor, *Proceedings of the First International Workshop in Information Hiding*, Lecture Notes in Computer Science, pages 279–294, Cambridge, UK, May/June 1996. Springer Verlag.

[10] J.F. Delaigle, C. De Vleeschouwer, and B Macq. A psychovisual approach for digital picture watermarking. submitted to the Journal of Electronic Imaging, 1996.

[11] Mario Ferraro and Terry M. Caelli. Lie transform groups, integral transforms, and invariant pattern recognition. *Spatial Vision*, 8(1):33–44, 1994.

[12] James Gibson. *The Senses Considered as Perceptual Systems*. Houghton-Mifflin, Boston, Massachusetts, 1966.

[13] K. Matsui and K. Tanaka. Video-Steganography: How to secretly embed a signature in a picture. In *IMA Intellectual Property Project Proceedings*, pages 187–206, January 1994.

[14] R. Milanese, S. Gil, and T. Pun. Attentive mechanisms for dynamic and static scene analysis. *Optical Engineering*, 34(8):2428–2434, August 1995.

[15] J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland. Phase watermarking of digital images. In *Proceedings of the IEEE Int. Conf. on Image Processing ICIP-96*, pages 239–242, Lausanne, Switzerland, September 16-19 1996.

[16] J. J. K. Ó Ruanaidh, W. J. Dowling, and F. M. Boland. Watermarking digital images for copyright protection. *IEE Proceedings on Vision, Image and Signal Processing*, 143(4):250–256, August 1996. Invited paper, based on the paper of the same title at the IEE Conference on Image Processing and Its Applications, Edinburgh, July 1995.

[17] A. V. Oppenheim and J. S. Lim. The importance of phase in signals. *Proceedings of the IEEE*, 69(5):529–541, May 1981.

[18] B Pfitzmann. Information hiding terminology. In Ross Anderson, editor, *Proceedings of the First International Workshop in Information Hiding*, Lecture Notes in Computer Science, pages 347–350, Cambridge, UK, May/June 1996. Springer Verlag.

[19] R. L. Pickholtz, D. L. Schilling, and L. B. Milstein. Theory of spread spectrum communications – a tutorial. *IEEE Transactions on Communications*, COM-30(5):855–884, May 1982.

[20] I Pitas. A method for signature casting on digital images. In *Proceedings of the IEEE Int. Conf. on Image Processing ICIP-96*, pages 215–218, Lausanne, Switzerland, September 16-19 1996.

[21] W.H. Press, S.A. Teukolsky, W.T. Vetterling, and B.P. Flannery. *Numerical Recipes in C*. Cambridge University Press, second edition, 1992.

[22] J. Puate and F. Jordan. Using fractal compression scheme to embed a digital signature into an image. http://ltswww.epfl.ch/~kutter/publications/fvt.html, November 1996.

[23] T. H. Reiss. *Recognizing planar Objects Using Invariant Image Features*. Lecture Notes in Computer Science. Springer-Verlag, 1993.

[24] B. Schneier. *Applied Cryptography*. Wiley, 2nd edition, 1995.

[25] J. Smith and B. Comiskey. Modulation and information hiding in images. In Ross Anderson, editor, *Proceedings of the First International Workshop in Information Hiding*, Lecture Notes in Computer Science, pages 207–226, Cambridge, UK, May/June 1996. Springer Verlag.

[26] D. McG. Squire. *Model-based Neural Networks for Invariant Pattern Recognition*. PhD thesis, Curtin University of Technology, Perth, Western Australia, October 1996.

[27] M. D. Swanson, B. Zhu, and A. Tewfik. Transparent robust image watermarking. In *Proceedings of the IEEE Int. Conf. on Image Processing ICIP-96*, pages 211–214, Lausanne, Switzerland, September 16-19 1996.

[28] P. Sweeney. *Error Control Coding: An Introduction*. Prentice-Hall, 1991.

[29] A. Z. Tirkel, G. A. Rankin, R. G. van Schyndel, W. J. Ho, N. R. A. Mee, and C. F. Osborne. Electronic watermark. In *Dicta-93*, pages 666–672, Macquarie University, Sydney, December 1993.

[30] A. Z. Tirkel, R. G. van Schyndel, and C. F. Osborne. A two-dimensional digital watermark. In *ACCV'95*, pages 378–383, University of Queensland, Brisbane, December 6-8 1995.

[31] A.Z. Tirkel. Image and watermark registration. Submitted to Signal processing, January 1997.

[32] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne. A digital watermark. In *IEEE Int. Conf. on Image Processing ICIP-95*, pages 86–90, Austin, Texas, 1994.

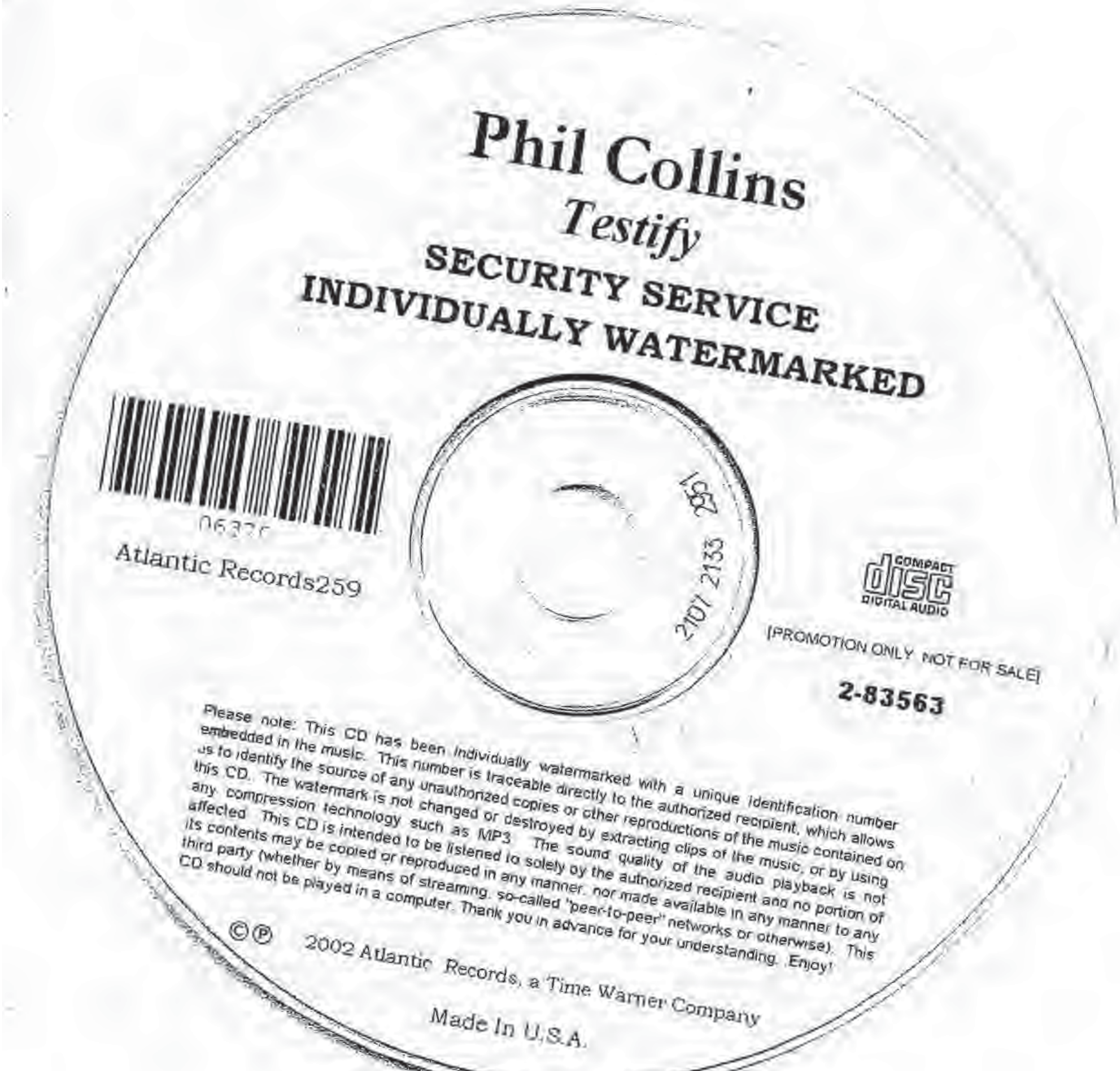
[33] R. G. van Schyndel, A. Z. Tirkel, and C. F. Osborne. Towards a robust digital watermark. In *Dicta-95*, pages 504–508, Nanyang Technological University, Singapore, December 5-8 1995.

[34] J. Zhao and E. Koch. Embedding robust labels into images for copyright protection. Technical report, Fraunhofer Institute for Computer Graphics, Darmstadt, Germany, 1994.

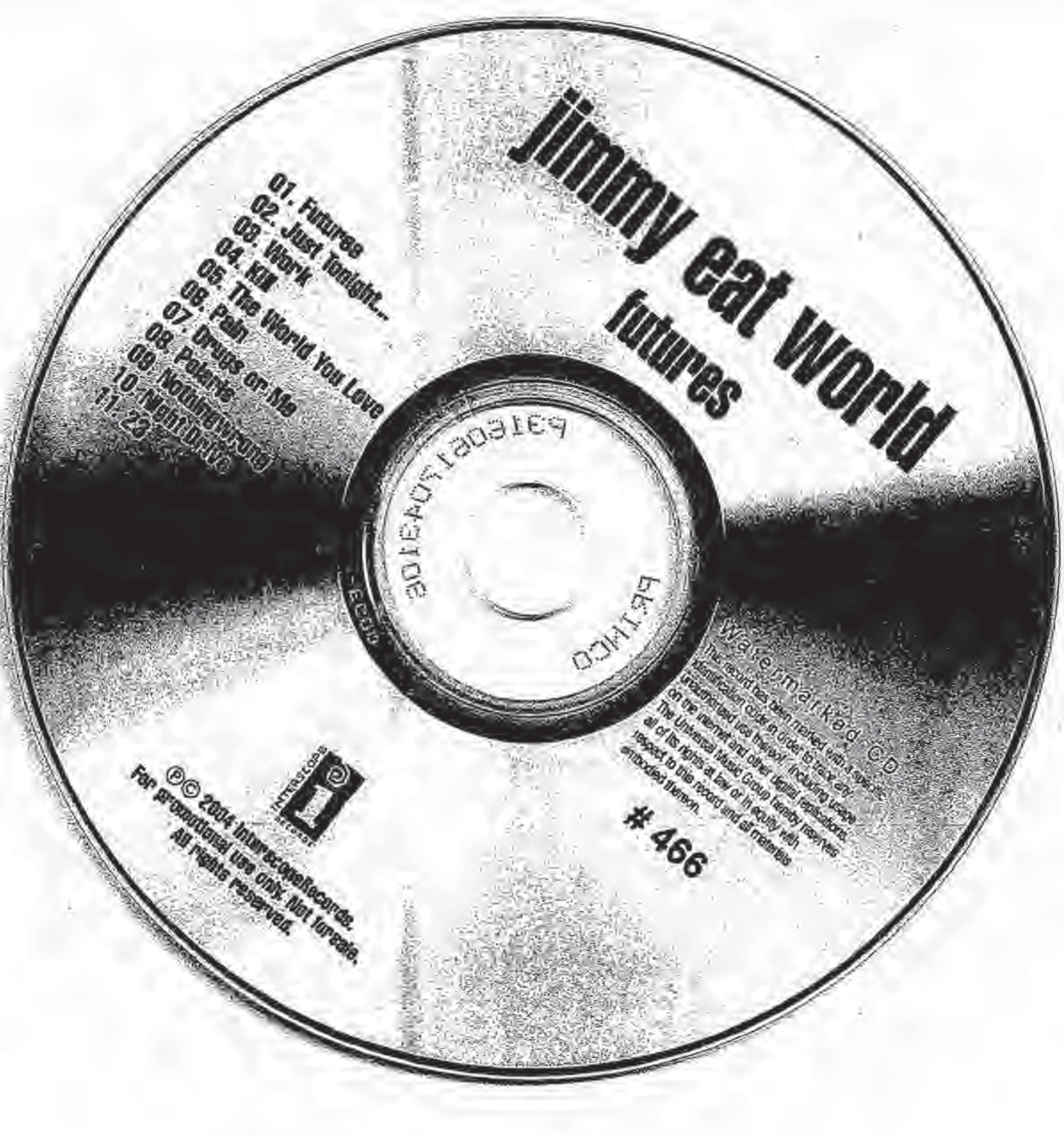

Staind
The Singles 1996-2006
THIS CD BELONGS TO:
Ashley White 142
WATERMARKED DISC
RESTRICTED RELEASE


Whate
ple Say I Am, That's What I'm Not
46. Chris Price
P 2005 Domino Recording Co
C 2005 Domino Recording Co
This sealed watermarked CD, for promotional
use, remains the property of Domino Recording Co
be surrendered on request. It is uniquely traceable to the
All copying, hiring, lending and distribution prohibited.
Domino


RADIOHEAD
CDP 7243 5 84543 2 1
Capitol®
215
"Hail To The Thief"
ADVANCE COPY - INTERNAL USE ONLY - DO NOT DUPLICATE
This record has been marked with a specific identification code in order to trace any unauthorized use thereof. Including usage on the Internet and other digital replications. The EMI Music Group hereby reserves all of its rights at law or in equity with respect to this record and all materials embodied thereon.
VERBATIM
DataLifePlus CD-R


Phil Collins
Testify
SECURITY SERVICE
INDIVIDUALLY WATERMARKED
Atlantic Records259
2107 2133
COMPACT DISC DIGITAL AUDIO
[PROMOTION ONLY NOT FOR SALE]
2-83563
Please note: This CD has been individually watermarked with a unique identification number embedded in the music. This number is traceable directly to the authorized recipient, which allows us to identify the source of any unauthorized copies or other reproductions of the music contained on this CD. The watermark is not changed or destroyed by extracting clips of the music, or by using any compression technology such as MP3. The sound quality of the audio playback is not affected. This CD is intended to be listened to solely by the authorized recipient and no portion of its contents may be copied or reproduced in any manner, nor made available in any manner to any third party (whether by means of streaming, so-called "peer-to-peer" networks or otherwise). This CD should not be played in a computer. Thank you in advance for your understanding. Enjoy!
©℗ 2002 Atlantic Records, a Time Warner Company
Made In U.S.A.


AEROSMITH
"Just Push Play"
(Final)
(This Product Has Been Watermarked)
Source Date:
February 1, 2001
February 2, 2001
MITSUI COLOR THERMAL
MITSUI COLOR THERMAL
1. Beyond Beautiful (4:45) 2. Just Push Play (3:51)
3. Jaded (3:34) 4. Fly Away From Here (5:01)
5. Trip Hoppin' (4:27) 6. Sunshine (3:37)
7. Under My Skin (3:45) 8. Luv Lies (4:26)
9. Outta Your Head (3:22)
10. Drop Dead Gorgeous (3:42)
11. Light Inside (3:34)
12. Avant Garden (4:52)


jimmy eat world
futures
01. Futures
02. Just Tonight...
03. Work
04. Kill
05. The World You Love
06. Pain
07. Drugs or Me
08. Polaris
09. Nothingwrong
10. Night Drive
11. 23
℗© 2004 InterscopeRecords.
For promotional use only. Not for sale.
All rights reserved.
watermarked CD
This record has been marked with a specific identification code in order to trace any unauthorized use thereof - including usage on the internet and other digital applications. The Universal Music Group hereby reserves all of its rights at law or in equity with respect to this record and all materials embodied thereon.
466

PATENT
ATTORNEY DOCKET NO. 066112.0132

METHOD AND DEVICE FOR MONITORING AND ANALYZING SIGNALS

CROSS-REFERENCE TO RELATED APPLICATIONS

This application claims the benefit of pending U.S. Patent Application Serial No. 08/999,766, filed July 23, 1997, entitled "Steganographic Method and Device"; pending U.S. Patent Application Serial No. 08/772,222, filed December 20, 1996, entitled "Z-Transform Implementation of Digital Watermarks"; pending U.S. Patent Application Serial No. 09/456,319, filed December 8, 1999, entitled "Transform Implementation of Digital Watermarks"; pending U.S. Patent Application Serial No. 08/674,726, filed July 2, 1996, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management"; pending U.S. Patent Application Serial No. 09/545,589, filed April 7, 2000, entitled "Method and System for Digital Watermarking"; pending U.S. Patent Application Serial No. 09/046,627, filed March 24, 1998, entitled "Method for Combining Transfer Function with Predetermined Key Creation"; pending U.S. Patent Application Serial No. 09/053,628, filed April 2, 1998, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking"; pending U.S. Patent Application Serial No. 09/281,279, filed March 30, 1999, entitled "Optimization Methods for the Insertion, Protection, and Detection..."; U.S. Patent Application Serial No.09,594,719, filed June 16, 2000, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems" (which is a continuation-in-part of PCT application No. PCT/US00/06522, filed March 14, 2000, which PCT application claimed priority to U.S. Provisional Application No. 60/125,990, filed March 24, 1999); pending U.S. Application No 60/169,274, filed December 7, 1999, entitled "Systems, Methods And Devices For Trusted Transactions"; and PCT Application No. PCT/US00/21189, filed August 4, 2000 (which claims priority to U.S. Patent Application Serial No. 60/147,134, filed August 4, 1999, and to US Patent Application No. 60/213,489, filed June 23, 2000, both of which are entitled, "A Secure Personal Content Server"). The previously identified patents and/or patent applications are hereby incorporated by reference, in their entireties.

In addition, this application hereby incorporates by reference, as if fully stated herein, the total disclosures of US Patent 5,613,004 "Steganographic Method and Device"; U.S. Patent 5,745,569 "Method for Stega-Cipher Protection of Computer Code"; and U.S. Patent 5,889,868 "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data."

BACKGROUND OF THE INVENTION

1. Field of the Invention

The invention relates to the monitoring and analysis of digital information. A method and device are described which relate to signal recognition to enhance identification and monitoring activities.

2. Description of the Related Art

Many methods and protocols are known for transmitting data in digital form for multimedia applications (including computer applications delivered over public networks such as the internet or World Wide Web ("WWW"). These methods may include protocols for the compression of data, such that it may more readily and quickly be delivered over limited bandwidth data lines. Among standard protocols for data compression of digital files may be mentioned the MPEG compression standards for audio and video digital compression, promulgated by the Moving Picture Experts Group. Numerous standard reference works and patents discuss such compression and transmission standards for digitized information.

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 general discussion of digital watermarking as it has been applied in the art may be found in U.S. Patent No. 5,687,236 (whose specification is incorporated in whole herein by reference).

Further applications of basic digital watermarking functionality have also been developed. Examples of such applications are shown in U.S. Patent No. 5,889,868 (whose specification is incorporated in whole herein by reference). Such applications have been drawn, for instance, to implementations of digital watermarks that were deemed most suited to particular transmissions, or particular distribution and storage mediums, given the nature of digitally sampled audio, video, and other multimedia works. There have also been developed techniques for adapting watermark application parameters to the individual characteristics of a given digital sample stream, and for implementation of digital watermarks that are feature-based - i.e., a system in which watermark information is not carried in individual samples, but is carried in the relationships between multiple samples, such as in a waveform shape. For instance, natural extensions may be added to digital watermarks that may also separate frequencies (color or audio), channels in 3D while utilizing discreteness in feature-based encoding only known to those with pseudo-random keys (i.e., cryptographic keys) or possibly tools to access such information, which may one day exist on a quantum level.

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.

SUMMARY OF THE INVENTION

A method for monitoring and analyzing at least one signal is disclosed, which method comprises the steps of: receiving at least one reference signal to be monitored; creating an abstract of the at least one reference signal; storing the abstract of the at least one reference signal in a reference database; receiving at least one query signal to be analyzed; creating an abstract of the at least one query signal; and comparing the abstract of the at least one query signal to the abstract of the at least one reference signal to determine if the abstract of the at least one query signal matches the abstract of the at least one reference signal.

A method for monitoring a plurality of reference signals is also disclosed, which method comprises the steps of: creating an abstract for each one of a plurality of reference signals; storing each of the abstracts in a reference database; receiving at least one query signal to be analyzed; creating an abstract of each at least one query signal; locating an abstract in the reference database that matches the abstract of each at least one query signal; and recording the identify of the reference signal whose abstract matched the abstract of each at least one query signal.

A computerized system for monitoring and analyzing at least one signal is also disclosed, which system comprises: a processor for creating an abstract of a signal using selectable criteria; a first input for receiving at least one reference signal to be monitored, the first input being coupled to the processor such that the processor may generate an abstract for each reference signal input to the processor; a reference database, coupled to the processor, for storing abstracts of each at least one reference signal; a second input for receiving at least one query signal to be analyzed, the second input being coupled to the processor such that the processor may generate an abstract for each query signal; and a comparing device, coupled to the reference database and to the second input, for comparing an abstract of the at least one query signal to the abstracts stored in the reference database to determine if the abstract of the at least one query signal matches any of the stored abstracts.

Further, an electronic system for monitoring and analyzing at least one signal is disclosed, which system comprises: a first input for receiving at least one reference signal to be monitored, a first processor for creating an abstract of each reference signal input to the first processor through the first input; a second input for receiving at least one query signal to be analyzed, a second processor for creating an abstract of each query signal; a reference database for storing abstracts of each at least one reference signal; and a comparing device for comparing an abstract of the at least one query signal to the abstracts stored in the reference database to determine if the abstract of the at least one query signal matches any of the stored abstracts.

DETAILED DESCRIPTION OF THE INVENTION

While there are many approaches to data reduction that can be utilized, a primary concern is the ability to reduce the digital signal in such a manner as to retain a "perceptual relationship" between the original signal and its data reduced version. This relationship may either be mathematically discernible or a result of market-dictated needs. The purpose is to afford a more consistent means for classifying signals than proprietary, related text-based approaches. A simple analogy is the way in which a forensic investigator uses a sketch artist to assist in determining the identity of a human.

In one embodiment of the invention, the abstract of a signal may be generated by the following steps: 1) analyze the characteristics of each signal in a group of audible/perceptible variations for the same signal (e.g., analyze each of five versions of the same song—which versions may have the same lyrics and music but which are sung by different artists); and 2) select those characteristics which achieve remain relatively constant (or in other words, which have minimum variation) for each of the signals in the group. Optionally, the null case may be defined using those characteristics which are common to each member of the group of versions.

Lossless and lossy compression schemes are appropriate candidates for data reduction technologies, as are those subset of approaches that are based on perceptual models, such as AAC, MP3, TwinVQ, JPEG, GIF, MPEG, etc. Where spectral transforms fail to assist in greater data reduction of the signal, other signal characteristics can be identified as candidates for further data reduction. Linear predictive coding (LPC), z-transform analysis, root mean square (rms), signal to peak, may be appropriate tools to measure signal characteristics, but other approaches or combinations of signal characteristic analysis are contemplated. While such signal characteristics may assist in determining particular applications of the present invention, a generalized approach to signal recognition is necessary to optimize the deployment and use of the present invention.

Increasingly, valuable information is being created and stored in digital form. For example, music, photographs and motion pictures can all be stored and transmitted as a series of binary digits — 1's and 0's. Digital techniques permit the original information to be duplicated repeatedly with perfect or near perfect accuracy, and each copy is perceived by viewers or listeners as indistinguishable from the original signal. Unfortunately, digital techniques also permit the information to be easily copied without the owner's permission. While digital representations of analog waveforms may be analyzed by perceptually-based or perceptually-limited analysis it is usually costly and time-consuming to model the processes of the highly effective ability of humans to identify and recognize a signal. In those applications where analog signals require analysis, the cost of digitizing the analog signal is minimal when compared to the benefits of increased accuracy and speed of signal analysis and monitoring when the processes contemplated by this invention are utilized.

The present invention relates to identification of digitally-sampled information, such as images, audio and video. Traditional methods of identification and monitoring of those signals do not rely on "perceptual quality," but rather upon a separate and additional signal. Within this application, such signals will be called "additive signals" as they provide information about the original images, audio or video, but such information is in addition to the original signal. One traditional, text-based additive signal is title and author information. The title and author, for example, is information about a book, but it is in addition to the text of the book. If a book is being duplicated digitally, the title and author could provide one means of monitoring the number of times the text is being duplicated, for example, through an Internet download. The present invention, however, is directed to the identification of a digital signal—whether text, audio, or video—using only the digital signal itself and then monitoring the number of times the signal is duplicated. Reliance on an additive signal has many shortcomings. For example, first, someone must incorporate the additive signal within the digital data being transmitted, for example, by concatenation or through an embedding process. Such an additive signal, however, can be easily identified and removed by one who wants to utilize the original signal without paying for its usage. If the original signal itself is used to identify the content, an unauthorized user could not avoid payment of a royalty simply by removing the additive signal—because there is no additive signal to remove. Hence, the present invention avoids a major disadvantage of the prior art.

One such additive signal that may be utilized is a digital watermark—which ideally cannot be removed without perceptually altering the original signal. A watermark may also be used as a monitoring signal (for example, by encoding an identifier that uniquely identifies the original digital signal into which the identifier is being embedded). A digital watermark used for monitoring is also an additive signal, and such a signal may make it difficult for the user who wants to duplicate a signal without paying a royalty—mainly by degrading the perceptual quality of the original signal if the watermark (and hence the additive monitoring signal) is removed.

This is, however, is a different solution to the problem.

The present invention eliminates the need of any additive monitoring signal because the present invention utilizes the underlying content signal as the identifier itself. Nevertheless, the watermark may increase the value of monitoring techniques by increasing the integrity of the embedded data and by indicating tampering of either the original content signal or the monitoring signal. Moreover, the design of a watermarking embedding algorithm is closely related to the perceptibility of noise in any given signal and can represent an ideal subset of the original signal: the watermark bits are an inverse of the signal to the extent that lossy compression schemes, which can be used, for instance, to optimize a watermarking embedding scheme, can yield information about the extent to which a data signal can be compressed while holding steadfast to the design requirement that the compressed signal maintain its perceptual relationship with the original, uncompressed signal. By describing those bits that are candidates for imperceptible embedding of watermark bits, further data reduction may be applied on the candidate watermarks as an example of retaining a logical and perceptible relationship with the original uncompressed signal.

Of course, the present invention may be used in conjunction with watermarking technology (including the use of keys to accomplish secure digital watermarking), but watermarking is not necessary to practice the present invention. Keys for watermarking may have many forms, including: descriptions of the original carrier file formatting, mapping of embedded data (actually imperceptible changes made to the carrier signal and referenced to the predetermined key or key pairs), assisting in establishing the watermark message data integrity (by incorporation of special one way functions in the watermark message data or key), etc. Discussions of these systems in the patents and pending patent applications are incorporated by reference above. The "recognition" of a particular signal or an instance of its transmission, and its monitoring are operations that may be optimized through the use of digital watermark analysis.

A practical difference between the two approaches of using a separate, additive monitoring signal and using the original signal itself as the monitoring signal is control. If a separate signal is used for monitoring, then the originator of the text, audio or video signal being transmitted and the entity doing the monitoring have to agree as to the nature of the separate signal to be used for monitoring—otherwise, the entity doing the monitoring would not know where to look, for what to look, or how to interpret the monitoring signal once it was identified and detected. On the other hand, if the original signal is used itself as a monitoring signal, then no such agreement is necessary. Moreover, a more logical and self-sufficient relationship between the original and its data-reduced abstract enhances the transparency of any resulting monitoring efforts. The entity doing the monitoring is not looking for a separate, additive monitoring system, and further, need not have to interpret the content of the monitoring signal.

Monitoring implementations can be handled by robust watermark techniques (those techniques that are able to survive many signal manipulations but are not inherently "secure" for verification of a carrier signal absent a logically-related watermarking key) and forensic watermark techniques (which enable embedding of watermarks that are not able to survive perceptible alteration of the carrier signal and thus enable detection of tampering with the originally watermarked carrier signal). The techniques have obvious trade-offs between speed, performance and security of the embedded watermark data.

In other disclosures, we suggest improvements and implementations that relate to digital watermarks in particular and embedded signaling in general. A digital watermark may be used to "tag" content in a manner that is not humanly-perceptible, in order to ensure that the human perception of the signal quality is maintained. Watermarking, however, must inherently alter at least one data bit of the original signal to represent a minimal change from the original signal's "unwatermarked state." The changes may affect only a bit, at the very least, or be dependent on information hiding relating to signal characteristics, such as phase information, differences between digitized samples, root mean square (RMS) calculations, z-transform analysis, or similar signal characteristic category.

There are weaknesses in using digital watermark technology for monitoring purposes. One weakness relates directly to the way in which watermarks are implemented. Often, the persons responsible for encoding and decoding the digital watermark are not the creator of the valuable work to be protected. As such, the creator has no input on the placement of the monitoring signal within the valuable work being protected. Hence, if a user wishing to avoid payment of the royalty can find a way to decode or remove the watermark, or at least the monitoring signal embedded in the watermark, then the unauthorized user may successfully duplicate the signal with impunity. This could occur, for example, if either of the persons responsible for encoding or decoding were to have their security compromised such that the encoding or decoding algorithms were discovered by the unauthorized user.

With the present invention, no such disadvantages exist because the creator need not rely on anyone to insert a monitoring signal—as no such signal is necessary. Instead, the creator's work itself is used as the monitoring signal. Accordingly, the value in the signal will have a strong relationship with its recognizability.

By way of improving methods for efficient monitoring as well as effective confirmation of the identity of a digitally-sampled signal, the present invention describes useful methods for using digital signal processing for benchmarking a novel basis for differencing signals with binary data comparisons. These techniques may be complemented with perceptual techniques, but are intended to leverage the generally decreasing cost of bandwidth and signal processing power in an age of increasing availability and exchange of digitized binary data.

So long as there exist computationally inexpensive ways of identifying an entire signal with some fractional representation or relationship with the original signal, or its perceptually observable representation, we envision methods for faster and more accurate auditing of signals as they are played, distributed or otherwise shared amongst providers (transmitters) and consumers (receivers). The ability to massively compress a signal to its essence—which is not strictly equivalent to "lossy" or "lossless" compression schemes or perceptual coding techniques, but designed to preserve some underlying "aesthetic quality" of the signal—represents a useful means for signal analysis in a wide variety of applications. The signal analysis, however, must maintain the ability to distinguish the perceptual quality of the signals being compared. For example, a method which analyzed a portion of a song by compressing it to a single line of lyrics fails to maintain the ability to distinguish the perceptual quality of the songs being compared. Specifically, for example, if the song "New York State of Mind" were compressed to the lyrics "I'm in a New York State of Mind," such a compression fails to maintain the ability to distinguish between the various recorded versions of the song, say, for example between Billy Joel's recording and Barbara Streisand's recording. Such a method is, therefore, incapable of providing accurate monitoring of the artist's recordings because it could not determine which of the two artists is deserving of a royalty—unless of course, there is a separate monitoring signal to provide the name of the artist or other information sufficient to distinguish the two versions. The present invention, however, aims to maintain some level of perceptual quality of the signals being compared and would deem such a compression to be excessive.

This analogy can be made clearer if it is understood that there are a large number of approaches to compressing a signal to, say, $1/10{,}000^{th}$ of its original size, not for maintaining its signal quality to ensure computational ease for commercial quality distribution, but to assist in identification, analysis or monitoring of the signal. Most compression is either lossy or lossless and is designed with psychoacoustic or psychovisual parameters. That is to say, the signal is compressed to retain what is "humanly-perceptible." As long as the compression successfully mimics human perception, data space may be saved when the compressed file is compared to the uncompressed or original file. While psychoacoustic and psychovisual compression has some relevance to the present invention, additional data reduction or massive compression is anticipated by the present invention. It is anticipated that the original signal may be compressed to create a realistic or self-similar representation of the original signal, so that the compressed signal can be referenced at a subsequent time as unique binary data that has computational relevance to the original signal. Depending on the application, general data reduction of the original signal can be as simple as massive compression or may relate to the watermark encoding envelope parameter (those bits which a watermarking encoding algorithm deem as candidate bits for mapping independent data or those bits deemed imperceptible to human senses but detectable to a watermark detection algorithm). In this manner, certain media which are commonly known by signal characteristics, a painting, a song, a TV commercial, a dialect, etc., may be analyzed more accurately, and perhaps, more efficiently than a text-based descriptor of the signal. So long as the sender and receiver agree that the data representation is accurate, even insofar as the data-reduction technique has logical relationships with the perceptibility of the original signal, as they must with commonly agreed to text descriptors, no independent cataloging is necessary.

The present invention generally contemplates a signal recognition system that has at least five elements. The actual number of elements may vary depending on the number of domains in which a signal resides (for example, audio is at least one domain while visual carriers are at least two dimensional). The present invention contemplates that the number of elements will be sufficient to effectively and efficiently meet the demands of various classes of signal recognition. The design of the signal recognition that may be used with data reduction is better understood in the context of the general requirements of a pattern or signal recognition system.

The first element is the reference database, which contains information about a plurality of potential signals that will be monitored. In one form, the reference database would contain digital copies of original works of art as they are recorded by the various artists, for example, contain digital copies of all songs that will be played by a particular radio station. In another form, the reference database would contain not perfect digital copies of original works of art, but digital copies of abstracted works of art, for example, contain digital copies of all songs that have been preprocessed such that the copies represent the perceptual characteristics of the original songs. In another form, the reference database would contain digital copies of processed data files, which files represent works of art that have been preprocessed in such a fashion as to identify those perceptual differences that can differentiate one version of a work of art from another version of the same work of art, such as two or more versions of the same song, but by different artists. These examples have obvious application to visually communicated works such as images, trademarks or photographs, and video as well.

The second element is the object locator, which is able to segment a portion of a signal being monitored for analysis (i.e., the "monitored signal"). The segmented portion is also referred to as an "object." As such, the signal being monitored may be thought of comprising a set of objects. A song recording, for example, can be thought of as having a multitude of objects. The objects need not be of uniform length, size, or content, but merely be a sample of the signal being monitored. Visually communicated informational signals have related objects; color and size are examples.

The third element is the feature selector, which is able to analyze a selected object and identify perceptual features of the object that can be used to uniquely describe the selected object. Ideally, the feature selector can identify all, or nearly all, of the perceptual qualities of the object that differentiate it from a similarly selected object of other signals. Simply, a feature selector has a direct relationship with the perceptibility of features commonly observed. Counterfeiting is an activity which specifically seeks out features to misrepresent the authenticity of any given object. Highly granular, and arguably successful, counterfeiting is typically sought for objects that are easily recognizable and valuable, for example, currency, stamps, and trademarked or copyrighted works and objects that have value to a body politic.

The fourth element is the comparing device which is able to compare the selected object using the features selected by the feature selector to the plurality of signals in the reference database to identify which of the signals matches the monitored signal. Depending upon how the information of the plurality of signals is stored in the reference database and depending upon the available computational capacity (e.g., speed and efficiency), the exact nature of the comparison will vary. For example, the comparing device may compare the selected object directly to the signal information stored in the database. Alternatively, the comparing device may need to process the signal information stored in the database using input from the feature selector and then compare the selected object to the processed signal information. Alternatively, the comparing device may need to process the selected object using input from the feature selector and then compare the processed selected object to the signal information. Alternatively, the comparing device may need to process the signal information stored in the database using input from the feature selector, process the selected object using input from the feature selector, and then compare the processed selected object to the processed signal information.

The fifth element is the recorder which records information about the number of times a given signal is analyzed and detected. The recorder may comprise a database which keeps track of the number of times a song, image, or a movie has been played, or may generate a serial output which can be subsequently processed to determine the total number of times various signals have been detected.

Other elements may be added to the system or incorporated into the five elements identified above. For example, an error handler may be incorporated into the comparing device. If the comparing device identifies multiple signals which appear to contain the object being sought for analysis or monitoring, the error handler may offer further processing in order to identify additional qualities or features in the selected object such that only one of the set of captured signals is found to contain the further analyzed selected object that actually conforms with the object thought to have been transmitted or distributed.

Moreover, one or more of the five identified elements may be implemented with software that runs on the same processor, or which uses multiple processors. In addition, the elements may incorporate dynamic approaches that utilize stochastic, heuristic, or experience-based adjustments to refine the signal analysis being conducted within the system, including, for example, the signal analyses being performed within the feature selector and the comparing device. This additional analyses may be viewed as filters that are designed to meet the expectations of accuracy or speed for any intended application.

Since maintenance of original signal quality is not required by the present invention, increased efficiencies in processing and identification of signals can be achieved. The present invention concerns itself with perceptible relationships only to the extent that efficiencies can be achieved both in accuracy and speed with enabling logical relationships between an original signal and its abstract.

The challenge is to maximize the ability to sufficiently compress a signal to both retain its relationship with the original signal while reducing the data overhead to enable more efficient analysis, archiving and monitoring of these signals. In some cases, data reduction alone will not suffice: the sender and receiver must agree to the accuracy of the recognition. In other cases, agreement will actually depend on a third party who authored or created the signal in question. A digitized signal may have parameters to assist in establishing more accurate identification, for example, a "signal abstract" which naturally, or by agreement with the creator, the copyright owner or other interested parties, can be used to describe the original signal. By utilizing less than the original signal, a computationally inexpensive means of identification can be used. As long as a realistic set of conditions can be arrived at governing the relationship between a signal and its data reduced abstract, increases in effective monitoring and transparency of information data flow across communications channels is likely to result. This feature is significant in that it represents an improvement over how a digitally-sampled signal can be cataloged and identified, though the use of a means that is specifically selected based upon the strengths of a general computing device and the economic needs of a particular market for the digitized information data being monitored. The additional benefit is a more open means to uniformly catalog, analyze, and monitor signals. As well, such benefits can exist for third parties, who have a significant interest in the signal but are not the sender or receiver of said information.

As a general improvement over the art, the present invention incorporates what could best be described as "computer-acoustic" and "computer-visual" modeling, where the signal abstracts are created using data reduction techniques to determine the smallest amount of data, at least a single bit, which can represent and differentiate two digitized signal representations for a given predefined signal set. Each of such representations must have at least a one bit difference with all other members of the database to differentiate each such representation from the others in the database. The predefined signal set is the object being analyzed. The signal identifier/detector should receive its parameters from a database engine. The engine will identify those characteristics (for example, the differences) that can be used to distinguish one digital signal from all other digital signals that are stored in its collection. For those digital signals or objects which are seemingly identical, excepting that the signal may have different performance or utilization in the newly created object, benefits over additive or text-based identifiers are achieved. Additionally, decisions regarding the success or failure of an accurate detection of any given object may be flexibly implemented or changed to reflect market-based demands of the engine. Appropriate examples are songs or works or art which have been sampled or re-produced by others who are not the original creator.

In some cases, the engine will also consider the NULL case for a generalized item not in its database, or perhaps in situations where data objects may have collisions. For some applications, the NULL case is not necessary, thus making the whole system faster. For instance, databases which have fewer repetitions of objects or those systems which are intended to recognize signals with time constraints or capture all data objects. Greater efficiency in processing a relational database can be obtained because the rules for comparison are selected for the maximum efficiency of the processing hardware and/or software, whether or not the processing is based on psychoacoustic or psychovisual models. The benefits of massive data reduction, flexibility in constructing appropriate signal recognition protocols and incorporation of cryptographic techniques to further add accuracy and confidence in the system are clearly improvements over the art. For example, where the data reduced abstract needs to have further uniqueness, a hash or signature may be required. And for objects which have further uniqueness requirements, two identical instances of the object could be made unique with cryptographic techniques.

Accuracy in processing and identification may be increased by using one or more of the following fidelity evaluation functions:

1) RMS (root mean square). For example, a RMS function may be used to assist in determining the distance between data based on mathematically determinable Euclidean distance between the beginning and end data points (bits) of a particular signal carrier.

2) Frequency weighted RMS. For example, different weights may be applied to different frequency components of the carrier signal before using RMS. This selective weighting can assist in further distinguishing the distance between beginning and end points of the signal carrier (at a given point in time, described as bandwidth, or the number of total bits that can be transmitted per second) and may be considered to be the mathematical equivalent of passing a carrier signal difference through a data filter and figuring the average power in the output carrier.

3) Absolute error criteria, including particularly the NULL set (described above) The NULL may be utilized in two significant cases: First, in instances where the recognized signal appears to be an identified object which is inaccurately attributed or identified to an object not handled by the database of objects; and second, where a collision of data occurs. For instance, if an artist releases a second performance of a previously recorded song, and the two performances are so similar that their differences are almost imperceptible, then the previously selected criteria may not be able to differentiate the two recordings. Hence, the database must be "recalibrated" to be able to differentiate these two versions. Similarly, if the system identifies not one, but two or more, matches for a particular search, then the database may need

"recalibration" to further differentiate the two objects stored in the database.

4) Cognitive Identification. For example, the present invention may use an experience-based analysis within a recognition engine. Once such analysis may involve mathematically determining a spectral transform or its equivalent of the carrier signal. A spectral transform enables signal processing and should maintain, for certain applications, some cognitive or perceptual relationship with the original analog waveform. As a novel feature to the present invention, additional classes may be subject to humanly-perceptible observation. For instance, an experience-based criteria which relates particularly to the envisioned or perceived accuracy of the data information object as it is used or applied in a particular market, product, or implementation. This may include a short 3 second segment of a commercially available and recognizable song which is used for commercials to enable recognition of the good or service being marketed. The complete song is marketed as a separately valued object from the use of a discrete segment of the song (that may be used for promotion or marketing—for the complete song or for an entirely different good or service). To the extent that an owner of the song in question is able to further enable value through the licensing or agreement for use of a segment of the original signal, cognitive identification is a form of filtering to enable differentiations between different and intended uses of the same or subset of the same signal (object). The implementation relating specifically, as disclosed herein, to the predetermined identification or recognition means and/or any specified relationship with subsequent use of the identification means can be used to create a history as to how often a particular signal is misidentified, which history can then be used to optimize identification of that signal in the future. The difference between use of an excerpt of the song to promote a separate and distinct good or service and use of the excerpt to promote recognition of the song itself (for example, by the artist to sell copies of the

song) relates informationally to a decision based on recognized and approved use of the song. Both the song and applications of the song in its entirety or as a subset are typically based on agreement by the creator and the sender who seeks to utilize the work. Trust in the means for identification, which can be weighted in the present invention (for example, by adjusting bit-addressable information), is an important factor in adjusting the monitoring or recognition features of the object or carrier signal, and by using any misidentification information, (including any experience-based or heuristic information), additional features of the monitored signal can be used to improve the performance of the monitoring system envisioned herein. The issue of central concern with cognitive identification is a greater understanding of the parameters by which any given object is to be analyzed. To the extent that a creator chooses varying and separate application of his object, those applications having a cognitive difference in a signal recognition sense (e.g., the whole or an excerpt), the system contemplated herein includes rules for governing the application of bit-addressable information to increase the accuracy of the database.

5) Finally, the predetermined parameters that are associated with a discrete case for any given object will have a significant impact upon the ability to accurately process and identify the signals. For example, if a song is transmitted over a FM carrier, then one skilled in the art will appreciate that the FM signal has a predetermined bandwidth which is different from the bandwidth of the original recording, and different even from song when played on an AM carrier, and different yet from a song played using an 8-bit Internet broadcast. Recognition of these differences, however, will permit the selection of an identification means which can be optimized for monitoring a FM broadcasted signal. In other words, the discreteness intended by the sender is limited and directed by the fidelity of the transmission means. Objects may be cataloged and assessing with the understanding

that all monitoring will occur using a specific transmission fidelity. For example, a database may be optimized with the understanding that only AM broadcast signals will be monitored. For maximum efficiency, different data bases may be created for different transmission channels, e.g., AM broadcasts, FM broadcasts, Internet broadcasts, etc.

For more information on increasing efficiencies for information systems, see The Mathematical Theory of Communication (1948), by Shannon.

Because bandwidth (which in the digital domain is equated to the total number of bits that can be transmitted in a fixed period of time) is a limited resource which places limitations upon transmission capacity and information coding schemes, the importance of monitoring for information objects transmitted over any given channel must take into consideration the nature and utilization of a given channel. The supply and demand of bandwidth will have a dramatic impact on the transmission, and ultimately, upon the decision to monitor and recognize signals. A discussion of this is found in a co-pending application by the inventor under U.S. Patent Application No. 08/674,726 "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management" (which application is incorporated herein by reference as if fully setforth herein).

If a filter is to be used in connection with the recognition or monitoring engine, it may be desirable for the filter to anticipate and take into consideration the following factors, which affect the economics of the transmission as they relate to triggers for payment and/or relate to events requiring audits of the objects which are being transmitted: 1) time of transmission (i.e., the point in time when the transmission occurred), including whether the transmission is of a live performance); 2) location of transmission (e.g., what channel was used for transmission, which usually determines the associated cost for usage of the transmission channel); 3) the point of origination of the transmission (which may be the same for a signal carrier over many distinct channels); and 4) pre-existence of the information carrier signal (pre-recorded or newly created information carrier signal, which may require differentiation in certain markets or instances).

In the case of predetermined carrier signals (those which have been recorded and stored for subsequent use), "positional information carrier signals" are contemplated by this invention, namely, perceptual differences between the seemingly "same" information carrier that can be recognized as consumers of information seek different versions or quality levels of the same carrier signal. Perceptual differences exist between a song and its reproduction from a CD, an AM radio, and an Internet broadcast. To the extent that the creator or consumer of the signal can define a difference in any of the four criteria above, means can be derived (and programmed for selectability) to recognize and distinguish these differences. It is, however, quite possible that the ability to monitor carrier signal transmission with these factors will increase the variety and richness of available carrier signals to existing communications channels. The differentiation between an absolute case for transmission of an object, which is a time dependent event, for instance a live or real time broadcast, versus the relative case, which is prerecorded or stored for transmission at a later point in time, creates recognizable differences for signal monitoring.

The monitoring and analysis contemplated by this invention may have a variety of purposes, including, for example, the following: to determine the number of times a song is broadcast on a particular radio broadcast or Internet site; to control security though a voice-activated security system; and to identify associations between a beginner's drawing and those of great artists (for example to draw comparisons between technique, compositions, or color schemes). None of these examples could be achieved with any significant degree of accuracy using a text-based analysis. Additionally, strictly text-based systems fail to fully capture the inherent value of the data recognition or monitoring information itself.

SAMPLE EMBODIMENTS

In order to better appreciate and understand the present invention, the following sample embodiments are provided. These sample embodiments are provided for exemplary purposes only, and in no way limit the present invention.

SAMPLE EMBODIMENT 1

A database of audio signals (e.g., songs) is stored or maintained by a radio station or Internet streaming company, who may select a subset of the songs are stored so that the subset may be later broadcast to listeners. The subset, for example, may comprise a sufficient number of songs to fill 24 hours of music programming (between 300 or 500 songs). Traditionally, monitoring is accomplished by embedding some identifier into the signal, or affixing the identifier to the signal, for later analysis and determination of royalty payments. Most of the traditional analysis is performed by actual persons who use play lists and other statistical approximations of audio play, including for example, data obtained through the manual (i.e., by persons) monitoring of a statistically significant sample of stations and transmission times so that an extrapolation may be made to a larger number of comparable markets.

The present invention creates a second database from the first database, wherein each of the stored audio signals in the first database is data reduced in a manner that is not likely to reflect the human perceptual quality of the signal, meaning that a significantly data-reduced signal is not likely to be played back and recognized as the original signal. As a result of the data reduction, the size of the second database (as measured in digital terms) is much smaller than the size of the first database, and is determined by the rate of compression. If, for example, if 24 hours worth of audio signals are compressed at a 10,000:1 compression rate, the reduced data could occupy a little more than 1 megabyte of data. With such a large compression rate, the data to be compared and/or analyzed may become computationally small such that computational speed and efficiency are significantly improved.

With greater compression rates, it is anticipated that similarity may exist between the data compressed abstractions of different analog signals (e.g., recordings by two different artists of the same song). The present invention contemplates the use of bit-addressable differences to distinguish between such cases. In applications where the data to be analyzed has higher value in some predetermined sense, cryptographic protocols, such as a hash or digital signature, can be used to distinguish such close cases.

In a preferred embodiment, the present invention may utilize a centralized database where copies of new recordings may be deposited to ensure that copyright owners, who authorize transmission or use of their recordings by others, can independently verify that the object is correctly monitored. The rules for the creator himself to enter his work would differ from a universally recognized number assigned by an independent authority (say, ISRC, ISBN for recordings and books respectively). Those skilled in the art of algorithmic information theory (AIT) can recognize that it is now possible to describe optimized use of binary data for content and functionality. The differences between objects must relate to decisions made by the user of the data, introducing subjective or cognitive decisions to the design of the contemplated invention as described above. To the extent that objects can have an optimized data size when compared with other objects for any given set of objects, the algorithms for data reduction would have predetermined flexibility directly related to computational efficiency and the set of objects to be monitored. The flexibility in having transparent determination of unique signal abstracts, as opposed to independent third party assignment, is likely to increase confidence in the monitoring effort by the owners of the original signals themselves. The prior art allows for no such transparency to the copyright creators.

SAMPLE EMBODIMENT 2

Another embodiment of the invention relates to visual images, which of course, involve at least two dimensions.

Similar to the goals of a psychoacoustic model, a psychovisual model attempts to represent a visual image with less data, and yet preserve those perceptual qualities that permit a human to recognize the original visual image. Using the very same techniques described above in connection with an audio signal, signal monitoring of visual images may be implemented.

One such application for monitoring and analyzing visual images involves a desire to find works of other artists that relate to a particular theme. For example, finding paintings of sunsets or sunrises. A traditional approach might involve a textual search involving a database wherein the works of other artists have been described in writing. The present invention, however, involves the scanning of an image involving a sun, compressing the data to its essential characteristics (i.e., those perceptual characteristics related to the sun) and then finding matches in a database of other visual images (stored as compressed or even uncompressed data). By studying the work of other artists using such techniques, a novice, for example, could learn much by comparing the presentations of a common theme by different artists.

Another useful application involving this type of monitoring and analyzing is the identification of photographs of potential suspects whose identity matches the sketch of a police artist.

Note that combinations of the monitoring techniques discussed above can be used for audio-visual monitoring, such as video-transmission by a television station or cable station. The techniques would have to compensate, for example, for a cable station that is broadcasting a audio channel unaccompanied by video.

Other embodiments and uses of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. The specification and examples should be considered exemplary only with the true scope and spirit of the invention indicated by the following claims. As will be easily understood by those of ordinary skill in the art, variations and modifications of each of the disclosed embodiments can be easily made within the scope of this invention as defined by the following claims.

WHAT IS CLAIMED IS:

1. A method for monitoring and analyzing at least one signal comprising:

receiving at least one reference signal to be monitored;

creating an abstract of said at least one reference signal;

storing the abstract of said at least one reference signal in a reference database;

receiving at least one query signal to be analyzed;

creating an abstract of said at least one query signal;

comparing the abstract of said at least one query signal to the abstract of said at least one reference signal to determine if the abstract of said at least one query signal matches the abstract of said at least one reference signal.

2. The method of claim 1 wherein

the step of creating an abstract of said at least one reference signal comprises:

inputting the reference signal to a processor;

creating an abstract of the reference signal using perceptual qualities of the reference signal such that the abstract retains a perceptual relationship to the reference signal from which it is derived; and

the step of creating an abstract of said at least one query signal comprises:

inputting the at least one query signal to the processor;

creating an abstract of the at least one query signal using perceptual qualities of the at least one query signal such that the abstract retains a perceptual relationship to the at least one query signal from which it is derived.

3. The method of claim 1 further comprising:

creating at least one counter corresponding to one of said at least one reference signals, said at least one counter being representative of the number of times a match is found between the abstract of said at least one query signal and the abstract of said at least one reference signal; and

incrementing the counter corresponding to a particular reference signal when a match is found between an abstract of said at least one query signal and the abstract of the particular reference signal.

4. The method of claim 1 further comprising:

recording an occurrence of a match between the abstract of said at least one query signal and the abstract of said at least one reference signal; and

generating a report that identifies the reference signal whose abstract matched the abstract of said at least one query signal.

5. The method of claim 4, further comprising:

recording an occurrence of a match between the abstract of said at least one query signal and the abstract of said at least one reference signal.

6. The method of claim 1, further comprising permitting access to a secured area when the abstract of said at least one query signal matches the abstract of said at least one reference signal.

7. The method of claim 1, wherein

the step of creating an abstract of said at least one reference signal comprises:

using a portion of said at least one reference signal to create an abstract of said at least one reference signal; and

the step of creating an abstract of said at least one query signal comprises:

using a portion of said at least one query signal to create an abstract of said at least one query signal.

8. A method for monitoring a plurality of reference signals, comprising:

creating an abstract for each of the plurality of reference signals;

storing each of said abstracts in a reference database;

receiving at least one query signal to be analyzed;

creating an abstract of each of the at least one query signals;

locating an abstract in the reference database that matches the abstract of each at least one query signal; and

recording the identify of the reference signal whose abstract matched the abstract of each at least one query signal.

9. The method of claim 8, wherein

the step of creating an abstract for each of a plurality of reference signals comprises:

inputting each of the plurality of reference signals to a processor;

creating an abstract of each one of the plurality of reference signals using perceptual qualities of each one of a plurality of reference signals such that the abstract retains a perceptual relationship to the reference signal from which it is derived; and

the step of creating an abstract of each of the at least one query signals comprises:

inputting each of the at least one query signals to a processor;

creating an abstract of each one of a plurality of reference signals using perceptual qualities of each one of a plurality of reference signals such that the abstract retains a perceptual relationship to the reference signal from which it is derived

10. The method of claim 8, wherein

the step of creating an abstract of said at least one reference signal comprises:

using a portion of said at least one reference signal to create an abstract of said at least one reference signal;

and the step of creating an abstract of said at least one query signal comprises:

using a portion of said at least one query signal to create an abstract of said at least one query signal.

11. The method of claim 8, further comprising:

creating at least one counter corresponding to one of said plurality of reference signals, said at least one counter being representative of the number of times a match is found between the abstract of said at least one query signal and an abstract of one of said plurality of reference signals; and

incrementing the counter corresponding to a particular reference signal when a match is found between an abstract of said at least one query signal and the abstract of the particular reference signal.

12. The method of claim 8, further comprising permitting access to a secured area when the abstract of said at least one query signal matches an abstract of one of said plurality of reference signals.

13. A computerized system for monitoring and analyzing at least one signal:

a processor that creates an abstract of a signal using selectable criteria;

a first input that receives at least one reference signal to be monitored, said first input being coupled to said processor such that said processor may generate an abstract for each reference signal input to said processor;

a reference database, coupled to said processor, that stores abstracts of each at least one reference signal;

a second input that receives at least one query signal to be analyzed, said second input being coupled to said processor such that said processor may generate an abstract for each query signal;

a comparing device, coupled to said reference database and to said second input, that compares an abstract of said at least one query signal to the abstracts stored in the reference database to determine if the abstract of said at least one query signal matches any of the stored abstracts.

14. The system of claim 13, further comprising:

a storage medium coupled to said first input, that stores each of said at least one reference signals to be monitored; and

a controller coupled to the first input, the processor, the comparing device, the reference database and the storage medium, said controller causing an abstract for each reference signal being input for the first time to be compared to all previously stored abstracts in the reference database, such that in the event that the comparing device determines that it cannot distinguish between the abstract of a reference signal being input for the first time from a previously stored abstract in the reference database, the controller adjusts the criteria being used by the processor and re-generates the reference database, by re-processing each reference signal stored on the storage medium to create new abstracts and storing said new abstracts in the reference database.

15. The system of claim 14, wherein the controller includes a means to adjust compression rates at which the processor processes a signal to create an abstract.

16. The system of claim 13, wherein the comparing device identifies at least two abstracts in the reference database that match the abstract of said at least one query signal and an index

of relatedness to said at least one query signal for each of said at least two matching abstracts.

17. The system of claim 13, further comprising:

a security controller that controls access to a secured area, such that access is granted only if the comparing device confirms that an abstract of said at least one query signal matches an abstract of said at least one reference signal.

18. The system of claim 13, wherein said first input and said second input are the same.

19. The system of claim 13, wherein said second input is remotely coupled to the processor.

20. The system of claim 13, further comprising:

a recorder that records the identify of the reference signal whose abstract matched the abstract of said at least one query signal; and

a report generator that generates a report that identifies the reference signals whose abstracts matched the abstract of said at least one query signal.

21. A electronic system for monitoring and analyzing at least one signal, comprising:

a first input that receives at least one reference signal to be monitored,

a first processor that creates an abstract of each reference signal input to said first processor through said first input;

a second input that receives at least one query signal to be analyzed,

a second processor that creates an abstract of each query signal;

a reference database that stores abstracts of each at least one reference signal;

a comparing device that compares an abstract of said at least one query signal to the abstracts stored in the reference database to determine if the abstract of said at least one query signal matches any of the stored abstracts.

22. The system of claim 21, wherein said second input is remotely coupled to the system.

23. The system of claim 21, wherein said second processor is remotely coupled to the system.

24. The system of claim 21, wherein the system transmits the criteria that are being used by the first processor to the second processor.

25. The system of claim 21, further comprising:

a storage medium coupled to said first input, that stores each of said at least one reference signals to be monitored; and

a controller that compares an abstract for each reference signal being input for the first time to be compared to all previously stored abstracts in the reference database, such that in the event that the comparing device determines that it cannot distinguish between the abstract of a reference signal being input for the first time from a previously stored abstract in the reference database, the controller adjusts the criteria being used by the processor and re-generates the reference database, by re-processing each reference signal stored on the storage medium to create new abstracts and storing said new abstracts in the reference database.

METHOD AND DEVICE FOR MONITORING AND ANALYZING SIGNALS

ABSTRACT OF THE DISCLOSURE

A method and system for monitoring and analyzing at least one signal are disclosed. An abstract of at least one reference signal is generated and stored in a reference database. An abstract of a query signal to be analyzed is then generated so that the abstract of the query signal can be compared to the abstracts stored in the reference database for a match. The method and system may optionally be used to record information about the query signals, the number of matches recorded, and other useful information about the query signals. Moreover, the method by which abstracts are generated can be programmable based upon selectable criteria. The system can also be programmed with error control software so as to avoid the re-occurrence of a query signal that matches more than one signal stored in the reference database.

EXCHANGE MECHANISMS FOR DIGITAL INFORMATION PACKAGES WITH BANDWIDTH SECURITIZATION, MULTICHANNEL DIGITAL WATERMARKS, AND KEY MANAGEMENT

RELATED APPLICATIONS

This application is related to patent applications entitled "Steganographic Method and Device", Serial No. 08/489,172 filed on June 7, 1995; "Method for Human-Assisted Random Key Generation and Application for Digital Watermark System", Serial No. 08/587,944 filed on January 17, 1996; "Method for Stega-Cipher Protection of Computer Code", Serial No. 08/587,943 filed on January 17, 1996; "Digital Information Commodities Exchange", Serial No. 08/365,454 filed on December 28, 1994, which is a continuation of Serial No. 08/083,593 filed on June 30, 1993; and "Optimization Methods For The Insertion, Protection, and Detection of Digital Watermarks In Digital Data", Serial No. ___ ______, filed on ___ __________. These related applications are all incorporated herein by reference.

This application is also related to U.S. Patent No. 5,428,606, "Digital Information Commodities Exchange", issued on June 27, 1995, which is incorporated herein by reference.

BACKGROUND OF THE INVENTION

The present invention relates to digital watermarks.

Digital watermarks exist at a convergence point where creators and publishers of digitized multimedia content demand localized, secured identification and authentication of that content. 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. 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 a reduction of its value, in order to remove such data for the purpose of subsequent, unauthorized distribution, commercial or otherwise. Legal precedent or attitudinal shifts recognizing the importance of digital watermarks as a necessary component of commercially-distributed content (audio, video, game, etc.) will further the development of acceptable parameters for the exchange of such content by the various parties engaged in such activities. These may include artists, engineers, studios, INTERNET access providers, publishers, agents, on-line service providers, aggregators of content for some form of electronic delivery, on-line retailers, individuals and other related parties that participate in the transfer of funds or arbitrate the actual delivery of content to intended recipients.

There are a number of hardware and software approaches that attempt to provide protection of multimedia content, including encryption, cryptographic containers, cryptographic envelopes or "cryptolopes", and trusted systems in general. None of these systems places control of copyrights in the hands of the content creator as content is created. Further, none of these systems provide an economically feasible model for the content to be exchanged with its identification embedded within the signals that comprise the content. Given the existence of over 100 million personal computers and many more noncopyright-protected consumer electronic goods (such as audio clips, still pictures and videos), copyrights are most suitably placed within the digitized signals. Playing content is necessary to determine or "establish" its commercial value. Likewise, advertising and broadcast of samples or complete works reinforces demand for the content by making its existence known to market participants (via radio, television, print media or even the INTERNET).

Generally, encryption and cryptographic containers serve copyright holders as a means to protect data in transit between a publisher or distributor and the purchaser of the data. That is, a method of securing the delivery of copyrighted material from one location to another is performed by using variations of public key cryptography or other cryptosystems. Cryptolopes are suited specifically for copyrighted text that is time sensitive, such as newspapers, where intellectual property rights and origin are made a permanent part of the file.

The basis for public key cryptography is provided, for example, in a number of patented inventions. Information on public-key cryptosystems can be obtained from U.S. Patent No. 4,200,770 to Hellman et al., U.S. Patent No. 4,218,582 to Hellman et al., U.S. Patent No. 4,405,829 to Riverst et al., and U.S. Patent No. 4,424,414 to Hellman et al. Digitally-sampled copyrighted material is a special case because of its long term value coupled with the ease and perfection in creating copies and transmitting by general purpose computing and telecommunications devices. In this special case of digitally-sampled material, there is no loss of quality in derivative works and no identifiable differences between one copy and any other subsequent copy.

For creators of content, distribution costs may be minimized with electronic transmission of copyrighted works. Unfortunately, seeking some form of informational or commercial return via electronic exchange is ill-advised, absent the establishment of responsibility of specific copies or instances of copies or some form of trusted system in general.

SUMMARY OF THE INVENTION

The present invention allows the establishing of responsibility of specific copies or instances of copies using digital watermarks.

The present invention relates to methods for the management and distribution of digital watermark keys (e.g., private, semiprivate and public) and the extension of information associated with such keys in order to create a mechanism for the securitization of multimedia titles to which the keys apply.

The present invention additionally relates to "distributed" keys to better define rights that are traded between transacting parties in exchanging information or content.

The present invention additionally provides improvements in using digital watermark information. For example, the speed of performing a key search for watermarks within content is increased. Additionally, more than one party can cooperate in adding distinguished watermarks at various stages of distribution without destroying watermarks previously placed in the content.

Digital watermarks make possible more objective commercial exchanges of content. Trusted systems are more costly but achieve the same goal by establishing the identity of all electronic exchange participants. Digital watermark per copy systems, however, are not on a simple level of establishing responsibility of a master work and its derivative copy only. Multichannel watermarks with private, semiprivate and public keys used as different levels of neighboring rights assist in the creation of a self-contained model for the exchange of copyrighted works. Private key watermarks can be inserted into content to establish ownership rights (copyright, master right, etc.) with the content creator or an agent of the content creator maintaining control over the key. Semiprivate watermark keys can exist in a separate channel of the information signals that make up the work to be exchanged for subsequently delegating responsibility to distributors or sales entities to restrict resale rights in the same manner that physical goods have an exchange of title corresponding to their sale. And finally, public watermark keys exist as an independent component of the identification, authentication or advertising of a given work to be widely distributed over networks for initiating the purchase of a sought-after work. The market will still rely upon trusted parties who report any distribution or exchange of derivative watermarked copies of these "protected" works. Recognition of copyrights as well as the desire to prevent piracy is a fundamental motive of enforcement which uses the mechanism of digital watermarks to alleviate fears of copyright holders and transacting parties that responsibility and payment for copyrights cannot be established and accomplished.

A necessity has arisen for a system that better defines methods for recognizing these rights and, with the further creation of bandwidth rights, as in the present invention, makes possible a distributed model for digital distribution of content which combines the security of a digital watermark system with efficient barter mechanisms for handling the actual delivery of digital goods.

The present invention relates to methods for the management and distribution of digital watermark keys (e.g., private, semiprivate and public) and the extension of information associated with such keys in order to create a mechanism for the securitization of multimedia titles to which the keys apply. To differentiate the present invention from public key cryptography, use of "private ", "semiprivate", and "public" keys herein refers to the use of such "information" with the stated purpose of distributing goods and watermarking content, not encryption or cryptography in the general sense.

The present invention additionally relates to "distributed" keys to better define rights that are traded between transacting parties in exchanging information or content. Such keys can carry additional pricing and timing information, and represent coupons, warrants or similar financial instruments for purchase of copies of the corresponding title at particular prices within a specified period of time. These instruments, as extended keys, can be collected on servers, distributed to individuals and redeemed as part of a transaction to purchase the content. The basis for this type of content trading system is described in U.S. Patent No. 5,428,606 entitled "Digital Information Commodities Exchange" (hereinafter, also referred to as "the DICE patent"). The present invention improves on the invention described in the DICE patent by integrating into the DICE exchange (i.e., The Digital Information Commodities Exchange) the copyright protection mechanism of digital watermarks. Digital watermarks are described in the following patent applications assigned to The DICE Company: "Steganographic Method and Device", Serial No. 08/489,172; "Method for Stega-Cipher Protection of Computer Code", Serial No. 08/587,943; "Method for Human Assisted

Random Key Generation and Application for Digital Watermark System", Serial No. 08/587,944; and "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data", Serial No. ___________.

In addition, the present invention improves upon the techniques of digital watermark systems, described in the patent applications listed above, by adding methods for the use of this information which allow for improvements in the speed of performing a key search for watermarks within content, and by allowing for more than one party to cooperate in adding distinguished watermarks at various stages of distribution without destroying watermarks previously placed in the content. At the same time, these methods minimize the amount of information which any one party must divulge to another party, and prevent "downstream" parties from compromising or otherwise gaining control of watermarks embedded by "upstream" parties.

Further improvements of the present invention include the incorporation of retail models using well-known commodities exchanges to accomplish more efficient means of advertising, negotiating, and delivering digital goods in an anonymous marketplace as commonly characterized by such systems as the INTERNET. Video-on-demand models, quality of service reservations considered in subscriber models, and related models that have been referred to as "time shares" for parceling up processing time in a general computing network will also be differentiated.

DETAILED DESCRIPTION

There are several issues preventing greater volumes of electronic distribution of multimedia content. While such distribution is in fact technically feasible at the present time, attempts at commercially-viable systems are still plagued by these problems, and render digital multimedia exchanges unsatisfactory on a scale comparable to mass retailing in consumer goods markets, such as that of digital audio recordings on compact discs (CDs). While it is possible to transmit a single copy of a digital recording, as 16-bit 44.1 kHz stereo (CD-quality), to an individual from an archive, making such copies available to a large number of paying consumers on demand is still not yet being implemented. The problems fall into several classes, including distribution bandwidth, copyright protection, technological complexities, and "efficient shopping."

In a similar vein to distribution of physical goods in the real world, bandwidth and developments that effectively increase bandwidth are creating profound new business models in how content creators and publishers can distribute their works. From the simplest compression schemes, to actual use of "wired" technology including ISDN, cable modems, ATM and fiber optic lines, the trend is moving toward greater amounts of bandwidth available to on-line users. It is a conundrum of the digital age that the object of bandwidth use will most likely require downloads of copyrighted works, or transaction-based models, to justify such increases in bandwidth availability.

The actual works sought exist as a predefined set of protocols or standards that, when adhered to by hardware or software, can be played back flawlessly many times over. Such works include 74 minute CDs and 300 MB CD-ROMs, among the many physical transport media that now exist. However, the actual digital signals that make up the audio or video clip are not dependent on new playback standards or PC playback software. Simply put, "clips" do not need additional steps to be played back. The signals that a CD carries are not dependent on the CD for its commercial value and could just as easily be carried on a DAT, Minidisc, DVD or any other physical medium that can carry to a consumer audio signals (for example) in a format of 44.1 kHz and 16 bits ("CD quality"). The most apparent drawback is that CDs are not recordable mediums, like cassettes or the above mentioned mediums, so that they are not as economical when coupled with prevalent recording devices such as DAT recorders, PC hard drives, DVD recorders, etc., or when coupled with the advent of electronic lines or "pipes" to the home.

Compression can be both lossless and lossy and has an effect on how a given piece of content can be commercially-valued in the marketplace. Physical goods pricing can be thought of similarly with cassette tapes and CDs which trade at divergent values because of audio quality and degradation, or lack thereof, of such quality over time. Although manufacturing costs of CDs are lower than cassettes, CDs are actually more expensive than cassettes in the marketplace. Presumably a premium is placed on the quality of the stored content, music or otherwise, and the durability of the medium itself, which can be played without loss of quality far more times than any analog tape. However, the CD is a storage media that must be manufactured, put into inventory, sent by carrier to physical locations, etc., and has an inherent tendency to standardization (the CD is actually a specification determined by manufacturers of both the hardware and software).

Hard costs for marketing and promotion may be better spent across a larger geographical segment, easily accomplished by such electronic networks as the INTERNET but harder to assess in terms of actual sales. Determining market reception is also difficult when buyers are relatively unknown and not available for localized comment or analysis in typical, physical retail store sites (such as Tower Records, Sam Goody's, Blockbuster, etc.).

What equalizes physical mediums such as DAT, CD and DVD, are the lines running between geographic locations, including POTs (i.e., Plain Old Telephone), cable, fiber optic, electric power lines and wireless access points including radio, satellite, cellular phones, and the like. The digitization of these access points and the networks that make them possible ultimately dictate what devices will be appropriate to consumers of the present day and the future. That is, matters of cost and even reputation will increasingly dictate the economics of the distribution of digital content, much the way matters of costs and reputation dictate sales in other consumer goods markets. No longer will it necessarily be important to manufacture X number of copies of a given work for distribution at N number of sites to capture the optimal market of consumers. The present invention is predicated on not only the existence of a plurality of access points, as discussed in the DICE patent (U.S. Patent No. 5,428,606), but also on a domain where digital content can pass freely between networks much as the INTERNET works with a common protocol (TCP/IP) to facilitate the exchange of data files. However, the ability and desire to orient delivery of digitized content around the specs that describe the content, rather than protocols necessary to redefine the content for exchange over a specific protocol (such as TCP/IP), can better define more convenient delivery of the content between publishers and subscribers given the heterogeneous nature of transmission media (POTs, cable, etc.), the unchanging behavior of "consumer electronically-described" media content (FM-quality, CD-quality, etc.), and the varying configurations of pipes utilized by both publishers and subscribers more concerned with the distribution and exchange of digital goods, not configurations of the immediate input and output devices that are linked by a multitude of electronic exchanges (cable, POTs, wireless, electric power, etc.). Indeed, shifting only the recordable media cost to consumers that, for the most part, already own one or more such devices and may have exposure to a number of broadcast and advertising media (INTERNET, on-line services, radio, cable, print, etc.) may afford both buyers and sellers the cheapest means of profitably exchanging digital goods.

At present, over 15% of the U.S. population has more than one phone line, 60 million households have cable television, and 15 million consumers are on-line subscribers. ISDN is also experiencing growing demand in the U.S. to give consumers higher bandwidth in the interim. Projected increases of bandwidth portend future supply and demand of larger data files of copyrighted passive works (e.g., music, pictures, video, etc.) and interactive works (e.g., games, software, etc.), thus putting pressure on the need for increases of bandwidth. Never before has increased available bandwidth suffered from a lack of demand by users. In other words, new bandwidth seems to create its own demand. Much of the presumption in increased investments in creating the bandwidth has been to enable the transfer of audio, video, and multimedia files that typically occupy more than 5 MB of space per file. The misanalyzed aspect of these investment plans is a method for addressing digital piracy of copyrighted works and efficient, market-based allocation of the subsequent bandwidth by users. The present invention better defines maximized operations dependent more on the specs that describe playback of content than redefining additional protocols which add additional and unnecessary levels to the playback of the content. With such advances, exchanging media content can potentially be made as easy as exchanging physical content.

The present invention additionally reduces costs in the distribution process, provides the monitoring of, and thus ability to protect, copyrights within the media, and allows the implementation of better payment systems suited to the distribution of digital goods. What is clear is that bandwidth may never be unlimited, but with consideration made to real world economics, efficient and realistic methods for considering "fill rate" (the actual titles "delivered" to a purchaser versus the titles "ordered"), speed (actual time it takes for a consumer to receive desired content), and cost (expense given trade-offs of immediate availability at a given price point to the consumer, e.g., immediate fulfilment equates to higher pricing, versus delayed delivery of the same content at a lower price) all represent input variables in a real world "retail experience" that may be replicated in the digital domain. The present invention takes into consideration the behavior of parties engaged in selling content that may not be initially valued at the same price by all market participants and is subject to the same promotion hype as goods in the real world. In the digital domain, sampling, trailers, and pre-release hype can be replicated to foster demand for a given title of a digital good with many of the same results that are experienced in the real world.

Evidence of supposedly more efficient schemes for retail include U.S. Patent No. 4,528,643 to Freeny, which shifts much of the manufacturing costs to physical retail sites, thus increasing the cost of doing business on the retail side with possible increases of convenience to the consumer. In the Freeny patent, retailers are envisioned to have localized reproduction of given digitized products (music, video, etc.) and a means to use "owner authorization codes" to verify the electronic transmission of a given work from some "master file unit" to recordable media (VCR, recordable CD, etc.). Freeny refers to mail order clubs and other direct marketing efforts as being inefficient versus the localized manufacturing structure. These predictions have since been proven false. It is because of the nebulous concept of intellectual property coupled with the extreme expense on retailers for the in-store manufacturing units that makes clear the benefit of leveraging available bandwidth to content creators, publishers, consumers and "pipe owners." The efficiency of such operations as Federal Express in delivering even small packages in under 24 hours and the ability of "fulfilment houses" to effectively carry all but the most obscure titles (music, books, videos, etc.) has made actual "manufacturing" of a given physical media object (CD, VHS tape, etc.) or what Freeny describes as a "material object" simply uneconomical and increasingly irrelevant in an age when bandwidth and digital recording devices such as PCs, Minidiscs, digital video disks (DVD), etc. make physical retail-based, or in-store, copying more of an inconvenience.

The paradox of digital copies is the ease and relatively inexpensive operation of making perfect copies from a single instance of a work, thus providing the potential of unauthorized copies or piracy. The binary data that comprises a digitized work is an approximation of an analog signal. As is well known binary ones and zeros can be manipulated to form words, audio, pictures, video, etc. Manners in which individual copies can be marked so that responsibility can be assigned to individual copies that are derivatives of the master copy is documented in the patent applications by The DICE Company referenced above (i.e., U.S. Patent No. 5,428,606, and the "Steganographicc Method and Device", "Method for Human-Assisted Random Key Generation and Application for Digital Watermark System", "Method for Stega-Cipher Protection of Computer Code", "Digital Information Commodities Exchange" and "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks In Digital Data" applications), and in alternative proposals by Digimarc Corporation (a form of pseudo-randomly encoding digital signatures into images), Bolt Beranek & Newman (Preuss et al. patent, U.S. Patent No. 5,319,735) (embedded signaling) and others. Additional proposals for cryptolopes and cryptographic containers by IBM and Electronic Publishing Resources (EPR) place control of copyrights and other "rights" in the control of IBM and EPR, not the individual content creator or publisher. IBM and EPR are creating a form of "trusted systems." What is clear is that trusted systems, where all parties are known in some way to establish responsibility for instances of copied files, are not realistically possible with the number and ease of manufacture of digitization systems such as general purpose computing devices. At present, over 100 million such devices are in existence, and it is not possible to guarantee that all of these systems will be made to adhere to the defined parameters of a trusted machine for verification and the establishment of responsibility for individual copies made of digital works. Profit motives continue to exist for individuals to make perfect copies and distribute these copies without paying the parties responsible for creating and distributing the content. Moreover, beyond considerations of digital exchanges that do establish responsibility for the goods being sought, the digital bits that comprise the commercially-valuable works suffer both from lack of use by parties seeking more secured means of distributing and marking content, and legal tanglings by parties that own the copyrights and seek any entity deemed to copy works illicitly for settlement of disputes. That is, with the great number of untrusted systems in existence, many copyright holders have resorted to legal challenges of on-line services and individuals found to be in possession of unauthorized copies of copyrighted works. The resultant digital marketplace tends to favor larger companies who can afford to seek legal settlements without delivering any substantial benefit over smaller companies that for many reasons would otherwise favor digital distribution of content to minimize overall costs. The remedy for such problems is addressed in the previously discussed related U.S. patent and patent applications by The DICE Company and other parties mentioned above (e.g., NEC, Digimarc, EPR, IBM, etc.)

The present invention relates to methods for parceling rights to benefit buyers and sellers of digital works in ways that even the playing field of the marketplace given the resource of electronic marketplaces that can work with such networks as the INTERNET. Too often physical world solutions are offered where digital domain considerations are completely ignored.

Another issue relating to the present invention involves haphazard grafting of physical world pricing and automated payment systems onto digital systems. Issues of inventory, physical movement, and manufacture of goods are completely muted in digital exchanges, but are replaced by bandwidth utilization and efficiency, one-to-one connections, and one-to-many connections, i.e., seeking and reaching customers in an anonymous marketplace. It is these issues that will better determine the price of a given digital good. Timing of the good (that is, live versus broadcast rerelease of the same digital good) and the necessity of filters or brokers which guide individuals to acceptable goods are variables that will play roles in determining the ultimate efficiency of exchanging digital goods.

Among some of the proposed systems are a proposal by Wave Systems, which necessitates the use of proprietary boxes using encryption to tie the user's "exchange device " to some party that can determine the validity of the box, a trusted system. Unfortunately, adoption of such a solution would necessitate the purchase of separate boxes for separate vendors of particular works or the routing of all digital goods through a proprietary system that then resembles closed cable, video-on-demand, and private networks. Similar approaches are used by merchants using credit card processors and the use of credit card authorization devices and paying incremental costs for the use and security delivered by the credit card processor. Further systems include log-in procedures to validate the accessing party's identification. The premium paid for such systems is arguably excessive when compared to content creator-controlled implementation of digital watermarks and an exchange by which all distribution parties are engaged in the marketplace to pay for bandwidth rights to market-test given digital goods. The only alternative available to smaller content creators and artists is to sell content at no charge, thus jeopardizing potential future returns, or purchasing outright the hardware to plug-in to existing networks, an excessive cost if such "bandwidth" could be more fairly-priced in a need-based system such as that discussed in this disclosure.

As an improvement to the system discussed in U.S. Patent No. 5,428,606, the present invention ties so-called "header" files into the actual content. U.S. Patent No. 5,428,606 addresses the separation of content from its references ("header") to facilitate more efficient access and exchange of digital content. The "headers" described in this patent might be construed in the real world as options or futures, and is discussed below. The present invention concerns itself with creating a method for introducing a layer of price and distribution determination given the necessity of payment in delivering digital content between points in the digital domain which may not suffer from any physical limitations but are limited by bandwidth considerations.

Some attempts at the exchange of content are being tried with existing networks such as the INTERNET. The complexities extant are apparent in the requirements of the operating protocols and the dependence of TCP/IP for orienting content and subsequently playing it back through "players" that are TCP/IP compliant, if the INTERNET is solely considered. More issues regarding the INTERNET are further discussed below.

Conceptually, "agents" partially meet some of the expectations of a content-based system, except agents are also dependent on participation by sites willing to allow for pure price comparisons and later reporting to the purchasing party. At present, many sites lock out such agents as they seek to profit by value-added services which are not considered by an agent when "shopping prices." Video-on-demand systems also propose a more closed system that is reliant on a proprietary network to deliver a video (or audio for that matter) to a consumer with the least amount of time delay while satisfying the demands for the video by many other consumers seeking the same video at the same time. The difference between such a system and that disclosed in the present invention is that such video-on-demand networks propose "subscriber" models where all consumers are deemed to have the same right to a given, demanded, piece of content at any time. That is, all participants are "subscribers" who prepay a fee structure that cannot necessarily be justified given bandwidth and processing limitations for delivering digital goods "on demand." In such a system, infrastructure cost can run as high as 5,000 dollars per subscriber, as with Time Warner's system in Orlando, Florida.

In the present invention, time is not an absolute standard to measure satisfaction. In the same manner that retail stores cannot always have a given audio or video work "on demand," other factors may play into the competitiveness of that entity to contribute to the satisfaction of a given consumer. These issues include a depth (number of copies or copyrights of a given title) or breadth (number) of titles offered, a variety of delivery mediums to satisfy customers with varying access infrastructure (cable, telephone, fiber optic, electric power, etc.), pricing, and, finally, service as it can be applied in an anonymous marketplace. Services may include the know-how of buyers employed by a given digital broker in offering samples of new releases or unknown artists, as well as special price offers given the amount and types of digital goods being purchased. What is certain is that a "subscriber" model is subject to the same deficiencies of a cable model or proprietary on-line service that may not be able to balance financial considerations with the variety and cost of titles sought by individuals at any given time. On the seller side, maximizing profit per title cannot always be satisfied if distribution control or proprietary rights are granted to any single entity which, by the present nature of the INTERNET and future interpretations of on-line commerce, cannot be guaranteed. Indeed, the above-mentioned U.S. Patent No. 5,428,606 discusses a situation where all subscribers can be publishers. For smaller parties, naturally lacking sufficient resources to initially and adequately market and promote titles, a more open system for negotiating distribution rights must be sought by commoditizing the good that most effects exchange of their goods in the digital domain (i.e., bandwidth).

Moreover, in an anonymous marketplace, even small aggregators of content may be able to adequately promote the digital properties of other small content creators with value-added services. These services, such as samples of content, used to entice buyers, just as trailers create demand for upcoming movies, could be delivered to a differing type of subscriber, much as the music aficionados who subscribe to College Music Journal (CMJ) and other resources to sample new, relatively uncommercial music. Samples of 10-30 seconds could be sent directly to consumer e-mail addresses replicating the prevalent listening bars set up by physical music retailers seeking to introduce new titles to eager listeners. Other services might be more representative of "music chat rooms" or special title web-sites, to more fully entice potential buyers with a greater amount of purchase information. Much of the premise of such services and fulfilling demand for content, however, will require a more efficient means to allocate bandwidth according to an embodiment of the present invention. Without such bandwidth allocation, even small digital goods vendors will need to purchase substantial hardware, from T1 lines to high-powered UNIX machines, meaning high entry or fixed costs, to effectively market what may only be a single title in a year.

The present invention deals with commoditization of the digital distribution of multimedia content. It is important to note that in creating such a market, one must consider two commodities. One is the title, or data itself, of which there is a theoretical unlimited supply over time (limited only by how many copies of a given title that can be made). The second commodity is bandwidth. This is a commodity which must be treated more like traditional commodities, since its supply is physically limited over discrete periods of time. "Fatter" pipes and compression can only increase upper limits given the observed tendency for larger data files to accompany bandwidth increases in the short term. In practice, bandwidth limits act as a parameter on the capacity of a distribution channel at any given moment in time, since there is a fixed amount of bandwidth. In dealing with commercial markets, where, for example, 80% of the consumers want 20% of the products, (and for digital marketplaces, generally all at the same instant), some premium can be observed as with "first come first serve" principles in physical sales channels. The difference is that an additional copy of a digital work can be made almost instantaneously, although additional bandwidth cannot be replicated. Even in instances with theoretically infinite time to fill all orders, most buyers will have given up and "left" the exchange after waiting a short period, during which time they get no satisfaction, measured explicitly by an access or download of a specifically desired title. On-line services today are typically plagued by this shortfall, leading most users to complaints of access and speed. Market-based principles could alleviate some of this problem on both the buyer and seller side if bandwidth is treated as the commodity it is. "Quality-of-service" proposals partially address this issue, though costs are stacked on the seller side because such systems are almost always proprietary given the requirement of high infrastructure expenses to enable timely delivery to all subscribers to the "private" network.

The present invention combines "efficient shopping" principles with the commoditization of bandwidth and titles to create an exchange, under principles as described in the DICE patent, where in place of a security, one can buy titles where a component of the title price is actually a bandwidth option, or bandwidth right. The purchaser buys a right on the underlying title to take delivery of the title via a particular transport medium which uses a particular allocation of transmission bandwidth at a particular time. According to an additional embodiment of the present invention, distributor or content aggregator-only purchases of bandwidth are stipulated as options for digital distribution increase, in terms of available channels (such as cable, satellite, etc.). In this case, the end user never deals with the bandwidth right, although the costs of such rights may by passed on in the retail price of the title which is purchased and downloaded. In other words, the distributor must purchase rights in advance to support a projected volume level of distribution. These pre-purchased rights are then attached to individual downloads. These instruments can vary in price, much like stock options, based on time. Only, in this case, it is the amount of time required to receive the underlying security, which implicitly indicates how much bandwidth will be used by the buyer. The bandwidth actually implies time. The spectrum could range from lowest bandwidth, such as an e-mail delivery by POTs lines, which uses bandwidth when it is otherwise not in use and is at the convenience o: the seller (sender), and not the buyer (receiver), to highest bandwidth that may be parallel or direct access fiber optic line which may be necessary for users acting as wholesalers between electronically -linked parties who seek content for negotiated delivery.

U.S. Patent No. 5,428,606 uses the concept of a "DIP" ("digital information packet") header to create an advertising, distribution, and pricing device which allows for the dissemination of references to and description of particular titles available electronically. The DICE Company's related digital watermark patent and patent applications as discussed previously disclose an exchange model for digitally-watermarked content and digital watermark keys whereby keys which allow a party to scan or imprint watermarks are distributed, possibly electronically, at the discretion of the controlling party. Both these methods have in common the fact that they allow for the distribution of some information related to an underlying work, without distributing the work itself. It is in the interest of simplicity, therefore, to allow for the combination or conjunction of these information items in addition to associating them with a bandwidth right or option for the downloading of the copyrighted work.

Essentially, some of this negotiation of bandwidth takes place between the "Baby Bells" and AT&T or other long distance providers when settling rights-of-way between points of a telephone conversation. At present, a key difference is that the utility value of a phone call sets the value of the "phone time" being sold. Bandwidth rights as envisioned in an embodiment of the present invention price the commodity of bandwidth given the luxury item being sought (i.e., data or content). The present invention seeks to value the immediacy as well as convenience (of which price may play a role) in receiving a given packet of data (media content, software, etc.) from one or many locations where it may be available to other locations. The lines may be heterogeneous between points, thus offering a more open bidding system between line owners, content creators and publishers, and end users or consumers. At present, no such "negotiation" can be handled by network operators running lines to the same home or office. Indeed, lines are usually charged at a fixed fee, not by what amount they are used. In some cases, lines are billed by a raw measure of the data transferred, but not in relation to the actual value of such data nor with respect to the value of other transfers which might occur simultaneously via the same line. This sort of billing-by-byte tends to discourage use, but it is a very coarse tool with which to manage utilization. To fill the middle market for demand of these lines for telecommunications lines in particular, long distance carriers such as AT&T, MCI and Sprint sell excess capacity to "wholesalers," while the larger companies generally have price constraints.

The potential demand for bandwidth is clearly evident with such widespread use of networks, epitomized by the INTERNET. But, as previously discussed, smaller, specialist "retailers" and "wholesalers" of services or content that could be marketed over these lines are not efficient. The potential for efficient pricing exists as demonstrated by "call-back" services, which route calls from one location through a third party location, benefitting from that location's line pricing, though the overall market for such services is still only about $300 million annually. What restricts more open allocation of bandwidth is political in nature. At the same time, cross subsidization of local phone access from more expensive long distance and international service is open for rationalization envisioned by the present invention. Even if more network services could offer greater returns for line use, and thus bandwidth use, public telephony accounts for over 85% of the market. A particular model being evaluated is called "sender takes all" where the access point, or the party that provides access to an end user, would take all the access charges. This is similar to the INTERNET, but is still stacked against smaller players, of which content providers are the least favored if they seek "distribution channels" over networks that still lack proper market incentives for use of bandwidth. Some other models being considered include a single access charge, which is an improvement over current international accounting standards being negotiated between countries. Still, this model does not take into consideration the available bandwidth controlled by non-telecommunications parties, such as cable companies, though ultimately the commodity being brokered is actually common bandwidth. The uneasy balance in negotiating access is being tempered by the steady increase by telecommunications companies to upgrade their lines to offer comparable bandwidth access as that presently available through cable companies. A final issue for consideration is the mobile market of cellular phones and other similar technologies though there are far more restrictions on the amount of available bandwidth for content distribution, the move to free up more radio spectrum for digital signals may lead to increases as high as a hundredfold in the capacity of the network which would make the electronic delivery of a single audio track realistic. Still, the present invention seeks the imposition of market-based pricing of available bandwidth to end users and content providers given the absence of any such system currently.

With the recent removal of barriers which previously prevented competition between cable companies, telecommunications companies, and regional Bell operating companies (RBOCs) the matter of cost of services or content being delivered over common pipes and the concept of a single entity dominating the "network" will almost surely come to an end as many companies are strongly positioned in their local markets. At present, "local loop" access to end users still presents formidable barriers to competition-- 40-45% of the cost of a long distance call is paid to the RBOC whose lines run into the home or business making the call. In total, the cost to a network for local distribution is approximately 80%. Proposals for separating a network into its infrastructure and service components would likely benefit from the invention being outlined. In such a scenario, the owner of the network would offer access to providers on the same terms, while managing the operation of the infrastructure. Simple models, such as flat rate INTERNET access, are problematic in the overall model for market-based pricing of bandwidth in that capital costs are completely ignored though such costs are the parameter by which any business model must be judged. Though the cost of an extra phone call over a given network may be negligible, the cost of pumping large multimedia files, which have far different utility value to users of the network versus a "telephone conversation, " is relatively high in the aggregate and can be witnessed with the progressively slow performance of many on-line providers and the INTERNET. The goal for network providers will be to offer value-added services to users as well as value-added access to content that is controlled by copyright holders seeking maximum distribution (given speed and quality) to content seekers. These parties may only need the network at certain times or for certain releases of content. Meanwhile, periphery services such as music sampling, game testing, beta software distribution, will most likely comprise value-added services beyond the present scope of strict telephony. The pressure, generated from capital cost concerns, to provide a system that prices speed and line capacity is aptly answered with the creation of bandwidth rights and incorporation of such rights into the electronic distribution of content. In this way, specialist companies will strive through buying bandwidth of transmission capacity and adding value by attracting customers seeking said companies' accessible content.

Bandwidth rights are necessary as an improvement over the art. The INTERNET currently dominates any discussion of digital distribution. The INTERNET is built over lines or pipes. It is an important observation that a) these pipes cost money to build, deploy and maintain, and b) the owners of the pipes must pay for their investment and earn some return, which is their motivation for building the infrastructure. The means by which files are transferred over the World Wide Web, the most mainstream segment of the INTERNET, is the use and interpretation of Hypertext Mark-up Language (HTML) and embedded URLs (Uniform Resource Locators) which is designed to "alias" and designate a single path between the party that is viewing a reference of a file and the underlying file. The user is unnecessarily "connected" to the actual file, which is called "aliasing," and has effectively created more network traffic and thus wasted bandwidth. This shortfall in HTML is affecting the INTERNET through inefficiencies resultant from the underlying connection-based TCP/IP protocol. In short, a lot of needless, bandwidth-wasting connections are continuously being created and destroyed. The current mechanics of the INTERNET will not be conducive to electronic commerce, and must necessarily change. This fundamental aspect of splitting content from references to that content is amply addressed in U.S. Patent No. 5,428,606.

The biggest problem can be summed up by observing that users of the INTERNET generally live under the misconception that data or content is, or should be, free. Although one can find specific instances of goods and services sold over the INTERNET, even downloadable software, the basic mechanism that underlies the sale is subject to this "fallacy of the free." There are actually many hidden costs, some of which were discussed above. As for the content creator or publisher of said works, monitoring of sites and legal enforcement of copyrights is still significantly difficult without better education of consumers and site administrators, as well as a means for detecting unauthorized copies on an archive as disclosed in the digital watermark filings. Recent legal actions against parties that distribute copyrighted music titles and game software has resulted in setting a "for price " trend that can be made more efficient by the present invention.

The present invention deals with creating a coherent pricing model for on-line distribution, which accounts for bandwidth utilization, maximizes pricing options and efficiency for sellers and buyers, and, additionally, as a result of the process of trading and pricing of the bandwidth options, ensures that usage of the limited bandwidth is orderly. All orders result from requests filled and thus are generally a function of the price of the so -called option on bandwidth. The present invention also presents improvements over exchanges that exist for the purpose of trading commodities such as stocks, bonds and other such securities. The distinctive feature of the preferred embodiment described below is the nature of the commodities being traded, bandwidth, and the unbounded potential of derivative copies of copyrighted works.

In current trading mechanisms NASDAQ (National Association of Securities Dealers Automated Quote system) is a well-known model. Looking at details of the NASDAQ market will illuminate exchange operations and the present invention's improvements over the present art for both market exchange mechanisms and implementations of a content-based system that monitors copyrights and optimizes the distribution of the underlying content.

The NASDAQ Market

NASDAQ is an exchange that trades in a finite number of "titles" or stock certificates, whereas the present invention is concerned with the potential of an infinite number of "titles" made up of digital bits-- each derivative copy having the same potential commercial value as the original master copy that was intended for trade. The limited or finite commodity in question on a DICE exchange is available bandwidth for the actual transmission and thus delivery of a demanded, digitized "piece" of content (audio clip, picture, video, virtual reality, software, etc.). Bandwidth is characterized by the pipes that connect buyers and sellers of digital information and include POTs, cable, fiber optic, ISDN, satellite, electric power lines, etc. On the other hand, NASDAQ deals with basic stock securities, publicly-traded shares in companies. There are a small number of derivative securities traded, notably warrants, but the mechanisms for supporting a particular security are fairly uniform. NASDAQ is primarily an electronic bulletin board where market makers advertise at what prices they are willing to buy and sell a particular security. These market makers maintain an inventory of tradeable securities for sale to other parties, whether agency or principal-based transactions. A market maker does not necessarily equal a broker, although a market maker can also be a broker. Both market makers and brokers can participate in the system, but market makers are the heart of it. A market maker is a paying member of the NASD (National Association of Securities Dealers). In effect, they own a stake in the market governing body, and agree to be obligated to buy or sell a certain minimal amount of shares, in order to provide liquidity in the market "Confidence" in the market mechanism, that is NASDAQ itself, is in the best interests of the participants or the ultimate buyers of securities will not be willing to bid on securities at uncompetitive prices. Similarly, an artist wishing to sell their commercially-valuable copyrighted content, must be relatively confident that each derivative, a perfect digital copy, has some mechanism for identifying the initial purchaser and give all subsequent market participants a way of ensuring the copy of the content they possess is not an illicit or unauthorized copy. Previously discussed disclosures on digital watermarks cover these issues as a means to bring more artists and publishers into the digital marketplace to increase activity and liquidity.

Like the "specialists" on the NYSE (New York Stock Exchange), NASDAQ market makers earn a profit on the spread between the BUY and SELL price of a stock, assuming they can buy low and sell high (or short high and buy low). Market makers risk their own capital, trading a group of stocks, and can generally make profits trading shares for incremental profits. Such an instance would be selling at 10 and buying at 9 7/8. Many market makers trade the same stocks competitively, and in general, the more firms that make a market in a given stock, the more liquid the trading of that stock is, simply because there are more ready buyers and sellers. Again as a means to describe the present invention some understanding of these market participants may be required in implementing the proposed system.

Although NASDAQ can be thought of as an "electronic" market, it is electronic, for the most part, only in the sense that instead of shouting across a floor at each other, traders generally advertise their price levels on a BBS (Bulletin Board System), which legally binds them to honor the price. They then field phone calls from traders at other member firms, who have seen the advertisements on the BBS, and agree to trades over the phone. Then, each side enters their transaction (if one side is a BUY, the other is a SELL) into on -site computers, which all feed into central mainframes and link up with each other. Many errors are introduced by this process, and an error report is produced at the end of the day, to be settled among the parties involved through after-hours reporting. So, there is really still a large low-tech component to NASDAQ which leads to discrepancies and inefficiencies.

The general public interacts with the market through brokers, who might also happen to work for a member firm. The chain of contact is individual to broker to trader, with traders interacting among each other, and filling orders for brokers. This also touches the issues of primary and secondary markets. When a stock goes public, called an IPO (Initial Public Offering), shares are bought up by a syndicate of market makers. This is the primary market. The proceeds of the IPO go to the issuing company, minus the underwriting fees, which are divided among the syndicate. The syndicate then sells shares to the public through brokers, and any other traders who want to trade them. The syndicate may profit again by selling the shares at higher prices than the original purchase price. This trading continues indefinitely or until bankruptcy. This is the secondary market. Prices in the secondary market can vary continuously and widely from the price set in the primary market.

Having summarized the system, we can discuss some of the inefficiencies and idiosyncrasies of NASDAQ to establish the parameters of the present invention in the preferred embodiment

One major problem is the uniform distribution of information. Theoretically, all traders should get the same information at the same time. However, NASDAQ does not accomplish this well. Since there are intermediate "concentrators" between the terminals and the hub, and specific terminals tend to watch specific groups of stocks, some of which may be significantly more active than others, generating a larger volume of information per second, which can cause back-ups, in general, the system is plagued by delays of an intermittent and non-uniformly distributed nature. There is no mechanism for detecting these problems, which may cause the display of old or incorrect prices for some stocks, and delay the dissemination of electronic orders on an unequal basis. Traders generally have several sources of information, and need to be "on their feet", so the burden of detection is, in effect, placed on humans. NASDAQ terminals do maintain a "heartbeat." If the terminal cannot get a response from the hub for a prescribed period of time, a problem is signaled by turning the screen a uniform yellow on black. However, most significant information delays do not trip this mechanism. Market makers have cooperated to run independent tests, and are well aware that one trader may see information up to several minutes before another. There is no aging of information. The present invention partially concerns itself with information aging as content can be time-sensitive, and up-to-date bandwidth rights pricing is important. Such instances include news reports, live broadcasts, initial "be first" demand for a particular piece of media content, and the like.

A NASDAQ hub may send out information to all routes simultaneously, but there can be large delays before it arrives at the destination. An example of a timing performance protocol, which can be employed to counter such problems, is NTP (Network Time Protocol) on UNIX networks. NTP does advanced diagnosis of point-to-point network performance to forecast timing delays between pairs of machines. It is used with time critical applications, but not widely so, as it is still considered quite esoteric. NASDAQ makes no use of such protocols. For more trustworthy information about bandwidth rights and the aging of a media content good, the present invention takes into account forecasted timing delays for pricing the subsequent bandwidth right as an overall component of the pricing of the media content being demanded, and delays in actually distributing this information. This is an improvement over the art as it is a more appropriate aspect of pricing media versus disseminating stock price information.

Before considering the present invention's clearing operations, which are vital to simplifying the otherwise tremendous task of figuring out who owes what to whom at the end of the day, a description of the art, a la NASDAQ, is required. Basically, clearing is the matching up of trades. If one side reports a SELL, and the other a BUY, these two sides must be put together to form a trade which results in the transfer of money to the seller, and the transfer of the security to a buyer. Any halves of trades that do not match are kicked back to the member firm who entered them, for resolution. Provided the trade is resolved, both sides again enter their sides, only late. The securities can be held in street name, meaning the brokerage house can hold the physical shares for the buyer. However, the task of transferring stock certificates and cash among brokerage houses is onerous. Instead, a special holding organization was created. This organization is independent of the stock exchanges, but works with their clearing computers. The holding organization maintains vaults filled with stock certificates, held for the brokerage, which in turn hold the stock in the names of their clients. Everyone maintains records of who owns what relative to their own organization. Should an owner actually request their certificates, they can be removed from the vault and delivered by way of the brokerage firm. At the end of a day's trading, the hub computers at each exchange (whether NASDAQ or NYSE) net out the differences among the member firms, in cash and stock, over many trades, and produce a report of who owes what to who, in net terms, relative to each stock. The firms have a certain number of days to settle the trades (which allows for correction of errors, and transfer of funds). This allows a single day to result in one transaction for each trading firm for each stock it trades. This sort of clearing is key to the efficiency of any trading system. With the exception of a certificate delivery request, no security certificates need be moved, and cash can be transferred by wire.

Defining the Value of Bandwidth Rights

It is an object of this invention to create a trading instrument which will break bandwidth resources into discrete, usable component pieces, and allow an electronic market system to set a price for this scarce commodity which sets an equilibrium level of supply and demand. The net effect of this instrument, and its trading system, will be to efficiently apportion bandwidth to users who wish to download or upload valuable information, in whatever form it takes. Bandwidth affects the speed of information transfer. If more bandwidth is used, speed increases, and the transfer is accomplished in less time. If an individual instance of this instrument is a bandwidth right, it can be observed that several factors will affect its value:

· Intrinsic Value

This value is measured versus a minimal standard telecommunications cost. If there is a single underlying telecommunications cost to the owner of the right of X dollars per minute, let min 0 represent the number of minutes it takes to download the information using the minimal bandwidth, and min 1 represent the number of minutes a to transfer the information at the bandwidth represented by this right. Note that min 0 >= min1.

Then the intrinsic value VI = X x (min0 - min1), or the amount of money saved in telecom costs at the higher bandwidth. The intrinsic value can be negative, which would imply a compensating premium placed on the time saved by using the more expensive transport.

· Percentage Chance of Failure

This probability recognizes the generally unreliable nature of the current telecommunications and transmission mediums as well as underlying computer systems. Rather than be burdened with the task of solving all of the "bugs" in a given piece of commercial software, it would be better to account for failure in the valuation. This value could be adjusted over time, as the failure probability of a system becomes more apparent, or changes. In short, this represents the percentage chance a user cannot exercise their right. It affects the expected value of the right. In this baseline approach, if the probability of failure is Pf, where 0 <= Pf <= 1, and the value of the right is V0, in the absence of failure, then Vf = (l-Pf)V0.

· Convenience Premium

This represents some premium, VC that a person is willing to pay to transfer their information within a specified period of time (i.e. "now" or "in the next 10 minutes"). This premium is likely to come out as the market sets the price for a right. If there is a formula for what the price should be, then the premium is simply the difference between the result of that formula, and the actual market price. This really measures the balance between supply and demand. The more demand in excess of supply, the higher C will rise. VC is then a function of supply and demand.

Vreal = Vtheoretical + VC

·Time Value

This is a function of the exercise period of the bandwidth right. It is proportional to Pf, since more time allows for recovery from an individual failure to transfer. There are two components of time, over what period a transfer can be initiated and for how long the transfer can last once it is initiated. Note that this is made more complex by congestion factors. For instance, if a user has a right for 10,000 kbps for 10 seconds, and the user wants to transfer 100,000 kb, it is not likely that the transfer can be done in exactly 10 seconds. Protocol overhead and congestion will add some increment of time. It is advisable to leave room in the exercise period for these factors, rather than trying to value the time value in some manner which accounts for these transient conditions. Thus:

$$V = (I-Pf)(VI + VT + VC)$$

$$\text{or } V = (1 - Pf)\,((X(min0-min1) + VT) + VC$$

The convenience premium, VC, should be independent of all other values (except V).

The equation behaves as such:

With increased failure probability decreasing rights value, independent of other variables, while increased demand relative to supply would drive up VC. We might try to compute VC by accounting for known demand and supply values, and in fact, it is of vital importance to know the supply, and to allocate it so that any right issued can be exercised within its exercise period.

Additionally, it is observed that a method is needed to allocate supply based on demand which accounts for unused rights. In other words, the system needs to over allocate supply to some degree, knowing that some rights may go unexercised, so that demand is filled as much as possible. This is similar to airlines' practice of overbooking flights.

Some mechanism must be in place to prevent attacks on the system, by a party, who, in effect, tries to corner the market in bandwidth, with no intention of using it, so that it goes unused. Naively, one would think that since one has to pay for the bandwidth, why would someone want to corner the market? Although bandwidth is not free, it should only comprise a small fraction of the value of the information to be transferred, and so this is not an unthinkable situation. The likeliest preventive measure is the existence of competition in transmission.

Another option is the potential need to necessitate a secondary market for the trading of bandwidth, which could be divided up by a trading syndicate, and traded on a secondary basis to users. In a manner of operations, telecommunications companies perform this role between national telecommunications systems to facilitate international phone usage. But the difference with the system envisioned in the present system is that "any" user could buy bandwidth rights at times of low demand, and hope to sell them at a profit in times of higher demand. This would seem to imply the exchange itself should do some proprietary trading in this manner, both to profit, and to ensure some bandwidth is available for sale to users when they need it. This will have a purpose to serve in making the market efficient in the future.

Bandwidth rights instruments are likely to be highly localized to specific subnets. Especially since certain types of connections may be available only from certain exchanges, and since failure probabilities are likely to vary with specific hardware, operating systems, and service providers. Additionally, the basic valuation equations above do not address telecommunications costs across various types of lines. This problem at least, might be solved by active maintenance of cost tables, designation codes for types of lines, and the designation of a low cost standard. The problem of moving rights between exchanges is made more difficult since supply/demand planning for one exchange will not translate to another, unless some means for interconnecting exchanges is developed, and exchange bandwidth planning is global. The race by many parties to link users to the INTERNET via varying access links (modem) including ISDN, POTs, cable, may further the need for common bandwidth pricing. What is clear is that the basic structure of the present invention would facilitate such planning to the benefit of all market participants: telecoms providers, INTERNET access companies, users and publishers as well as more general aggregators of content and bandwidth such as, phone companies, cable companies and satellite companies intending on providing services across multifarious line types.

Bandwidth Rights Accounting and Clearing

If a bandwidth right is securitized, the creation and supply of certificates, made unique by cryptographic methods to manage them, will also be necessary. Transferring certificates between individuals is complicated and unnecessary. Following the general principles of the securities clearing model described above seems to be in order. In this case, the exchange needs to create and manage an account for each party that can own or trade bandwidth rights. Additionally, a method for authenticating the party is required. With these two elements, a trading market can be implemented by the following methods:

The exchange creates and manages a supply of uniquely distinguished bandwidth rights certificates. These certificates are good for a specific period only. They may traded over the course of time, anywhere from the moment they are created to the expiration time. It is questionable whether a right should be exercisable once it is clear that even if a transfer is initiated, it cannot be completed given that right only. However, consider that the right is usable, but its value decreases rapidly as it approaches expiration (i.e. value is based on time left, not total transfer time). Once a certificate is expired it is deleted. Hash values incorporating a time-stamp could be used to serialize certificates. Such a cryptographic method is well noted in the art. US Pat No 5,136,646 and 5,136,647 ("Digital Document Time-Stamping With Catenate Certificate" and "Method For Secure Time-Stamping Of Digital Documents" respectively) describe methods for cryptographic time-stamping.

The exchange creates a central hub for planning bandwidth supply, accounting, and disseminating pricing information. Client-side software will value the rights relative to a particular user's needs, and used by any party trading rights. A seller creates a SELL advertisement, which is entered into the "exchange". The exchange verifies that the seller actually holds the right in their account. A buyer then enters a BUY offer against the sell advertisement.

The exchange validates the buyers, and then clears the transaction, transferring money from the buyer's payment method (credit card, etc.) to the seller's account, and the right to the buyer's account. The unbundled right may be so infinitesimal that the actual cost of the right must be bundled with the underlying content or information being sought. The rights could also be bound to underlying titles. This may be similar to attaching sales taxes, handling charges, and credit card use charges that are typically bundled with the cost of a given physical goods purchase.

Multichannel Watermarking Mechanisms and Techniques

One problem with previous digital watermark systems is the need for a mechanism by which multiple parties may add watermarks to a given piece of content at different stages of distribution, without requiring any one party to compromise the security of its watermarks to any other party. Although an "exchange" system allows for two-way communication, a particular "distribution path" may be taken to be the path by which a package of data travels from a source party to a destination party. So, a distribution may be a single side of an "exchange". In this context, it is useful to speak of parties to the distribution as "upstream" or "downstream" in relation to each other. The initial source would be farthest upstream, while the ultimate destination party would be farthest downstream, with any number of parties along points in the middle. If the data in a distribution flows from party A, through party B, to party C, then:

party A is upstream from parties B and C;

party B is downstream from party A, but upstream from party C;

and party C is downstream from parties A and B.

The above example should make clear the relationships between upstream and downstream parties.

It is a useful goal, and an accomplishment of embodiments of the present invention, to provide a mechanism and technique for the purpose of allowing any party to the distribution to add at least one channel of watermark information, which exists separately and is secured by means of a separate key, to the data of the distribution in such a manner as to ensure that one or more watermarks of the other parties to the distribution remain present in the data when it reaches its final destination.

A significant improvement over traditional metering systems is that exchange mechanisms are beneficially tied into content for more realistic metering of playing or recording content. With multichannel digital watermarks, a more robust means for metering content is made possible by parties not willing to create expensive proprietary distribution channels, but who do wish to capitalize on selling content in the economic method of metering. There are two immediately apparent schemes which might accomplish this. The first is described as a "passive" scheme and the second is described as an "active" scheme.

In a passive scheme, several assumptions must be decided and jointly agreed upon beforehand by all parties who wish to add watermarks. Based upon the total number of watermark channels to be used, where each party that wants to add a watermark is assumed to use at least one watermark channel, and the amount of data, and the desired minimal level of watermark security, a watermark system could encode watermarks at an appropriate sparsity such that random chance will cause some watermarks added by downstream parties to obliterate watermarks added by upstream parties. But by the same token, random chance will allow some of the watermarks of upstream parties to survive the encoding of watermarks by downstream parties by virtue of the fact that such watermarks do not occupy enough of the same data space to cause one to significantly interfere with the reading of another. The end result is that at least one watermark added by each party will be readable at the final destination. While such a passive scheme is appealing because of its relative simplicity, in which each party can add watermarks without considering the impact of any other party, once some initial parameters are set, this type of scheme requires a lot of testing to determine optimal settings given various initial conditions, and does not guarantee any particular level of watermark redundancy. It is quite haphazard, although technically feasible.

According to an advantageous embodiment of the present invention, an active scheme is implemented which is described as follows. The farthest party upstream, who presumably controls the ultimate copyrights and distribution rights of the data generates two keys. The first key is a regular watermark key, as described in previous related patent application disclosures by The DICE Company, particularly, including the "Method for Stega-Cipher Protection of Computer Code" application. This key is used for actual encoding and decoding of information from the watermark channel "owned" by this party. The second key is a new type of watermark key, called a master framework key, which dictates

how the entire data stream in general is to be packetized;

how the data stream packets are to be allocated among a predetermined number of reserved watermark channels; and

how the channels are to be assigned to downstream parties.

This information is the minimal amount of information which must be shared with downstream parties to enable them to add watermarks using their own regular watermark keys to their assigned channels. Notice that within a given channel, another key is still needed to extract a watermark. Therefore, while some information is potentially leaked, the watermarks are still secure. The master framework key, in effect, creates several virtual data streams within the real data stream, each of which can be accessed separately by the watermark system. The master framework key can then be shared on a limited or protected basis with only those downstream parties who the upstream party chooses to participate in the distribution. Such master keys could be distributed using well-known cryptographic art for key transmission. Each downstream party is responsible for generating their own regular watermark key, and watermarking their assigned channel with appropriately generated information using the combination of the master framework key and the regular watermark key, as the data is received and forwarded. This active scheme is much better than the passive scheme, since it ensures that watermarks added by downstream parties do not interfere in any way with those added by upstream parties, thus guaranteeing a maximal level of watermark redundancy, which is desirable, while minimizing the disclosure of watermark information necessary to downstream parties, which is undesirable. It is envisioned that systems that use a hybrid approach, incorporating some mechanisms and methods of the active scheme, but also relying on some methods of the passive scheme may be developed.

Keysearch Optimization Mechanisms and Techniques

Another issue of digital watermark system which must be adequately addressed is key search. When a suspect copy of content is obtained, the amount of work done to extract watermark information from the copy is bounded by the set of watermark keys which are potential candidates which may have been used to encode the hypothetical watermark(s) in the suspect data. It is an object of the invention described herein to minimize the amount of work and hence time required to search this set of keys, or keyspace, while ensuring confidence that all potential candidate keys have been searched, or at least those candidates with a significant probability of constituting the actual target of the search.

The watermark decode operation proceeds generally as follows: First a candidate key search group is generated, then a decode process is run using each candidate key until either all keys are exhausted and no watermark is extracted, or a watermark is extracted using a candidate key. Depending on the nature of the information in the extracted watermark, the search might continue with remaining keys, or terminate. One obvious method for improvement is to perform parallel searches trying multiple keys at the same time. Using powerful parallel hardware, real gains may be obtained using this method simply.

On slower, serial CPU-based hardware, real parallel gains are more difficult to make. However, using dynamic programming techniques and intelligent search scoring and management, one could configure the search engine to start with several or all keys, checking each packet of data against each key before proceeding. As each iteration is completed, factoring in the next data packet, cumulative "scores" for the results of each key may be computed and compared. Keys which appear to have more potential to ultimately yield a match and extract a watermark continue to be used in the process, while those with lower potential, as measured by score, are dropped from the process. This process has an attractive characteristic that it gets faster as more keys are progressively eliminated from the search space, and can consider a large number of keys. Its drawback, in the absence of other techniques, is that the initial key space may be very large, and it may take considerable time to narrow the search keys to the point where the search proceeds at a reasonably fast pace. It is also possible that the process of finding a match does not score in a monotonically increasing manner, resulting in the early elimination of the correct key. In other words, scores may get worse before they get better.

Without considering any information about the source copy used to generate the suspect copy, one could limit the search work done by imposing a limit on how much time a decoder can spend checking data versus a particular key, or a maximal percentage, or number of packets of the copy to process before giving up on a given key. One could do well with a heuristic rule that says, "if I have checked 50% of the recording without finding a watermark, then in all likelihood I will not find a watermark in the other 50% of the recording with this particular key," for instance. However, the best gains can be made by eliminating as many keys as possible from the initial search pool. In order to do this the keys are expanded to included several items of information regarding the source copy or master that was watermarked using the key in question. This information includes any of the following items:

Title, Artist, Date, size of recording, format of the recording, quality of the recording;

and may also include mathematically calculated properties of the recording which can identify the recording to some significant degree of probability while using only a small amount of data (i.e. localized hash values, etc.). When a suspect copy is obtained, this same set of information describing the suspect copy is generated by the decoder system, which can then select a set of candidate keys which match to a desired degree, any or all the criteria stored with the keys.

Finally, the best potential results may be obtained by taking advantage of the multiple access levels made possible by the watermark system described in previous filings. A watermark embedded in a higher privacy channel corresponds with a particular key. Every key has a unique identification which allows the key custodian to find the key in a database, but provides no information on the key itself. This identification may have no meaning outside the custodial system. If the higher privacy key identification is included in a lower privacy watermark such as a protected or public watermark, then the party searching for the higher privacy watermark makes use of an intentionally limited set of lower privacy keys to first extract the key identification of the higher privacy key. At this point, no additional key search is necessary, thus allowing significant time savings. This assumes the lower privacy watermark has not somehow been removed from the digital sample stream.

An embodiment of the decoder key search system encodes private key identifiers in lower privacy watermarks and uses descriptive information in the keys to compare versus the suspect copy to narrow the key search space. This embodiment makes use of parallel hardware to facilitate as much gain as possible from parallel search techniques described above, including progressive elimination of keys which appear to diverge from a match as the comparison progresses.

In an exchange mechanism according to an embodiment of the present invention, the exchange is not the source of any of the sought-after works or digital information packages (DIPs). The exchange is ultimately measured by available transmission resources. Whereas DIPs are measured in a digitization system, the size of the underlying data file, its file structure, which dictates any potential compression and buffering, and data overhead for error correction, will provide exchange participants with an estimate for the resources, including time required to distribute said DIP. Given the heterogeneous nature of existing and proposed line infrastructure, any DIP can potentially be exchanged over vastly different lines between points. These may include copper, coaxial, fiber optic, etc. Distribution of a given DIP may occur on different lines for the same work (say for instances of a wcrk available over POTs and satellite, etc.) or over a number of different media in the distribution of a work as it is transmitted over a network with a plurality of transmission media (say, the backbone of the network may be fiber but the end loop is coax, etc.). Given the existence of other traffic over these lines, including telephony, the pricing of a given DIP should necessarily include the price of the bandwidth resources necessary to transfer the DIP between at least two parties. As previously discussed, the difference in this embodiment and systems such as video-on-demand or proprietary cable and satellite systems is the necessity to value bandwidth between points in a network to facilitate the exchange of a demanded work at a given instant in time not continuously as with traditional "subscriber models." Similarly, "time-share" systems are oriented around selling a parcel of time to users seeking "processor" access to perform some activity, while, bandwidth is not the commodity being bid, time shares are reservation systems not capable of bidirectional or end-to-end "negotiation" of resources to facilitate the exchange of a DIP in real or next-to-real time. Further, the preferred embodiment differs in that all participants may have significantly different access infrastructure (differing modems, cable, electric powerline, satellite, etc.) and pricing preferences given demand for a particular DIP.

The price of the bandwidth resources is, thus, proportional to the percentage of bandwidth allocated to the transfer of the DIP and inversely proportional to the duration of the transfer. With these factors, the aggregate of available bandwidth must change with time and can appropriately be priced given the demand of certain DIPs or publishers seeking to effectively distribute DIPs. Bandwidth allocation can then be securitized to reflect the varying needs of market participants to exchange DIPs. How this security is priced relates to the nature of the underlying DIP which is most likely a luxury item such as a musical recording or video game. The securities must then trade independently of the DIPs and are based in part on a convenience premium, given demand for bandwidth allocation at any given time. Additionally, network resources as measured by present digital packet switches provide the variable of "supply of bandwidth resources" and estimated demand for said resources at a given time. For networks that are more centralized, such as cable or satellite, estimating bandwidth resources may actually be far easier as traffic is generally downstream to customers not bidirectional like telephone networks. Further means for computing bandwidth securitization instruments take into consideration probability of failure to exercise an instrument, the time period for which said instrument is valid, intrinsic value relative to minimum standard bandwidth utilization for the line in question. These factors, when coupled with a convenience premium, are improvements over the prior art as described in the U.S. Patent No. 5,428,606. Bidirectional exchange of content by parties who can be both subscribers or publishers or both, are possible when the party wishing to sell content or DIPs can set distribution, pricing, and other informational fields at its discretion. These issues are well documented in U.S. Patent No. 5,428,606 and are increasingly important in the growing popularity of the World Wide Web (WWW) portion of the INTERNET. But, given that the marketplace in which digital goods can be traded digitally is itself digital, the evident or potential scarcity of bandwidth or the ability to value existing bandwidth given a commercial market for digital goods exchange is invaluable.

Further, security of the content and records of said content can be further described as an improvement over methods to undeniably identify content through the use of digital watermarks and other similar technologies. It is desirable to take appropriate measures to protect as many parties as possible in the transaction of a copyrighted work. These parties may include the copyright holder, publisher, distributor, retailer, and consumer. As with the physical monitoring of media products such as CDs, where physical checks are conducted by the label, manufacturer, distributor, retailer and even outside parties such as SoundScan, Billboard, etc. the digital domain contains far less means for "hands-on" metering without including watermarks as "secured identification" for parties involved in the distribution chain. As a preferred embodiment of the present invention, a record of a given DIP should include at least two of any of the following three elements: a digital watermark key, a DIP header, and a bandwidth securitization instrument (bandwidth right). The DIP header describes the content, its address, pricing, and distribution. The bandwidth right is unique in its instance but also varies according to network bandwidth availability for a given period of time and the duration of the actual use of bandwidth on said network.

Optimizing key searches and increased use of multichannel digital watermarks are delineated in the discussions that follow this preferred embodiment as they are additional improvements over the art. The embodiment thus far discussed makes possible a more "democratically" or "economically" feasible market for the exchange of digital goods. With bandwidth rights, multichannel watermarking, optimized key searches, content-base metering, it will be possible to more fully replicate retail and wholesale environments as they exist in the physical world. Decisions about depth and breadth of services and goods that can be offered by on-line market participants will differ only in the ability to offer access to archives (POTs, cable, satellite, wireless, etc.) which will be determined by pricing and speed of transmission as well as by content providers interested in tapping into the potential distribution market that the pipe owner's network includes. Market participants will also be able to appeal to the anonymous parties that seek content through attractiveness of a "site, " amount of processing speed available for distributing digital goods, staff responsible for purchasing or creating available content for downloads, the number of available repurchase rights of copyrighted works: "electronic window-shopping" can be realized given heterogeneous networks, many digital goods, and the creation of bandwidth rights to complement digital watermarking systems. Simply, content can better be valued given the infrastructure of the digital domain while recognizing/he importance of tracking and monitoring the exchange of digital goods.

WHAT IS CLAIMED IS:

1. A method of pricing on-line distribution of digital information packages comprising determining an on-line distribution net price based on a price of bandwidth resources necessary to transfer the digital information package between at least two parties and based on an underlying price of the digital information package itself.

2. The method according to claim 1, wherein the price of bandwidth resources is proportional to a percentage of bandwith allocated to transfer of the digital information, and is indirectly inversely proportional to a duration of the transfer.

3. A method of creating a bandwidth securitization instrument comprising valuing bandwidth allocation as a scarce commodity.

4. A method of valuing a price and a convenience premium of bandwidth securitization instruments by facilitating an electronic market for free trading of said bandwidth securitization instruments independently of any particular digital information packages ultimately transferred using said bandwidth.

5. A method of computing a convenience premium, comprising steps of:

determining a supply of bandwidth resources;

determining a plurality of bandwidth securitization instruments which allocate the bandwidth resources; and

determining an estimated demand at a given moment in time for the bandwidth resources.

6. A method of computing a price for a bandwidth securitization security instrument as a function of its intrinsic value relative to a minimum standard bandwidth utilization, comprising steps of:

a) obtaining a minimum standard price;

b) determining an estimated convenience premium of the bandwidth securitization security instrument with respect to said minimum standard price;

c) determining a probability of failure to effect an exercise of the security;

d) determining an exercise period of the security instrument corresponding to a time during which it may be executed or redeemed; and

e) determining a price for the bandwidth securitization security instrument based on said steps a), b), c), and d).

7. A method of combining into one record, at least two of:

a digital watermark key,

a digital information packet (DIP) header, and a bandwidth securitization instrument (Bandwidth Right);

wherein the DIP header contains information including content description, content addressing and content pricing;

wherein a bandwidth securitization instrument may be incorporated by including a serialization identification code which is unique to an individual bandwidth right, where record of said right may exist separately from the record containing the serialization identification code;

wherein the bandwidth securitization instrument is a unique security which values the right to use a specific allocation of telecommunications bandwidth for a specific duration, where such right exists for a specified period of time, and where the duration begins at or after the temporal issuance of the security, and the exercise period ends contemporaneously with the termination of the duration period.

8. The method according to claim 7, wherein the bandwidth securitization instrument provides a right to use a given bandwidth allocation for a net duration over the exercise period where the net duration may be comprised of smaller sub-durations which are not necessarily temporally contiguous.

9. A method for optimizing key search operations comprising steps of:

associating content descriptive information with a key used to watermark content for candidate keys;

comparing the content descriptive information from each candidate key in a key;

searching against a suspect copy of a title, and using said comparison to eliminate keys which are evaluated as unlikely based on the matching criteria of the content descriptive information;

wherein criteria includes at least one of:

media format;

content length;

content title;

content author; and

content signal metrics which provide heuristic characterizations of the recorded signal.

10. A method for performing multi-party, multi-channel encoding of watermarks comprising generating a master framework key, wherein the master framework key describes packetization and channel allocation of a complete signal.

11. The method according claim 10, further comprising a step of:

distributing the master key and a channel assignment to each party who needs to watermark a channel described in the master key.

12. The method according to claim 11, further comprising a step of limiting distribution of the master key only to parties who need to add watermarks to the signal.

13. The method according to claim 12, further comprising a step performed at least one stage thereafter of:

generating a general watermark key, for use with the master key which dictates watermarking of packets assigned to a single channel of the master key watermarking said packets with said key.

14. A method of including a key identifier for a distinct watermark channel in the watermark contained in an additional separate and distinct watermark channel in the same digital sample stream, which is encoded and decoded with its own distinct key.

15. The method according to claim 14 further comprising a step of:

including the key identifier of a higher privacy watermark channel in the watermark contained in a lower privacy watermark channel for a purpose of expediting watermark search operations.

ABSTRACT OF THE DISCLOSURE

Responsibility can be established for specific copies or instances of copies of digitized multimedia content using digital watermarks. Management and distribution of digital watermark keys (e.g., private, semiprivate and public) and the extension of information associated with such keys is implemented to create a mechanism for the securitization of multimedia titles to which the keys apply. Bandwidth rights can be created to provide for a distributed model for digital distribution of content which combines the security of a digital watermark with efficient barter mechanisms for handling the actual delivery of digital goods. Distributed keys better define rights that are traded between transacting parties in exchanging information or content. More than one party can cooperate in adding distinguished watermarks at various stages of distribution without destroying watermarks previously placed in the content. Additionally, the amount of information which any one party must divulge to another party can be minimized, and "downstream" parties can be prevented from compromising or otherwise gaining control of watermarks embedded by "upstream" parties.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/08159

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04B 13/00; H04J 3/26; H04L 12/40
US CL :370/60, 85.11, 85.11; 375/260
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. : 370/32, 53, 54, 58.1, 58.2, 60, 60.1, 61, 62, 85.1, 85.11, 94.1; 375/257, 260, 267; 348/6, 7, 8, 10, 12, 16; 379/110, 219, 220

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 4,491,983, (PINNOW et al) 01 January 1985, col. 3, lines 22-45, col. 4, lines 16-33, col. 4, line 44 to col. 5, line 20.	1-7, 18-20, 26-27 and 30
Y	US, A, 4,958,341 (HEMMADY et al) 18 September 1990, col. 6, lines 4-59 and figure 2.	1-7, 18-20, 26-27 and 30

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be part of particular relevance

"E" earlier document published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search

13 SEPTEMBER 1995

Date of mailing of the international search report

17 NOV 1995

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
B. Harden for
HUY D. VU

Telephone No. (703) 308-6602

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US95/08159

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [ ] Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. [ ] Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Telephone Practice

I. Claims 1-7, 18-20, 26-27 and 30, drawn to an apparatus for exchanging information packets between plurality of modular expandable units over two transmission media. (375/260)

II. Claims 8-17, drawn to a method for publishing directory entries and publisher address. (375/260)

III. Claims 21-25, 28-29 and 31, drawn to a bus transmission system having a data bus and a separate control bus. (370/85.11)

1. [X] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[ ] No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet(1))(July 1992)★

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/00	A3	(11) International Publication Number: WO 96/42151
		(43) International Publication Date: 27 December 1996 (27.12.96)

(21) International Application Number: PCT/US96/10257

(22) International Filing Date: 7 June 1996 (07.06.96)

(30) Priority Data:
08/489,172 9 June 1995 (09.06.95) US

(71) Applicant: THE DICE COMPANY [US/US]; P.O. Box 60471, Palo Alto, CA 94306-0471 (US).

(72) Inventors: COOPERMAN, Marc, S.; 2929 Ramona, Palo Alto, CA 94306 (US). MOSKOWITZ, Scott, A.; Townhouse 4, 20191 East Country Club Drive, North Miami Beach, FL 33180 (US).

(74) Agents: ALTMILLER, John, C. et al.; Kenyon & Kenyon, 1025 Connecticut Avenue, N.W., Washington, DC 20036 (US).

(81) Designated States: CA, CN, FI, JP, KR, SG, European patent (AT, BE, CH, 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.

(88) Date of publication of the international search report: 13 February 1997 (13.02.97)

(54) Title: STEGANOGRAPHIC METHOD AND DEVICE

(57) Abstract

An apparatus and method for encoding and decoding additional information into a stream of digitized samples in an integral manner. The information is encoded using special keys. The information is contained in the samples, not prepended or appended to the sample stream. The method makes it extremely difficult to find the information in the samples if the proper keys are not possessed by the decoder. The method does not cause a significant degradation to the sample stream. The method is used to establish ownership of copyrighted digital multimedia content and provide a disincentive to piracy of such material.

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.

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/10257

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL :380/28

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. : 380/28; 340/825.34, 4, 23

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US, A, 4,908,873 (PHILIBERT et al) 13 MARCH 1990, See col. 5, lines 1-25.	1-32
A	US,A, 4,979,210 (NAGATA et al) 18 DECEMBER 1990, See Fig. 13.	1-32
A	US,A, 5,073,925 (NAGATA et al) 17 DECEMBER 1991, See Fig. 1.	1-32
A	US,A, 5,287,407 (HOLMES) 15 FEBRUARY 1994, See Fig. 1.	1-32
A	US,A, 5,365,586 (INDECK et al) 15 NOVEMBER 1994, See cols. 3 and 4.	1-32
A	US,A, 5,408,505 (INDECK et al) 18 APRIL 1995, See Fig. 4.	1-32

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 JUNE 1996	24 DEC 1996

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	SALVATORE CANGIALOSI
Facsimile No. (703) 305-3230	Telephone No. (703) 305-1837

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/10257

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US,A, 5,412,718 (NARASIMHALU et al) 02 MAY 1995, See Figs. 6A-6C	1-32

European Patent Office

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 96 91 9405

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
X	EP 0 581 317 A (INTERACTIVE HOME SYSTEMS) 2 February 1994 (1994-02-02) * page 3, line 6 - page 4, line 48 * ---	1,3,7	H04L9/00 H04N1/32
X	BENDER W ET AL: "TECHNIQUES FOR DATA HIDING" PROCEEDINGS OF THE SPIE, SPIE, BELLINGHAM, VA, US, vol. 2420, 9 February 1995 (1995-02-09), pages 164-173, XP000566794 ISSN: 0277-786X * paragraphs [03.4],[3.4.1] * ---	1,2,4,8	
L	ZHAO J ET AL: "EMBEDDING ROBUST LABELS INTO IMAGES FOR COPYRIGHT PROTECTION" PROCEEDINGS OF THE KNOWRIGHT. CONFERENCE. PROCEEDINGS OF THE INTERNATIONAL CONGRESS ON INTELLECTUAL PROPERTY RIGHTS FOR SPECIALIZED INFORMATION, KNOWLEDGE AND NEW TECHNOLOGY, XX, XX, 1995, pages 242-251, XP000571967 -----		

TECHNICAL FIELDS SEARCHED (Int.Cl.6)

H04N
G06T

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search	Date of completion of the search	Examiner
THE HAGUE	5 March 2004	Hazel, J

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

2

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00651

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL : 380/54
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. : 380/54, 2, 4, 9, 21, 23, 25, 28, 49, 50, 59; 283/73, 113, 17

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,349,655 A (MANN) 20 September 1994, see Abstract.	1
X	US 4,262,329 A (BRIGHT et al) 14 April 1981, see Abstract.	7

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search
04 APRIL 1997

Date of mailing of the international search report
29 APR 1997

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
BERNARR EARL GREGORY

Telephone No. (703) 306-4153

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00652

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :H04L 9/00
US CL :380/20
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. : 380/20, 54

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y, P	US, A, 5,530,759 (BRAUDAWAY ET AL) 25 June 1996, see Figs. 1-2.	1-11, 22

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document published on or after the international filing date
"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)
"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

"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
"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
"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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
06 MAY 1997	09 JUN 1997
Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer SALVATORE CANGIALOSI
Facsimile No. (703) 305-3230	Telephone No. (703) 305-1837

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00652

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. ☐ Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. ☐ Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. ☐ Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

Please See Extra Sheet.

1. ☐ As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. ☐ As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. ☐ As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. ☒ No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:
1-11 and 22

Remark on Protest
☐ The additional search fees were accompanied by the applicant's protest.
☐ No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet(1))(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/00652

BOX II. OBSERVATIONS WHERE UNITY OF INVENTION WAS LACKING
This ISA found multiple inventions as follows:

Group I, Claims 1-11, 22, drawn to an method of generating an encrypted digital watermark.

Group II, Claims 12-21 and 23 method of making and using a digital watermark.

The inventions listed as Groups I-II do not relate to a single inventive concept under PCT Rule 13.1 because under PCT Rule 13.2, they lack the same or corresponding technical features for the following Reasons: The invention of Group I lack the separate software, hardware devices or content monitoring. The invention of Group II lack the pseudo-Random key.

Form PCT/ISA/210 (extra sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US97/11455

A. CLASSIFICATION OF SUBJECT MATTER
IPC(6) :G09C 5/00 H04L 9/00
US CL :380/54, 3, 4, 23, 55; 283/73, 113, 17
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. : 380/54, 3, 4, 23, 55, 49, 51, 59; 283/73, 113, 17

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A, E	US 5,664,018 A (LEIGHTON) 02 SEPTEMBER 1997	1-27
A, P	US, 5,636,292 A (RHOADS) 03 JUNE 1997	1-27
A, P	US 5,617,119 A (BRIGGS ET AL.) 01 APRIL 1997	1-27
A, P	US 5,568,570 A (RABBANI) 22 OCTOBER 1996	1-27
A, P	US 5,530,759 A (BRAUDAWAY, ET AL.) 25 JUNE 1996	1-27
A	US 5,493,677 A (BALOGH, ET AL.) 20 FEBRUARY 1996	1-27

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document published on or after the international filing date
"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)
"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
"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
"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
"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
"&" document member of the same patent family

Date of the actual completion of the international search
23 OCTOBER 1997

Date of mailing of the international search report
23 DEC 1997

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
for DAVID CAIN
Telephone No. (703) 305-1836

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/07262

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N1/32

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)
IPC 6 H04N H04L

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 613 004 A (MOSKOWITZ SCOTT A ET AL) 18 March 1997 (1997-03-18) abstract column 6, line 30 - column 9, line 49 column 16, line 8 - line 64	1,2, 15-17, 26-28, 30-38,42
A	DELAIGLE J -F ET AL: "DIGITAL WATERMARKING" PROCEEDINGS OF THE SPIE, vol. 2659, 1 February 1996 (1996-02-01), pages 99-110, XP000604065 the whole document	1,5,6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"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)

"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

"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

"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

"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.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 July 1999	21/07/1999

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Hubeau, R

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/07262

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	SCHNEIDER M ET AL: "ROBUST CONTENT BASED DIGITAL SIGNATURE FOR IMAGE AUTHENTICATION" PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON IMAGE PROCESSING (IC, LAUSANNE, SEPT. 16 - 19, 1996, vol. 3, 16 September 1996 (1996-09-16), pages 227-230, XP002090178 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERSISBN: 0-7803-3259-8 the whole document	1,17,18, 26-28
A	COX I J ET AL: "SECURE SPREAD SPECTRUM WATERMARKING FOR MULTIMEDIA" IEEE TRANSACTIONS ON IMAGE PROCESSING, vol. 6, no. 12, 1 December 1997 (1997-12-01), pages 1673-1686, XP000724633 ISSN: 1057-7149 the whole document	1-3,5,6, 26,27
A,P	PING WAH WONG: "A Public Key Watermark for Image Verification and Authentication" IEEE INTERNATIONAL CONFERENCE ON IMAGE PROCESSING, vol. 1, 4 - 7 October 1998, pages 455-459, XP002108799 Los Alamitos, CA, USA the whole document	1-4

2

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 99/07262

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5613004 A	18-03-1997	EP 0872073 A WO 9642151 A US 5687236 A	21-10-1998 27-12-1996 11-11-1997

Form PCT/ISA/210 (patent family annex) (July 1992)

PATENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To: FLOYD B. CHAPMAN BAKER BOTTS L.L.P. 1299 PENNSYLVANIA AVE., NW WASHINGTON DC 20004	**PCT** NOTIFICATION OF TRANSMITTAL OF THE INTERNATIONAL SEARCH REPORT OR THE DECLARATION (PCT Rule 44.1)
	Date of Mailing (*day/month/year*) 18 AUG 2000
Applicant's or agent's file reference 066112.0135	FOR FURTHER ACTION See paragraphs 1 and 4 below
International application No. PCT/US00/06522	International filing date (*day/month/year*) 14 MARCH 2000
Applicant BLUE SPIKE, INC.	

1. [X] The applicant is hereby notified that the international search report has been established and is transmitted herewith.

Filing of amendments and statement under Article 19:
The applicant is entitled, if he so wishes, to amend the claims of the international application (see Rule 46):

When? The time limit for filing such amendments is normally 2 months from the date of transmittal of the international search report; however, for more details, see the notes on the accompanying sheet.

Where? Directly to the International Bureau of WIPO
34, chemin des Colombettes
1211 Geneva 20, Switzerland
Facsimile No.: (41-22) 740.14.35

For more detailed instructions, see the notes on the accompanying sheet.

2. [ ] The applicant is hereby notified that no international search report will be established and that the declaration under Article 17(2)(*a*) to that effect is transmitted herewith.

3. [ ] **With regard to the protest** against payment of (an) additional fee(s) under Rule 40.2, the applicant is notified that:

[ ] the protest together with the decision thereon has been transmitted to the International Bureau together with the applicant's request to forward the texts of both the protest and the decision thereon to the designated Offices.

[ ] no decision has been made yet on the protest; the applicant will be notified as soon as a decision is made.

4. **Further action(s):** The applicant is reminded of the following:

Shortly after **18 months** from the priority date, the international application will be published by the International Bureau. If the applicant wishes to avoid or postpone publication, a notice of withdrawal of the international application, or of the priority claim, must reach the International Bureau as provided in rules 90 *bis* 1 and 90 *bis* 3, respectively, before the completion of the technical preparations for international publication.

Within **19 months** from the priority date, a demand for international preliminary examination must be filed if the applicant wishes to postpone the entry into the national phase until 30 months from the priority date (in some Offices even later).

Within **20 months** from the priority date, the applicant must perform the prescribed acts for entry into the national phase before all designated Offices which have not been elected in the demand or in a later election within 19 months from the priority date or could not be elected because they are not bound by Chapter II.

Name and mailing address of the ISA/US Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	Authorized officer PAUL E. CALLAHAN

PATENT COOPERATION TREATY

PCT

INTERNATIONAL SEARCH REPORT

(PCT Article 18 and Rules 43 and 44)

Applicant's or agent's file reference 066112.0135	FOR FURTHER ACTION see Notification of Transmittal of International Search Report (Form PCT/ISA/220) as well as, where applicable, item 5 below.	
International application No. PCT/US00/06522	International filing date (*day/month/year*) 14 MARCH 2000	(Earliest) Priority Date (*day/month/year*) 24 MARCH 1999
Applicant BLUE SPIKE, INC.		

This international search report has been prepared by this International Searching Authority and is transmitted to the applicant according to Article 18. A copy is being transmitted to the International Bureau.

This international search report consists of a total of 4 sheets.

[X] It is also accompanied by a copy of each prior art document cited in this report.

1. **Basis of the report**
   a. With regard to the language, the international search was carried out on the basis of the international application in the language in which it was filed, unless otherwise indicated under this item.
   [ ] the international search was carried out on the basis of a translation of the international application furnished to this Authority (Rule 23.1(b)).
   b. With regard to any nucleotide and/or amino acid sequence disclosed in the international application, the international search was carried out on the basis of the sequence listing:
   [ ] contained in the international application in written form.
   [ ] filed together with the international application in computer readable form.
   [ ] furnished subsequently to this Authority in written form.
   [ ] furnished subsequently to this Authority in computer readable form.
   [ ] the statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.
   [ ] the statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.
2. [ ] **Certain claims were found unsearchable** (See Box I).
3. [ ] **Unity of invention is lacking** (See Box II).
4. With regard to the **title**,
   [X] the text is approved as submitted by the applicant.
   [ ] the text has been established by this Authority to read as follows:
5. With regard to the **abstract**,
   [ ] the text is approved as submitted by the applicant.
   [X] the text has been established, according to Rule 38.2(b), by this Authority as it appears in Box III. The applicant may, within one month from the date of mailing of this international search report, submit comments to this Authority.
6. The figure of the **drawings** to be published with the abstract is Figure No. 1
   [X] as suggested by the applicant.
   [ ] because the applicant failed to suggest a figure.
   [ ] because this figure better characterizes the invention.
   [ ] None of the figures.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/06522

Box III TEXT OF THE ABSTRACT (Continuation of item 5 of the first sheet)

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 reduced 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].

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, 300, 301, 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:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search

30 JUNE 2000

Date of mailing of the international search report

18 AUG 2000

Name and mailing address of the ISA/US
Commissioner of Patents and Trademarks

Authorized officer

PAUL E. CALLAHAN

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

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:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

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	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	PAUL E. CALLAHAN
Facsimile No. (703) 305-3230	Telephone No. (703) 305-1[illegible]

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

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

European Patent Office

SUPPLEMENTARY EUROPEAN SEARCH REPORT

Application Number
EP 00 91 9398

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.7)
X	WO 98 37513 A (TELSTRA R & D MAN PTY LTD ;BIGGAR MICHAEL (AU); JOHNSON ANDREW (AU) 27 August 1998 (1998-08-27) * page 6, line 25 - page 7, line 10 * ---	6	H04N7/167 H04N7/26 H04N1/32 G06F17/30
Y	US 4 969 204 A (MELNYCHUCK PAUL W ET AL) 6 November 1990 (1990-11-06) * column 2, line 9 - column 2, line 48 * ---	1-10	
Y	EP 0 651 554 A (EASTMAN KODAK CO) 3 May 1995 (1995-05-03) * column 6, line 43 - column 9, line 19; figure 2 * ---	1-10	
A	JOHNSON A ET AL: "TRANSFORM PERMUTED WATERMARKING FOR COPYRIGHT PROTECTION OF DIGITAL VIDEO" IEEE GLOBECOM 1998. GLOBECOM '98. THE BRIDGE TO GLOBAL INTEGRATION. SYDNEY, NOV. 8 - 12, 1998, IEEE GLOBAL TELECOMMUNICATIONS CONFERENCE, NEW YORK, NY: IEEE, US, vol. 2, 1998, pages 684-689, XP000825846 ISBN: 0-7803-4985-7 * page 685, left-hand column, paragraph 2 - page 685, left-hand column, paragraph 3 * ---	1-10	TECHNICAL FIELDS SEARCHED (Int.Cl.7) H04N G06F
P,X	WO 99 62044 A (HANDEL THEODORE G ;UNIV CALIFORNIA (US); SANDFORD MAXELL T II (US)) 2 December 1999 (1999-12-02) * abstract * * page 4, line 17 - page 5, line 5 * -----	6	

The supplementary search report has been based on the last set of claims valid and available at the start of the search.

Place of search	Date of completion of the search	Examiner
MUNICH	27 June 2002	Schoeyer, M

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

3

EPO FORM 1503 03.82 (P04C09)

P ENT COOPERATION TREATY

From the INTERNATIONAL SEARCHING AUTHORITY

To:
BAKER BOTTS L.L.P.
Attn. CHAPMAN, Floyd B.
THE WARNER
1299 PENNSYLVANIA AVENUE, N.W.
WASSHINGTON, D.C. 20004
UNITED STATES OF AMERICA

PCT

INVITATION TO PAY ADDITIONAL FEES

(PCT Article 17(3)(a) and Rule 40.1)

Date of mailing (day/month/year)	15/03/2001
Applicant's or agent's file reference: 066358.0106 031890.0007	PAYMENT DUE within 45 days from the above date of mailing
International application No.: PCT/US 00/18411	International filing date (day/month/year): 05/07/2000
Applicant: MOSKOWITZ, Scott A.	

1. This International Searching Authority

(i) considers that there are 2 *(number of)* inventions claimed in the international application covered by the claims indicated on the extra sheet:

and it considers that the international application does not comply with the requirements of unity of invention (Rules 13.1, 13.2 and 13.3) for the reasons indicated on the extra sheet:

(ii) [X] has carried out a partial international search (see Annex) [ ] will establish the international search report on those parts of the international application which relate to the invention first mentioned in claims Nos.:
1-5, 26-29

(iii) will establish the international search report on the other parts of the international application only if, and to the extent to which, additional fees are paid

2. The applicant is hereby **invited,** within the time limit indicated above, to pay the amount indicated below:

EUR 945,00 x 1 = EUR 945,00
Fee per additional invention — number of additional inventions — total amount of additional fees

Or, ______ x ______ = ______

The applicant is informed that, according to Rule 40.2(c), the payment of any additional fee may be made under protest, i.e., a reasoned statement to the effect that the international application complies with the requirement of unity of invention or that the amount of the required additional fee is excessive.

3. [ ] Claim(s) Nos. ______ have been found to be unsearchable under Article 17(2)(b) because of defects under Article 17(2)(a) and therefore have not been included with any invention.

Name and mailing address of the International Searching Authority European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Marja Brouwers

Form PCT/ISA/206 (July 1992)

COMMUNICATIC. ·ELATING TO THE RESULTS OF THE PARTIAL INTERNATIONAL SEARCH

In. ·ational Application No
PCT/US 00/18411

1. The present communication is an Annex to the invitation to pay additional fees (Form PCT/ISA/206). It shows the results of the international search established on the parts of the international application which relate to the invention first mentioned in claims Nos.:
1-5, 26-29

2. This communication is not the international search report which will be established according to Article 18 and Rule 43.

3. If the applicant does not pay any additional search fees, the information appearing in this communication will be considered as the result of the international search and will be included as such in the international search report.

4. If the applicant pays additional fees, the international search report will contain both the information appearing in this communication and the results of the international search on other parts of the international application for which such fees will have been paid.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	NL 1 005 523 C (EINDHOVEN TECH HOCHSCHULE) 15 September 1998 (1998-09-15) abstract; figure 4 page 1, line 35 -page 3, line 9 page 9, line 21 -page 10, line 5	1,2, 26-29
X	WO 97 44736 A (APPLE COMPUTER) 27 November 1997 (1997-11-27) abstract; figures 2A,2B,2C,3 page 2, line 35 -page 3, line 27 page 9, line 10 -page 11, line 28	1,2
Y		3,4
Y	EP 0 649 261 A (CANON KK) 19 April 1995 (1995-04-19) page 3, line 53 -page 4, line 5 page 7, line 18 - line 23	3,4
A	US 5 974 141 A (SAITO MAKOTO) 26 October 1999 (1999-10-26) abstract; figures 4A-4G column 8, line 24 - line 67	5,26

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"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)

"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

"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

"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

"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.

"&" document member of the same patent family

3

Form PCT/ISA/206 (Annex, first sheet) (July 1992)

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-5, 26-29

Protecting the distribution of digital data to be used with a digital player charachterized by encrypting format information and allowing low quality play back in case of lack of decrypting key.

2. Claims: 6-25

Digital signal encrypting technique combining transfer functions with predetermined key creation.

This finding is based on the following reasons.

The prior art has been identified as NL1005523 (D1). This document shows a method for protecting the distribution of digital information, the digital information including two subparts, a digital sample and format information, comprising the steps of: identifying and separating the two subparts; encoding the format information subpart using a key; recombining the encoded first subpart with the un-encoded second subpart, generating in this way an encoded version of the digital information. A predetermined key corresponding to the encoding key is then required for the decryption of the format information. All the features which form the subject matter of claims 1 and 2 are then disclosed by D1 (see following passages: abstract, page 1, line 35 - page 3, line 9; page 9, line 21 - page 10, line 5, fig. 4)

From the comparison between D1 and the 1st invention (see claim 3) the following technical features can be seen to make a contribution over this prior art (in the sense of PCT rule 13.2):
- the digital information is configured to be used with a digital player and the information output from said digital player has a degraded quality unless it is provided with a predetermined key (Special Technical Features 1, STF1).
From these STF1 the objective problem to be solved can be summarized as:
- permitting preview of distributed digital information

From the comparison between D1 and the 2nd invention (see claim 6) the following feature can be seen to make a contribution over the same prior art:
- using a transfer function-based mask set for creating a key to manipulate data at the inherent granularity of the file format of a digital sample (STF2).
From this STF2 the objective problem to be solved can be summarized as:
- improving the security of techniques for data protection

The above analysis shows that inventions 1 and 2 do not have same or similar Special Technical Features. Furthermore, a comparison of the objective problem 1 with the objective problem 2, both seen in the light of the description and the drawings of the present application, indicates that there is no technical correspondence between these problems nor do they show any corresponding technical effect.

As a result, inventions 1 and 2 fail to demonstrate a single general inventive concept as required by PCT rule 13.1.

Int. ...onal Application No
PCT/US 00/18411

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
NL 1005523	C	15-09-1998	NONE		
WO 9744736	A	27-11-1997	AU	3206397 A	09-12-1997
EP 0649261	A	19-04-1995	JP	7115638 A	02-05-1995
			US	5933499 A	03-08-1999
US 5974141	A	26-10-1999	US	6076077 A	13-06-2000
			US	6002772 A	14-12-1999
			US	6097818 A	01-08-2000

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/18411

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G11B20/00 G06F1/00

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)
IPC 7 G11B G06F H04N

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

Electronic data base consulted during the international search (name of data base and, where practical, search terms used)
EPO-Internal, WPI Data, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	NL 1 005 523 C (EINDHOVEN TECH HOCHSCHULE) 15 September 1998 (1998-09-15) abstract; figure 4 page 1, line 35 -page 3, line 9 page 9, line 21 -page 10, line 5	1,2, 26-29
X	WO 97 44736 A (APPLE COMPUTER) 27 November 1997 (1997-11-27) abstract; figure 4 page 2, line 35 -page 3, line 27 page 9, line 10 -page 11, line 28	1,2
Y		3,4

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"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)

"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

"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

"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

"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.

"&" document member of the same patent family

Date of the actual completion of the international search

20 July 2001

Date of mailing of the international search report

30.07.2001

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL - 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Sigolo, A

Form PCT/ISA/210 (second sheet) (July 1992)

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 687 236 A (MOSKOWITZ SCOTT A ET AL) 11 November 1997 (1997-11-11) cited in the application column 5, line 1 -column 6, line 37 column 7, line 54 -column 10, line 11 column 11, line 31 -column 12, line 10 column 15, line 42 -column 16, line 32	6-12, 19-21
A		22,23
A	US 5 974 141 A (SAITO MAKOTO) 26 October 1999 (1999-10-26) abstract; figures 4A-46 column 8, line 24 - line 67	5,26
X	WO 99 52271 A (MOSKOWITZ SCOTT A) 14 October 1999 (1999-10-14) abstract page 11, line 15 -page 13, line 13	6,7,10
Y	EP 0 649 261 A (CANON KK) 19 April 1995 (1995-04-19) page 3, line 53 -page 4, line 5 page 7, line 18 - line 23	3,4
A	WO 99 63443 A (DATAMARK TECHNOLOGIES PTE LTD; HO ANTHONY TUNG SHUEN (SG); TAM SIU) 9 December 1999 (1999-12-09) page 2, line 10 -page 5, line 16	6-8,11, 12

INTERNATIONAL SEARCH REPORT	International application No. PCT/US 00/18411

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [ ] Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. [ ] Claims Nos.:
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

see additional sheet

1. [X] As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[X] No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (1)) (July 1998)

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-5,26-29

   Protecting the distribution of digital data to be used with a digital player characterized by encrypting format information and allowing low quality play back in case of lack of decrypting key.

2. Claims: 6-25

   Digital signature encrypting technique combining transfer functions with predetermined key creation.

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 00/18411

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
NL 1005523	C	15-09-1998	NONE		
WO 9744736	A	27-11-1997	AU	3206397 A	09-12-1997
US 5687236	A	11-11-1997	US	5613004 A	18-03-1997
			EP	0872073 A	21-10-1998
			WO	9642151 A	27-12-1996
US 5974141	A	26-10-1999	US	6076077 A	13-06-2000
			US	6002772 A	14-12-1999
			US	6097818 A	01-08-2000
WO 9952271	A	14-10-1999	US	6205249 B	20-03-2001
			EP	1068720 A	17-01-2001
EP 0649261	A	19-04-1995	JP	7115638 A	02-05-1995
			US	5933499 A	03-08-1999
WO 9963443	A	09-12-1999	AU	7683398 A	20-12-1999
			EP	1103026 A	30-05-2001

Form PCT/ISA/210 (patent family annex) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/33126

A. CLASSIFICATION OF SUBJECT MATTER
IPC 7 G06F17/60

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)
IPC 7 G06F

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 903 721 A (SIXTUS TIMOTHY) 11 May 1999 (1999-05-11) abstract column 3, line 26 -column 5, line 31	1-19
X	US 5 790 677 A (SPELMAN JEFFREY F ET AL) 4 August 1998 (1998-08-04) abstract column 2, line 6 -column 4, line 39	1-19
X	WO 96 29795 A (MICALI SILVIO) 26 September 1996 (1996-09-26) abstract page 5, line 27 -page 8, line 6	1-19

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"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)

"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

"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

"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

"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.

"&" document member of the same patent family

Date of the actual completion of the international search

20 March 2001

Date of mailing of the international search report

04.04.01

Name and mailing address of the ISA

European Patent Office, P.B. 5818 Patentlaan 2
NL – 2280 HV Rijswijk
Tel. (+31-70) 340-2040, Tx. 31 651 epo nl,
Fax: (+31-70) 340-3016

Authorized officer

Corcoran, P

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/33126

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	WO 97 24833 A (MICALI SILVIO) 10 July 1997 (1997-07-10) abstract page 2, line 12 -page 5, line 8	1-19
A	US 5 539 735 A (MOSKOWITZ SCOTT A) 23 July 1996 (1996-07-23) abstract column 1, line 60 -column 4, line 29	1-19
A	SIRBU M ET AL: "NETBILL: AN INTERNET COMMERCE SYSTEM OPTIMIZED FOR NETWORK DELIVERED SERVICES" DIGEST OF PAPERS OF THE COMPUTER SOCIETY COMPUTER CONFERENCE (SPRING) COMPCON,US,LOS ALAMITOS, IEEE COMP. SOC. PRESS, vol. CONF. 40, 5 March 1995 (1995-03-05), pages 20-25, XP000577034 ISBN: 0-7803-2657-1 The whole document	1-19
A	SCHUNTER M ET AL: "A status report on the SEMPER framework for secure electronic commerce" COMPUTER NETWORKS AND ISDN SYSTEMS,NL,NORTH HOLLAND PUBLISHING. AMSTERDAM, vol. 30, no. 16-18, 30 September 1998 (1998-09-30), pages 1501-1510, XP004138681 ISSN: 0169-7552 2. Model for electronic commerce 3. The SEMPER framework	1-19
A	KONRAD K ET AL: "Trust and electronic commerce-more than a technical problem" PROCEEDINGS OF THE 18TH IEEE SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS, PROCEEDINGS 18TH IEEE SYMPOSIUM ON RELIABLE DISTRIBUTED SYSTEMS, LAUSANNE, SWITZERLAND, 19-22 OCT. 1999, pages 360-365, XP002162270 1999, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-7695-0290-3 3. Trust, Security and Electronic Commerce 4. Technology and Institutions	1-19

-/--

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 00/33126

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category °	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	KINI A ET AL: "Trust in electronic commerce: definition and theoretical considerations" PROCEEDINGS OF THE THIRTY-FIRST HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES (CAT. NO.98TB100216), PROCEEDINGS OF THE THIRTY-FIRST HAWAII INTERNATIONAL CONFERENCE ON SYSTEM SCIENCES, KOHALA COAST, HI, USA, 6-9 JAN. 1998, pages 51-61, XP002162271 1998, Los Alamitos, CA, USA, IEEE Comput. Soc, USA ISBN: 0-8186-8255-8 1.3 The Significance of Trust in Electronic Commerce,	1-19
A	STEINAUER D D ET AL: "Trust and traceability in electronic commerce" STANDARD VIEW, SEPT. 1997, ACM, USA, vol. 5, no. 3, pages 118-124, XP002162272 ISSN: 1067-9936 The whole document	1-19
A	US 5 687 236 A (MOSKOWITZ SCOTT A ET AL) 11 November 1997 (1997-11-11) abstract	8,9
A	US 5 745 569 A (MOSKOWITZ SCOTT A ET AL) 28 April 1998 (1998-04-28) abstract	8,9

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

International Application No
PCT/US 00/33126

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
US 5903721	A	11-05-1999	AU	6549498 A	29-09-1998
			DE	1008022 T	25-01-2001
			EP	1008022 A	14-06-2000
			ES	2150892 T	16-12-2000
			NO	994428 A	09-11-1999
			WO	9840809 A	17-09-1998
US 5790677	A	04-08-1998	NONE		
WO 9629795	A	26-09-1996	WO	9806198 A	12-02-1998
			CA	2215908 A	26-09-1996
			EP	0815671 A	07-01-1998
			US	5553145 A	03-09-1996
			US	5629982 A	13-05-1997
			US	5666420 A	09-09-1997
			US	6137884 A	24-10-2000
			US	6141750 A	31-10-2000
			EP	0917781 A	26-05-1999
			JP	2000515649 T	21-11-2000
WO 9724833	A	10-07-1997	US	5615269 A	25-03-1997
			AU	1951497 A	28-07-1997
US 5539735	A	23-07-1996	US	5428606 A	27-06-1995
			WO	9701892 A	16-01-1997
US 5687236	A	11-11-1997	US	5613004 A	18-03-1997
			EP	0872073 A	21-10-1998
			WO	9642151 A	27-12-1996
US 5745569	A	28-04-1998	AU	1829497 A	11-08-1997
			WO	9726732 A	24-07-1997

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US 00/33126

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This International Search Report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [ ] Claims Nos.:
because they relate to subject matter not required to be searched by this Authority, namely:

2. [X] Claims Nos.: 20-186
because they relate to parts of the International Application that do not comply with the prescribed requirements to such an extent that no meaningful International Search can be carried out, specifically:
see FURTHER INFORMATION sheet PCT/ISA/210

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. [ ] As all required additional search fees were timely paid by the applicant, this International Search Report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this International Search Report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this International Search Report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest

[ ] The additional search fees were accompanied by the applicant's protest.

[ ] No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet (1)) (July 1998)

FURTHER INFORMATION CONTINUED FROM PCT/ISA/ 210

Continuation of Box I.2

Claims Nos.: 20-186

In view of the large number and also the wording of the claims presently on file, which render it difficult, if not impossible, to determine the matter for which protection is sought, the present application fails to comply with the clarity and conciseness requirements of Article 6 PCT (see also Rule 6.1(a) PCT) to such an extent that a meaningful search is impossible.

Moreover, the proliferation of independent claims and the broad manner in which these have been worded make it impossible to determine which parts of the claims may be said to define subject-matter for which protection might legitimately be sought (Article 6 PCT). For these reasons, a meaningful search over the whole breadth of the claim(s) is impossible.

Consequently, the search has been restricted to the subject matter recited in claims 1-19.

The applicant's attention is drawn to the fact that claims, or parts of claims, relating to inventions in respect of which no international search report has been established need not be the subject of an international preliminary examination (Rule 66.1(e) PCT). The applicant is advised that the EPO policy when acting as an International Preliminary Examining Authority is normally not to carry out a preliminary examination on matter which has not been searched. This is the case irrespective of whether or not the claims are amended following receipt of the search report or during any Chapter II procedure.

(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
15 March 2001 (15.03.2001)

PCT

(10) International Publication Number
WO 01/18628 A3

(51) International Patent Classification[7]: H04L 9/32, H04N 7/167

(21) International Application Number: PCT/US00/21189

(22) International Filing Date: 4 August 2000 (04.08.2000)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/147,134 4 August 1999 (04.08.1999) US
60/213,489 23 June 2000 (23.06.2000) US

(71) Applicant (for all designated States except US): BLUE SPIKE, INC. [US/US]; 16711 Collins Avenue #2505, Miami, FL 33160 (US).

(72) Inventors; and
(75) Inventors/Applicants (for US only): MOSKOWITZ, Scott, A. [US/US]; 16711 Collins Avenue #2505, Miami, FL 33160 (US). BERRY, Michael [US/US]; 12401 Princess Jeanne, Albuquerque, NM 87112 (US).

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

(81) Designated States (national): JP, US.

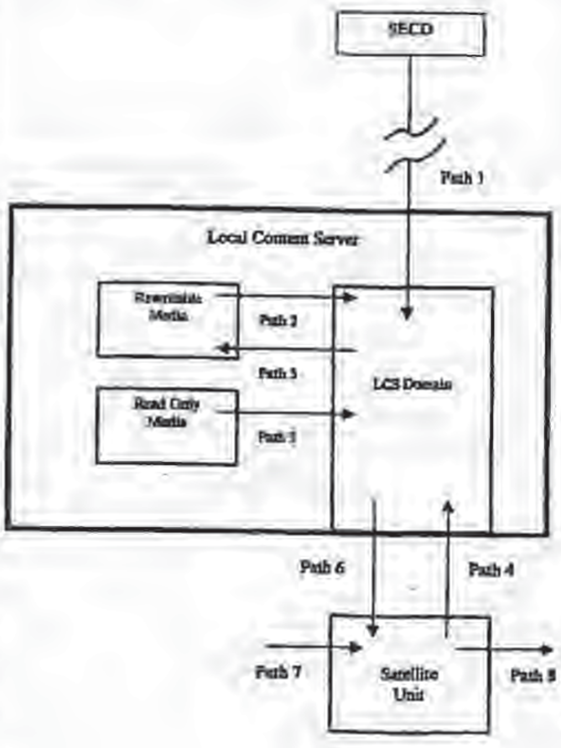
(84) Designated States (regional): European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published:
— with international search report

(88) Date of publication of the international search report: 22 November 2001

[Continued on next page]

(54) Title: A SECURE PERSONAL CONTENT SERVER



(57) Abstract: A local content server system (LCS) for creating a secure environment for digital content is disclosed, which system comprises: a communications port in communication (Path 1) for connecting the LCS via a network to at least one Secure Electronic Content Distributor (SECD), which SECD is capable of storing a plurality of data sets, is capable of receiving a request to transfer at least one content data set, is capable of transmitting the at least one content data set in a secured transmission; a rewritable storage medium (Rewritable Media) whereby content received from outside the LCS may be stored and retrieved; a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS; and a programmable address module which can be programmed with an identification code uniquely associated with the LCS. Optionally, the system may further comprise: an interface to permit the LCS to communicate with one or more Satellite Units (SU).

WO 01/18628 A3

For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US00/21189

A. CLASSIFICATION OF SUBJECT MATTER

IPC(7) :H04L 9/32; H04N 7/167
US CL :713/176; 705/51, 52, 57; 380/203, 231
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. : 713/153; 705/51, 52, 57; 380/203, 231

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

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

APS EAST/BRS text search terms: watermark, audio, copy protect, distribution

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US 5,636,292 A (RHOADS) 03 JUNE 1997, col. 33, line 42-col. 34, line 8.	4, 6-15 and 17-29
Y	US 5,629,980 A (STEFIK et al) 13 MAY 1997, col. 26, line 37-col. 27, line 26.	1-30
Y, P	US 5,943,422 A (VAN WIE et al) 24 AUGUST 1999, col. 6, line 53-62 and col. 10, line 18-56.	4, 6-15 and 17-29.
Y	US 5,636,276 A (BRUGGER) 03 JUNE 1997, col. 5, line 53-col. 6, line 8.	1-30.
Y	US 5,341,429 A (STRINGER et al) 23 AUGUST 1994, col. 4, lines 1-22.	30

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search: 26 JANUARY 2001

Date of mailing of the international search report: 23 MAR 2001

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
GILBERTO BARRON
Telephone No. (703) 305-3900

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

2280 HV RIJSWIJK
NETHERLANDS
Tel: +31 70 340 2040
Fax: +31 70 340 3016

Best Available Copy

EINGEGANGEN
Vossius & Partner
19. Okt. 2007
Frist
bearb.: CZI

Vossius & Partner
Siebertstrasse 4
81675 München
ALLEMAGNE

EPO Customer Services
Tel.: +31 (0)70 340 45 00

Date	19.10.07

Reference	Application No./Patent No.
B3379 EP/1	07112420.0 - 1228
Applicant/Proprietor: Wistaria Trading, Inc.	

Communication

The extended European search report is enclosed.

The extended European search report includes, pursuant to Rule 44a EPC, the European search report (R. 44 EPC) or the partial European search report/ declaration of no search (R. 45 EPC) and the European search opinion.

Copies of documents cited in the European search report are attached.

☐ additional set(s) of copies of such documents is (are) enclosed as well.

The following have been approved:

☑ Abstract ☑ Title

☐ the Abstract was modified and the definitive text is attached to this communication.

The following figure will be published together with the abstract:

Refund of the search fee

If applicable under Article 10 Rules relating to fees, a separate communication from the Receiving Section on the refund of the search fee will be sent later.

Europäisches Patentamt · European Patent Office · Office européen des brevets

EPO Form 1507N 01.05

European Patent Office

Best Available Copy

EUROPEAN SEARCH REPORT

Application Number
EP 07 11 2420

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (IPC)
X	EP 0 581 317 A (INTERACTIVE HOME SYSTEMS) 2 February 1994 (1994-02-02) * page 3, line 6 - page 4, line 48 *	1,3,7	INV. H04L9/00 H04N1/32
X	BENDER W ET AL: "TECHNIQUES FOR DATA HIDING" PROCEEDINGS OF THE SPIE, SPIE, BELLINGHAM, VA, US, vol. 2420, 9 February 1995 (1995-02-09), pages 164-173, XP000566794 ISSN: 0277-786X * paragraphs [03.4], [3.4.1] *	1,2,4,8	
L	ZHAO J ET AL: "EMBEDDING ROBUST LABELS INTO IMAGES FOR COPYRIGHT PROTECTION" PROCEEDINGS OF THE KNOWRIGHT. CONFERENCE. PROCEEDINGS OF THE INTERNATIONAL CONGRESS ON INTELLECTUAL PROPERTY RIGHTS FOR SPECIALIZED INFORMATION, KNOWLEDGE AND NEW TECHNOLOGY, XX, XX, 1995, pages 242-251, XP000571967		TECHNICAL FIELDS SEARCHED (IPC) H04N G06T

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
The Hague	15 October 2007	Hazel, James

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

ANNEX TO THE EUROPEAN SEARCH REPORT ON EUROPEAN PATENT APPLICATION NO.

EP 07 11 2420

This annex lists the patent family members relating to the patent documents cited in the above-mentioned European search report.
The members are as contained in the European Patent Office EDP file on
The European Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

15-10-2007

Patent document cited in search report		Publication date	Patent family member(s)			Publication date
EP 0581317	A	02-02-1994	CA	2101673	A1	01-02-1994
			JP	6343128	A	13-12-1994
			JP	3837432	B2	25-10-2006
			JP	2005328528	A	24-11-2005
			JP	2007006504	A	11-01-2007
			JP	2006314125	A	16-11-2006
			US	5721788	A	24-02-1998
			US	5809160	A	15-09-1998

EPO FORM P0459

For more details about this annex : see Official Journal of the European Patent Office, No. 12/82

The examination is being carried out on the **following application documents**:

Description, Pages

1-37 as originally filed

Claims, Numbers

1-28 as originally filed

The following documents (D) are referred to in this communication; the numbering will be adhered to in the rest of the procedure:

D1: EP-A-0 581 317 (INTERACTIVE HOME SYSTEMS) 2 February 1994 (1994-02-02)

D2: BENDER W ET AL: 'TECHNIQUES FOR DATA HIDING' PROCEEDINGS OF THE SPIE, SPIE, BELLINGHAM, VA, US, vol. 2420, 9 February 1995 (1995-02-09), pages 164-173, XP000566794 ISSN: 0277-786X

0. It is noted that the present application is a divisional from EP96 919 405.9, which has ended its examination procedure with a grant. The present application has been filed with an identical set of claims to that of the parent application. According to the Guidelines C.IV 6.4, two patents cannot be granted to the same applicant for one invention. It is permissible to allow an applicant to proceed with two applications having the same description where the claims are quite distinct in scope and directed to different inventions.

1. Clarity

The application does not meet the requirements of Article 84 EPC, because claims 1-4,7 and 8 are not clear.

1.1 Claims 1,3 and 4 have been drafted as separate independent claims.

Under Article 84 in combination with Rule 29(2) EPC an application may contain more than one independent claim in a particular category only if the subject matter claimed falls within one or more of the exceptional situations set out in paragraphs (a), (b) or (c) of Rule 29(2) EPC. This appears not to be the case in the present application.

The aforementioned claims therefore lack conciseness, which is contrary to Article 84 EPC. Moreover, lack of clarity of the claims as a whole arises, since the plurality of independent claims makes it difficult, if not impossible, to determine the matter for which protection is sought, and places an undue burden on others seeking to establish the extent of the protection.

1.2 Similar objections arise for independent claims 7 and 8.

1.3 The applicant is requested to file an amended set of claims which complies with Rule 29(2). Failure to do so, or to submit convincing arguments as to why the current set of claims does in fact comply with these provisions, will lead to refusal of the application under Article 97(1) EPC.

1.4 Claim 1 does not meet the requirements of Article 84 EPC in that the matter for which protection is sought is not defined. The claim attempts to define the subject-matter in terms of the result to be achieved (this definition is embodied by the repeated use of the expression "such that"). Such a definition is only allowable under the conditions elaborated in the Guidelines C-III, 4.7. In this instance, however, such a formulation is not allowable because it appears possible to define the subject-matter in more concrete terms, viz. in terms of how the effect is to be achieved.

1.5 The expressions "key" and "mask" seem to be used for the same or corresponding features in claims 1-4,7 and 8. This is confusing and detracts from the clarity of the claims. It is suggested to use only one of these terms. "key" would appear to be preferable since this is a generally accepted term for this feature.

2. Novelty and Inventive Step

The present application does not meet the requirements of Article 52(1) EPC, because the subject-matter of claims 1-4,7 and 8, in so far as it can be understood, does not involve an inventive step in the sense of Article 56 EPC.

D1 (see page 3, line 6 - page 4, line 48) discloses a method and system (apparatus) for encoding (embedding) additional information (a signature) into digitized samples (digital image 24) at a number of signature points, which signature points (in one embodiment) are chosen randomly. It is well known in the field of generating random sequences to use a key as a seed.

D2 (see sections 3.4 and 3.4.1 in particular) discloses a spread spectrum technique for hiding data by encoding it using a pseudo-random noise sequence to spread the frequency spectrum of the data over an available frequency band. The spread data sequence is then added to an original file to hide the data in the file. A key is used to encode the information, and the same key is used to decode it.

The features of the independent claims which are not explicitly disclosed in D1 or D2, in so far as they can be understood, appear to relate to particular details of alternative methods or apparatus for performing known encoding or decoding of additional information. These features would seem obvious to the skilled person as ways of implementing the method or apparatus known according to D1 or D2, and don't appear to solve any particular problem associated with said known method or apparatus. They cannot, therefore, be regarded as inventive.

3. Conclusion

3.1 It is not at present apparent which part of the application could serve as a basis for a new, allowable claim. Should the applicant nevertheless regard some particular matter as patentable, independent claims should be filed taking account of Rule 29 EPC. **The applicant should also indicate in the letter of reply the difference of the subject-matter of the new claim vis-à-vis the state of the art and the**

significance thereof. In particular the problem to be solved by the subject matter of the new independent claim(s) (not more than one in each category) should be discussed in the letter of reply to assist the examining division in assessing the inventive step of the claim(s).

3.2 These independent claims, one per category, should be in two-part form in accordance with Rule 29(1) EPC, with those features known in combination from the prior art (D1) being placed in the preamble (Rule 29(1)(a) EPC) and with the remaining features being included in the characterising part (Rule 29(1)(b) EPC). If, however, the applicant is of the opinion that the two part form would be inappropriate, then reasons therefor should be provided in the letter of reply.

3.3 To meet the requirements of Rule 27(1)(b) EPC, the documents D1 and D2 should be identified in the description and the relevant background art disclosed therein should be briefly discussed.

3.4 The attention of the applicant is drawn to the fact that the application may not be amended in such a way that it contains subject-matter which extends beyond the content of the application as filed (Article 123(2) EPC). Care should be taken to conform with this Article when bringing the description into conformity with any amended claims, in particular during revision of the introductory portion or any statements of problem or advantage.

3.5 In order to facilitate the examination of the conformity of the amended application with the requirements of Article 123(2) EPC, the applicant is requested to clearly identify the amendments carried out, irrespective of whether they concern amendments by addition, replacement or deletion, and to indicate the passages of the application as filed on which these amendments are based.

3.6 When drawing up the new independent claims, the applicant should further take care to:
1) include all features essential to the definition of the invention (Rule 29 EPC);
2) avoid using features relating to a method in the apparatus claim (Art. 84, EPC); 3) ensure that any additional features introduced, e.g. from the dependent claims, are

clear (Art. 84); and

4) provide the features of the claims with reference signs placed in parantheses to increase the intelligibility of the claims (Rule 29(7) EPC).

XS CPRTENFRDE

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	10/049,101	Confirmation No. 8028
Applicant	:	Scott MOSKOWITZ	
Filed	:	July 23, 2002	
TC/A.U.	:	2131	
Examiner	:	Jeremiah L. AVERY	
Docket No.	:	80408.0011	

MAIL STOP: AMENDMENT - IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Dear Sir:

Applicant(s) submit copies of the references listed on the attached SB08 Form(s) for consideration and request that the U.S. Patent and Trademark Office make them of record in this application.

Applicant(s) state the following:

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the Information Disclosure Statement; or

☐ No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and to the knowledge of Applicant(s) no item of information contained in this

Information Disclosure Statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement.

☐ In accordance with 37 C.F.R. § 1.97(b), this Information Disclosure Statement is believed to be submitted prior to issuance of a first Office Action and/or within three months of the filing date of the application. It is respectfully submitted that no fee is required for consideration of this information.

☒ This Information Disclosure Statement is being submitted after the mailing of a non-final Office Action, but is believed to be prior to a final Office Action or a Notice of Allowance. Pursuant to 37 C.F.R. § 1.97(c), payment in the amount of $180.00 as set forth in 37 C.F.R. § 1.17(p) is enclosed.

While the information and references disclosed in this Information Disclosure Statement are submitted pursuant to 37 C.F.R. § 1.56, this submission is not intended to constitute an admission that any patent, publication or other information referred to is "prior art" to this invention. Applicant(s) reserve the right to contest the "prior art" status of any information submitted or asserted against the application.

Additionally, pursuant to C.F.R. § 1.78, Applicant(s) wish to inform the Examiner of the existence of the following co-pending U.S. patents and patent applications that share a common inventor with the present application. Under 37 C.F.R. § 1.98(a)(1), Applicant(s) also wish to inform the Examiner of the existence of the following co-pending foreign patents and patent applications that share a common inventor with the present application in the "section separate from the citations of other documents" entitled "Foreign Patent Documents", below:

U.S. PATENT DOCUMENTS

EXAMINER'S
INITIALS

_____ U.S. Patent Application No. 08/999,766, filed July 23, 1997, entitled "Steganographic Method and Device";

_____ U.S. Patent Application No. 11/894,443, filed August 21, 2007, entitled "Steganographic Method and Device" – Projected Publication Date – March 27, 2008;

_____ U.S. Patent Application No. 11/894,476, filed August 21, 2007, entitled "Steganographic Method and Device" – Publication No. 20070294536 – December 20, 2007;

_____ U.S. Patent Application No. 11/050,779, filed February 7, 2005, entitled "Steganographic Method and Device" – Publication No. 20050177727 – August 11, 2005;

_____ U.S. Patent Application No. 08/674,726, filed July 2, 1996, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management" (unpublished – issue fee paid – January 23, 2008);

_____ U.S. Patent Application No. 12/009,914, filed January 23, 2008, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management";

_____ U.S. Patent Application No. 09/545,589, filed April 7, 2000, entitled "Method and System for Digital Watermarking" (issued as U.S. Patent No 7,007,166);

_____ U.S. Patent Application No. 11/244,213, filed October 5, 2005, entitled "Method and System for Digital Watermarking" – Publication No. 20060101269 – May 11, 2006 (issue fee paid – December 26, 2007);

_____ U.S. Patent Application No. 11/649,026, filed January 3, 2007, entitled "Method and System for Digital Watermarking" – Publication No. 20070113094 – May 17, 2007;

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ U.S. Patent Application No. 12/005,230, filed December 26, 2007, entitled "Method and System for Digital Watermarking";

_____ U.S. Patent Application No. 09/046,627, filed March 24, 1998, entitled "Method for Combining Transfer Function with Predetermined Key Creation" (issued as U.S. Patent No. 6,598,162);

_____ U.S. Patent Application 10/602,777, filed June 25, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation" – Publication No. 20040086119 – May 6, 2004;

_____ U.S. Patent Application 11/895,388, filed August 24, 2007, entitled "Data Protection Method and Device" – Publication No. 20080016365 – January 17, 2008;

_____ U.S. Patent Application No. 09/053,628, filed April 2, 1998, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" (issued as U.S. Patent No. 6,205,249);

_____ U.S. Patent Application No. 09/644,098, filed August 23, 2000, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" (issued as U.S. Patent No. 7,035,409);

_____ U.S. Patent Application No. 09/767,733, filed January 24, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" – Publication No. 20010010078 - July 26, 2001;

_____ U.S. Patent Application No. 11/358,874, filed February 21, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" – Publication No. 20060140403 – June 29, 2006;

_____ U.S. Patent Application No. 10/417,231, filed April 17, 2003, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth" – Publication No. 20030200439 – October 23, 2003 (issued as U.S. Patent No. 7,287,275);

_____ U.S. Patent Application No. 11/900,065, filed September 10, 2007, entitled "Methods, Systems And Devices For Packet Watermarking And

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

Efficient Provisioning Of Bandwidth" – Publication No. 20080005571 – January 3, 2008;

_____ U.S. Patent Application No. 11/900,066, filed September 10, 2007, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth" – Publication No. 20080005572 – January 3, 2008;

_____ U.S. Patent Application No. 09/789,711, filed February 22, 2001, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20010010078 – October 11, 2001 (issued as U.S. Patent No. 7,107,451);

_____ U.S. Patent Application No. 11/497,822, filed August 2, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070011458 – January 11, 2007;

_____ U.S. Patent Application No. 11/599,964, filed November 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20080046742 – February 21, 2008;

_____ U.S. Patent Application No. 11/599,838, filed November 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070226506 – September 27, 2007;

_____ U.S. Patent Application No. 11/897,790, filed August 31, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070300072 – December 27, 2007;

_____ U.S. Patent Application No. 11/897,791, filed August 31, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20080022113 – January 24, 2008;

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ U.S. Patent Application No. 11/899,661, filed September 7, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070300073 – December 27, 2007;

_____ U.S. Patent Application No. 11/899,662, filed September 7, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20080022114 – January 24, 2008;

_____ U.S. Patent Application No. 10/369,344, filed February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data" – Publication No. 20030219143 – November 27, 2003 (issued as U.S. Patent No. 7,095,874);

_____ U.S. Patent Application No. 11/482,654, filed July 7, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data" – Publication No. 20060285722 – December 21, 2006;

_____ U.S. Patent Application No. 09/594,719, filed June 16, 2000, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems" (issued as U.S. Patent 7,123,718);

_____ U.S. Patent Application No. 11/519,467, filed September 12, 2006, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems" – Publication No. 20070064940 – March 22, 2007;

_____ U.S. Patent Application No 09/731,040, filed December 7, 2000, entitled "Systems, Methods And Devices For Trusted Transactions" – Publication No. 20020010684 – January 24, 2002 (issued as U.S. Patent 7,159,116);

_____ U.S. Patent Application No 11/512,701, filed August 29, 2006, entitled "Systems, Methods And Devices For Trusted Transactions" – Publication No. 20070028113 – February 1, 2007;

_____ U.S. Patent Application No. 10/049,101, filed February 8, 2002, entitled "A Secure Personal Content Server" (which claims priority to International

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

Application No. PCT/US00/21189, filed August 4, 2000, which claims priority to U.S. Patent Application No. 60/147,134, filed August 4, 1999, and to U.S. Patent Application No. 60/213,489, filed June 23, 2000);

_____ U.S. Patent Application No. 09/657,181, filed September 7, 2000, entitled "Method And Device For Monitoring And Analyzing Signals" (paid issue fee January 23, 2008);

_____ U.S. Patent Application No. 12/005,229, filed December 26, 2007, entitled "Method And Device For Monitoring And Analyzing Signals" -- Publication No. NA --;

_____ U.S. Patent Application No. 10/805,484, filed March 22, 2004, entitled "Method And Device For Monitoring And Analyzing Signals"(which claims priority to U.S. Patent Application No. 09/671,739, filed September 29, 2000, which is a CIP of U.S. Patent Application No. 09/657,181) – Publication No. 20040243540 – December 2, 2004 – abandoned;

_____ U.S. Patent Application No. 09/956,262, filed September 20, 2001, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects" – Publication No. 20020056041 – May 9, 2002 (issued as U.S. Patent No. 7,127,615);

_____ U.S. Patent Application No. 11/518,806, filed September 11, 2006, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects" – Publication No. 20080028222 – January 31, 2008;

_____ U.S. Patent Application No. 11/026,234, filed December 30, 2004, entitled "Z-Transform Implementation of Digital Watermarks" – Publication No. 20050135615 – June 23, 2005 (issued as U.S. Patent No. 7,152,162);

_____ U.S. Patent Application No. 11/592,079, filed November 2, 2006, entitled "Linear Predictive Coding Implementation of Digital Watermarks" – Publication No. 20070079131 – April 5, 2007;

_____ U.S. Patent Application No. 09/731,039, filed December 7, 2000, entitled "System and Methods for Permitting Open Access to Data Objects and

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

for Securing Data within the Data Objects" – Publication No. 20020071556 – June 13, 2002 (issued as U.S. Patent No. 7,177,429);

_____ U.S. Patent Application No. 11/647,861, filed December 29, 2006, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects" – Publication No. 20070110240 – April 5, 2007;

_____ U.S. Patent No. 5,428,606, issued June 27, 1995, entitled "Digital Commodities Exchange";

_____ U.S. Patent No. 5,539,735, issued July 23, 1996, entitled "Digital Information Commodities Exchange";

_____ U.S. Patent No. 5,613,004, issued March 18, 1997, entitled "Steganographic Method and Device";

_____ U.S. Patent No. 5,687,236, issued November 11, 1997, entitled "Steganographic Method and Device";

_____ U.S. Patent No. 5,745,569, issued April 28, 1998, entitled "Method for Stega-Protection of Computer Code";

_____ U.S. Patent No. 5,822,432, issued October 13, 1998, entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System";

_____ U.S. Patent No. 5,889,868, issued July 2, 1996, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 5,905,800, issued May 18, 1999, entitled "Method & System for Digital Watermarking";

_____ U.S. Patent No. 6,078,664, issued June 20, 2000, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 6,205,249, issued March 20, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ U.S. Patent No. 6,522,767, issued February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 6,598,162, issued July 22, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation";

_____ U.S. Patent No. 6,853,726, issued February 8, 2005, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 7,007,166, issued February 28, 2006, entitled "Method & System for Digital Watermarking";

_____ U.S. Patent No. 7,035,049, issued April 25, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

_____ U.S. Patent No. 7,095,874, issued August 22, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 7,107,451, issued September 12, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

_____ U.S. Patent No. 7,123,718, issued October 17, 2006, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems";

_____ U.S. Patent No. 7,127,615, issued October 24, 2006, "Improved Security Based on Subliminal and Supraliminal Channels for Data Objects";

_____ U.S. Patent No. 7,152,162, issued December 19, 2006, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 7,159,116, issued January 2, 2007, entitled "Systems, Methods and Devices for Trusted Transactions";

_____ U.S. Patent No. 7,177,429, issued February 13, 2007, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects";

_____ U.S. Patent No. 7,287,275, issued October 23, 2007, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth"

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

FOREIGN PATENT DOCUMENTS

EXAMINER'S
INITIALS

_____ PCT Application No. PCT/US95/08159, filed June 26, 1995, entitled, "Digital Information Commodities Exchange with Virtual Menuing";

_____ PCT Application No. PCT/US96/10257, filed June 7, 1996, entitled, "Steganographic Method and Device" – corresponding to – EPO Application No. 96919405.9, entitled "Steganographic Method and Device";

_____ PCT Application No. PCT/US97/00651, filed January 16, 1997, entitled, "Method for Stega-Cipher Protection of Computer Code" – corresponding to AU199718294A (not available);

_____ PCT Application No. PCT/US97/00652, filed January 17, 1997, entitled, "Method for an Encrypted Digital Watermark" – corresponding to AU199718295A (not available);

_____ PCT Application No. PCT/US97/11455, filed July 2, 1997, entitled, "Optimization Methods for the Insertion, Protection and Detection of Digital Watermarks in Digitized Data" – corresponding to AU199735881A (not available);

_____ PCT Application No. PCT/US99/07262, filed April 2, 1999, entitled, "Multiple Transform Utilization and Applications for Secure Digital Watermarking" – corresponding to – Japan App. No. 2000-542907, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

_____ PCT Application No. PCT/US00/06522, filed March 14, 2000, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems";

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

_____ PCT Application No. PCT/US00/18411, filed July 5, 2000, entitled, "Copy Protection of Digital Data Combining Steganographic and Cryptographic Techniques" – corresponding to AU200060709A5 (not available);

_____ PCT Application No. PCT/US00/21189, filed August 4, 2000, entitled, "A Secure Personal Content Server";

_____ PCT Application No. PCT/US00/33126, filed December 7, 2000, entitled, "Systems, Methods and Devices for Trusted Transactions" – corresponding to AU200120659A5 (not available);

_____ EPO Divisional Patent Application No. 07112420.0, entitled "Steganographic Method and Device" (corresponding to PCT Application No. PCT/US96/10257, filed June 7, 1996, entitled, "Steganographic Method and Device" – cited above – previously provided)

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. This Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed documents and information.

Respectfully submitted,

Date: February 29, 2008

By:

Scott A. Moskowitz
Tel# (305) 956-9041
Fax# (305) 956-9042

For Blue Spike, Inc.

Scott A. Moskowitz
President

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

OIPE
FEB 29 2008

PTO/SB/21 (01-08)
Approved for use through 03/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	MOSKOWITZ
Art Unit	2131
Examiner Name	AVERY
Attorney Docket Number	80408.0011
Total Number of Pages in This Submission	

ENCLOSURES (Check all that apply)

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [x] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [x] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s)
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please identify below)

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name			
Signature	[signature]		
Printed name	SCOTT MOSKOWITZ		
Date	FEB 29 2008	Reg. No.	

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	[signature]		
Typed or printed name	SCOTT MOSKOWITZ	Date	

This collection of information is required by 37 CFR 1.5. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.11 and 1.14. This collection is estimated to 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

OIPE FEB 2 9 2008 PATENT & TRADEMARK OFFICE

PTO/SB/17 (10-07)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

Effective on 12/08/2004
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818)

FEE TRANSMITTAL
For FY 2008

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT (\$) 240.00

Complete if Known	
Application Number	10/049101
Filing Date	July 23 2002
First Named Inventor	Moskowitz
Examiner Name	AVERY
Art Unit	2131
Attorney Docket No.	80408.0011

METHOD OF PAYMENT (check all that apply)

☐ Check ☑ Credit Card ☐ Money Order ☐ None ☐ Other (please identify):

☐ Deposit Account Deposit Account Number: Deposit Account Name:

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☐ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

Application Type	FILING FEES Fee (\$)	Small Entity Fee (\$)	SEARCH FEES Fee (\$)	Small Entity Fee (\$)	EXAMINATION FEES Fee (\$)	Small Entity Fee (\$)	Fees Paid (\$)
Utility	310	155	510	255	210	105	
Design	210	105	100	50	130	65	
Plant	210	105	310	155	160	80	
Reissue	310	155	510	255	620	310	
Provisional	210	105	0	0	0	0	

2. EXCESS CLAIM FEES

Fee Description	Fee (\$)	Small Entity Fee (\$)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	210	105
Multiple dependent claims	370	185

\$240.00

Total Claims ___ - 20 or HP = ___ Extra Claims × ___ Fee (\$) = ___ Fee Paid (\$)

HP = highest number of total claims paid for, if greater than 20.

Multiple Dependent Claims: Fee (\$) ___ Fee Paid (\$) ___

Indep. Claims ___ - 3 or HP = ___ Extra Claims × ___ Fee (\$) = ___ Fee Paid (\$)

HP = highest number of independent claims paid for, if greater than 3.

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is \$260 (\$130 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets ___ - 100 = ___ Extra Sheets / 50 = ___ Number of each additional 50 or fraction thereof (round up to a whole number) × ___ Fee (\$) = ___ Fee Paid (\$)

4. OTHER FEE(S) Fees Paid (\$)

Non-English Specification, \$130 fee (no small entity discount) / \$60.00 / \$180.00 — \$240.00

Other (e.g., late filing surcharge): ONE MONTH EXTENSION / 1DS AFTER 1st OA

SUBMITTED BY			
Signature	[signature]	Registration No. (Attorney/Agent)	Telephone 305 956 9041
Name (Print/Type)	SCOTT MOSKOWITZ		Date FEB 29, 2008

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 565 947 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
28.05.1997 Bulletin 1997/22

(51) Int Cl.[5]: **H04B 14/04**

(21) Application number: **93105323.6**

(22) Date of filing: **31.03.1993**

(54) **Procedure for including digital information in an audio signal prior to channel coding**

Verfahren zum Einfügen digitaler Daten in ein Audiosignal vor der Kanalkodierung

Méthode pour inclusion d'information digitale dans un signal audio avant decoder le canal

(84) Designated Contracting States:
DE FR GB IT

(30) Priority: **13.04.1992 FI 921644**

(43) Date of publication of application:
20.10.1993 Bulletin 1993/42

(73) Proprietor: **NOKIA TECHNOLOGY GmbH**
75175 Pforzheim (DE)

(72) Inventor: **Kuusama, Juha**
SF-33720 Tampere (FI)

(56) References cited:
EP-A- 0 137 855
EP-A- 0 167 364
WO-A-89/10661
US-A- 5 136 586

Printed by Jouve, 75001 PARIS (FR)

EP 0 565 947 B1

Description

The present invention relates to a method with which data information can be added in an audio signal present in digital form so that after the channel coding of an audio signal accomplished in a transmitter and the coding of an audio signal accomplished in a receiver no information is lost.

In a conference proceedings paper Proc. ICASSP 90, Alberquerque, New Mexico, April 3-6, 1990, p. 1097-1100, Wilen Kate, L. van de Kerkhof and F. Zijderveld: Digital Audio Carrying Extra Information, a encoding method is described with which a four-channel audio signal can be encoded to be appropriate for use in a transmission path of a two-channel audio signal. In said encoding method two characteristic features of the human hearing sense are made use of: hearing threshold and masking effect. The masking effect means that in any audio signal another, less powerful signal can be added, which is not audible to the ear because of the masking effect. The masking effect is a psychoacoustic phenomenon in which the hearing threshold moves upwards when other sounds are present. The masking effect is most successful in sounds in which the spectrum components are in the proximity of the components of the masking sound. The frequency masking declines more rapidly when moving to lower sounds. This is true also in the time plane: the masking effect is greatest in sounds which are simultaneously audible. The dependence of the masking effect on time and frequency is well known in simple signals. The existence of masking effect can be utilized in that signals below the hearing threshold can be added into an audio signal. In principle, this takes place so that an analogous audio signal is sampled and in the place of the bits of the samples not audible to the human ear other information is placed. Thus, information is inserted in place of the less significant bits of the sample in digital form. When such a signal is repeated, the human ear is not at all able to hear the signal added therein because the actual signal intended to be heard masks it. It is the masking ability of the human ear which determines how many less significant bits can be substituted without still being audible. A signal thus added can be used for various purposes. Similarly, when a sound signal is compressed, the signals below the hearing threshold can be excluded from storage, or only the signals audible to the human ear are transmitted.

The principle of said known coding method utilizing the masking effect is presented in Fig. 1. An incoming audio signal is sampled and divided first in a filter bank 1 into a great number of subbands and the signal samples of the subbands are decimated in means 2. The subbands are preferably equal in size so that the sampling frequency meeting the Nyqvist criterion in the decimalizing means 2 of each subband is equal. The samples of each subband are then grouped into subsequent time windows in means 3. The length of a time window is Δ t and it includes samples of one and same point of time from each subband. So, the simultaneous time windows of each subband constitute one block. A power spectrum is calculated for each block in spectrum analysis means 4 and from the spectrum thus derived a masking threshold is determined for each block in means 5. After determining the masking threshold it is clear what the maximum signal power is which can be added in an audio signal of a subband in said time window. DATA IN bits of the data signal are added below the masking threshold calculated for the audio signal. It is carried out so that a given number of subsequent bits of a data flow, e.g. three subsequent bits, form one word. Each word is interpreted to be an address representing a given sample value; thus, in a three bit case there are eight pieces of sample values. Selection of a word and the sample value corresponding thereto is carried out in means 6. The sample values are grouped for appropriate sample windows of the subbands corresponding to the equivalence of the sample value and the threshold of the sample window of a subband, and data bits are substituted for bits of the audio signal samples of a subband in an adder 7. After the substitution, the sample frequency of the signals of the subbands is increased in means 2 and the signals are again connected in the filter bank 9 into a wide-band audio signal which to a listener sounds totally similar to the original audio signal although data information has been added therein. The reception is in principle a reverse incident to the transmission. A typical feature in this method of prior art is that a hearing threshold benefiting the masking effect has to be calculated both in the encoder of the transmitter and in the decoder of the receiver by using a mask modelling model of the human hearing system (i.e. Psycho Acoustic Model). Thus, the encoder and the coder act independent of one another. This results in certain problems.

In the Finnish patent application No. 915114, filing date October 30, 1991, corresponding to EP-A-0 540 330, published 05 May 1993, said application being included as reference in the present application, the information produced by the encoder of the above described system is made use of. Such information includes information concerning data mode, information related to quantisation, and information related to dematrixing. Said information is transmitted on a separate side channel at the same time as the audio signals to a receiver, which controlled by side channel information is enabled to process the two-channel audio signal received and to convert it e.g. into a multichannel audio signal. Thus, the coder of the receiver acts controlled by the transmitter encoder, i.e. as a slave decoder. An audio signal transmitted on a stereo channel and the information data hidden therein are therefore separated using the control information transmitted by the encoder and received on a separate channel.

The principle of the Finnish patent application is shown in Fig. 2. A coding block therein is indicated by reference numeral 31, said block being in essential elements similar to the prior art encoding block shown in Fig. 1. The encoder combines an incoming multichannel audio signal into a combined stereo signal "hiding" a data signal therein by making use of the masking effect. Information about the data mode, quantization and matrixing are received from the encoder. The data mode describes the special arrangements needed for maximizing the transmission capacity of the hidden data. Such arrangements are e.g. information about that certain channels contain no signals compared with the state of the rest of the channels, so that after being coded said channels are attenuatable. On the whole, the mode contains the way of processing the special instances concerning signal coding when these are not included in normal mix-up. The quantization data informs of the quantization steps of the masking signal and the signal to be masked (hidden), and the number of bits as well as the masking threshold calculated for the time intervals of each subband in the manner described above. The matrixing information yields information about how the original multichannel audio signal was downmixed. In brief, all the information required in carrying out the coding can be achieved from the encoder. The combined stereosignal derived from the encoder, in which data has been "hidden", is adapted for the audio signal to be used on a radio path to be transmitted to e.g. the NICAM format. The above information required in coding is transmitted simultaneously on a separate low-speed digital channel. If the data hidden in the audio channel cannot at a point of time be included in the audio channel, because the "masking capacity" of the audio signal does not suffice, said data can be transmitted on said separate data channel, the information transmitted whereon can be called side information because it is transmitted on the side of the actual audio channel.

The coder 32 in the receiver receives the signal of the audio channel and the side information of the data channel, so that controlled by the coding information transmitted therein it is enabled to code the signal of the audio channel and to separate the data hidden therein. Controlled by the matrixing information it is further enabled to form e.g. a multichannel audio signal.

The method of said Finnish patent application is in principle well appropriate for use in transmitting an audio signal containing hidden data on a transmission path, one of its application being the sound transmission of any HDTV system. In transmitting an audio signal digitally through the radio, it must first be encoded to be appropriate for a transmission channel. There are a great number of channel-coding systems available using compressing; the NICAM system may be mentioned here as an example thereof, as it is already in use and as it may become the audio transmission system in the European HDTV system. When the above-described method is applied in the audio signal, which is channel-coded thereafter using any existing method, this raises a difficult problem in practice: the received coded audio signal is not precisely the same as the audio signal of the transmission head prior to channel-coding. This is due to the fact that independent on the system, the channel-coding causes errors. Most often, one or two of the least significant bits may become converted in the encoder, so that the coded bit stream is almost, but not precisely, the same as the bit stream prior to the encoding. Consequently, if an audio signal is used as such in a transmitter as a signal masking some data to be hidden, it would lead either to a significant increase in error rate of the bits being transmitted or to a significant drop in the hiding capacity because the data is hidden specifically by substituting the least significant bits.

According to the invention, this problem can be solved using the characteristic feature of the method disclosed in the Finnish patent application No. 915114, said feature meaning a separate side information channel containing information formation for controlling the encoder. Since not only on the amount of the data to be used is transmitted on said side channel, as suggested in the application, but also precise information on the location of said data samples, an immaculate original data signal can be provided with the aid of said information. Knowledge of the location of the data samples prerequires information about which of the least significant bits of the audio signal can be substituted for data information, that is, which of the bits are sure to pass through the channel-coder without being changed.

This information is described according to claim 1.

The insight of the invention lies in that an original audio signal is separated into two branches, in the first of which the signal is first channel-coded and immediately thereafter it is decoded. In the second branch the signal is delayed as long as in the first branch the signal is encoded and coded. In this step such signals are resulted which almost resemble one another: In the signal of the first branch the encoding/decoding operation caused a few bit errors. Thereafter, the audio signals of both branches are divided into a plurality of subbands in the filter bank and the signal samples of the subbands are decimated. The subbands have to be equal in size. In each branch the samples of every subband are then grouped into subsequent time windows. The length of one time window is Δ T and it includes samples of the same point of time from each subband. The simultaneous time windows of each subband thus form each time one block. Now, the equivalent samples of the subbands of each branch block are mutually comparable. If all bits are the same it is known that said bits have not been affected by the channel-coding. If, instead, e.g. the lowest, i.e. the least significant bit of the sample of the encoding/coding branch differs from the lowest bit of the sample of the non-encoded branch, while the rest of the bits are equal, said lowest bit is known to be a bit not expected to outlast the channel-coding operation, so that a data bit is not substituted therefor. Part of the other bits can be replaced by data bits because they are known to outlive in channel coding. This is the method which is used for all subbands. The masking threshold is then calculated for the audio signal and the data to be hidden is added in place of the bits of the audio signal which are known to outlive. The information about which of the bits in each sample have been substituted is included in the side channel information SI, on the basis of which the receiver is able to reconstruct the correct hidden information precisely.

An implementation of the invention is described below, reference being made to the accompanying schematic figures, in which:

Fig. 1 presents an encoder used in the method of prior art,

Fig. 2 shows the coder as disclosed in the Finnish application No. FI-915114, and

Fig. 3 shows principally the procedure of the invention.

The procedures shown in Figs 1 and 2 are already described above. The principle of the method according to the invention is presented in Fig. 3. A digital audio signal AUDIO IN, within which DATA IN data information has been hidden utilizing the masking effect, is separated into two branches. In the upper branch the audio signal is channel-coded in an encoder 325 using the same coding method as used in the actual transmission path, for instance in the NICAM coding. An audio signal channel-coded immediately thereafter is coded in a coder 316, whereby it should result in the original audio signal. The audio signal AUDIO IN is at the same time conducted also into the lower branch in which it is delayed in a delay means 317 precisely the time which passes for the encoding and coding in the upper branch. In the interface, marked with P_1, the audio signals are not, however, bit by bit the same, owing to errors caused by the encoder 325 and decoder 316. The defective bits are found by dividing the audio signal in the filter banks 31 and 311, after the interface P_1, into a plurality of subbands, and the signal samples of the subbands are decimated in means 32 and 312. Said subbands are preferably equal in size. The samples of each subband are thereafter grouped into subsequent time windows in means 33 and 315. The lengths Δ T of the time window are the same and they include the same amount of samples of one and same point of time from each subband. Thus the simultaneous time windows of each subband always form one block. So, at one point of time, the signal samples of both the branch of the coded audio signal and of the branch of the delayed audio signal are known, grouped according to their frequency bands. The samples of one point of time are then compared in a comparator 010 so that a sample of one subband of means 33 is compared with a sample of the correspondent subband of means 315. If the encoding / coding process has changed any of the bits, the comparison reveals which of the bits were changed. For instance, if the lowest, i.e. the least significant bit in a sample of block 33 is different from the one in the sample of block 315, it is known that no data bit should be placed in the place of said bit because it will in any case be lost in the course of channel-coding. After the interface marked with P_2 it was thus found out which of the bits of the audio signal should not be substituted for by data bits. The essential core of the invention lies precisely in this fact, and the information obtained thereafter can be applied in an encoder complying with the Finnish application No. 915114. The mode of operation is described below in outline.

A spectrum analysis is accomplished in a manner known in the art in the lower branch in means 34 and the calculation of the masking threshold in means 35. After finding out how many of the bits of the audio signal can be substituted for by data bits and which of the bits in the audio signal do not outlive the channel-coding, only the bits below the masking threshold can be substituted in an adder 310 which outlive in the channel coding. On the basis of the masking threshold information by block 35 and the information provided by reference block 313, the data to be hidden is arranged to be appropriate in an arrangement block 36.

The information divulged in reference means 313 is conveyed to the adder 310. For instance, if the spectrum analysis and the calculation of the masking threshold indicate that data bits could be substituted for three bits in a sample, without being audible to the human ear, and if it has been analysed in reference means 313 from the same sample that the first bit will perish in the channel-coding process, only the two bits of the sample are substituted for by data bits which were learnt to outlive the channel coding. The information on the point of a sample of an audio signal at which some data has been hidden, i.e. which of the bits have been substituted for by data bits, is transmitted as side information on a SI channel. On the basis of said information and other information transmitted on the side channel, the receiver is enabled to discover in the audio signal a data signal hidden therein.

All audio samples are analysed similarly in each subband, regarding the duration of the channel coding, and only those bits below the masking threshold are substituted which are sure to outlive the channel-coding. After summing up, the sample frequency of the signals of the subbands is increased in means 38 and the signals are recombined in filter bank 39 into a wideband audio signal which after being channel-coded in the transmitter and decoded in the receiver sound to the listener's ear the same as the original audio signal irrespective of the fact that data information has been added therein and that the data information is received without any deficiencies. A low-speed side channel SI is produced in the manner disclosed in Finnish application No. 915114, included therein an addition that now also information about the location of the bits hidden therein is added therein.

The main features of the method are described above. It is obvious that a practical implementation can be accomplished in a number of ways while remaining within the protective scope of the claims. The method is particularly appropriate for use in association with the method disclosed in Finnish patent application No. 915114 because the side channel disclosed therein is particularly well appropriate for mediating the information about the location of the substituted bits to the receiver.

Claims

1. A method for combining a data signal with an audio signal prior to channel-coding the combined signal, in which

   - an audio signal entering in sample sequence mode is conducted to a first branch and divided into subbands, whereby in each subband an array of audio signal samples of equal size is obtained in one and the same time window,
   - a masking threshold is calculated simultaneously for said sample array in each subband, the sounds wherebelow being unaudible to the human ear,
   - the bits of the data signal are substituted for the bits of the samples of the sample arrays remaining below the masking threshold,
   - the subbands are combined, whereby a combined signal to be transmitted on an audio channel is obtained, and
   - all the information is gathered that is needed in re-separating the combined signal, and said information is transmitted in the form of side information on a separate data channel at the same time with the combined signal,

   whereby

   - an audio signal is conducted also to a second branch in which it is channel-coded and decoded, and thereafter it is divided into as many subbands as in the first branch, whereby in each subband an array of audio signal samples of equal magnitude is obtained in the same time window as in the first branch,
   - the audio signal conducted into the first branch is delayed for a time equivalent to the time required for channel-coding and decoding,
   - the audio signal samples of one and same point of time of the corresponding subbands of each branch are compared,
   - only the bits of the samples of the first branch are substituted for by data bits which are the same as in the second branch, and
   - information on the location of the substituting data bits in the sample is transmitted in the form of side information on said data channel.

2. Method for separating an audio signal and a data signal combined in the manner disclosed in claim 1 in a receiver in which a signal entering in sample sequence mode is coded, divided into subbands, and the bits are separated from the combined signal which remain below the masking threshold, and the separated bits are combined, whereby the receiver receives in the form of side information on a separate data channel such information which is needed for separating the data signal from the audio signal, whereby the decoder accomplishes said separation controlled by the coder, characterized in that the side information also includes information about which of the bits in the audio sample have been substituted for by data bits.

3. An apparatus for combining a data signal with an audio signal before channel-coding the combined signal in the transmitter, said apparatus comprising:

   - a first filter means (311) for dividing an audio signal entering in the form of sample sequence mode into subbands,
   - a grouping means (315) to group in each subband an array of audio signal samples of the same size in one and same time window,
   - an analysing and calculating means (34,35), simultaneously calculating in each subband a masking threshold for a sample group, the sounds below which the human ear is not able to hear,
   - a substituting means (37) in which the bits of a data signal are substituted for the bits of the samples of the sample groups which remain below the masking threshold,
   - a second filter means (39) to combine the subbands, whereby a combined signal to be transmitted on an audio channel is obtained,
   - a data channel control means to gather all the information needed for reseparating the combined signal, which information is transmitted as side information on the data channel simultaneously with the combined signal,

   whereby the apparatus comprises further

   - a parallel branch to which the audio signal is also conducted, while the branch comprises in succession a channel-coder (325) and a decoder (316), a third filter means (31) to divide the output signal of the encoder into as many subbands as the first filter means (311), a second grouping means (33) to group within each subband an equal number of audiosignal samples in one time window, whereby in said sub-band an equal number of audiosignal samples are obtained in one and the same time window as in the first branch,

- a delay means (317) to delay the audio signal entering the first filter means (311) for a period of time which corresponds to the delay of the channel coder (315) and the decoder (316),
- a comparator means (313) which compares the same-moment audio signal samples of the corresponding subbands of the first (315) and the second grouping means (33) with one another, whereby the substituting means substitutes with data bits only for the bits of the samples of the first grouping means (315) which are the same as those in the samples of the second grouping means (33), and the comparator (313, 314) informs the control means of the side channel of the location of the substituting data bits in the sample.

Patentansprüche

1. Verfahren zum Kombinieren eines Datensignals mit einem Tonsignal vor der Kanalcodierung des kombinierten Signals, bei dem

   - ein im Abtastsequenzmodus eingehendes Tonsignal zu einer ersten Verzweigung geleitet und in Teilbänder unterteilt wird, so daß in jedem Teilband eine Reihe von Tonsignalproben gleicher Größe in ein und demselben Zeitfenster erhalten wird,
   - für die genannte Probenreihe gleichzeitig in jedem Teilband eine Maskierungsschwelle errechnet wird, unterhalb derer die Töne für das menschliche Ohr unhörbar sind,
   - die Bits des Datensignals durch die Bits der Proben der unter der Maskierungsschwelle verbleibenden Probenreihen substituiert werden,
   - die Teilbänder kombiniert werden, so daß ein auf einem Tonkanal zu übertragendes kombiniertes Signal erhalten wird, und
   - die Informationen gesammelt werden, die beim erneuten Trennen des kombinierten Signals benötigt werden, und diese Informationen in der Form von Nebeninformationen auf einem separaten Datenkanal gleichzeitig mit dem kombinierten Signal übertragen werden, wobei
   - ein Tonsignal auch zu einer zweiten Verzweigung geleitet wird, in der es kanalcodiert und -decodiert und danach in ebenso viele Teilbänder wie in der ersten Verzweigung unterteilt wird, so daß in jedem Teilband eine Reihe von Tonsignalproben gleicher Größe in demselben Zeitfenster erhalten wird wie in der ersten Verzweigung,
   - das in die erste Verzweigung geleitete Tonsignal für eine Zeit verzögert wird, die gleich der Zeit ist, die zur Kanalcodierung und -decodierung erforderlich ist,
   - die Tonsignalproben von ein und demselben Zeitpunkt der entsprechenden Teilbänder jeder Verzweigung verglichen werden,
   - nur diejenigen Bits der Proben der ersten Verzweigung durch Datenbits substituiert werden, die dieselben sind wie in der zweiten Verzweigung, und
   - Informationen über den Ort der Substitution von Datenbits in der Probe in der Form von Nebeninformationen über den genannten Datenkanal übertragen werden.

2. Verfahren zum Trennen eines Tonsignals und eines in der in Anspruch 1 offenbarten Weise kombinierten Datensignals in einem Empfänger, in dem ein im Abtastsequenzmodus eingehendes Signal codiert und in Teilbänder unterteilt wird und diejenigen Bits von dem kombinierten Signal getrennt werden, die unterhalb der Maskierungsschwelle bleiben, und die getrennten Bits kombiniert werden, so daß der Empfänger in der Form von Nebeninformationen auf einem separaten Datenkanal solche Informationen erhält, die zum Trennen des Datensignals von dem Tonsignal erforderlich sind, so daß der Decoder die genannte Trennung durch den Codierer gesteuert durchführt, dadurch gekennzeichnet, daß die Nebeninformationen auch Informationen darüber enthalten, welche der Bits in der Tonprobe durch Datenbits substituiert wurden.

3. Vorrichtung zum Kombinieren eines Datensignals mit einem Tonsignal vor der Kanalcodierung des kombinierten Signals in dem Sender, wobei die genannte Vorrichtung folgendes umfaßt:

   - einen ersten Filter (311) zum Unterteilen eines im Abtastsequenzmodus eingehenden Tonsignals in Teilbänder,
   - ein Gruppierungsmittel (315), um in jedem Teilband eine Reihe von Tonsignalproben derselben Größe in ein und demselben Zeitfenster zu gruppieren,
   - ein Analyse- und Berechnungsmittel (34, 35), das gleichzeitig in jedem Teilband eine Maskierungsschwelle für eine Probengruppe errechnet, unterhalb derer der Ton für das menschliche Ohr nicht hörbar ist,
   - ein Substitutionsmittel (37), bei dem die Bits eines Datensignals durch Bits der Proben der Probengruppen substituiert werden, die unterhalb der Maskierungsschwelle bleiben,
   - einen zweiten Filter (39) zum Kombinieren der Teilbänder, so daß ein auf einem Tonkanal zu

übertragendes kombiniertes Signal erhalten wird,

- ein Datenkanal-Steuermittel zum Sammeln aller Informationen, die für die erneute Trennung des kombinierten Signals benötigt werden, wobei diese Informationen als Nebeninformationen gleichzeitig mit dem kombinierten Signal auf dem Datenkanal übertragen werden, wobei die Vorrichtung ferner folgendes umfaßt:
- eine parallele Verzweigung, auf die das Tonsignal ebenso geleitet wird, während die Verzweigung nacheinander folgendes umfaßt: einen Kanalcodierer (325) und einen Decodierer (316), einen dritten Filter (31) zum Unterteilen des Ausgangssignals des Codierers in ebenso viele Teilbänder wie der erste Filter (311), ein zweites Gruppierungsmittel (33), um innerhalb jedes Teilbandes eine gleiche Zahl von Tonsignalproben in einem Zeitfenster zu gruppieren, so daß in dem genannten Teilband eine gleiche Zahl von Tonsignalproben in ein und demselben Zeitfenster wie in der ersten Verzweigung erhalten werden,
- ein Verzögerungsmittel (317) zum Verzögern des in dem ersten Filter (311) eingehenden Tonsignals für eine Zeitperiode, die der Verzögerung des Kanalcodierers (315) und des Decodierers (316) entspricht,
- einen Komparator (313), der die zeitgleichen Tonsignalproben der entsprechenden Teilbänder des ersten (315) und des zweiten (33) Gruppierungsmittels miteinander vergleicht, so daß das Substituierungsmittel nur diejenigen Bits der Proben des ersten Gruppierungsmittels (315) durch Datenbits substituiert, die dieselben sind wie die in den Proben des zweiten Gruppierungsmittels (33), und der Komparator (313, 314) informiert das Steuermittel des Seitenkanals des Ortes der substituierenden Datenbits in der Probe.

Revendications

1. Procédé pour combiner un signal de données avec un signal audio avant de coder en canaux le signal combiné, dans lequel

   - un signal audio entrant dans un mode séquentiel d'échantillons est amené jusqu'à une première branche et divisé en sous-bandes, moyennant quoi dans chaque sous-bande, un ensemble d'échantillons de signal audio de tailles égales est obtenu dans une seule et même fenêtre temporelle,
   - un seuil de masquage est calculé en même temps pour ledit ensemble d'échantillons dans chaque sous-bande, les sons au-dessous de celui-ci étant inaudibles pour l'oreille humaine,
   - les bits du signal de données viennent remplacer les bits des échantillons des ensembles d'échantillons restant sous le seuil de masquage.
   - les sous-bandes sont combinées, moyennant quoi un signal combiné devant être transmis sur un canal audio est obtenu, et
   - toutes les informations sont rassemblées, qui sont nécessaires pour séparer de nouveau le signal combiné, et lesdites informations sont transmises sous la forme d'informations secondaires sur un canal de données séparé au même moment que le signal combiné, moyennant quoi
   - un signal audio est également amené jusqu'à une seconde branche dans lequel il est codé en canaux et décodé, et par la suite, il est divisé en autant de sous-bandes que dans la première branche, moyennant quoi, dans chaque sous-bande, un ensemble d'échantillons de signal audio d'amplitudes égales est obtenu dans la même fenêtre temporelle que dans la première branche
   - le signal audio amené dans la première branche est retardé pendant une durée équivalente à celle requise pour coder en canaux et décoder,
   - les échantillons de signal audio d'un seul et même instant des sous-bandes correspondantes de chaque branche sont comparés,
   - seuls les bits des échantillons de la première branche sont remplacés par des bits de données qui sont les mêmes que dans la seconde branche, et
   - les informations sur l'emplacement des bits de données de remplacement dans l'échantillon sont transmises sous la formes d'informations secondaires sur ledit canal de données.

2. Procédé pour séparer un signal audio et un signal de données combinés de la manière décrite dans la revendication 1, dans un récepteur dans lequel un signal entrant dans un mode séquentiel d'échantillons est codé, divisé en sous-bandes, et les bits sont séparés du signal combiné qui restent au-dessous du seuil de masquage, et les bits séparés sont combinés, moyennant quoi le récepteur reçoit sous la forme d'informations secondaires, sur un canal de données séparé, les informations qui sont nécessaires pour séparer le signal de données du signal audio, moyennant quoi le décodeur réalise ladite séparation commandée par le codeur, caractérisé en ce que les informations secondaires comprennent également des informations au sujet des bits dans l'échantillon audio qui ont été remplacés par les bits de données.

3. Dispositif pour combiner un signal de données avec un signal audio avant de coder en canaux le signal combiné dans l'émetteur, ledit dispositif comprenant :

- des premiers moyens de filtre (311) pour diviser un signal audio entrant sous la forme d'un mode séquentiel d'échantillons en sous-bandes,
- des moyens de groupement (315) pour grouper dans chaque sous-bande un ensemble d'échantillons de signal audio de la même taille, dans une seule et même fenêtre temporelle,
- des moyens d'analyse et de calcul (34, 35), calculant en même temps dans chaque sous-bande un seuil de masquage pour un groupe d'échantillons, l'oreille humaine n'étant pas capable d'entendre les sons au-dessous de celui-ci,
- des moyens de substitution (37) dans lesquels les bits d'un signal de données remplacent les bits des échantillons des groupes d'échantillons qui restent au-dessous du seuil de masquage,
- des deuxièmes moyens de filtre (39) pour combiner les sous-bandes, moyennant quoi un signal combiné devant être transmis sur un canal audio est obtenu,
- des moyens de commande de canal de données pour rassembler toutes les informations nécessaires pour séparer de nouveau le signal combiné, lesquelles informations sont transmises en tant qu'informations secondaires sur le canal de données en même temps que le signal combiné, le dispositif comprenant en outre
- une branche parallèle vers laquelle le signal audio est également amené, tandis que la branche comprend, à la suite, un codeur (325) de canaux et un décodeur (316), des troisièmes moyens de filtre (31) pour diviser le signal de sortie du codeur en autant de sous-bandes que dans les premiers moyens de filtre (311), des seconds moyens de groupement (33) pour grouper à l'intérieur de chaque sous-bande un nombre égal d'échantillons de signal audio dans une fenêtre temporelle, moyennant quoi on obtient dans ladite sous-bande un nombre égal d'échantillons de signal audio dans une seule et même fenêtre temporelle comme dans la première branche,
- des moyens de retardement (317) pour retarder le signal audio entrant dans les premiers moyens de filtre (311) pour une durée qui correspond au retard du codeur (315) et du décodeur (316) de canaux,
- des moyens formant comparateur (313) qui comparent, les uns avec les autres, les échantillons de signal audio, pris au même moment, des sous-bandes correspondantes des premiers (315) et seconds (33) moyens de groupement, moyennant quoi les moyens de remplacement remplacent par des bits de données seulement les bits des échantillons des premiers moyens de groupement (315) qui sont les mêmes que ceux dans les échantillons des seconds moyens de groupement (33), et le comparateur (313, 314) informe les moyens de commande du canal secondaire de l'emplacement des bits de données de remplacement dans l'échantillon.

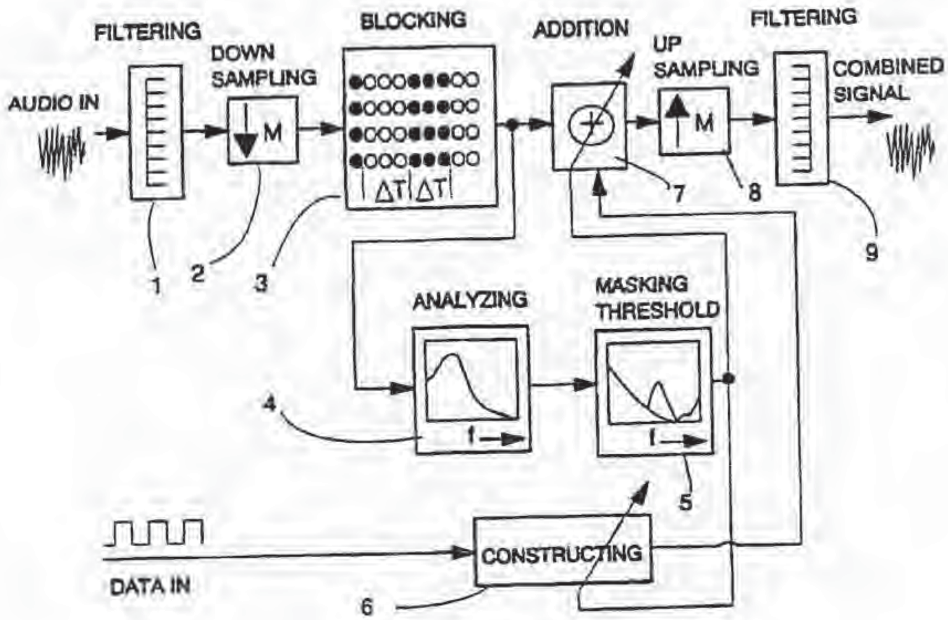

FILTERING
DOWN SAMPLING
BLOCKING
ADDITION
UP SAMPLING
FILTERING
AUDIO IN
M
ΔT ΔT
M
COMBINED SIGNAL
1
2
3
7
8
9
ANALYZING
MASKING THRESHOLD
4
f
f
5
DATA IN
CONSTRUCTING
6

Fig. 1

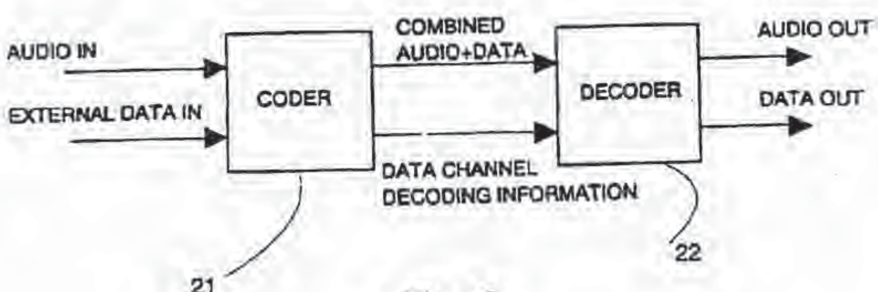

AUDIO IN
EXTERNAL DATA IN
CODER
COMBINED AUDIO+DATA
DATA CHANNEL DECODING INFORMATION
DECODER
AUDIO OUT
DATA OUT
21
22

Fig. 2

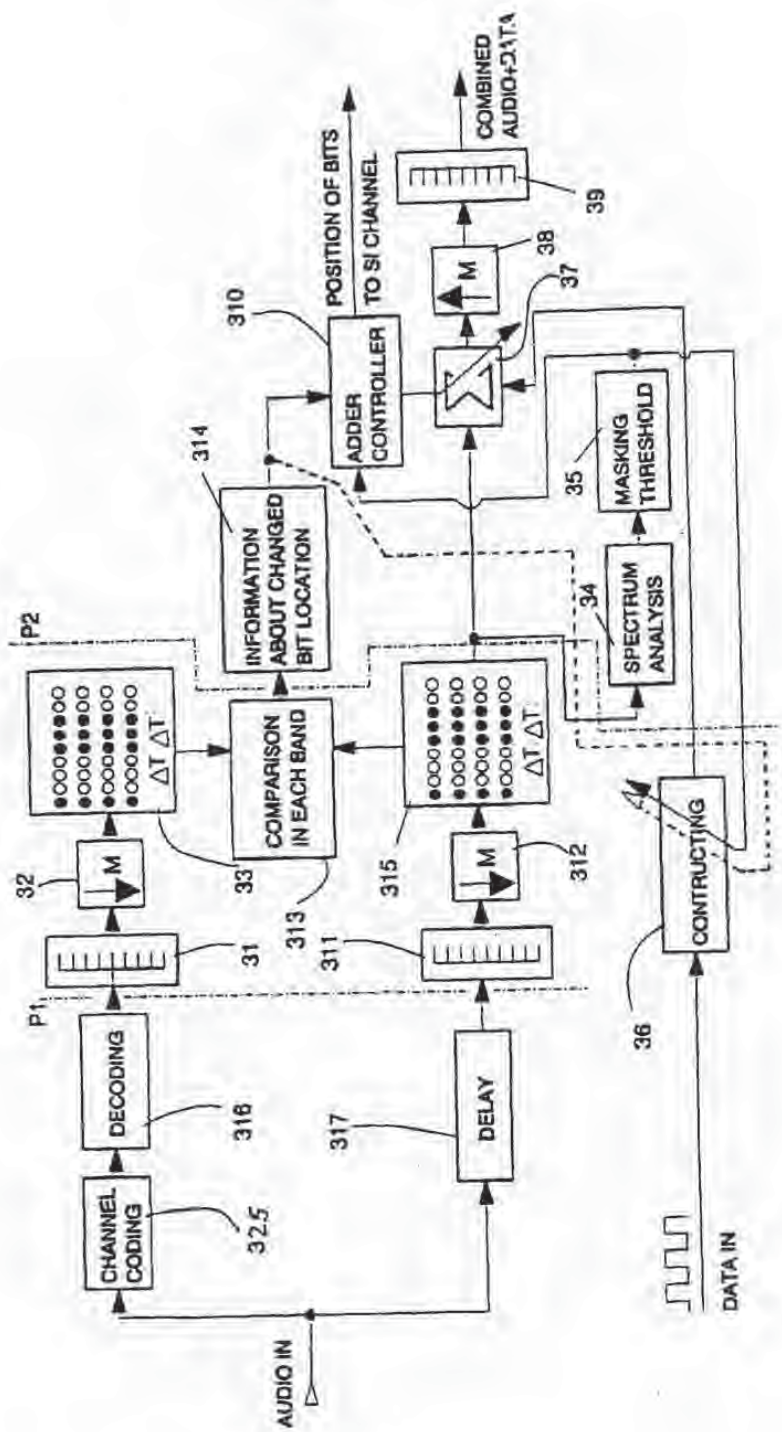

AUDIO IN
CHANNEL CODING
32.5
DECODING
318
P1
31
32
M
33
COMPARISON IN EACH BAND
313
ΔT ΔT
P2
INFORMATION ABOUT CHANGED BIT LOCATION
314
ADDER CONTROLLER
310
POSITION OF BITS TO SI CHANNEL
DELAY
317
311
312
M
315
ΔT ΔT
34
SPECTRUM ANALYSIS
35
MASKING THRESHOLD
37
38
M
39
COMBINED AUDIO+DATA
36
CONTRUCTING
DATA IN

Fig. 3

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 19/14	A2	(11) International Publication Number: WO 95/14289 (43) International Publication Date: 26 May 1995 (26.05.95)

(21) International Application Number: PCT/US94/13366

(22) International Filing Date: 16 November 1994 (16.11.94)

(30) Priority Data:

154,866	18 November 1993 (18.11.93)	US
215,289	17 March 1994 (17.03.94)	US
327,426	21 October 1994 (21.10.94)	US

(60) Parent Application or Grant
(63) Related by Continuation
US 08/327,426 (CIP)
Filed on 21 October 1994 (21.10.94)

(71) Applicant (*for all designated States except US*): PINECONE IMAGING CORPORATION [US/US]; 363 S.W. Tualatin Loop, West Linn, OR 97068 (US).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): RHOADS, Geoffrey, B. [US/US]; 363 S.W. Tualatin Loop, West Linn, OR 97068 (US).

(74) Agent: CONWELL, William, Y.; Klarquist, Sparkman, Campbell, Leigh & Whinston, One World Trade Center, Suite 1600, 121 S.W. Salmon Street, Portland, OR 97204 (US).

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

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: IDENTIFICATION/AUTHENTICATION CODING METHOD AND APPARATUS

(57) Abstract

An identification code signal is impressed on a carrier to be identified (such as an electronic data signal or a physical medium) in a manner that permits the identification signal later to be discerned and the carrier thereby identified. The method and apparatus are characterized by robustness despite degradation of the encoded carrier, and by holographic permeation of the identification signal throughout the carrier. An exemplary embodiment is a processor that embeds the identification signal onto a carrier signal in real time.

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.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgystan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo			SE	Sweden
CH	Switzerland	KR	Republic of Korea	SI	Slovenia
CI	Côte d'Ivoire	KZ	Kazakhstan	SK	Slovakia
CM	Cameroon	LI	Liechtenstein	SN	Senegal
CN	China	LK	Sri Lanka	TD	Chad
CS	Czechoslovakia	LU	Luxembourg	TG	Togo
CZ	Czech Republic	LV	Latvia	TJ	Tajikistan
DE	Germany	MC	Monaco	TT	Trinidad and Tobago
DK	Denmark	MD	Republic of Moldova	UA	Ukraine
ES	Spain	MG	Madagascar	US	United States of America
FI	Finland	ML	Mali	UZ	Uzbekistan
FR	France	MN	Mongolia	VN	Viet Nam
GA	Gabon				

IDENTIFICATION/AUTHENTICATION CODING METHOD AND APPARATUS

Field of the Invention

The present invention relates to the embedding of robust identification codes in electronic, optical and physical media, and the subsequent, objective discernment of such codes for identification purposes even after intervening distortion or corruption of the media.

The invention is illustrated with reference to several exemplary applications, including identification/authentication coding of electronic imagery, serial data signals (e.g. audio and video), emulsion film, and paper currency, but is not so limited.

Background and Summary of the Invention

"I would never put it in the power of any printer or publisher to suppress or alter a work of mine, by making him master of the copy"

Thomas Paine, *Rights of Man*, 1792.

"The printer dares not go beyond his licensed copy"

Milton, *Aeropagetica*, 1644.

Since time immemorial, unauthorized use and outright piracy of proprietary source material has been a source of lost revenue, confusion, and artistic corruption.

These historical problems have been compounded by the advent of digital technology. With it, the technology of copying materials and redistributing them in unauthorized manners has reached new heights of sophistication, and more importantly, omnipresence. Lacking objective means for comparing an alleged copy of material with the original, owners and possible litigation proceedings are left with a subjective opinion of whether the alleged copy is stolen, or has been used in an unauthorized manner. Furthermore, there is no simple means of tracing a path to an original purchaser of the material, something which can be valuable in tracing where a possible "leak" of the material first occurred.

A variety of methods for protecting commercial material have been attempted. One is to scramble signals via an encoding method prior to distribution, and descramble prior to use. This technique, however, requires that both the original and later descrambled signals never leave closed and controlled networks, lest they be intercepted and recorded. Furthermore, this arrangement is of little use in the broad field of mass marketing audio and visual material, where even a few dollars extra cost causes a major reduction in market, and where the signal must eventually be descrambled to be perceived, and thus can be easily recorded.

Another class of techniques relies on modification of source audio or video signals to include a subliminal identification signal, which can be sensed by electronic means. Examples of such systems are found in U.S. Patent 4,972,471 and European patent publication EP 441,702, as well as in Komatsu et al, "Authentication System Using Concealed Image in Telematics," Memoirs of the School of Science & Engineering, Waseda University, No. 52, p. 45-60 (1988) (Komatsu uses the term "digital watermark" for this technique). An elementary introduction to these methods is found in the article "Digital Signatures," Byte Magazine, November, 1993, p. 309 These techniques have the common characteristic that deterministic signals with well defined patterns and sequences within the source material convey the identification information. For certain applications this is not a drawback. But in general, this is an inefficient form of embedding identification information for a variety of reasons: (a) the whole of the source material is not used; (b) deterministic patterns have a higher likelihood of being discovered and removed by a would-be pirate; and (c) the signals are not generally "holographic" in that identifications may be difficult to make given only sections of the whole. ("Holographic" is used herein to refer to the property that the identification information is distributed globally throughout the coded signal, and can be fully discerned from an examination of even a fraction of the coded signal. Coding of this type is sometimes termed "distributed" herein.)

Among the cited references are descriptions of several programs which perform steganography - described in one document as "... the ancient art of hiding information in some otherwise inconspicuous information." These programs variously allow computer users to hide their own messages inside digital image files and digital audio files. All do so by toggling the least significant bit (the lowest order bit of a single data sample) of a given audio data stream or rasterized image. Some of these programs embed messages quite directly into the least significant bit, while other "pre-encrypt" or scramble a message first and then embed the encrypted data into the least significant bit.

Our current understanding of these programs is that they generally rely on error-free transmission of the of digital data in order to correctly transmit a given message in its entirety. Typically the message is passed only once, i.e., it is not repeated. These programs also seem to "take over" the least significant bit entirely, where actual data is obliterated and the message placed accordingly. This might mean that such codes could be easily erased by merely stripping off the least significant bit of all data values in a given image or audio file. It is these and other considerations which suggest that the only similarity between our invention and the established art of steganography is in the placement of information into data files with minimal perceptibility. The specifics of embedding and the uses of that buried information diverge from there.

Another cited reference is U.S. Patent 5,325,167 to Melen. In the service of authenticating a given document, the high precision scanning of that document reveals patterns and "microscopic grain structure" which apparently is a kind of unique fingerprint for the underlying document media, such as paper itself or post-applied materials such as toner. Melen further teaches that scanning and storing this fingerprint can later be used in authentication by scanning a purported document and comparing it to the original fingerprint. Applicant is aware of a similar idea employed in the very high precision recording of credit card magnetic strips, as reported in the February 8, 1994, Wall Street Journal, page B1, wherein very fine magnetic fluxuations tend to be unique from one card to the next, so that credit card authentication could be achieved through pre-recording these fluxuations later to be compared to the recordings of the purportedly same credit card.

Both of the foregoing techniques appear to rest on the same identification principles on which the mature science of fingerprint analysis rests: the innate uniqueness of some localized physical property. These methods then rely upon a single judgement and/or measurement of "similarity" or "correlation" between a suspect and a pre-recording master. Though fingerprint analysis has brought this to a high art, these methods are nevertheless open to a claim that preparations of the samples, and the "filtering" and "scanner specifications" of Melen's patent, unavoidably tend to bias the resulting judgement of similarity, and would create a need for more esoteric "expert testimony" to explain the confidence of a found match or mis-match. An object of the present invention is to avoid this reliance on expert testimony and to place the confidence in a match into simple "coin flip" vernacular, i.e., what are the odds you can call the correct coin flip 16 times in a row. Attempts to identify fragments of a fingerprint, document, or otherwise, exacerbate this issue of confidence in a judgment, where it is an object of the present invention to objectively apply the intuitive "coin flip" confidence to the smallest fragment possible. Also, storing unique fingerprints for each and every document or credit card magnetic strip, and having these fingerprints readily available for later cross-checking, should prove to be quite an economic undertaking. It is an object of this invention to allow for the "re-use" of noise codes and "snowy images" in the service of easing storage requirements.

U.S. Patent 4,921,278 to Shiang et al. teaches a kind of spatial encryption technique wherein a signature or photograph is splayed out into what the untrained eye would refer to as noise, but which is actually a well defined structure referred to as Moire patterns. The similarities of the present invention to Shiang's system appear to be use of noise-like patterns which nevertheless carry information, and the use of this principle on credit cards and other identification cards.

Others of the cited patents deal with other techniques for identification and/or authentication of signals or media. U.S. Patent 4,944,036 to Hyatt does not appear to be applicable to the present invention, but does point out that the term "signature" can be equally applied to signals which carry unique characteristics based on physical structure.

Despite the foregoing and other diverse work in the field of identification/authentication, there still remains a need for a reliable and efficient method for performing a positive identification between a copy of an original signal and the original. Desirably, this method should not only perform identification, it should also be able to convey source-version information in order to better pinpoint the point of sale. The method should not compromise the innate quality of material which is being sold, as does the placement of localized logos on images. The method should be robust so that an identification can be made even after multiple copies have been made and/or compression and decompression of the signal has taken place. The identification method should be largely unerasable or "uncrackable." The method should be capable of working even on fractional pieces of the original signal, such as a 10 second "riff" of an audio signal or the "clipped and pasted" sub-section of an original image.

The existence of such a method would have profound consequences on piracy in that it could (a) cost effectively monitor for unauthorized uses of material and perform "quick checks"; (b) become a deterrent to unauthorized uses when the method is known to be in use and the consequences well publicized; and (c) provide unequivocal proof of identity, similar to fingerprint identification, in litigation, with potentially more reliability than that of fingerprinting.

In accordance with an exemplary embodiment of the invention, the foregoing and additional objects are achieved by embedding an imperceptible identification code throughout a source signal. In the preferred embodiment, this embedding is achieved by modulating the source signal with a small noise signal in a coded fashion. More particularly, bits of a binary identification code are referenced, one at a time, to control modulation of the source signal with the noise signal.

The copy with the embedded signal (the "encoded" copy) becomes the material which is sold, while the original is secured in a safe place. The new copy is nearly identical to the original except under the finest of scrutiny; thus, its commercial value is not compromised. After the new copy has been sold and distributed and potentially distorted by multiple copies, the present disclosure details methods for positively identifying any suspect signal against the original.

Among its other advantages, the preferred embodiments' use of identification signals which are global (holographic) and which mimic natural noise sources allows the maximization of identification signal energy, as opposed to merely having it present 'somewhere in the original material.' This allows the identification coding to be much more robust in the face of thousands of real world degradation processes and material transformations, such as cutting and cropping of imagery.

The foregoing and additional features and advantages of the present invention will be more readily apparent from the following detailed description thereof, which proceeds with reference to the accompanying drawings.

Brief Description of the Drawings

Fig. 1 is a simple and classic depiction of a one dimensional digital signal which is discretized in both axes.

Fig. 2 is a general overview, with detailed description of steps, of the process of embedding an "imperceptible" identification signal onto another signal.

Fig. 3 is a step-wise description of how a suspected copy of an original is identified.

Fig. 4 is a schematic view of an apparatus for pre-exposing film with identification information in accordance with another embodiment of the present invention.

Fig. 5 is a diagram of a "black box" embodiment of the present invention.

Fig. 6 is a schematic block diagram of the embodiment of Fig. 5.

Fig. 7 shows a variant of the Fig. 6 embodiment adapted to encode successive sets of input data with different code words but with the same noise data.

Fig. 8 shows a variant of the Fig. 6 embodiment adapted to encode each frame of a videotaped production with a unique code number.

Figs. 9A-9C are representations of an industry standard noise second that can be used in one embodiment of the present invention.

Fig. 10 shows an integrated circuit used in detecting standard noise codes.

Fig. 11 shows a process flow for detecting a standard noise code that can be used in the Fig. 10 embodiment.

Fig. 12 is an embodiment employing a plurality of detectors in accordance with another embodiment of the present invention.

Detailed Description

In the following discussion of an illustrative embodiment, the words "signal" and "image" are used interchangeably to refer to both one, two, and even beyond two dimensions of digital signal. Examples will routinely switch back and forth between a one dimensional audio-type digital signal and a two dimensional image-type digital signal.

In order to fully describe the details of an illustrative embodiment of the invention, it is necessary first to describe the basic properties of a digital signal. Fig. 1 shows a classic representation of a one dimensional digital signal. The x-axis defines the index numbers of sequence of digital "samples," and the y-axis is the instantaneous value of the signal at that sample, being constrained to exist only at a finite number of levels defined as the "binary depth" of a digital sample. The example depicted in Fig. 1 has the value of 2 to the fourth power, or "4 bits," giving 16 allowed states of the sample value.

For audio information such as sound waves, it is commonly accepted that the digitization process discretizes a continuous phenomena both in the time domain and in the signal level domain. As such, the process of digitization itself introduces a fundamental error source, in that it cannot record detail smaller than the discretization interval in either domain. The industry has referred to this, among other ways, as "aliasing" in the time domain, and "quantization noise" in the signal level domain. Thus, there will always be a basic error floor of a digital signal. Pure quantization noise, measured in a root mean square sense, is theoretically known to have the value of one over the square root of twelve, or about 0.29 DN, where DN stands for 'Digital Number' or the finest unit increment of the signal level. For example, a perfect 12-bit digitizer will have 4096 allowed DN with an innate root mean square noise floor of ~0.29 DN.

All known physical measurement processes add additional noise to the transformation of a continuous signal into the digital form. The quantization noise typically adds in quadrature (square root of the mean squares) to the "analog noise" of the measurement process as it is sometimes referred to.

With almost all commercial and technical processes, the use of the decibel scale is used as a measure of signal and noise in a given recording medium. The expression "signal-to-noise ratio" is generally used, as it will be in this disclosure. As an example, this disclosure refers to signal to noise ratios in terms of signal power and noise power, thus 20 dB represents a 10 times increase in signal amplitude.

In summary, the presently preferred embodiments of the invention embed an N-bit value onto an entire signal through the addition of a very low amplitude encodation signal which has the look of pure noise. N is usually at least 8 and is capped on the higher end by ultimate signal-to-noise considerations and "bit error" in retrieving and decoding the N-bit value. As a practical matter, N is chosen based on application specific considerations, such as the number of unique different "signatures" that are desired. To illustrate, if N=128, then the number of unique digital signatures is in excess of 10^^38 (2^^128). This number is believed to be more than adequate to both identify the material with sufficient statistical certainty and to index exact sale and distribution information.

The amplitude or power of this added signal is determined by the aesthetic and informational considerations of each and every application using the present methodology. For instance, non-professional video can stand to have a higher embedded signal level without becoming noticeable to the average human eye, while high precision audio may only be able to accept a relatively small signal level lest the human ear perceive an objectionable increase in "hiss." These statements are generalities and each application has its own set of criteria in choosing the signal level of the embedded identification signal. The higher the level of embedded signal, the more corrupted a copy can be and still be identified. On the other hand, the higher the level of embedded signal, the more objectionable the perceived noise might be, potentially impacting the value of the distributed material.

To illustrate the range of different applications to which the principles of the present invention can be applied, the present specification details two different systems. The first (termed, for lack of a better name, a "batch encoding" system), applies identification coding to an existing data signal. The second (termed, for lack of a better name, a "real time encoding" system), applies identification coding to a signal as it is produced. Those skilled in the art will recognize that the principles of the present invention can be applied in a number of other contexts in addition to these particularly described.

The discussions of these two systems can be read in either order. Some readers may find the latter more intuitive than the former; for others the contrary may be true.

<u>BATCH ENCODING</u>

The following discussion of a first class of embodiments is best prefaced by a section defining relevant terms:

The <u>original signal</u> refers to either the original digital signal or the high quality digitized copy of a non-digital original.

The N-bit identification word refers to a unique identification binary value, typically having N range anywhere from 8 to 128, which is the identification code ultimately placed onto the original signal via the disclosed transformation process. In the illustrated embodiment, each N-bit identification word begins with the sequence of values '0101,' which is used to determine an optimization of the signal-to-noise ratio in the identification procedure of a suspect signal (see definition below).

The m'th bit value of the N-bit identification word is either a zero or one corresponding to the value of the m'th place, reading left to right, of the N-bit word. E.g., the first (m=1) bit value of the N=8 identification word 01110100 is the value '0;' the second bit value of this identification word is '1', etc.

The m'th individual embedded code signal refers to a signal which has dimensions and extent precisely equal to the original signal (e.g. both are a 512 by 512 digital image), and which is (in the illustrated embodiment) an independent pseudo-random sequence of digital values. "Pseudo" pays homage to the difficulty in philosophically defining pure randomness, and also indicates that there are various acceptable ways of generating the "random" signal. There will be exactly N individual embedded code signals associated with any given original signal.

The acceptable perceived noise level refers to an application-specific determination of how much "extra noise," i.e. amplitude of the composite embedded code signal described next, can be added to the original signal and still have an acceptable signal to sell or otherwise distribute. This disclosure uses a 1 dB increase in noise as a typical value which might be acceptable, but this is quite arbitrary.

The composite embedded code signal refers to the signal which has dimensions and extent precisely equal to the original signal, (e.g. both are a 512 by 512 digital image), and which contains the addition and appropriate attenuation of the N individual embedded code signals. The individual embedded signals are generated on an arbitrary scale, whereas the amplitude of the composite signal must not exceed the pre-set acceptable perceived noise level, hence the need for "attenuation" of the N added individual code signals.

The distributable signal refers to the nearly similar copy of the original signal, consisting of the original signal plus the composite embedded code signal. This is the signal which is distributed to the outside community, having only slightly higher but acceptable "noise properties" than the original.

A suspect signal refers to a signal which has the general appearance of the original and distributed signal and whose potential identification match to the original is being questioned. The suspect signal is then analyzed to see if it matches the N-bit identification word.

The detailed methodology of this first embodiment begins by stating that the N-bit identification word is encoded onto the original signal by having each of the m bit values multiply their corresponding individual embedded code signals, the resultant being accumulated in the composite signal, the fully summed composite signal then being attenuated down to the acceptable perceived noise amplitude, and the resultant composite signal added to the original to become the distributable signal.

The original signal, the N-bit identification word, and all N individual embedded code signals are then stored away in a secured place. A suspect signal is then found. This signal may have undergone multiple copies, compressions and decompressions, resamplings onto different spaced digital signals, transfers from digital to analog back to digital media, or any combination of these items. IF the signal still appears similar to the original, i.e. its innate quality is not thoroughly destroyed by all of these transformations and noise additions, then depending on the signal to noise properties of the embedded signal, the identification process should function to some objective degree of statistical confidence. The extent of corruption of the suspect signal and the original acceptable perceived noise level are two key parameters in determining an expected confidence level of identification.

The identification process on the suspected signal begins by resampling and aligning the suspected signal onto the digital format and extent of the original signal. Thus, if an image has been reduced by a factor of two, it needs to be digitally enlarged by that same factor. Likewise, if a piece of music has been "cut out," but may still have the same sampling rate as the original, it is necessary to register this cut-out piece to the original, typically done by performing a local digital cross-correlation of the two signals (a common digital operation), finding at what delay value the correlation peaks, then using this found delay value to register the cut piece to a segment of the original.

Once the suspect signal has been sample-spacing matched and registered to the original, the signal levels of the suspect signal should be matched in an rms sense to the signal level of the original. This can be done via a search on the parameters of offset, amplification, and gamma being optimized by using the minimum of the mean squared error between the two signals as a function of the three parameters. We can call the suspect signal normalized and registered at this point, or just normalized for convenience.

The newly matched pair then has the original signal subtracted from the normalized suspect signal to produce a difference signal. The difference signal is then cross-correlated with each of the N individual embedded code signals and the peak cross-correlation value recorded. The first four bit code ('0101') is used as a calibrator both on the mean values of the zero value and the one value, and on further registration of the two signals if a finer signal to noise ratio is desired (i.e., the optimal separation of the 0101 signal will indicate an optimal registration of the two signals and will also indicate the probable existence of the N-bit identification signal being present.)

The resulting peak cross-correlation values will form a noisy series of floating point numbers which can be transformed into 0's and 1's by their proximity to the mean values of 0 and 1 found by the 0101 calibration sequence. If the suspect signal has indeed been derived from the original, the identification number resulting from the above process will match the N-bit identification word of the original, bearing in mind either predicted or unknown "bit error" statistics. Signal-to-noise considerations will determine if there will be some kind of "bit error" in the identification process, leading to a form of X% probability of identification where X might be desired to be 99.9% or whatever. If the suspect copy is indeed not a copy of the original, an essentially random sequence of 0's and 1's will be produced, as well as an apparent lack of separation of the resultant values. This is to say, if the resultant values are plotted on a histogram, the existence of the N-bit identification signal will exhibit strong bi-level characteristics, whereas the non-existence of the code, or the existence of a different code of a different original, will exhibit a type of random gaussian-like distribution. This histogram separation alone should be sufficient for an identification, but it is even stronger proof of identification when an exact binary sequence can be objectively reproduced.

Specific Example

Imagine that we have taken a valuable picture of two heads of state at a cocktail party, pictures which are sure to earn some reasonable fee in the commercial market. We desire to sell this picture and ensure that it is not used in an unauthorized or uncompensated manner. This and the following steps are summarized in Fig. 2.

Assume the picture is transformed into a positive color print. We first scan this into a digitized form via a normal high quality black and white scanner with a typical photometric spectral response curve. (It is possible to get better ultimate signal to noise ratios by scanning in each of the three primary colors of the color image, but this nuance is not central to describing the basic process.)

Let us assume that the scanned image now becomes a 4000 by 4000 pixel monochrome digital image with a grey scale accuracy defined by 12-bit grey values or 4096 allowed levels. We will call this the "original digital image" realizing that this is the same as our "original signal" in the above definitions.

During the scanning process we have arbitrarily set absolute black to correspond to digital value '30'. We estimate that there is a basic 2 Digital Number root mean square noise existing on the original digital image, plus a theoretical noise (known in the industry as "shot noise") of the square root of the brightness value of any given pixel. In formula, we have:

$$\langle \text{RMS Noise}_{n,m} \rangle = \text{sqrt}(4 + (V_{n,m}-30)) \qquad (1)$$

Here, n and m are simple indexing values on rows and columns of the image ranging from 0 to 3999. Sqrt is the square root. V is the DN of a given indexed pixel on the original digital image. The < > brackets around the RMS noise merely indicates that this is an expected average value, where it is clear that each and every pixel will have a random error individually. Thus, for a pixel value having 1200 as a digital number or "brightness value", we find that its expected rms noise value is sqrt(1204) = 34.70, which is quite close to 34.64, the square root of 1200.

We furthermore realize that the square root of the innate brightness value of a pixel is not precisely what the eye perceives as a minimum objectionable noise, thus we come up with the formula:

$$\langle \text{RMS Addable Noise}_{n,m} \rangle = X^{*}\text{sqrt}(4+(V_{n,m}-30)^{\wedge}Y) \quad (2)$$

Where X and Y have been added as empirical parameters which we will adjust, and "addable" noise refers to our acceptable perceived noise level from the definitions above. We now intend to experiment with what exact value of X and Y we can choose, but we will do so at the same time that we are performing the next steps in the process.

The next step in our process is to choose N of our N-bit identification word. We decide that a 16 bit main identification value with its 65536 possible values will be sufficiently large to identify the image as ours, and that we will be directly selling no more than 128 copies of the image which we wish to track, giving 7 bits plus an eighth bit for an odd/even adding of the first 7 bits (i.e. an error checking bit on the first seven). The total bits required now are at 4 bits for the *0101* calibration sequence, 16 for the main identification, 8 for the version, and we now throw in another 4 as a further error checking value on the first 28 bits, giving 32 bits as N. The final 4 bits can use one of many industry standard error checking methods to choose its four values.

We now randomly determine the 16 bit main identification number, finding for example, 1101 0001 1001 1110; our first versions of the original sold will have all 0's as the version identifier, and the error checking bits will fall out where they may. We now have our unique 32 bit identification word which we will embed on the original digital image.

To do this, we generate 32 independent random 4000 by 4000 encoding images for each bit of our 32 bit identification word. The manner of generating these random images is revealing. There are numerous ways to generate these. By far the simplest is to turn up the gain on the same scanner that was used to scan in the original photograph, only this time placing a pure black image as the input, then scanning this 32 times. The only drawback to this technique is that it does require a large amount of memory and that "fixed pattern" noise will be part of each independent "noise image." But, the fixed pattern noise can be removed via normal "dark frame" subtraction techniques. Assume that we set the absolute black average value at digital number '100,' and that rather than finding a 2 DN rms noise as we did in the normal gain setting, we now find an rms noise of 10 DN about each and every pixel's mean value.

We next apply a mid-spatial-frequency bandpass filter (spatial convolution) to each and every independent random image, essentially removing the very high and the very low spatial frequencies from them. We remove the very low frequencies because simple real-world error sources like geometrical warping, splotches on scanners, mis-registrations, and the like will exhibit themselves most at lower frequencies also, and so we want to concentrate our identification signal at higher spatial frequencies in order to avoid these types of corruptions. Likewise, we remove the higher frequencies because multiple generation copies of a given image, as well as compression-decompression transformations, tend to wipe out higher frequencies anyway, so there is no point in placing too much identification signal into these frequencies if they will be the ones most prone to being attenuated. Therefore, our new filtered independent noise images will be dominated by mid-spatial frequencies. On a practical note, since we are using 12-bit values on our scanner and we have removed the DC value effectively and our new rms noise will be slightly less than 10 digital numbers, it is useful to boil this down to a 6-bit value ranging from -32 through 0 to 31 as the resultant random image.

Next we add all of the random images together which have a '1' in their corresponding bit value of the 32-bit identification word, accumulating the result in a 16-bit signed integer image. This is the unattenuated and un-scaled version of the composite embedded signal.

Next we experiment visually with adding the composite embedded signal to the original digital image, through varying the X and Y parameters of equation 2. In formula, we visually iterate to both maximize X and to find the appropriate Y in the following:

$$V_{dist;n,m} = V_{orig;n,m} + V_{comp;n,m}*X*sqrt(4+V_{orig;n,m}\hat{\ }Y) \qquad (3)$$

where dist refers to the candidate distributable image, i.e. we are visually iterating to find what X and Y will give us an acceptable image; orig refers to the pixel value of the original image; and comp refers to the pixel value of the composite image. The n's and m's still index rows and columns of the image and indicate that this operation is done on all 4000 by 4000 pixels. The symbol V is the DN of a given pixel and a given image.

As an arbitrary assumption, now, we assume that our visual experimentation has found that the value of X= 0.025 and Y=0.6 are acceptable values when comparing the original image with the candidate distributable image. This is to say, the distributable image with the "extra noise" is acceptably close to the original in an aesthetic sense. Note that since our individual random images had a random rms noise value around 10 DN, and that adding approximately 16 of these images together will increase the composite noise to around 40 DN, the X multiplication value of 0.025 will bring the added rms noise back to around 1 DN, or half the amplitude of our innate noise on the original. This is roughly a 1 dB gain in noise at the dark pixel values and correspondingly more at the brighter values modified by the Y value of 0.6.

So with these two values of X and Y, we now have constructed our first versions of a distributable copy of the original. Other versions will merely create a new composite signal and possibly change the X slightly if deemed necessary. We now lock up the original digital image along with the 32-bit identification word for each version, and the 32 independent random

4-bit images, waiting for our first case of a suspected piracy of our original. Storage wise, this is about 14 Megabytes for the original image and 32*0.5bytes*16 million = ~256 Megabytes for the random individual encoded images. This is quite acceptable for a single valuable image. Some storage economy can be gained by simple lossless compression.

Finding a Suspected Piracy of our Image

We sell our image and several months later find our two heads of state in the exact poses we sold them in, seemingly cut and lifted out of our image and placed into another stylized background scene. This new "suspect" image is being printed in 100,000 copies of a given magazine issue, let us say. We now go about determining if a portion of our original image has indeed been used in an unauthorized manner. Fig. 3 summarizes the details.

The first step is to take an issue of the magazine, cut out the page with the image on it, then carefully but not too carefully cut out the two figures from the background image using ordinary scissors. If possible, we will cut out only one connected piece rather than the two figures separately. We paste this onto a black background and scan this into a digital form. Next we electronically flag or mask out the black background, which is easy to do by visual inspection.

We now procure the original digital image from our secured place along with the 32-bit identification word and the 32 individual embedded images. We place the original digital image onto our computer screen using standard image manipulation software, and we roughly cut along the same borders as our masked area of the suspect image, masking this image at the same time in roughly the same manner. The word 'roughly' is used since an exact cutting is not needed, it merely aids the identification statistics to get it reasonably close.

Next we rescale the masked suspect image to roughly match the size of our masked original digital image, that is, we digitally scale up or down the suspect image and roughly overlay it on the original image. Once we have performed this rough registration, we then throw the two images into an automated scaling and registration program. The program performs a search on the three parameters of x position, y position, and spatial scale, with the figure of merit being the mean squared error between the two images given any given scale variable and x and y offset. This is a fairly standard image processing methodology. Typically this would be done using generally smooth interpolation techniques and done to sub-pixel accuracy. The search method can be one of many, where the simplex method is a typical one.

Once the optimal scaling and x-y position variables are found, next comes another search on optimizing the black level, brightness gain, and gamma of the two images. Again, the figure of merit to be used is mean squared error, and again the simplex or other search methodologies can be used to optimize the three variables. After these three variables are optimized, we apply their corrections to the suspect image and align it to exactly the pixel spacing and masking of the original digital image and its mask. We can now call this the standard mask.

The next step is to subtract the original digital image from the newly normalized suspect image only within the standard mask region. This new image is called the difference image.

Then we step through all 32 individual random embedded images, doing a local cross-correlation between the masked difference image and the masked individual embedded image. 'Local' refers to the idea that one need only start correlating over an offset region of +/- 1 pixels of offset between the nominal registration points of the two images found during the search procedures above. The peak correlation should be very close to the nominal registration point of 0,0 offset, and we can add the 3 by 3 correlation values together to give one grand correlation value for each of the 32 individual bits of our 32-bit identification word.

After doing this for all 32 bit places and their corresponding random images, we have a quasi-floating point sequence of 32 values. The first four values represent our calibration signal of 0101. We now take the mean of the first and third floating point value and call this floating point value '0,' and we take the mean of the second and the fourth value and call this floating point value '1.' We then step through all remaining 28 bit values and assign either a '0' or a '1' based simply on which mean value they are closer to. Stated simply, if the suspect image is indeed a copy of our original, the embedded 32-bit resulting code should match that of our records, and if it is not a copy, we should get general randomness. The third and the fourth possibilities of 3) Is a copy but doesn't match identification number and 4) isn't a copy but does match are, in the case of 3), possible if the signal to noise ratio of the process has plummeted, i.e. the 'suspect image' is truly a very poor copy of the original, and in the case of 4) is basically one chance in four billion since we were using a 32-bit identification number. If we are truly worried about 4), we can just have a second independent lab perform their own tests on a different issue of the same magazine. Finally, checking the error-check bits against what the values give is one final and possibly overkill check on the whole process. In situations where signal to noise is a possible problem, these error checking bits might be eliminated without too much harm.

Benefits

Now that a full description of the first embodiment has been described via a detailed example, it is appropriate to point out the rationale of some of the process steps and their benefits.

The ultimate benefits of the foregoing process are that obtaining an identification number is fully independent of the manners and methods of preparing the difference image. That is to say, the manners of preparing the difference image, such as cutting, registering, scaling, etcetera, cannot increase the odds of finding an identification number when none exists; it only helps the signal-to-noise ratio of the identification process when a true identification number is present. Methods of preparing images for identification can be different from each other even, providing the possibility for multiple independent methodologies for making a match.

The ability to obtain a match even on sub-sets of the original signal or image is a key point in today's information-rich world. Cutting and pasting both images and sound clips is becoming more common, allowing such an embodiment to be used in detecting a copy even when original material has been thus corrupted. Finally, the signal to noise ratio of matching should begin to become difficult only when the copy material itself has been significantly altered either by noise or by significant distortion; both of these also will affect that copy's commercial value, so that trying to thwart the system can only be done at the expense of a huge decrease in commercial value.

An early conception of this invention was the case where only a single "snowy image" or random signal was added to an original image, i.e. the case where N=1. "Decoding" this signal would involve a subsequent mathematical analysis using (generally statistical) algorithms to make a judgment on the presence or absence of this signal. The reason this approach was abandoned as the preferred embodiment was that there was an inherent gray area in the certainty of detecting the presence or absence of the signal. By moving onward to a multitude of bit planes, i.e. N > 1, combined with simple pre-defined algorithms prescribing the manner of choosing between a "0" and a "1", the invention moved the certainty question from the realm of expert statistical analysis into the realm of guessing a random binary event such as a coin flip. This is seen as a powerful feature relative to the intuitive acceptance of this invention in both the courtroom and the marketplace. The analogy which summarizes the inventor's thoughts on this whole question is as follows: The search for a single identification signal amounts to calling a coin flip only once, and relying on arcane experts to make the call; whereas the N>1 preferred embodiment of this invention relies on the broadly intuitive principle of correctly calling a coin flip N times in a row. This situation is greatly exacerbated, i.e. the problems of "interpretation" of the presence of a single signal, when images and sound clips get smaller and smaller in extent.

Another important reason that the N>1 case is the preferred embodiment over the N=1 embodiment is that in the N=1 case, the manner in which a suspect image is prepared and manipulated has a direct bearing on the likelihood of making a positive identification. Thus, the manner with which an expert makes an identification determination becomes an integral part of that determination. The existence of a multitude of mathematical and statistical approaches to making this determination leave open the possibility that some tests might make positive identifications while others might make negative determinations, inviting further arcane debate about the relative merits of the various identification approaches. The N>1 preferred embodiment of this invention avoids this further gray area by presenting a method where no amount of pre-processing of a signal - other than pre-processing which surreptitiously uses knowledge of the private code signals - can increase the likelihood of "calling the coin flip N times in a row."

The fullest expression of the present system will come when it becomes an industry standard and numerous independent groups set up with their own means or 'in-house' brand of applying embedded identification numbers and in their decipherment. Numerous independent group identification will further enhance the ultimate objectivity of the method, thereby enhancing its appeal as an industry standard.

Use of True Polarity in Creating the Composite Embedded Code Signal

The foregoing discussion made use of the 0 and 1 formalism of binary technology to accomplish its ends. Specifically, the 0's and 1's of the N-bit identification word directly multiplied their corresponding individual embedded code signal to form the composite embedded code signal (step 8, figure 2). This approach certainly has its conceptual simplicity, but the multiplication of an embedded code signal by 0 along with the storage of that embedded code contains a kind of inefficiency.

It is preferred to maintain the formalism of the 0 and 1 nature of the N-bit identification word, but to have the 0's of the word induce a subtraction of their corresponding embedded code signal. Thus, in step 8 of figure 2, rather than only 'adding' the individual embedded code signals which correspond to a '1' in the N-bit identification word, we will also 'subtract' the individual embedded code signals which correspond to a '0' in the N-bit identification word.

At first glance this seems to add more apparent noise to the final composite signal. But it also increases the energy-wise separation of the 0's from the 1's, and thus the 'gain' which is applied in step 10, figure 2 can be correspondingly lower.

We can refer to this improvement as the use of true polarity. The main advantage of this improvement can largely be summarized as 'informational efficiency.'

'Perceptual Orthogonality' of the Individual Embedded Code Signals

The foregoing discussion contemplates the use of generally random noise-like signals as the individual embedded code signals. This is perhaps the simplest form of signal to generate. However, there is a form of informational optimization which can be applied to the set of the individual embedded signals, which the applicant describes under the rubric 'perceptual orthogonality.' This term is loosely based on the mathematical concept of the orthogonality of vectors, with the current additional requirement that this orthogonality should maximize the signal energy of the identification information while maintaining it below some perceptibility threshold. Put another way, the embedded code signals need not necessarily be random in nature.

Use and Improvements of the First Embodiment in the Field of Emulsion-Based Photography

The foregoing discussion outlined techniques that are applicable to photographic materials. The following section explores the details of this area further and discloses certain improvements which lend themselves to a broad range of applications.

The first area to be discussed involves the pre-application or pre-exposing of a serial number onto traditional photographic products, such as negative film, print paper, transparencies, etc. In general, this is a way to embed *a priori* unique serial numbers (and by implication, ownership and tracking information) into photographic material. The serial numbers themselves would be a permanent part of the normally exposed picture, as opposed to being relegated to the margins or stamped on the back of a printed photograph, which all require separate locations and separate methods of copying. The 'serial number' as it is called here is generally synonymous with the N-bit identification word, only now we are using a more common industrial terminology.

In Figure 2, step 11, the disclosure calls for the storage of the "original [image]" along with code images. Then in figure 3, step 9, it directs that the original be subtracted from the suspect image, thereby leaving the possible identification codes plus whatever noise and corruption has accumulated. Therefore, the previous disclosure made the tacit assumption that there exists an original without the composite embedded signals.

Now in the case of selling print paper and other duplication film products, this will still be the case, i.e., an "original" without the embedded codes will indeed exist and the basic methodology of the first embodiment can be employed. The original film serves perfectly well as an 'unencoded original.'

However, in the case where pre-exposed negative film is used, the composite embedded signal pre-exists on the original film and thus there will never be an "original" separate from the pre-embedded signal. It is this latter case, therefore, which will be examined a bit more closely, along with observations on how to best use the principles discussed above (the former cases adhering to the previously outlined methods).

The clearest point of departure for the case of pre-numbered negative film, i.e. negative film which has had each and every frame pre-exposed with a very faint and unique composite embedded signal, comes at step 9 of figure 3 as previously noted. There are certainly other differences as well, but they are mostly logistical in nature, such as how and when to embed the signals on the film, how to store the code numbers and serial number, etc. Obviously the pre-exposing of film would involve a major change to the general mass production process of creating and packaging film.

Fig. 4 has a schematic outlining one potential post-hoc mechanism for pre-exposing film. 'Post-hoc' refers to applying a process after the full common manufacturing process of film has already taken place. Eventually, economies of scale may dictate placing this pre-exposing process directly into the chain of manufacturing film. Depicted in Fig. 4 is what is commonly known as a film writing system. The computer, 106, displays the composite signal produced in step 8, figure 2, on its phosphor screen. A given frame of film is then exposed by imaging this phosphor screen, where the exposure level is generally very faint, i.e. generally imperceptible. Clearly, the marketplace will set its own demands on how faint this should be, that is, the level of added 'graininess' as practitioners would put it. Each frame of film is sequentially exposed, where in general the composite image displayed on the CRT 102 is changed for each and every frame, thereby giving each frame of film a different serial number. The transfer lens 104 highlights the focal conjugate planes of a film frame and the CRT face.

Getting back to the applying the principles of the foregoing embodiment in the case of pre-exposed negative film... At step 9, figure 3, if we were to subtract the "original" with its embedded code, we would obviously be "erasing" the code as well since the code is an integral part of the original. Fortunately, remedies do exist and identifications can still be made. However, it will be a challenge to artisans who refine this embodiment to have the signal to noise ratio of the identification process in the pre-exposed negative case approach the signal to noise ratio of the case where the un-encoded original exists.

A succinct definition of the problem is in order at this point. Given a suspect picture (signal), find the embedded identification code IF a code exists at al. The problem reduces to one of finding the amplitude of each and every individual embedded code signal within the suspect picture, not only within the context of noise and corruption as was previously explained, but now also within the context of the coupling between a captured image and the codes. 'Coupling' here refers to the idea that the captured image "randomly biases" the cross-correlation.

So, bearing in mind this additional item of signal coupling, the identification process now estimates the signal amplitude of each and every individual embedded code signal (as opposed to taking the cross-correlation result of step 12, figure 3). If our identification signal exists in the suspect picture, the amplitudes thus found will split into a polarity with positive amplitudes being assigned a '1' and negative amplitudes being assigned a '0'. Our unique identification code manifests itself. If, on the other hand, no such identification code exists or it is someone else's code, then a random gaussian-like distribution of amplitudes is found with a random hash of values.

It remains to provide a few more details on <u>how</u> the amplitudes of the individual embedded codes are found. Again, fortunately, this exact problem has been treated in other technological applications. Besides, throw this problem and a little food into a crowded room of mathematicians and statisticians and surely a half dozen optimized methodologies will pop out after some reasonable period of time. It is a rather cleanly defined problem.

One specific example solution comes from the field of astronomical imaging. Here, it is a mature prior art to subtract out a "thermal noise frame" from a given CCD image of an object. Often, however, it is not precisely known what scaling factor to use in subtracting the thermal frame, and a search for the correct scaling factor is performed. This is precisely the task of this step of the present embodiment.

General practice merely performs a common search algorithm on the scaling factor, where a scaling factor is chosen and a new image is created according to:

$$\text{NEW IMAGE} = \text{ACQUIRED IMAGE} - \text{SCALE} * \text{THERMAL IMAGE} \qquad (4)$$

The new image is applied to the fast fourier transform routine and a scale factor is eventually found which minimizes the integrated high frequency content of the new image. This general type of search operation with its minimization of a particular quantity is exceedingly common. The scale factor thus found is the sought-for "amplitude." Refinements which are contemplated but not yet implemented are where the coupling of the higher derivatives of the acquired image and the embedded codes are estimated and removed from the calculated scale factor. In other words, certain bias effects from the coupling mentioned earlier are present and should be eventually accounted for and removed both through theoretical and empirical experimentation.

Use and Improvements in the Detection of Signal or Image Alteration

Apart from the basic need of identifying a signal or image as a whole, there is also a rather ubiquitous need to detect possible alterations to a signal or image. The following section describes how the foregoing embodiment, with certain modifications and improvements, can be used as a powerful tool in this area. The potential scenarios and applications of detecting alterations are innumerable.

To first summarize, assume that we have a given signal or image which has been positively identified using the basic methods outlined above. In other words, we know its N-bit identification word, its individual embedded code signals, and its composite embedded code. We can then fairly simply create a spatial map of the composite code's amplitude within our given signal or image. Furthermore, we can divide this amplitude map by the known composite code's spatial amplitude, giving a normalized map, i.e. a map which should fluctuate about some global mean value. By simple examination of this map, we can visually detect any areas which have been significantly altered wherein the value of the normalized amplitude dips below some statistically set threshold based purely on typical noise and corruption (error).

The details of implementing the creation of the amplitude map have a variety of choices. One is to perform the same procedure which is used to determine the signal amplitude as described above, only now we step and repeat the multiplication of any given area of the signal/image with a gaussian weight function centered about the area we are investigating.

Universal Versus Custom Codes

The disclosure thus far has outlined how each and every source signal has its own unique set of individual embedded code signals. This entails the storage of a significant amount of additional code information above and beyond the original, and many applications may merit some form of economizing.

One such approach to economizing is to have a given set of individual embedded code signals be common to a batch of source materials. For example, one thousand images can all utilize the same basic set of individual embedded code signals. The storage requirements of these codes then become a small fraction of the overall storage requirements of the source material.

Furthermore, some applications can utilize a universal set of individual embedded code signals, i.e., codes which remain the same for all instances of distributed material. This type of requirement would be seen by systems which wish to hide the N-bit identification word itself, yet have standardized equipment be able to read that word. This can be used in systems which make go/no go decisions at point-of-read locations. The potential drawback to this set-up is that the universal codes are more prone to be sleuthed or stolen; therefore they will not be as secure as the apparatus and methodology of the previously disclosed arrangement. Perhaps this is just the difference between 'high security' and 'air-tight security,' a distinction carrying little weight with the bulk of potential applications.

Use in Printing, Paper, Documents, Plastic Coated Identification Cards, and Other Material Where Global Embedded Codes Can Be Imprinted

The term 'signal' is often used narrowly to refer to digital data information, audio signals, images, etc. A broader interpretation of 'signal,' and the one more generally intended, includes any form of modulation of any material whatsoever. Thus, the micro-topology of a piece of common paper becomes a 'signal' (e.g. it height as a function of x-y coordinates). The reflective properties of a flat piece of plastic (as a function of space also) becomes a signal. The point is that photographic emulsions, audio signals, and digitized information are not the only types of signals capable of utilizing the principles of the present invention.

As a case in point, a machine very much resembling a braille printing machine can be designed so as to imprint unique 'noise-like' indentations as outlined above. These indentations can be applied with a pressure which is much smaller than is typically applied in creating braille, to the point where the patterns are not noticed by a normal user of the paper. But by following the steps of the present disclosure and applying them via the mechanism of micro-indentations, a unique identification code can be placed onto any given sheet of paper, be it intended for everyday stationary purposes, or be it for important documents, legal tender, or other secured material.

The reading of the identification material in such an embodiment generally proceeds by merely reading the document optically at a variety of angles. This would become an inexpensive method for deducing the micro-topology of the paper surface. Certainly other forms of reading the topology of the paper are possible as well.

In the case of plastic encased material such as identification cards, e.g. driver's licenses, a similar braille-like impressions machine can be utilized to imprint unique identification codes. Subtle layers of photoreactive materials can also be embedded inside the plastic and 'exposed.'

It is clear that wherever a material exists which is capable of being modulated by 'noise-like' signals, that material is an appropriate carrier for unique identification codes and utilization of the principles of the invention. All that remains is the matter of economically applying the identification information and maintaining the signal level below an acceptability threshold which each and every application will define for itself.

Appendix A Description

Appendix A contains the source code of an implementation and verification of the foregoing embodiment for an 8-bit black and white imaging system.

REAL TIME ENCODER

While the first class of embodiments most commonly employs a standard microprocessor or computer to perform the encodation of an image or signal, it is possible to utilize a custom encodation device which may be faster than a typical Von Neuman-type processor. Such a system can be utilized with all manner of serial data streams.

Music and videotape recordings are examples of serial data streams -- data streams which are often pirated. It would assist enforcement efforts if authorized recordings were encoded with identification data so that pirated knock-offs could be traced to the original from which they were made.

Piracy is but one concern driving the need for the present invention. Another is authentication. Often it is important to confirm that a given set of data is really what it is purported to be (often several years after its generation).

To address these and other needs, the system 200 of Fig. 5 can be employed. System 200 can be thought of as an identification coding black box 202. The system 200 receives an input signal (sometimes termed the "master" or "unencoded" signal) and a code word, and produces (generally in real time) an identification-coded output signal. (Usually, the system provides key data for use in later decoding.)

The contents of the "black box" 202 can take various forms. An exemplary black box system is shown in Fig. 6 and includes a look-up table 204, a digital noise source 206, first and second scalers 208, 210, an adder/subtracter 212, a memory 214, and a register 216.

The input signal (which in the illustrated embodiment is an 8 - 20 bit data signal provided at a rate of one million samples per second, but which in other embodiments could be an analog signal if appropriate A/D and D/A conversion is provided) is applied from an input 218 to the address input 220 of the look-up table 204. For each input sample (i.e. look-up table address), the table provides a corresponding 8-bit digital output word. This output word is used as a scaling factor that is applied to one input of the first scaler 208.

The first scaler 208 has a second input, to which is applied an 8-bit digital noise signal from source 206. (In the illustrated embodiment, the noise source 206 comprises an analog noise source 222 and an analog-to-digital converter 224 although, again, other implementations can be used.) The noise source in the illustrated embodiment has a zero mean output value, with a full width half maximum (FWHM) of 50 - 100 digital numbers (e.g. from -75 to +75).

The first scaler 208 multiplies the two 8-bit words at its inputs (scale factor and noise) to produce -- for each sample of the system input signal -- a 16-bit output word. Since the noise signal has a zero mean value, the output of the first scaler likewise has a zero mean value.

The output of the first scaler 208 is applied to the input of the second scaler 210. The second scaler serves a global scaling function, establishing the absolute magnitude of the identification signal that will ultimately be embedded into the input data signal. The scaling factor is set through a scale control device 226 (which may take a number of forms, from a simple rheostat to a graphically implemented control in a graphical user interface), permitting this factor to be changed in accordance with the requirements of different applications. The second scaler 210 provides on its output line 228 a scaled noise signal. Each sample of this scaled noise signal is successively stored in the memory 214.

(In the illustrated embodiment, the output from the first scaler 208 may range between -1500 and +1500 (decimal), while the output from the second scaler 210 is in the low single digits, (such as between -2 and +2).)

Register 216 stores a multi-bit identification code word. In the illustrated embodiment this code word consists of 8 bits, although larger code words (up to hundreds of bits) are commonly used. These bits are referenced, one at a time, to control how the input signal is modulated with the scaled noise signal.

In particular, a pointer 230 is cycled sequentially through the bit positions of the code word in register 216 to provide a control bit of "0" or "1" to a control input 232 of the adder/subtracter 212. If, for a particular input signal sample, the control bit is a "1", the scaled noise signal sample on line 232 is added to the input signal sample. If the control bit is a "0", the scaled noise signal sample is subtracted from the input signal sample. The output 234 from the adder/subtracter 212 provides the black box's output signal.

The addition or subtraction of the scaled noise signal in accordance with the bits of the code word effects a modulation of the input signal that is generally imperceptible. However, with knowledge of the contents of the memory 214, a user can later decode the encoding, determining the code number used in the original encoding process. (Actually, use of memory 214 is optional, as explained below.)

It will be recognized that the encoded signal can be distributed in well known ways, including converted to printed image form, stored on magnetic media (floppy diskette, analog or DAT tape, etc.), CD-ROM, etc. etc.

Decoding

A variety of techniques can be used to determine the identification code with which a suspect signal has been encoded. Two are discussed below. The first is less preferable than the latter for most applications, but is discussed herein so that the reader may have a fuller context within which to understand the invention.

More particularly, the first decoding method is a difference method, relying on subtraction of corresponding samples of the original signal from the suspect signal to obtain difference samples, which are then examined (typically individually) for deterministic coding indicia (i.e. the stored noise data). This approach may thus be termed a "sample-based, deterministic" decoding technique.

The second decoding method does not make use of the original signal. Nor does it examine particular samples looking for predetermined noise characteristics. Rather, the statistics of the suspect signal (or a portion thereof) are considered in the aggregate and analyzed to discern the presence of identification coding that permeates the entire signal. The reference to permeation means the entire identification code can be discerned from a small fragment of the suspect signal. This latter approach may thus be termed a "holographic, statistical" decoding technique.

Both of these methods begin by registering the suspect signal to match the original. This entails scaling (e.g. in amplitude, duration, color balance, etc.), and sampling (or resampling) to restore the original sample rate. As in the earlier described embodiment, there are a variety of well understood techniques by which the operations associated with this registration function can be performed.

As noted, the first decoding approach proceeds by subtracting the original signal from the registered, suspect signal, leaving a difference signal. The polarity of successive difference signal samples can then be compared with the polarities of the corresponding stored noise signal samples to determine the identification code. That is, if the polarity of the first difference signal sample matches that of the first noise signal sample, then the first bit of the identification code is a "1." (In such case, the polarity of the 9th, 17th, 25th, etc. samples should also all be positive.) If the polarity of the first difference signal sample is opposite that of the corresponding noise signal sample, then the first bit of the identification code is a "0."

By conducting the foregoing analysis with eight successive samples of the difference signal, the sequence of bits that comprise the original code word can be determined. If, as in the preferred embodiment, pointer 230 stepped through the code word one bit at a time, beginning with the first bit, during encoding, then the first 8 samples of the difference signal can be analyzed to uniquely determine the value of the 8-bit code word.

In a noise-free world (speaking here of noise independent of that with which the identification coding is effected), the foregoing analysis would always yield the correct identification code. But a process that is only applicable in a noise-free world is of limited utility indeed.

(Further, accurate identification of signals in noise-free contexts can be handled in a variety of other, simpler ways: e.g. checksums; statistically improbable correspondence between suspect and original signals; etc.)

While noise-induced aberrations in decoding can be dealt with -- to some degree -- by analyzing large portions of the signal, such aberrations still place a practical ceiling on the confidence of the process. Further, the villain that must be confronted is not always as benign as random noise. Rather, it increasingly takes the form of human-caused corruption, distortion, manipulation, etc. In such cases, the desired degree of identification confidence can only be achieved by other approaches.

The presently preferred approach (the "holographic, statistical" decoding technique) relies on recombining the suspect signal with certain noise data (typically the data stored in memory 214), and analyzing the entropy of the resulting signal. "Entropy" need not be understood in its most strict mathematical definition, it being merely the most concise word to describe randomness (noise, smoothness, snowiness, etc.).

Most serial data signals are not random. That is, one sample usually correlates -- to some degree -- with the adjacent samples. Noise, in contrast, typically is random. If a random signal (e.g. noise) is added to (or subtracted from) a non-random signal, the entropy of the resulting signal generally increases. That is, the resulting signal has more random variations than the original signal. This is the case with the encoded output signal produced by the present encoding process; *it has more entropy than the original*, unencoded signal.

If, in contrast, the addition of a random signal to (or subtraction from) a non-random signal reduces entropy, then something unusual is happening. It is this anomaly that the preferred decoding process uses to detect embedded identification coding.

To fully understand this entropy-based decoding method, it is first helpful to highlight a characteristic of the original encoding process: the similar treatment of every eighth sample.

In the encoding process discussed above, the pointer 230 increments through the code word, one bit for each successive sample of the input signal. If the code word is eight bits in length, then the pointer returns to the same bit position in the code word every eighth signal sample. If this bit is a "1", noise is added to the input signal; if this bit is a "0", noise is subtracted from the input signal. Due to the cyclic progression of the pointer 230, every eighth sample of an encoded signal thus shares a characteristic: they are all either augmented by the corresponding noise data (which may be negative), or they are all diminished, depending on whether the bit *of the code word* then being *addressed* by pointer 230 is a "1" or a "0".

To exploit this characteristic, the entropy-based decoding process treats every eighth sample of the suspect signal in like fashion. In particular, the process begins by adding to the 1st, 9th, 17th, 25th, etc. samples of the suspect signal the corresponding scaled noise signal values stored in the memory 214 (i.e. those stored in the 1st, 9th, 17th, 25th, etc., memory locations, respectively). The entropy of the resulting signal (i.e. the suspect signal with every 8th sample modified) is then computed.

(Computation of a signal's entropy or randomness is well understood by artisans in this field. One generally accepted technique is to take the derivative of the signal at each sample point, square these values, and then sum over the entire signal. However, a variety of other well known techniques can alternatively be used.)

The foregoing step is then repeated, this time subtracting the stored noise values from the 1st, 9th, 17th, 25 etc. suspect signal samples.

One of these two operations will undo the encoding process and reduce the *resulting signal's* entropy; *the other* will *aggravate it. If* adding the noise data in memory 214 to the suspect signal reduces its entropy, then this data must earlier have been subtracted from the original signal. This indicates that pointer 230 was pointing to a "0" bit when these samples were encoded. (A "0" at the control input of adder/subtracter 212 caused it to subtract the scaled noise from the input signal.)

Conversely, if subtracting the noise data from every eighth sample of the suspect signal reduces its entropy, then the encoding process must have earlier added this noise. This indicates that pointer 230 was pointing to a "1" bit when samples 1, 9, 17, 25, etc., were encoded.

By noting whether entropy decreases by (a) adding or (b) subtracting the stored noise data to/from the suspect signal, it can be determined that the first bit of the code word is (a) a "0", or (b) a "1".

The foregoing operations are then conducted for the group of spaced samples of the suspect signal beginning with the second sample (i.e. 2, 10, 18, 26 ...). The entropy of the resulting signals indicate whether the second bit of the code word is a "0" or a "1". Likewise with the following 6 groups of spaced samples in the suspect signal, until all 8 bits of the code word have been discerned.

It will be appreciated that the foregoing approach is not sensitive to corruption mechanisms that alter the values of individual samples; instead, the process considers the entropy of the signal as a whole, yielding a high degree of confidence in the results. Further, even small excerpts of the signal can be analyzed in this manner, permitting piracy of even small details of an original work to be detected. The results are thus statistically robust, both in the face of natural and human corruption of the suspect signal.

It will further be appreciated that the use of an N-bit code word in this real time embodiment provides benefits analogous to those discussed above in connection with the batch encoding system. (Indeed, the present embodiment may be conceptualized as making use of N different noise signals, just as in the batch encoding system. The first noise signal is a signal having the same extent as the input signal, and comprising the scaled noise signal at the 1st, 9th, 17th, 25th, etc., samples (assuming N=8), with zeroes at the intervening samples. The second noise signal is a similar one comprising the scaled noise signal at the 2d, 10th, 18th, 26th, etc., samples, with zeroes at the intervening samples. Etc. These signals are all combined to provide a composite noise signal.) One of the important advantages inherent in such a system is the high degree of statistical confidence (confidence which doubles with each successive bit of the identification code) that a match is really a match. The system does not rely on subjective evaluation of a suspect signal for a single, deterministic embedded code signal.

Illustrative Variations

From the foregoing description, it will be recognized that numerous modifications can be made to the illustrated systems without changing the fundamental principles. A few of these variations are described below.

The above-described decoding process tries both adding and subtracting stored noise data to/from the suspect signal in order to find which operation reduces entropy. In other embodiments, only one of these operations needs to be conducted. For example, in one alternative decoding process the stored noise data corresponding to every eighth sample of the suspect signal is only added to said samples. If the entropy of the resulting signal is thereby increased, then the corresponding bit of the code word is a "1" (i.e. this noise was added earlier, during the encoding process, so adding it again only compounds the signal's randomness). If the entropy of the resulting signal is thereby decreased, then the corresponding bit of the code word is a "0". A further test of entropy if the stored noise samples are subtracted is not required.

The statistical reliability of the identification process (coding and decoding) can be designed to exceed virtually any confidence threshold (e.g. 99.9%, 99.99%, 99.999%, etc. confidence) by appropriate selection of the global scaling factors, etc. Additional confidence in any given application (unnecessary in most applications) can be achieved by rechecking the decoding process.

One way to recheck the decoding process is to remove the stored noise data from the suspect signal in accordance with the bits of the discerned code word, yielding a "restored" signal (e.g. if the first bit of the code word is found to be "1," then the noise samples stored in the 1st, 9th, 17th, etc. locations of the memory 214 are subtracted from the corresponding samples of the suspect signal). The entropy of the restored signal is measured and used as a baseline in further measurements. Next, the process is repeated, this time removing the stored noise data from the suspect signal in accordance with a modified code word. The modified code word is the same as the discerned code word, except 1 bit is toggled (e.g. the first). The entropy of the resulting signal is determined, and compared with the baseline. If the toggling of the bit in the discerned code word resulted in increased entropy, then the accuracy of that bit of the discerned code word is confirmed. The process repeats, each time with a different bit of the discerned code word toggled, until all bits of the code word have been so checked. Each change should result in an increase in entropy compared to the baseline value.

The data stored in memory 214 is subject to a variety of alternatives. In the foregoing discussion, memory 214 contains the scaled noise data. In other embodiments, the unscaled noise data can be stored instead.

In still other embodiments, it can be desirable to store at least part of the input signal itself in memory 214. For example, the memory can allocate 8 signed bits to the noise sample, and 16 bits to store the most significant bits of an 18- or 20-bit audio signal sample. This has several benefits. One is that it simplifies registration of a "suspect" signal. Another is that, in the case of encoding an input signal which was already encoded, the data in memory 214 can be used to discern which of the encoding processes was performed first. That is, from the input signal data in memory 214 (albeit incomplete), it is generally possible to determine with which of two code words it has been encoded.

Yet another alternative for memory 214 is that is can be omitted altogether.

One way this can be achieved is to use a deterministic noise source in the encoding process, such as an algorithmic noise generator seeded with a known key number. The same deterministic noise source, seeded with the same key number, can be used in the decoding process. In such an arrangement, only the key number needs be stored for later use in decoding, instead of the large data set usually stored in memory 214.

Alternatively, if the noise signal added during encoding does not have a zero mean value, and the length N of the code word is known to the decoder, then a universal decoding process can be implemented. This process uses the same entropy test as the foregoing procedures, but cycles through possible code words, adding/subtracting a small dummy noise value (e.g. less than the expected mean noise value) to every Nth sample of the suspect signal, in accordance with the bits of the code word being tested, until a reduction in entropy is noted. Such an approach is not favored for most applications, however, because it offers less security than the other embodiments (e.g. it is subject to cracking by brute force).

Many applications are well served by the embodiment illustrated in Fig. 7, in which different code words are used to produce several differently encoded versions of an input signal, each making use of the same noise data. More particularly, the embodiment 240 of Fig. 7 includes a noise store 242 into which noise from source 206 is written during the identification-coding of the input signal with a first code word. (The noise source of Fig. 7 is shown outside of the real time encoder 202 for convenience of illustration.) Thereafter, additional identification-coded versions of the input signal can be produced by reading the stored noise data from the store and using it in conjunction with second through Nth code words to encode the signal. (While binary-sequential code words are illustrated in Fig. 7, in other embodiments arbitrary sequences of code words can be employed.) With such an arrangement, a great number of differently-encoded signals can be produced, without requiring a proportionally-sized long term noise memory. Instead, a fixed amount of noise data is stored, whether encoding an original once or a thousand times.

(If desired, several differently-coded output signals can be produced at the same time, rather than seriatim. One such implementation includes a plurality of adder/subtracter circuits 212, each driven with the same input signal and with the same scaled noise signal, but with different code words. Each, then, produces a differently encoded output signal.)

In applications having a great number of differently-encoded versions of the same original, it will be recognized that the decoding process need not always discern every bit of the code word. Sometimes, for example, the application may require identifying only a group of codes to which the suspect signal belongs. (E.g., high order bits of the code word might indicate an organization to which several differently coded versions of the same source material were provided, with low-order bits identifying specific copies. To identify the organization with which a suspect signal is associated, it may not be necessary to examine the low order bits, since the organization can be identified by the high order bits alone.) If the identification requirements can be met by discerning a subset of the code word bits in the suspect signal, the decoding process can be shortened.

Some applications may be best served by restarting the encoding process -- sometimes with a different code word -- several times within an integral work. Consider, as an example, videotaped productions (e.g. television programming). Each frame of a videotaped production can be identification-coded with a unique code number, processed in real-time with an arrangement 248 like that shown in Fig. 8. Each time a vertical retrace is detected by sync detector 250, the noise source 206 resets (e.g. to repeat the sequence just produced) and an identification code increments to the next value. Each frame of the videotape is thereby uniquely identification-coded. Typically, the encoded signal is stored on a videotape for long term storage (although other storage media, including laser disks, can be used).

Returning to the encoding apparatus, the look-up table 204 in the illustrated embodiment exploits the fact that high amplitude samples of the input data signal can tolerate (without objectionable degradation of the output signal) a higher level of encoded identification coding than can low amplitude input samples. Thus, for example, input data samples having decimal values of 0, 1 or 2 may be correspond (in the look-up table 204) to scale factors of unity (or even zero), whereas input data samples having values in excess of 200 may correspond to scale factors of 15. Generally speaking, the scale factors and the input sample values correspond by a square root relation. That is, a four-fold increase in a value of the sampled input signal corresponds to approximately a two-fold increase in a value of the scaling factor associated therewith.

(The parenthetical reference to zero as a scaling factor alludes to cases, e.g., in which the source signal is temporally or spatially devoid of information content. In an image, for example, a region characterized by several contiguous sample values of zero may correspond to a jet black region of the frame. A scaling value of zero may be appropriate here since there is essentially no image data to be pirated.)

Continuing with the encoding process, those skilled in the art will recognized the potential for "rail errors" in the illustrated embodiment. For example, if the input signal consists of 8-bit samples, and the samples span the entire range from 0 to 255 (decimal), then the addition or subtraction of scaled noise to/from the input signal may produce output signals that cannot be represented by 8 bits (e.g. -2, or 257). A number of well-understood techniques exist to rectify this situation, some of them proactive and some of them reactive. (Among these known techniques are: specifying that the input signal shall not have samples in the range of 0-4 or 251-255, thereby safely permitting modulation by the noise signal; or including provision for detecting and adaptively modifying input signal samples that would otherwise cause rail errors.)

While the illustrated embodiment describes stepping through the code word sequentially, one bit at a time, to control modulation of successive bits of the input signal, it will be appreciated that the bits of the code word can be used other than sequentially for this purpose. Indeed, bits of the code word can be selected in accordance with any predetermined algorithm.

The dynamic scaling of the noise signal based on the instantaneous value of the input signal is an optimization that can be omitted in many embodiments. That is, the look-up table 204 and the first scaler 208 can be omitted entirely, and the signal from the digital noise source 206 applied directly (or through the second, global scaler 210) to the adder/subtracter 212.

It will be further recognized that the use of a zero-mean noise source simplifies the illustrated embodiment, but is not necessary to the invention. A noise signal with another mean value can readily be used, and D.C. compensation (if needed) can be effected elsewhere in the system.

The use of a noise source 206 is also optional. A variety of other signal sources can be used, depending on application- dependent constraints (e.g. the threshold at which the encoded identification signal becomes perceptible). In many instances, the level of the embedded identification signal is low enough that the identification signal needn't have a random aspect; it is imperceptible regardless of its nature. A pseudo random source 206, however, is usually desired because it provides the greatest identification code signal S/N ratio (a somewhat awkward term in this instance) for a level of imperceptibility of the embedded identification signal.

It will be recognized that identification coding need not occur after a signal has been reduced to stored form as data (i.e. "fixed in tangible form," in the words of the U.S. Copyright Act). Consider, for example, the case of popular musicians whose performance are often recorded illicitly. By identification coding the audio before it drives concert hall speakers, unauthorized recordings of the concert can be traced to a particular place and time. Likewise, live audio sources such as 911 emergency calls can be encoded prior to recording so as to facilitate their later authentication.

While the black box embodiment has been described as a stand alone unit, it will be recognized that it can be integrated into a number of different tools/instruments as a component. One is a scanner, which can embed identification codes in the scanned output data. (The codes can simply serve to memorialize that the data was generated by a particular scanner). Another is in creativity software, such as popular drawing/graphics/animation/paint programs offered by Adobe, Macromedia, Corel, and the like.

Finally, while the real-time encoder 202 has been illustrated with reference to a particular hardware implementation, it will be recognized that a variety of other implementations can alternatively be employed. Some utilize other hardware configurations. Others make use of software routines for some or all of the illustrated functional blocks. (The software routines can be executed on any number of different general purpose programmable computers, such as 80x86 PC-compatible computers, RISC-based workstations, etc.)

<u>TYPES OF NOISE, QUASI-NOISE, AND OPTIMIZED-NOISE</u>

Heretofore this disclosure postulated Gaussian noise, "white noise," and noise generated directly from application instrumentation as a few of the many examples of the kind of carrier signal appropriate to carry a single bit of information throughout an image or signal. It is possible to be even more proactive in "designing" characteristics of noise in order to achieve certain goals. The "design" of using Gaussian or instrumental noise was aimed somewhat toward "absolute" security. This section of the disclosure takes a look at other considerations for the design of the noise signals which may be considered the ultimate carriers of the identification information.

For some applications it might be advantageous to design the noise carrier signal (e.g. the Nth embedded code signal in the first embodiment; the scaled noise data in the second embodiment), so as to provide more absolute signal strength to the identification signal relative to the perceptibility of that signal. One example is the following. It is recognized that a true Gaussian noise signal has the value '0' occur most frequently, followed by 1 and -1 at equal probabilities to each other but lower than '0', 2 and -2 next, and so on. Clearly, the value zero carries no information as it is used in the service of this invention. Thus, one simple adjustment, or design, would be that any time a zero occurs in the generation of the embedded code signal, a new process takes over, whereby the value is converted "randomly" to either a 1 or a -1. In logical terms, a decision would be made: if '0', then random(1,-1). The histogram of such a process would appear as a Gaussian/Poissonian type distribution, except that the 0 bin would be empty and the 1 and -1 bin would be increased by half the usual histogram value of the 0 bin.

In this case, identification signal energy would always be applied at all parts of the signal. A few of the trade-offs include: there is a (probably negligible) lowering of security of the codes in that a "deterministic component" is a part of generating the noise signal. The reason this might be completely negligible is that we still wind up with a coin flip type situation on randomly choosing the 1 or the -1. Another trade-off is that this type of designed noise will have a higher threshold of perceptibility, and will only be applicable to applications where the least significant bit of a data stream or image is already negligible relative to the commercial value of the material, i.e. if the least significant bit were stripped from the signal (for all signal samples), no one would know the difference and the value of the material would not suffer. This blocking of the zero value in the example above is but one of many ways to "optimize" the noise properties of the signal carrier, as anyone in the art can realize. We refer to this also as "quasi-noise" in the sense that natural noise can be transformed in a pre-determined way into signals which for all intents and purposes will read as noise. Also, cryptographic methods and algorithms can easily, and often by definition, create signals which are perceived as completely random. Thus the word "noise" can have different connotations, primarily between that as defined subjectively by an observer or listener, and that defined mathematically. The difference of the latter is that mathematical noise has different properties of security and the simplicity with which it can either be "sleuthed" or the simplicity with which instruments can "automatically recognize" the existence of this noise.

"Universal" Embedded Codes

The bulk of this disclosure teaches that for absolute security, the noise-like embedded code signals which carry the bits of information of the identification signal should be unique to each and every encoded signal, or, slightly less restrictive, that embedded code signals should be generated sparingly, such as using the same embedded codes for a batch of 1000 pieces of film, for example. Be this as it may, there is a whole other approach to this *issue* wherein the use of what we will call "universal" embedded code signals can open up large new applications for this technology. The economics of these uses would be such that the de facto lowered security of these universal codes (e.g. they would be analyzable by time honored cryptographic decoding methods, and thus potentially thwarted or reversed) would be economically negligible relative to the economic gains that the intended uses would provide. Piracy and illegitimate uses would become merely a predictable "cost" and a source of uncollected revenue only; a simple line item in an economic analysis of the whole. A good analogy of this is in the cable industry and the scrambling of video signals. Everybody seems to know that crafty, skilled technical individuals, who may be generally law abiding citizens, can climb a ladder and flip a few wires in their cable junction box in order to get all the pay channels for free. The cable industry knows this and takes active measures to stop it and prosecute those caught, but the "lost revenue" derived from this practice remains prevalent but almost negligible as a percentage of profits gained from the scrambling system as a whole. The scrambling system as a whole is an economic success despite its lack of "absolute security."

The same holds true for applications of this technology wherein, for the price of lowering security by some amount, large economic opportunity presents itself. This section first describes what is meant by universal codes, then moves on to some of the interesting uses to which these codes can be applied.

Universal embedded codes generally refer to the idea that knowledge of the exact codes can be distributed. The embedded codes won't be put into a dark safe never to be touched until litigation arises (as alluded to in other parts of this disclosure), but instead will be distributed to various locations where on-the-spot analysis can take place. Generally this distribution will still take place within a security controlled environment, meaning that steps will be taken to limit the knowledge of the codes to those with a need to know. Instrumentation which attempts to automatically detect copyrighted material is a non-human example of "something" with a need to know the codes.

There are many ways to implement the idea of universal codes, each with their own merits regarding any given application. For the purposes of teaching this art, we separate these approaches into three broad categories: universal codes based on libraries, universal codes based on deterministic formula, and universal codes based on pre-defined industry standard patterns. A rough rule of thumb is that the first is more secure than the latter two, but that the latter two are possibly more economical to implement than the first.

<u>Universal Codes: 1) Libraries of Universal Codes</u>

The use of libraries of universal codes simply means that the techniques of this invention are employed as described, except for the fact that only a limited set of the individual embedded code signals are generated and that any given encoded material will make use of some sub-set of this limited "universal set." An example is in order here. A photographic print paper manufacturer may wish to pre-expose every piece of 8 by 10 inch print paper which they sell with a unique identification code. They also wish to sell identification code recognition software to their large customers, service bureaus, stock agencies, and individual photographers, so that all these people can not only verify that their own material is correctly marked, but so that they can also determine if third party material which they are about to acquire has been identified by this technology as being copyrighted. This latter information will help them verify copyright holders and avoid litigation, among many other benefits. In order to "economically" institute this plan, they realize that generating unique individual embedded codes for each and every piece of print paper would generate Terabytes of independent information, which would need storing and to which recognition software would need access. Instead, they decide to embed their print paper with 16 bit identification codes derived from a set of only 50 independent "universal" embedded code signals. The details of how this is done are in the next paragraph, but the point is that now their recognition software only needs to contain a limited set of embedded codes in their library of codes, typically on the order of 1 Megabyte to 10 Megabytes of information for 50x16 individual embedded codes splayed out onto an 8x10 photographic print (allowing for digital compression). The reason for picking 50 instead of just 16 is one of a little more added security, where if it were the same 16 embedded codes for all photographic sheets, not only would the serial number capability be limited to 2 to the 16th power, but lesser and lesser sophisticated pirates could crack the codes and remove them using software tools.

There are many different ways to implement this scheme, where the following is but one exemplary method. It is determined by the wisdom of company management that a 300 pixels per inch criteria for the embedded code signals is sufficient resolution for most applications. This means that a composite embedded code image will contain 3000 pixels by 2400 pixels to be exposed at a very low level onto each 8x10 sheet. This gives 7.2 million pixels. Using our suggested coding system such as described in the black box implementation of Figs. 5 and 6, each individual embedded code signal will contain only 7.2 million divided by 16, or approximately 450K true information carrying pixels, i.e. every 16th pixel along a given raster line. These values will typically be in the range of 2 to -2 in digital numbers, or adequately described by a signed 3 bit number. The raw information content of an embedded code is then approximately 3/8th's bytes times 450K or about 170 Kilobytes. Digital compression can reduce this further. All of these decisions are subject to standard engineering optimization principles as defined by any given application at hand, as is well known in the art. Thus we find that 50 of these independent embedded codes will amount to a few Megabytes. This is quite reasonable level to distribute as a "library" of universal codes within the recognition software. Advanced standard encryption devices could be employed to mask the exact nature of these codes if one were concerned that would-be pirates would buy the recognition software merely to reverse engineer the universal embedded codes. The recognition software could simply unencrypt the codes prior to applying the recognition techniques taught in this disclosure.

The recognition software itself would certainly have a variety of features, but the core task it would perform is determining if there is some universal copyright code within a given image. The key questions become WHICH 16 of the total 50 universal codes it might contain, if any, and if there are 16 found, what are their bit values. The key variables in determining the answers to these questions are: registration, rotation, magnification (scale), and extent. In the most general case with no helpful hints whatsoever, all variables must be independently varied across all mutual combinations, and each of the 50 universal codes must then be checked by adding and subtracting to see if an entropy decrease occurs. Strictly speaking, this is an enormous job, but many helpful hints will be found which make the job much simpler, such as having an original image to compare to the suspected copy, or knowing the general orientation and extent of the image relative to an 8x10 print paper, which then through simple registration techniques can determine all of the variables to some acceptable degree. Then it merely requires cycling through the 50 universal codes to find any decrease in entropy. If one does, then 15 others should as well. A protocol needs to be set up whereby a given order of the 50 translates into a sequence of most significant bit through least significant bit of the ID code word. Thus if we find that universal code number "4" is present, and we find its bit value to be "0", and that universal codes "1" through "3" are definitely not present, then our most significant bit of our N-bit ID code number is a "0". Likewise, we find that the next lowest universal code present is number "7" and it turns out to be a "1", then our next most significant bit is a "1". Done properly, this system can cleanly trace back to the copyright owner so long as they registered their photographic paper stock serial number with some registry or with the manufacturer of the paper itself. That is, we look up in the registry that a paper using universal embedded codes 4,7,11,12,15,19,21,26,27,28,34,35,37,38,40, and 48, and having the embedded code 0110 0101 0111 0100 belongs to Leonardo de Boticelli, an unknown wildlife photographer and glacier cinematographer whose address is in Northern Canada. We know this because he dutifully registered his film and paper stock, a few minutes of work when he bought the stock, which he plopped into the "no postage necessary" envelope that the manufacturing company kindly provided to make the process ridiculously simple. Somebody owes Leonardo a royalty check it would appear, and certainly the registry has automated this royalty payment process as part of its services.

One final point is that truly sophisticated pirates and others with illicit intentions can indeed employ a variety of cryptographic and not so cryptographic methods to crack these universal codes, sell them, and make software and hardware tools which can assist in the removing or distorting of codes. We shall not teach these methods as part of this disclosure, however. In any event, this is one of the prices which must be paid for the ease of universal codes and the applications they open up.

Universal Codes: 2) Universal Codes Based on Deterministic Formulas

The libraries of universal codes require the storage and transmittal of Megabytes of independent, generally random data as the keys with which to unlock the existence and identity of signals and imagery that have been marked with universal codes. Alternatively, various deterministic formulas can be used which "generate" what appear to be random data/image frames, thereby obviating the need to store all of these codes in memory and interrogate each and of the "50" universal codes. Deterministic formulas can also assist in speeding up the process of determining the ID code once one is *known to exist in* a given signal or image. On the other hand, deterministic formulas lend themselves to sleuthing by less sophisticated pirates. And once sleuthed, they lend themselves to easier communication, such as posting on the Internet to a hundred newsgroups. There may well be many applications which do not care about sleuthing and publishing, and deterministic formulas for generating the individual universal embedded codes might be just the ticket.

Universal Codes: 3) "Simple" Universal Codes

This category is a bit of a hybrid of the first two, and is most directed at truly large scale implementations of the principles of this technology. The applications employing this class are of the type where staunch security is much less important than low cost, large scale implementation and the vastly larger economic benefits that this enables. One exemplary application is placement of identification recognition units directly within modestly priced home audio and video instrumentation (such as a TV). Such recognition units would typically monitor audio and/or video looking for these copyright identification codes, and thence triggering simple decisions based on the findings, such as disabling or enabling recording capabilities, or incrementing program specific billing meters which are transmitted back to a central audio/video service provider and placed onto monthly invoices. Likewise, it can be foreseen that "black boxes" in bars and other public places can monitor (listen with a microphone) for copyrighted materials and generate detailed reports, for use by ASCAP, BMI, and the like.

A core principle of simple universal codes is that some basic industry standard "noiselike" and seamlessly repetitive patterns are injected into signals, images, and image sequences so that inexpensive recognition units can either A) determine the mere existence of a copyright "flag", and B) additionally to A, determine precise identification information which can facilitate more complex decision making and actions.

In order to implement this particular embodiment of the present invention, the basic principles of generating the individual embedded noise signals need to be simplified in order to accommodate inexpensive recognition signal processing circuitry, while maintaining the properties of effective randomness and holographic permeation. With large scale industry adoption of these simple codes, the codes themselves would border on public domain information (much as cable scrambling boxes are almost de facto public domain), leaving the door open for determined pirates to develop black market countermeasures, but this situation would be quite analogous to the scrambling of cable video and the objective economic analysis of such illegal activity.

One prior art known to the applicant in this general area of pro-active copyright detection is the Serial Copy Management System adopted by many firms in the audio industry. To the best of applicant's knowledge, this system employs a non-audio "flag" signal which is not part of the audio data stream, but which is nevertheless grafted onto the audio stream and can indicate whether the associated audio data should or should not be duplicated. One problem with this system is that it is restricted to media and instrumentation which can support this extra "flag" signal. Another deficiency is that the flagging system carries no identity information which would be useful in making more complex decisions. Yet another difficulty is that high quality audio sampling of an analog signal can come arbitrarily close to making a perfect digital copy of some digital master and there seems to be no provision for inhibiting this possibility.

The principles of this invention can be brought to bear on these and other problems, in audio applications, video, and all of the other applications previously discussed. An exemplary application of simple universal codes is the following. A single industry standard "1.000000 second of noise" would be defined as the most basic indicator of the presence or absence of the copyright marking of any given audio signal. Fig. 9 has an example of what the waveform of an industry standard noise second might look like, both in the time domain 400 and the frequency domain 402. It is by definition a continuous function and would adapt to any combination of sampling rates and bit quantizations. It has a normalized amplitude and can be scaled arbitrarily to any digital signal amplitude. The signal level and the first M'th derivatives of the signal are continuous at the two boundaries 404 (Fig. 9C), such that when it is repeated, the "break" in the signal would not be visible (as a waveform) or audible when played through a high end audio system. The choice of 1 second is arbitrary in this example, where the precise length of the interval will be derived from considerations such as audibility, quasi-white noise status, seamless repeatability, simplicity of recognition processing, and speed with which a copyright marking determination can be made. The injection of this repeated noise signal onto a signal or image (again, at levels below human perception) would indicate the presence of copyright material. This is essentially a one bit identification code, and the embedding of further identification information will be discussed later on in this section. The use of this identification technique can extend far beyond the low cost home implementations discussed here, where studios could use the technique, and monitoring stations could be set up which literally monitor hundreds of channels of information simultaneously, searching for marked data streams, and furthermore searching for the associated identity codes which could be tied in with billing networks and royalty tracking systems.

This basic, standardized noise signature is seamlessly repeated over and over again and added to audio signals which are to be marked with the base copyright identification.

Part of the reason for the word "simple" is seen here: clearly pirates will know about this industry standard signal, but their illicit uses derived from this knowledge, such as erasure or corruption, will be economically minuscule relative to the economic value of the overall technique to the mass market. For most high end audio this signal will be some 80 to 100 dB down from full scale, or even much further; each situation can choose its own levels though certainly there will be recommendations. The amplitude of the signal can be modulated according to the audio signal levels to which the noise signature is being applied, i.e. the amplitude can increase significantly when a drum beats, but not so dramatically as to become audible or objectionable. These measures merely assist the recognition circuitry to be described.

Recognition of the presence of this noise signature by low cost instrumentation can be effected in a variety of ways. One rests on basic modifications to the simple principles of audio signal power metering. Software recognition programs can also be written, and more sophisticated mathematical detection algorithms can be applied to audio in order to make higher confidence detection identifications. In such embodiments, detection of the copyright noise signature involves comparing the time averaged power level of an audio signal with the time averaged power level of that same audio signal which has had the noise signature subtracted from it. If the audio signal with the noise signature subtracted has a lower power level that the unchanged audio signal, then the copyright signature is present and some status flag to that effect needs to be set. The main engineering subtleties involved in making this comparison include: dealing with audio speed playback discrepancies (e.g. an *instrument* might be 0.5% "slow" relative to exactly one second intervals); and, dealing with the unknown phase of the one second noise signature within any given audio (basically, its "phase" can be anywhere from 0 to 1 seconds). Another subtlety, not so central as the above two but which nonetheless should be addressed, is that the recognition circuits should not subtract a higher amplitude of the noise signature than was originally embedded onto the audio signal. Fortunately this can be accomplished by merely subtracting only a small amplitude of the noise signal, and if the power level goes down, this is an indication of "heading toward a trough" in the power levels. Yet another related subtlety is that the power level changes will be very small relative to the overall power levels, and calculations generally will need to be done with appropriate bit precision, e.g. 32 bit value operations and accumulations on 16-20 bit audio in the calculations of time averaged power levels.

Clearly, designing and packaging this power level comparison processing circuitry for low cost applications is an engineering optimization task. One trade-off will be the accuracy of making an identification relative to the "short-cuts" which can be made to the circuitry in order to lower its cost and complexity. A preferred embodiment for the placement of this recognition circuitry inside of instrumentation is through a single programmable integrated circuit which is custom made for the task. Fig. 10 shows one such integrated circuit 506. Here the audio signal comes in, 500, either as a digital signal or as an analog signal to be digitized inside the IC 500, and the output is a flag 502 which is set to one level if the copyright noise signature is found, and to another level if it is not found. Also depicted is the fact that the standardized noise signature waveform is stored in Read Only Memory, 504, inside the IC 506. There will be a slight time delay between the application of an audio signal to the IC 506 and the output of a valid flag 502, due to the need to monitor some finite portion of the audio before a recognition can place. In this case, there may need to be a "flag valid" output 508 where the IC informs the external world if it has had enough time to make a proper determination of the presence or absence of the copyright noise signature.

There are a wide variety of specific designs and philosophies of designs applied to accomplishing the basic function of the IC 506 of Fig. 10. Audio engineers and digital signal processing engineers are able to generate several fundamentally different designs. One such design is depicted in Fig. 11 by a process 599, which itself is subject to further engineering optimization as will be discussed. Fig. 11 depicts a flow chart for any of: an analog signal processing network, a digital signal processing network, or programming steps in a software program. We find an input signal 600 which along one path is applied to a time averaged power meter 602, and the resulting power output itself treated as a signal P_{sig}. To the upper right we find the standard noise signature 504 which will be read out at 125% of normal speed, 604, thus changing its pitch, giving the "pitch changed noise signal" 606. Then the input signal has this pitch changed noise signal subtracted in step 608, and this new signal is applied to the same form of time averaged power meter as in 602, here labelled 610. The output of this operation is also a time based signal here labelled as P_{s-sig}, 610. Step 612 then subtracts the power signal 602 from the power signal 610, giving an output difference signal P_{out}, 613. If the universal standard noise signature does indeed exist on the input audio signal 600, then case 2, 616, will be created wherein a beat signal 618 of approximately 4 second period will show up on the output signal 613, and it remains to detect this beat signal with a step such as in Fig. 12, 622. Case 1, 614, is a steady noisy signal which exhibits no periodic beating. 125% at step 604 is chosen arbitrarily here, where engineering considerations would determine an optimal value, leading to different beat signal frequencies 618. Whereas waiting 4 seconds in this example would be quite a while, especially is you would want to detect at least two or three beats, Fig. 12 outlines how the basic design of Fig. 11 could be repeated and operated upon various delayed versions of the input signal, delayed by something like 1/20th of a second, with 20 parallel circuits working in concert each on a segment of the audio delayed by 0.05 seconds from their neighbors. In this way, a beat signal will show up approximately every 1/5th of a second and will look like a travelling wave down the columns of beat detection circuits. The existence or absence of this travelling beat wave triggers the detection flag 502. Meanwhile, there would be an audio signal monitor 624 which would ensure that, for example, at least two seconds of audio has been heard before setting the flag valid signal 508.

Though the audio example was described above, it should be clear to anyone in the art that the same type of definition of some repetitive universal noise signal or image could be applied to the many other signals, images, pictures, and physical media already discussed.

The above case deals only with a single bit plane of information, i.e., the noise signature signal is either there (1) or it isn't (0). For many applications, it would be nice to detect serial number information as well, which could then be used for more complex decisions, or for logging information on billing statements or whatnot. The same principles as the above would apply, but now there would be N independent noise signatures as depicted in Fig. 9 instead one single such signature. Typically, one such signature would be the master upon which the mere existence of a copyright marking is detected, and this would have generally higher power than the others, and then the other lower power "identification" *noise signatures* would be embedded into audio. Recognition circuits, once having found the existence of the primary noise signature, would then step through the other N noise signatures applying the same steps as described above. Where a beat signal is detected, this indicates the bit value of '1', and where no beat signal is detected, this indicates a bit value of '0'. It might be typical that N will equal 32, that way 2^{32} number of identification codes are available to any given industry employing this invention.

Use of this Technology When the Length of the Identification Code is 1

The principles of this invention can obviously be applied in the case where only a single presence or absence of an identification signal -- a fingerprint if you will -- is used to provide confidence that some signal or image is copyrighted. The example above of the industry standard noise signature is one case in point. We no longer have the added confidence of the coin flip analogy, we no longer have tracking code capabilities or basic serial number capabilities, but many applications may not require these attributes and the added simplicity of a single fingerprint might outweigh these other attributes in any event.

The "Wallpaper" Analogy

The term "holographic" has been used in this disclosure to describe how an identification code number is distributed in a largely integral form throughout an encoded signal or image. This also refers to the idea that any given fragment of the signal or image contains the entire unique identification code number. As with physical implementations of holography, there are limitations on how small a fragment can become before one begins to lose this property, where the resolution limits of the holographic media are the main factor in this regard for holography itself. In the case of an uncorrupted distribution signal which has used the encoding device of figure 5, and which furthermore has used our "designed noise" of above wherein the zero's were randomly changed to a 1 or -1, then the extent of the fragment required is merely N contiguous samples in a signal or image raster line, where N is as defined previously being the length of our identification code number. This is an informational extreme; practical situations where noise and corruption are operative will require generally one, two or higher orders of magnitude more samples than this simple number N. Those skilled in the art will recognize that there are many variables involved in pinning down precise statistics on the size of the smallest fragment with which an identification can be made.

For tutorial purposes, the applicant also uses the analogy that the unique identification code number is "wallpapered" across and image (or signal). That is, it is repeated over and over again all throughout an image. This repetition of the ID code number can be regular, as in the use of the encoder of figure 5, or random itself, where the bits in the ID code 216 of figure 6 are not stepped through in a normal repetitive fashion but rather are randomly selected on each sample, and the random selection stored along with the value of the output 228 itself. In any event, the information carrier of the ID code, the individual embedded code signal, does change across the image or signal. Thus as the wallpaper analogy summarizes: the ID code repeats itself over and over, but the patterns that each repetition imprints change randomly accordingly to a generally unsleuthable key.

Lossy Data Compression

As earlier mentioned, the identification coding of the preferred embodiment withstands lossy data compression, and subsequent decompression. Such compression is finding increasing use, particularly in contexts such as the mass distribution of digitized entertainment programming (movies, etc.).

While data encoded according to the preferred embodiment of the present invention can withstand all types of lossy compression known to applicant, those expected to be most commercially important are the CCITT G3, CCITT G4, JPEG, MPEG and JBIG compression/decompression standards. The CCITT standards are widely used in black-and-white document compression (e.g. facsimile and document-storage). JPEG is most widely used with still images. MPEG is most widely used with moving images. JBIG is a likely successor to the CCITT standards for use with black-and-white imagery. Such techniques are well known to those in the lossy data compression field; a good overview can be found in Pennebaker et al, *JPEG, Still Image Data Compression Standard*, Van Nostrand Reinhold, N.Y., 1993.

Towards Steganography Proper and the Use of this Technology in Passing More Complex Messages or Information

This disclosure concentrates on what above was called wallpapering a single identification code across an entire signal. This appears to be a desirable feature for many applications. However, there are other applications where it might be desirable to pass messages or to embed very long strings of pertinent identification information in signals and images. One of many such possible applications would be where a given signal or image is meant to be manipulated by several different groups, and that certain regions of an image are reserved for each group's identification and insertion of pertinent manipulation information.

In these cases, the code word 216 in figure 6 can actually change in some pre-defined manner as a function of signal or image position. For example, in an image, the code could change for each and every raster line of the digital image. It might be a 16 bit code word, 216, but each scan line would have a new code word, and thus a 480 scan line image could pass a 980 (480 x 2 bytes) byte message. A receiver of the message would need to have access to either the noise signal stored in memory 214, or would have to know the universal code structure of the noise codes if that method of coding was *being used*. To the best of applicant's knowledge, this is a novel approach to the mature field of steganography.

In all three of the foregoing applications of universal codes, it will often be desirable to append a short (perhaps 8- or 16-bit) private code, which users would keep in their own secured places, in addition to the universal code. This affords the user a further modicum of security against potential erasure of the universal codes by sophisticated pirates.

Conclusion

In view of the great number of different embodiments to which the principles of my invention can be put, it should be recognized that the detailed embodiments are illustrative only and should not be taken as limiting the scope of my invention. Rather, I claim as my invention all such embodiments as may come within the scope and spirit of the following claims, and equivalents thereto.

APPENDIX A

```
#include "main.h"

#define XDIM 512L
#define XDIMR 512
#define YDIM 480L
#define BITS 8
#define RMS_VAL 5.0
#define NUM_NOISY 16
#define NUM_DEMOS 3
#define GRAD_THRESHOLD 10

struct char_buf {
    char filename[80];
    FILE *fp;
    fpos_t fpos;
    char buf[XDIMR];
};
struct uchar_buf {
    char filename[80];
    FILE *fp;
    fpos_t fpos;
    unsigned char buf[XDIMR];
};
struct int_buf {
    char filename[80];
    FILE *fp;
    fpos_t fpos;
    int buf[XDIMR];
};
struct cortex_s {
    char filename[80];
    FILE *fp;
    fpos_t fpos;
    unsigned char buf[XDIMR];
};

struct uchar_buf test_image;
struct char_buf snow_composite;
struct uchar_buf distributed_image;
struct uchar_buf temp_image;
struct int_buf temp_wordbuffer;
struct int_buf temp_wordbuffer2;
struct uchar_buf snow_images;
struct cortex_s cortex;

int demo=0;  /* which demo is being performed, see notes */

int our_code;  /* id value embedded onto image */
int found_code=0;  /* holder for found code*/


int waitvbb(void){
    while( (_inp(PORT_BASE)&8) );
    while( !(_inp(PORT_BASE)&8) );
    return(1);
}

int grabb(void){
    waitvbb();
    _outp(PORT_BASE+1,0);
    _outp(PORT_BASE,8);
    waitvbb();
    waitvbb();
    _outp(PORT_BASE,0x10);
    return(1);
```

```
}

int livee(void){
    _outp(PORT_BASE,0x00);
    return(1);
}


int live_video(void){
    livee();
    return(1);
}

int freeze_frame(void){
    grabb();
    return(1);
}

int grab_frame(struct uchar_buf *image){
    long i;

    grabb();
    fsetpos(image->fp, &image->fpos  );
    fsetpos(cortex.fp, &cortex.fpos  );
    for(i=0;i<YDIM;i++){
        fread(cortex.buf,sizeof(unsigned char),XDIMR,cortex.fp);
        fwrite(cortex.buf,sizeof(unsigned char),XDIMR,image->fp);
    }
    livee();
    return(1);
}

int wait_vertical_blanks(int number){
    long i;
    for(i=0;i<number;i++)waitvbb();
    return(1);
}


int clear_char_image(struct char_buf *charbuffer){
    long i,j;
    char *pchar;
    fpos_t tmp_fpos;

    fsetpos(charbuffer->fp, &charbuffer->fpos  );
    for(i=0;i<YDIM;i++){
        fgetpos(charbuffer->fp, &tmp_fpos  );
        pchar = charbuffer->buf;
        fread(charbuffer->buf,sizeof(char),XDIMR,charbuffer->fp);
        for(j=0;j<XDIM;j++) *(pchar++) = 0;
        fsetpos(charbuffer->fp, &tmp_fpos  );
        fwrite(charbuffer->buf,sizeof(char),XDIMR,charbuffer->fp);
    }
    return(1);
}

int display_uchar(struct uchar_buf *image,int stretch){
    unsigned char *pimage;
    unsigned char highest = 0;
    unsigned char lowest = 255;
    long i,j;
    double dtemp,scale,dlowest;
    fpos_t tmp_fpos;

    if(stretch){
        fsetpos(image->fp, &image->fpos  );
        fread(image->buf,sizeof(unsigned char),XDIMR,image->fp);
        fread(image->buf,sizeof(unsigned char),XDIMR,image->fp);
```

```
        for(i=2;i<(YDIM-2);i++){
            fread(image->buf,sizeof(unsigned char),XDIMR,image->fp);
            pimage = &image->buf[3];
            for(j=3;j<(XDIM-3);j++){
                if( *pimage > highest )highest = *pimage;
                if( *pimage < lowest )lowest = *pimage;
                pimage++;
            }
        }
        if(highest == lowest ){
            printf("something wrong in contrast stretch, zero
 contrast");
            exit(1);
        }
        scale = 255.0 / ( (double)highest - (double)lowest );
        dlowest = (double)lowest;
        fsetpos(image->fp, &image->fpos  );
        for(i=0;i<YDIM;i++){
            fgetpos(image->fp, &tmp_fpos  );
            fread(image->buf,sizeof(unsigned char),XDIMR,image->fp);
            pimage = image->buf;
            for(j=0;j<XDIM;j++){
                dtemp = ((double)*pimage - dlowest)*scale;
                if(dtemp < 0.0)*(pimage++) = 0;
                else if(dtemp > 255.0)*(pimage++) = 255;
                else *(pimage++) = (unsigned char)dtemp;
            }
            fsetpos(image->fp, &tmp_fpos  );
            fwrite(image->buf,sizeof(unsigned
char),XDIMR,image->fp);
        }
    }

    fsetpos(image->fp, &image->fpos  );
    fsetpos(cortex.fp, &cortex.fpos  );
    for(i=0;i<YDIM;i++){
        fread(image->buf,sizeof(unsigned char),XDIMR,image->fp);
        fwrite(image->buf,sizeof(unsigned char),XDIMR,cortex.fp);
    }
    return(1);
}


int clear_int_image(struct int_buf *wordbuffer){
    long i,j;
    int *pword;
    fpos_t tmp_fpos;

    fsetpos(wordbuffer->fp, &wordbuffer->fpos  );
    for(i=0;i<YDIM;i++){
        fgetpos(wordbuffer->fp, &tmp_fpos  );
        pword = wordbuffer->buf;
        fread(wordbuffer->buf,sizeof(int),XDIMR,wordbuffer->fp);
        for(j=0;j<XDIM;j++) *(pword++) = 0;
        fsetpos(wordbuffer->fp, &tmp_fpos  );
        fwrite(wordbuffer->buf,sizeof(int),XDIMR,wordbuffer->fp);
    }
    return(1);
}

double find_mean_int(struct int_buf *wordbuffer){
    long i,j;
    int *pword;
    double mean=0.0;

    fsetpos(wordbuffer->fp, &wordbuffer->fpos  );
```

```
    for(i=0;i<YDIM;i++){
        pword = wordbuffer->buf;
        fread(wordbuffer->buf,sizeof(int),XDIMR,wordbuffer->fp);
        for(j=0;j<XDIM;j++) mean += (double) *(pword++);
    }
    mean /= ((double)XDIM * (double)YDIM);

    return(mean);
}

int add_uchar_to_int(struct uchar_buf *image,struct int_buf *word){
    unsigned char *pimage;
    int *pword;
    long i,j;
    fpos_t tmp_fpos;

    fsetpos(image->fp, &image->fpos  );
    fsetpos(word->fp, &word->fpos  );
    for(i=0;i<YDIM;i++){
        pword = word->buf;
        fgetpos(word->fp, &tmp_fpos  );
        fread(word->buf,sizeof(int),XDIMR,word->fp);
        pimage = image->buf;
        fread(image->buf,sizeof(unsigned char),XDIMR,image->fp);
        for(j=0;j<XDIM;j++) *(pword++) += (int)*(pimage++);
        fsetpos(word->fp, &tmp_fpos  );
        fwrite(word->buf,sizeof(int),XDIMR,word->fp);
    }
    return(1);
}


int add_char_to_uchar_creating_uchar(struct char_buf *cimage,
    struct uchar_buf *image,
    struct uchar_buf *out_image){
    unsigned char *pimage,*pout_image;
    char *pcimage;
    int temp;
    long i,j;

    fsetpos(image->fp, &image->fpos  );
    fsetpos(out_image->fp, &out_image->fpos  );
    fsetpos(cimage->fp, &cimage->fpos  );
    for(i=0;i<YDIM;i++){
        pcimage = cimage->buf;
        fread(cimage->buf,sizeof(char),XDIMR,cimage->fp);
        pimage = image->buf;
        fread(image->buf,sizeof(unsigned char),XDIMR,image->fp);
        pout_image = out_image->buf;
        for(j=0;j<XDIM;j++){
            temp = (int) *(pimage++) + (int) *(pcimage++);
            if(temp<0)temp = 0;
            else if(temp > 255)temp = 255;
            *(pout_image++) = (unsigned char)temp;
        }
        fwrite(out_image->buf,sizeof(unsigned
char),XDIMR,out_image->fp);
    }
    return(1);
}


int copy_int_to_int(struct int_buf *word2,struct int_buf *word){
    long i;

    fsetpos(word2->fp, &word2->fpos  );
```

```
    fsetpos(word->fp, &word->fpos  );
    for(i=0;i<YDIM;i++){
        fread(word->buf,sizeof(int),XDIMR,word->fp);
        fwrite(word->buf,sizeof(int),XDIMR,word2->fp);
    }
    return(1);
}


void get_snow_images(void){
    unsigned char *psnow,*ptemp;
    int number_snow_inputs;
    int temp,*pword,*pword2,bit;
    long i, j;
    double rms,dtemp;

    live_video(); /* device specific */

    printf("\n\nPlease point camera at a medium lit blank wall. ");
    printf("\nDefocus the lens a bit as well ");
    printf("\nIf possible, place the camera into its highest gain,
and ");
    printf("\nput the gamma to 1.0.");
    printf("  Ensure that the video is not saturated ");
    printf("\nPress any key when ready... ");

    while( !kbhit() );
    printf("\nNow finding difference frame rms value... ");

    /* subtract one image from another, find the rms difference */
    live_video();
    wait_vertical_blanks(2);
    grab_frame(&temp_image);
    live_video();
    wait_vertical_blanks(2);
    grab_frame(&distributed_image); /* use first image as buffer */

    rms = 0.0;
    fsetpos(temp_image.fp, &temp_image.fpos  );
    fsetpos(distributed_image.fp, &distributed_image.fpos  );
    for(i=0;i<YDIM;i++){
        ptemp = temp_image.buf;
        fread(temp_image.buf,sizeof(unsigned
char),XDIMR,temp_image.fp);
        psnow = distributed_image.buf;
        fread(distributed_image.buf,sizeof(unsigned
char),XDIMR,distributed_image.fp);
        for(j=0;j<XDIM;j++){
            temp = (int) *(psnow++)  -  (int) *(ptemp++);
            dtemp = (double)temp;
            dtemp *= dtemp;
            rms += dtemp;
        }
    }
    rms /= ( (double)XDIM * (double)YDIM );
    rms = sqrt(rms);
    printf("\n\nAn rms frame difference noise value of %lf was
found.",rms);
    printf("\nWe want at least %lf for good measure",RMS_VAL);
    /* we want rms to be at least RMS_VAL DN, so ...   */
    if(rms > RMS_VAL) number_snow_inputs = 1;
    else {
        dtemp = RMS_VAL / rms;
        dtemp *= dtemp;
        number_snow_inputs = 1 + (int)dtemp;
    }
    printf("\n%d images will achieve this noise
level",number_snow_inputs);
```

```
    /* now create each snowy image */

    printf("\nStarting to create snow pictures... \n");
    fsetpos(snow_images.fp, &snow_images.fpos  ); /* set on first
image*/
    for(bit = 0; bit < BITS; bit++){

        clear_int_image(&temp_wordbuffer);
        for(i=0;i<number_snow_inputs;i++){
            live_video();
            wait_vertical_blanks(2);
            grab_frame(&temp_image);
            add_uchar_to_int(&temp_image,&temp_wordbuffer);
        }

        clear_int_image(&temp_wordbuffer2);
        for(i=0;i<number_snow_inputs;i++){
            live_video();
            wait_vertical_blanks(2);
            grab_frame(&temp_image);
            add_uchar_to_int(&temp_image,&temp_wordbuffer2);
        }

        /* now load snow_images[bit] with the difference frame
biased by
        128 in an unsigned char form just to keep things clean */
        /* display it on cortex also */
        fsetpos(temp_wordbuffer2.fp, &temp_wordbuffer2.fpos  );
        fsetpos(temp_wordbuffer.fp, &temp_wordbuffer.fpos  );
        fsetpos(temp_image.fp, &temp_image.fpos  );
        for(i=0;i<YDIM;i++){
            pword = temp_wordbuffer.buf;
            fread(temp_wordbuffer.buf,sizeof(int),XDIMR,temp_wordbuf
fer.fp);
            pword2 = temp_wordbuffer2.buf;
            fread(temp_wordbuffer2.buf,sizeof(int),XDIMR,temp_wordbu
ffer2.fp);
            psnow = snow_images.buf;
            ptemp = temp_image.buf;
            for(j=0;j<XDIM;j++) {
                *(psnow++) = *(ptemp++) = (unsigned char)
(*(pword++) - *(pword2++) + 128);
            }
            fwrite(snow_images.buf,sizeof(unsigned
char),XDIMR,snow_images.fp);
            fwrite(temp_image.buf,sizeof(unsigned
char),XDIMR,temp_image.fp);
        }
        freeze_frame();
        display_uchar(&temp_image,0); /*1 signifies to stretch the
contrast*/
        printf("\rDone snowy %d   ",bit);
        wait_vertical_blanks(30);
    }

    return;
}




void loop_visual(void){
    unsigned char *psnow;
    char *pcomp;
    long i,j,count = 0;
    int ok=0,temp,bit,add_it;
```

```
void search_1(struct uchar_buf *suspect){
    unsigned char *psuspect,*psnow;
    int bit,*pword,temp;
    long i,j;
    double add_metric,subtract_metric;
    fpos_t tmp_fpos;

    /* this algorithm is conceptually the simplest.  The idea is to
step
    through each bit at a time and merely see if adding or
subtracting the
    individual snowy picture minimizes some 'contrast' metric.
    This should be the most crude and inefficient, no where to go
but
    better */

    fsetpos(snow_images.fp, &snow_images.fpos  );
    temp=256;
    clear_int_image(&temp_wordbuffer);
    add_uchar_to_int(suspect,&temp_wordbuffer);
    find_grad(&temp_wordbuffer,1); /* 1 means load temp_wordbuffer2
*/
    for(bit=0;bit<BITS;bit++){
        /* add first */
        fgetpos(snow_images.fp, &tmp_fpos  );
        fsetpos(suspect->fp, &suspect->fpos  );
        fsetpos(temp_wordbuffer.fp, &temp_wordbuffer.fpos  );
        for(i=0;i<YDIM;i++){
            pword = temp_wordbuffer.buf;
            psuspect = suspect->buf;
            psnow = snow_images.buf;
            fread(suspect->buf,sizeof(unsigned
char),XDIMR,suspect->fp);
            fread(snow_images.buf,sizeof(unsigned
char),XDIMR,snow_images.fp);
            for(j=0;j<XDIM;j++){
                *(pword++)=(int)*(psuspect++)+(int)*(psnow++)-128;
            }
            fwrite(temp_wordbuffer.buf,sizeof(int),XDIMR,temp_wordbu
ffer.fp);
        }
        add_metric = find_grad(&temp_wordbuffer,0);

        /* then subtract */
        fsetpos(snow_images.fp, &tmp_fpos  );
        fsetpos(suspect->fp, &suspect->fpos  );
        fsetpos(temp_wordbuffer.fp, &temp_wordbuffer.fpos  );
        for(i=0;i<YDIM;i++){
            pword = temp_wordbuffer.buf;
            psuspect = suspect->buf;
            psnow = snow_images.buf;
            fread(suspect->buf,sizeof(unsigned
char),XDIMR,suspect->fp);
            fread(snow_images.buf,sizeof(unsigned
char),XDIMR,snow_images.fp);
            for(j=0;j<XDIM;j++){
                *(pword++)=(int)*(psuspect++)-(int)*(psnow++)+128;
            }
            fwrite(temp_wordbuffer.buf,sizeof(int),XDIMR,temp_wordbu
ffer.fp);
        }
        subtract_metric = find_grad(&temp_wordbuffer,0);

        printf("\nbit place %d: add=%le ,
sub=%le",bit,add_metric,subtract_metric);
        temp/=2;
        if(add_metric < subtract_metric){
            printf("  bit value = 0");
```

```
            }
            else {
                printf("  bit value = 1");
                found_code += temp;
            }
        }
        printf("\n\nYour magic number was %d",found_code);
        return;
}


void search_2(unsigned char *suspect){

        if(suspect);

        return;
}



void loop_simulation(void){
        unsigned char *ptemp,*pdist;
        int *pword,int_mean,ok=0,temp;
        long i,j;
        double mean,scale;

        /* grab a noisy image into one of the temp buffers */
        printf("\ngrabbing noisy frame...\n");
        clear_int_image(&temp_wordbuffer);
        for(i=0;i<NUM_NOISY;i++){
            live_video();
            wait_vertical_blanks(2);
            grab_frame(&temp_image);
            add_uchar_to_int(&temp_image,&temp_wordbuffer);
            j=(long)NUM_NOISY;
            printf("\r%ld of %ld     ",i+1,j);
        }

        /* find mean value of temp_wordbuffer */
        mean = find_mean_int(&temp_wordbuffer);
        int_mean = (int)mean;

        /* now we will add scaled version of this 'corruption' to our
distributed
        image */
        scale = 1.0;
        while( !ok ){
            /* add noise to dist image storing in temp_image */
            fsetpos(distributed_image.fp, &distributed_image.fpos  );
            fsetpos(temp_wordbuffer.fp, &temp_wordbuffer.fpos  );
            fsetpos(temp_image.fp, &temp_image.fpos  );
            for(i=0;i<YDIM;i++){
                pdist = distributed_image.buf;
                pword = temp_wordbuffer.buf;
                ptemp = temp_image.buf;
                fread(distributed_image.buf,sizeof(unsigned
char),XDIMR,distributed_image.fp);
                fread(temp_wordbuffer.buf,sizeof(int),XDIMR,temp_wordbuf
fer.fp);
                for(j=0;j<XDIM;j++){
                    temp = (int) *(pdist++) + *(pword++) - int_mean;
                    if(temp<0)temp = 0;
                    else if(temp > 255)temp = 255;
                    *(ptemp++) = (unsigned char)temp;
                }
```

```
                fwrite(temp_image.buf,sizeof(unsigned
char),XDIMR,temp_image.fp);
        }

        /* display the dist image and the corrupted image */
        display_uchar(&temp_image,0);

        /* apply new 'corrupted' image to search algorithm 1 for id
value */
        search_1(&temp_image);

        /* apply new 'corrupted' image to search algorithm 2 for id
value */
        /*
        search_2(temp_image);
        */

        /* prompt for upping noise content or ok */
        ok = 1;
    }

    return;
}



int initialize_everything(void){
    long i,j;
    unsigned char *pucbuf;
    char *pcbuf;
    int *pibuf;

    /* initialize cortex */
    strcpy(cortex.filename,"f:image");
    if((cortex.fp=fopen(cortex.filename,"rb"))==NULL){
        system("v f g");
    }
    else fclose(cortex.fp);
    if( (_inp(PORT_BASE) == 0xFF) ){
        printf("oops ");
        exit(0);
    }

    /* open cortex for read and write */
    if((cortex.fp=fopen(cortex.filename,"rb+"))==NULL){
        printf(" No good on open file joe ");
        exit(0);
    }
    fgetpos(cortex.fp, &cortex.fpos );

/* test_image;  original image */
    strcpy(test_image.filename,"e:tst_img");
    if((test_image.fp=fopen(test_image.filename,"wb"))==NULL){
        printf(" No good on open file joe ");
        exit(0);
    }
    pucbuf = test_image.buf;
    for(i=0;i<XDIM;i++)*(pucbuf++)=0;
    for(i=0;i<YDIM;i++){
        fwrite(test_image.buf,sizeof(unsigned
char),XDIMR,test_image.fp);
    }
    fclose(test_image.fp);
    if((test_image.fp=fopen(test_image.filename,"rb+"))==NULL){
        printf(" No good on open file joe ");
        exit(0);
```

```
    }
    fgetpos(test_image.fp, &test_image.fpos  );

/* snow_composite;  ultimate image added to original image */
    strcpy(snow_composite.filename,"e:snw_cmp");

if((snow_composite.fp=fopen(snow_composite.filename,"wb"))==NULL){
        printf(" No good on open file joe ");
        exit(0);
    }
    pcbuf = snow_composite.buf;
    for(i=0;i<XDIM;i++)*(pcbuf++)=0;
    for(i=0;i<YDIM;i++){

fwrite(snow_composite.buf,sizeof(char),XDIMR,snow_composite.fp);
    }
    fclose(snow_composite.fp);

if((snow_composite.fp=fopen(snow_composite.filename,"rb+"))==NULL){
        printf(" No good on open file joe ");
        exit(0);
    }
    fgetpos(snow_composite.fp, &snow_composite.fpos  );

/* distributed_image;   test_img plus snow_composite */
    strcpy(distributed_image.filename,"e:dst_img");

if((distributed_image.fp=fopen(distributed_image.filename,"wb"))==NU
LL){
        printf(" No good on open file joe ");
        exit(0);
    }
    pucbuf = distributed_image.buf;
    for(i=0;i<XDIM;i++)*(pucbuf++)=0;
    for(i=0;i<YDIM;i++){
        fwrite(distributed_image.buf,sizeof(unsigned
char),XDIMR,distributed_image.fp);
    }
    fclose(distributed_image.fp);

if((distributed_image.fp=fopen(distributed_image.filename,"rb+"))==N
ULL){
        printf(" No good on open file joe ");
        exit(0);
    }
    fgetpos(distributed_image.fp, &distributed_image.fpos  );


/* temp_image;   buffer if needed */
    strcpy(temp_image.filename,"e:temp_img");
    if((temp_image.fp=fopen(temp_image.filename,"wb"))==NULL){
        printf(" No good on open file joe ");
        exit(0);
    }
    pucbuf = temp_image.buf;
    for(i=0;i<XDIM;i++)*(pucbuf++)=0;
    for(i=0;i<YDIM;i++){
        fwrite(temp_image.buf,sizeof(unsigned
char),XDIMR,temp_image.fp);
    }
    fclose(temp_image.fp);
    if((temp_image.fp=fopen(temp_image.filename,"rb+"))==NULL){
        printf(" No good on open file joe ");
        exit(0);
    }
    fgetpos(temp_image.fp, &temp_image.fpos  );

/*  temp_wordbuffer;   16 bit image buffer for averaging */
```

```
     strcpy(temp_wordbuffer.filename,"e:temp_wrd");
  if((temp_wordbuffer.fp=fopen(temp_wordbuffer.filename,"wb"))==NULL){
          printf(" No good on open file joe ");
          exit(0);
     }
     pibuf = temp_wordbuffer.buf;
     for(i=0;i<XDIM;i++)*(pibuf++)=0;
     for(i=0;i<YDIM;i++){

  fwrite(temp_wordbuffer.buf,sizeof(int),XDIMR,temp_wordbuffer.fp);
     }
     fclose(temp_wordbuffer.fp);

  if((temp_wordbuffer.fp=fopen(temp_wordbuffer.filename,"rb+"))==NULL)
  {
          printf(" No good on open file joe ");
          exit(0);
     }
     fgetpos(temp_wordbuffer.fp, &temp_wordbuffer.fpos  );

  /* temp_wordbuffer2;  /* 16 bit image buffer for averaging */
     strcpy(temp_wordbuffer2.filename,"e:tmp_wrd2");

  if((temp_wordbuffer2.fp=fopen(temp_wordbuffer2.filename,"wb"))==NULL
  ){
          printf(" No good on open file joe ");
          exit(0);
     }
     pibuf = temp_wordbuffer2.buf;
     for(i=0;i<XDIM;i++)*(pibuf++)=0;
     for(i=0;i<YDIM;i++){

  fwrite(temp_wordbuffer2.buf,sizeof(int),XDIMR,temp_wordbuffer2.fp);
     }
     fclose(temp_wordbuffer2.fp);

  if((temp_wordbuffer2.fp=fopen(temp_wordbuffer2.filename,"rb+"))==NUL
  L){
          printf(" No good on open file joe ");
          exit(0);
     }
     fgetpos(temp_wordbuffer2.fp, &temp_wordbuffer2.fpos  );

  /* snow_images,  BITS number of constituent snowy pictures */
     strcpy(snow_images.filename,"snw_imgs");
     if((snow_images.fp=fopen(snow_images.filename,"wb"))==NULL){
          printf(" No good on open file joe ");
          exit(0);
     }
     pucbuf = snow_images.buf;
     for(i=0;i<XDIM;i++)*(pucbuf++)=0;
     for(j=0;j<BITS;j++){
     for(i=0;i<YDIM;i++){
          fwrite(snow_images.buf,sizeof(unsigned
 char),XDIMR,snow_images.fp);
     }
     }
     fclose(snow_images.fp);
     if((snow_images.fp=fopen(snow_images.filename,"rb+"))==NULL){
          printf(" No good on open file joe ");
          exit(0);
     }
     fgetpos(snow_images.fp, &snow_images.fpos  );

     return(1);
  }
```

```
int close_everything(void){

     fclose(test_image.fp);
     fclose(snow_composite.fp);
     fclose(distributed_image.fp);
     fclose(temp_image.fp);
     fclose(temp_wordbuffer.fp);
     fclose(temp_wordbuffer2.fp);
     fclose(snow_images.fp);

     return(1);
}


main(){
     int i,j;

     printf("\nInitializing...\n\n");
     initialize_everything();  /* device specific and global mallocs
*/

     live_video();

     /* prompt for which of the three demos to perform */
     while( demo < 1 || demo > NUM_DEMOS){
          printf("Which demo do you want to run?\n\n");
          printf("1: Digital Imagery and Very High End Photography
Simulation\n");
          printf("2: Pre-exposed Print Paper and other Dupping\n");
          printf("3: Pre-exposed Original Film (i.e. In-Camera)\n");
          printf("\nEnter number and return:  ");
          scanf("%d",&demo);
          if(demo < 1 || demo > NUM_DEMOS){
               printf("\n eh eh  ");
          }
     }

     /* acquire test image */
     printf("\nPress any key after your test scene is ready... ");
     getch();
     grab_frame(&test_image);  /*grab_frame takes care of device
specific stuff*/

     /* prompt for id number, 0 through 255 */
     printf("\nEnter any number between 0 and 255.\n");
     printf("This will be the unique magic code placed into the
image:  ");
     scanf("%d",&our_code);
     while(our_code<1 || our_code>256){
          printf(" Between 0 and 255 please  ");
          scanf("%d",&our_code);
     }

     /* feed back the binary code which will be embedded in the image
*/
     printf("\nThe binary sequence ");
     for(i=0;i<BITS;i++){
          j = 128 >> i;
          if( our_code & j)printf("1");
          else printf("0");
     }
     printf(" (%d) will be embedded on the image\n",our_code);

     /* now generate the individual snow images  */
     get_snow_images();
```

```
    loop_visual();  /* this gives visual feedback on 'tolerable'
noise level */

    printf("\nWe're now to the simulated suspect... \n");
    loop_simulation();

    close_everything();
    return(0);
}
```

Claims

1. A method of identification coding an input signal so as to permit its later identification, the method including the steps:

modulating a noise signal with a code number to produce a signature signal; and

modulating the input signal with the signature signal to produce an identification coded output signal;

wherein the coded output signal can be analyzed to discern the code number with which it was modulated.

2. A method of identification coding an input signal so as to produce an encoded output signal, the input signal being a quantized signal having inherent noise, said signal corresponding to aural or visual information, the identification coding of the output signal preserving the corresponding aural/visual information without human-perceptible degradation, the identification coding permitting later identification of the output signal, the method including modulating a noise signal with a code number to produce a signature signal, adding the signature signal to the input signal to produce an identification coded output signal, the signature signal having an amplitude below a threshold of human aural/visual perceptibility when added to the input signal, the adding step effecting distribution of the signature signal throughout the entirety of the output signal.

3. A method of data processing including: providing a digital carrier signal, and modulating the digital carrier signal to imperceptibly embed an identification signal thereon, the method characterized by: compressing the modulated digital carrier signal with lossy data compression to produce a compressed signal, decompressing the compressed signal, and discerning the embedded identification signal from the decompressed signal, wherein the lossy data compression does not preclude recovery of the embedded identification signal.

4. An apparatus for encoding a sampled input signal, the sampled input signal having inherent noise, the apparatus including an input terminal, a digital noise source, storage for an identification code word, means for maintaining a pointer to a bit of the identification code word, an adder, and an output terminal, the input terminal being coupled to a first input of the adder, the noise source being coupled to a second input of the adder, the pointer providing said bit of the identification code word to a control input of the adder, an output of the adder being coupled to the output terminal.

5. The apparatus of claim 4 which further includes a look-up table, a first scaler, a second scaler, a scale control device, and a memory, the look-up table having an input coupled to the input terminal, one of said scalers having a control input coupled to an output of the look-up table, the other of said scalers having a control input coupled to the scale control device, said scalers being serially interposed between the noise source and the adder, the memory having an input coupled to a location between the noise source and the second input of the adder.

6. A method of identification coding a sampled input signal, the sampled input signal having inherent noise, the method comprising:

providing an N-bit code number;

for each of a plurality of *samples* of the input signal:

(a) providing a sample of a time- or spatially-varying modulation signal;

(b) selecting one bit of the N-bit code number; and

(c) if said bit has a first value, adding the modulation signal sample to the sample of the input signal, yielding a sample of an identification coded output signal.

7. The method of claim 6 which includes performing steps (a) - (c) for each sample of the input signal.

8. The method of claim 6 which further includes storing, for later use, data from which the modulation signal sample can be reconstructed.

9. The method of claim 6 which includes generating the time-varying modulation signal sample by providing a pseudo-random number and weighting said number with a scaling factor, said scaling factor being a function of the input signal sample.

10. The method of claim 6 which includes selecting the one bit of the N-bit code number by cycling through the number, advancing one bit position for each successive sample of the input signal.

11. The method of claim 6 which further includes:

if said selected bit of the N-bit code number has a second value, subtracting the modulation signal sample from the sample of the input signal, yielding a sample of the identification coded output signal.

12. Storage medium having stored thereon a signal processed in accordance with the method of claim 6.

13. The invention of claim 12 in which the storage medium is a magnetic medium.

14. The invention of claim 12 in which the storage medium is a printed medium.

15. The invention of claim 12 in which the storage medium is a compact disk (CD).

16. A method of identification coding each of a plurality of samples of a sampled input signal, the input signal having inherent noise, characterized by:

using the sample of the input signal to obtain a scaling factor uniquely associated thereto;

weighting a signature datum in accordance with said scaling factor; and

modulating the sample of the input signal in accordance with said weighted signature datum.

17. The method of claim 16 in which the scaling factors increase monotonically with the values of the input signal samples with which they are associated.

18. The method of claim 16 in which a four-fold increase in a value of the sampled input signal corresponds to approximately a two-fold increase in a value of the scaling factor associated therewith.

19. A method of processing a sampled input signal with an N-bit signature word to produce an identification-coded output signal, the sampled input signal having inherent noise, wherein the complete N-bit signature finds expression M times in an excerpt of the identification-coded output signal having a length of M*N samples, for some value of M greater than one.

20. The method of claim 19 characterized by processing each sample of the input signal in accordance with at least part of the signature word.

21. In a method of processing a source signal that includes a number of elements, each with an associated value, an improvement characterized by altering the source signal in accordance with an embedded signal so as to encode an identification code therein, the embedded and altered signals each including a number of elements, each with an associated value, wherein an element of the altered signal has a value different than that of corresponding elements in both the source and embedded signals, and in which the identification code and certain pseudo-random reference data are used to generate the embedded signal, the association between the embedded signal and the identification code being undiscernible without availability of the reference data.

22. In a method of processing a source signal that includes a number of elements, each with an associated value, an improvement characterized by:

providing an N bit digital identification code, each bit having a "1" or "0" value;

providing N different reference signals, one being associated with each bit position in the digital identification code;

summing the reference signals for which the corresponding bit position in the identification code has a "1" value, thereby producing an embedded signal;

altering the source signal in accordance with the embedded signal so as to encode an identification code therein;

the embedded and altered signals each including a number of elements, each with an associated value, wherein an element of the altered signal has a value different than that of corresponding elements in both the source and embedded signals.

FIG. 4

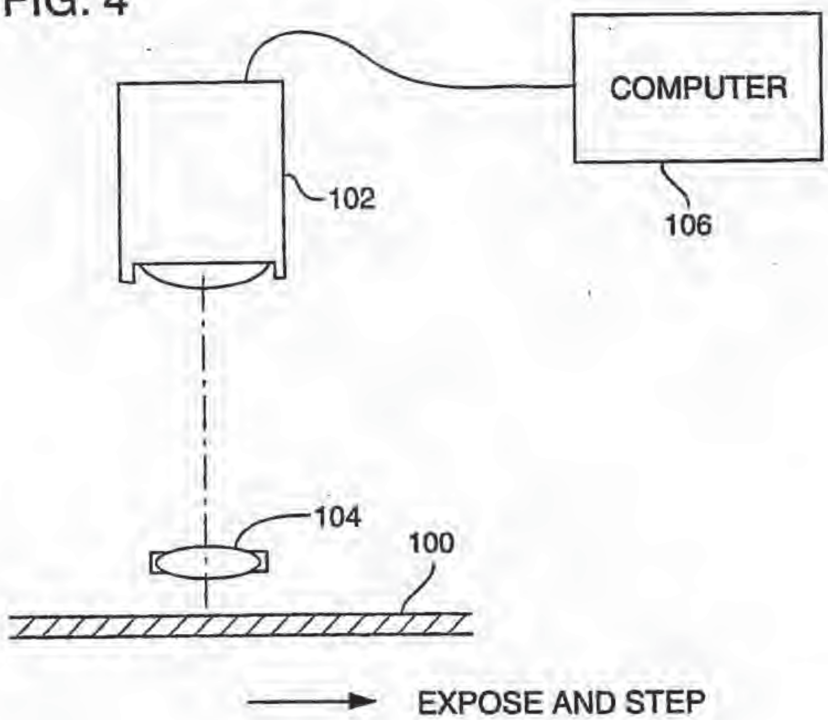

COMPUTER
102
106
104
100
EXPOSE AND STEP

FIG. 1

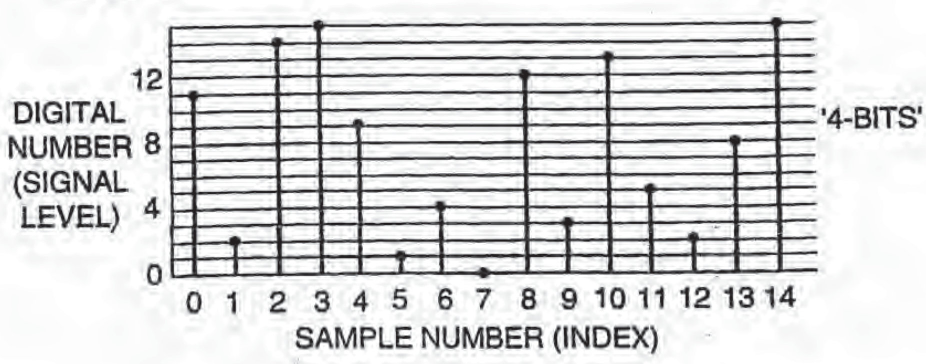

12
DIGITAL
NUMBER
(SIGNAL
LEVEL)
8
4
0
'4-BITS'
0 1 2 3 4 5 6 7 8 9 10 11 12 13 14
SAMPLE NUMBER (INDEX)

FIG. 2

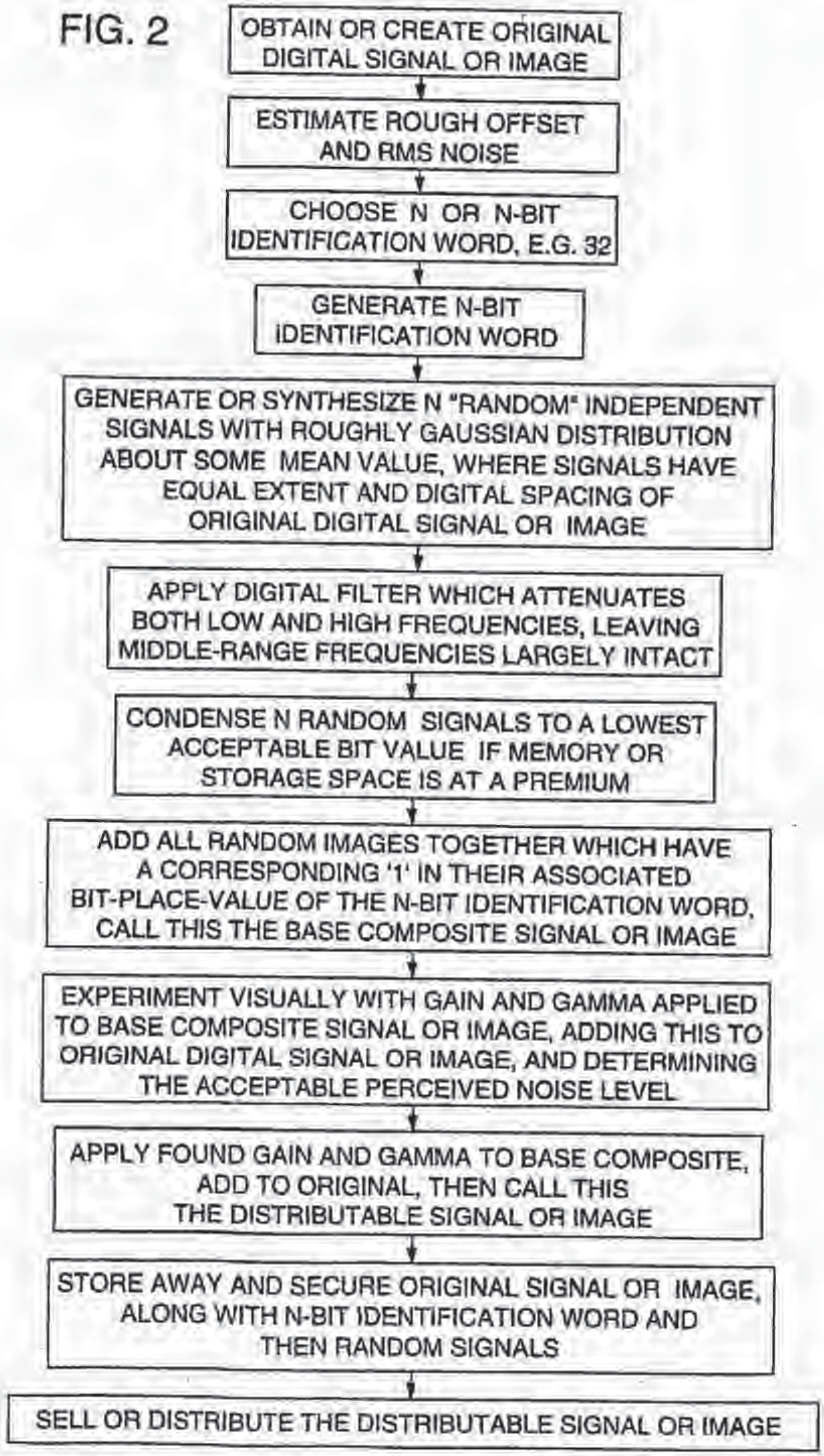

OBTAIN OR CREATE ORIGINAL DIGITAL SIGNAL OR IMAGE
ESTIMATE ROUGH OFFSET AND RMS NOISE
CHOOSE N OR N-BIT IDENTIFICATION WORD, E.G. 32
GENERATE N-BIT IDENTIFICATION WORD
GENERATE OR SYNTHESIZE N "RANDOM" INDEPENDENT SIGNALS WITH ROUGHLY GAUSSIAN DISTRIBUTION ABOUT SOME MEAN VALUE, WHERE SIGNALS HAVE EQUAL EXTENT AND DIGITAL SPACING OF ORIGINAL DIGITAL SIGNAL OR IMAGE
APPLY DIGITAL FILTER WHICH ATTENUATES BOTH LOW AND HIGH FREQUENCIES, LEAVING MIDDLE-RANGE FREQUENCIES LARGELY INTACT
CONDENSE N RANDOM SIGNALS TO A LOWEST ACCEPTABLE BIT VALUE IF MEMORY OR STORAGE SPACE IS AT A PREMIUM
ADD ALL RANDOM IMAGES TOGETHER WHICH HAVE A CORRESPONDING '1' IN THEIR ASSOCIATED BIT-PLACE-VALUE OF THE N-BIT IDENTIFICATION WORD, CALL THIS THE BASE COMPOSITE SIGNAL OR IMAGE
EXPERIMENT VISUALLY WITH GAIN AND GAMMA APPLIED TO BASE COMPOSITE SIGNAL OR IMAGE, ADDING THIS TO ORIGINAL DIGITAL SIGNAL OR IMAGE, AND DETERMINING THE ACCEPTABLE PERCEIVED NOISE LEVEL
APPLY FOUND GAIN AND GAMMA TO BASE COMPOSITE, ADD TO ORIGINAL, THEN CALL THIS THE DISTRIBUTABLE SIGNAL OR IMAGE
STORE AWAY AND SECURE ORIGINAL SIGNAL OR IMAGE, ALONG WITH N-BIT IDENTIFICATION WORD AND THEN RANDOM SIGNALS
SELL OR DISTRIBUTE THE DISTRIBUTABLE SIGNAL OR IMAGE

FIG. 3

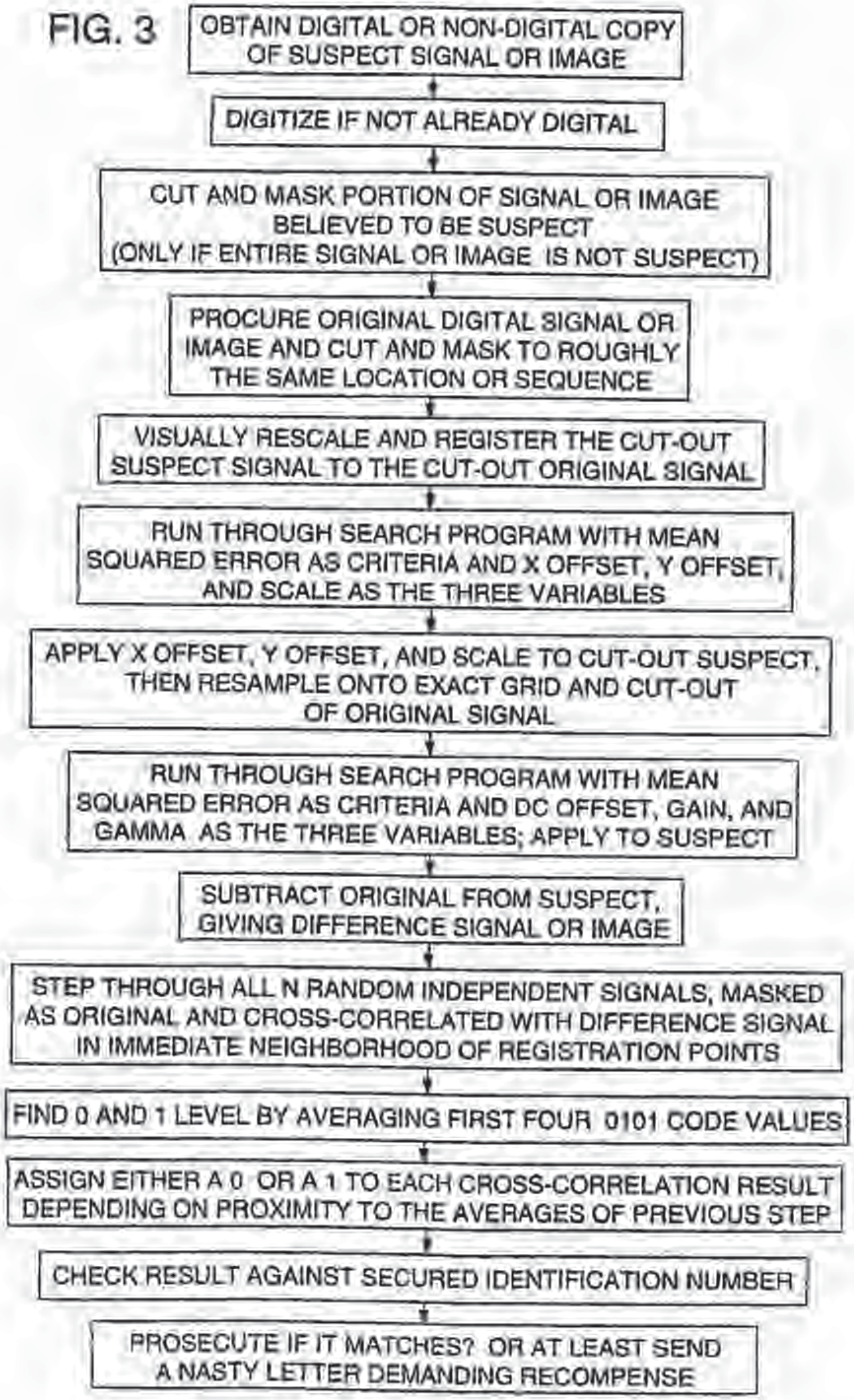

OBTAIN DIGITAL OR NON-DIGITAL COPY OF SUSPECT SIGNAL OR IMAGE
DIGITIZE IF NOT ALREADY DIGITAL
CUT AND MASK PORTION OF SIGNAL OR IMAGE BELIEVED TO BE SUSPECT (ONLY IF ENTIRE SIGNAL OR IMAGE IS NOT SUSPECT)
PROCURE ORIGINAL DIGITAL SIGNAL OR IMAGE AND CUT AND MASK TO ROUGHLY THE SAME LOCATION OR SEQUENCE
VISUALLY RESCALE AND REGISTER THE CUT-OUT SUSPECT SIGNAL TO THE CUT-OUT ORIGINAL SIGNAL
RUN THROUGH SEARCH PROGRAM WITH MEAN SQUARED ERROR AS CRITERIA AND X OFFSET, Y OFFSET, AND SCALE AS THE THREE VARIABLES
APPLY X OFFSET, Y OFFSET, AND SCALE TO CUT-OUT SUSPECT, THEN RESAMPLE ONTO EXACT GRID AND CUT-OUT OF ORIGINAL SIGNAL
RUN THROUGH SEARCH PROGRAM WITH MEAN SQUARED ERROR AS CRITERIA AND DC OFFSET, GAIN, AND GAMMA AS THE THREE VARIABLES; APPLY TO SUSPECT
SUBTRACT ORIGINAL FROM SUSPECT, GIVING DIFFERENCE SIGNAL OR IMAGE
STEP THROUGH ALL N RANDOM INDEPENDENT SIGNALS, MASKED AS ORIGINAL AND CROSS-CORRELATED WITH DIFFERENCE SIGNAL IN IMMEDIATE NEIGHBORHOOD OF REGISTRATION POINTS
FIND 0 AND 1 LEVEL BY AVERAGING FIRST FOUR 0101 CODE VALUES
ASSIGN EITHER A 0 OR A 1 TO EACH CROSS-CORRELATION RESULT DEPENDING ON PROXIMITY TO THE AVERAGES OF PREVIOUS STEP
CHECK RESULT AGAINST SECURED IDENTIFICATION NUMBER
PROSECUTE IF IT MATCHES? OR AT LEAST SEND A NASTY LETTER DEMANDING RECOMPENSE

FIG. 5

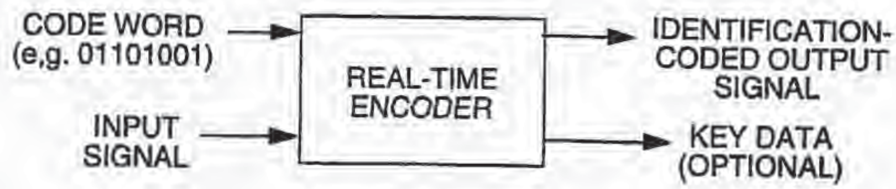
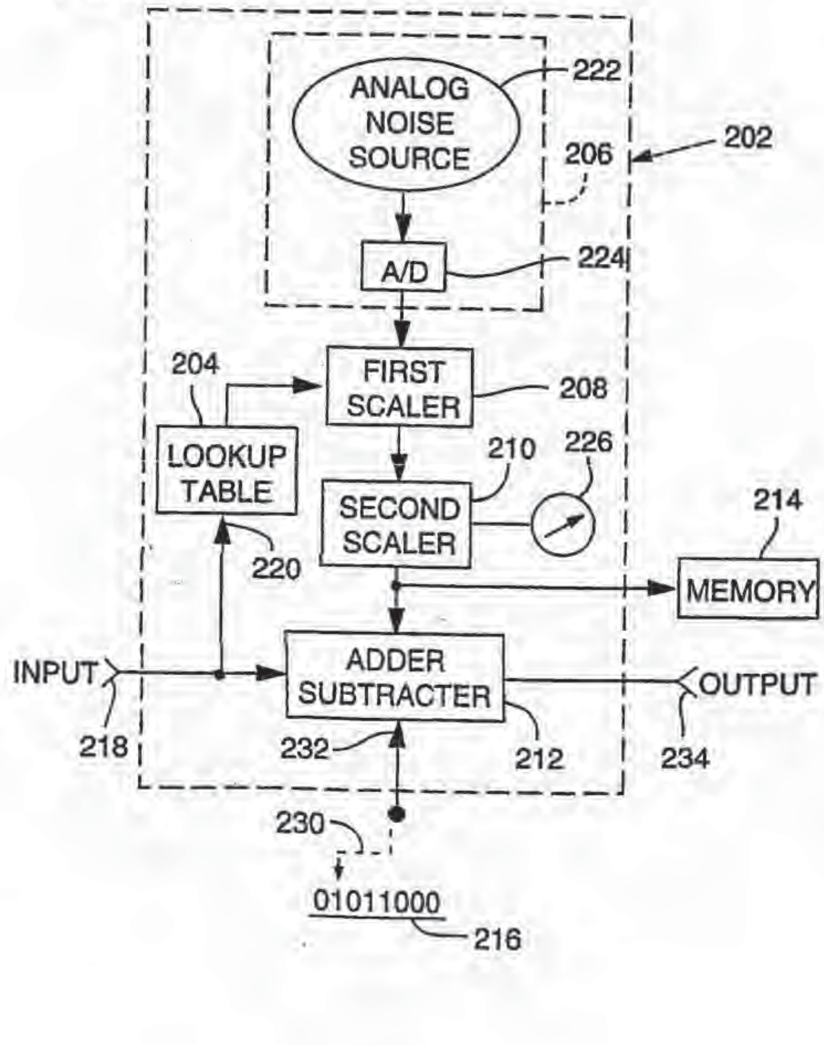

CODE WORD
(e,g. 01101001)
INPUT
SIGNAL
REAL-TIME
ENCODER
IDENTIFICATION-
CODED OUTPUT
SIGNAL
KEY DATA
(OPTIONAL)

FIG. 6


ANALOG
NOISE
SOURCE
222
206
202
A/D
224
204
FIRST
SCALER
208
LOOKUP
TABLE
210
226
SECOND
SCALER
214
220
MEMORY
INPUT
ADDER
SUBTRACTER
OUTPUT
218
232
212
234
230
01011000
216

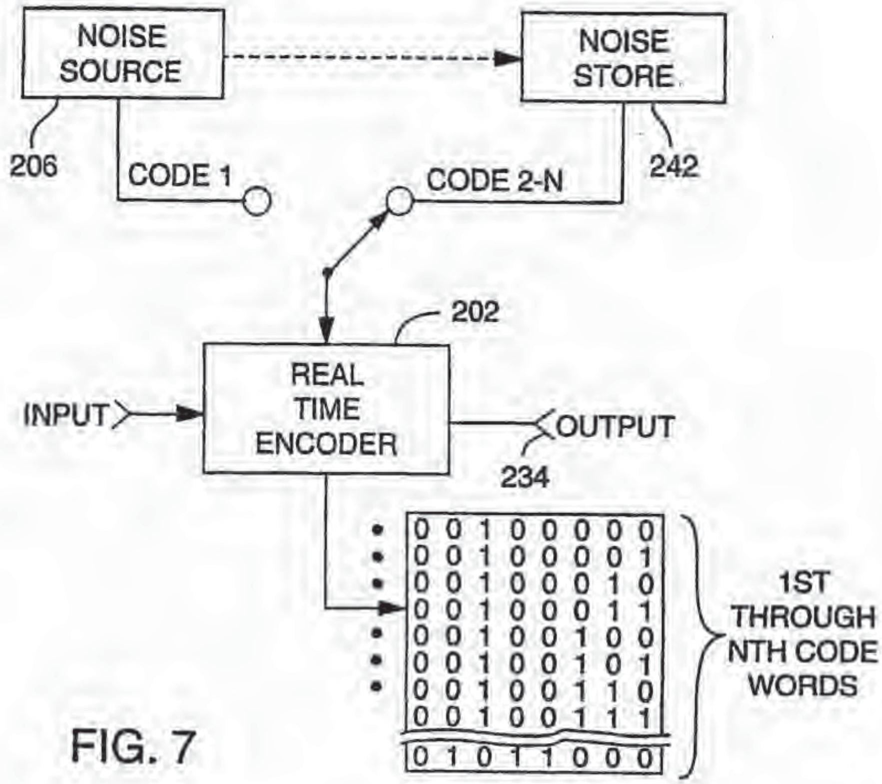

NOISE SOURCE
NOISE STORE
206
242
CODE 1
CODE 2-N
202
REAL TIME ENCODER
INPUT
OUTPUT
234
0 0 1 0 0 0 0 0
0 0 1 0 0 0 0 1
0 0 1 0 0 0 1 0
0 0 1 0 0 0 1 1
0 0 1 0 0 1 0 0
0 0 1 0 0 1 0 1
0 0 1 0 0 1 1 0
0 0 1 0 0 1 1 1
0 1 0 1 1 0 0 0
1ST THROUGH NTH CODE WORDS

FIG. 7

FIG. 8

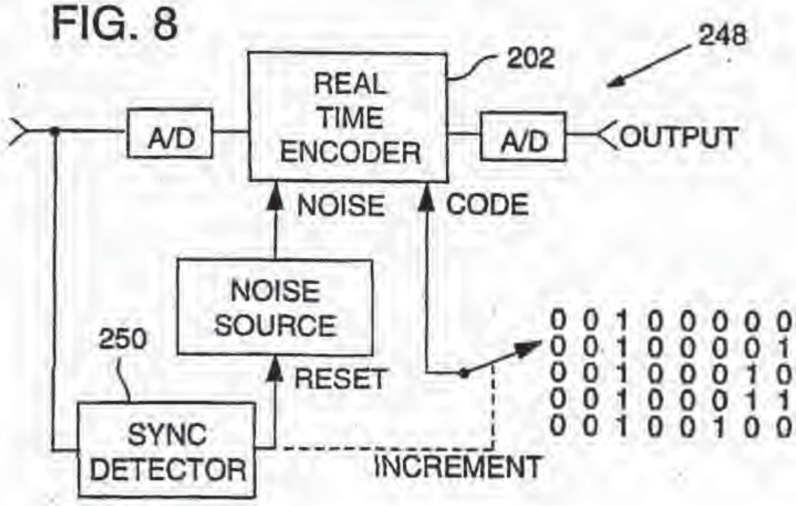

248
202
REAL TIME ENCODER
A/D
A/D
OUTPUT
NOISE
CODE
NOISE SOURCE
250
RESET
SYNC DETECTOR
INCREMENT
0 0 1 0 0 0 0 0
0 0 1 0 0 0 0 1
0 0 1 0 0 0 1 0
0 0 1 0 0 0 1 1
0 0 1 0 0 1 0 0

FIG. 9A

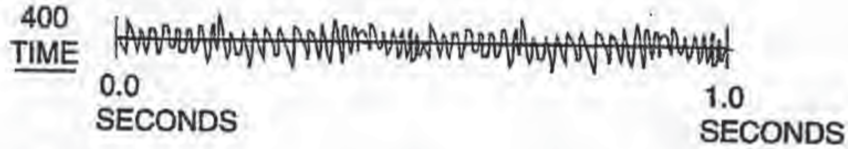


FIG. 9B

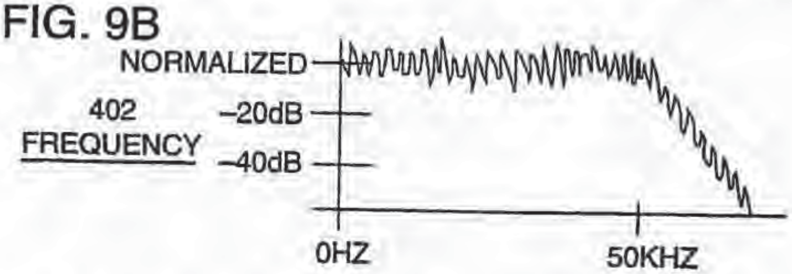


FIG. 9C

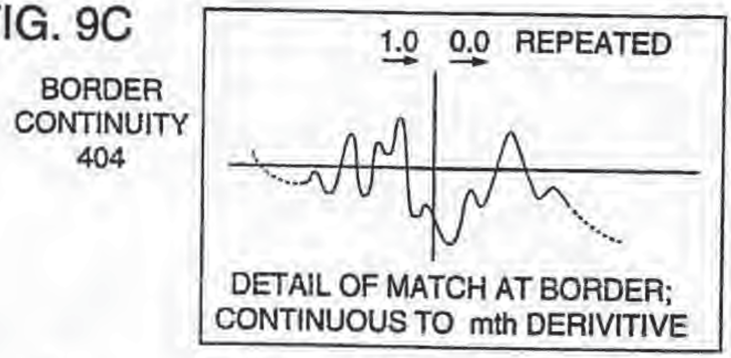


FIG. 10

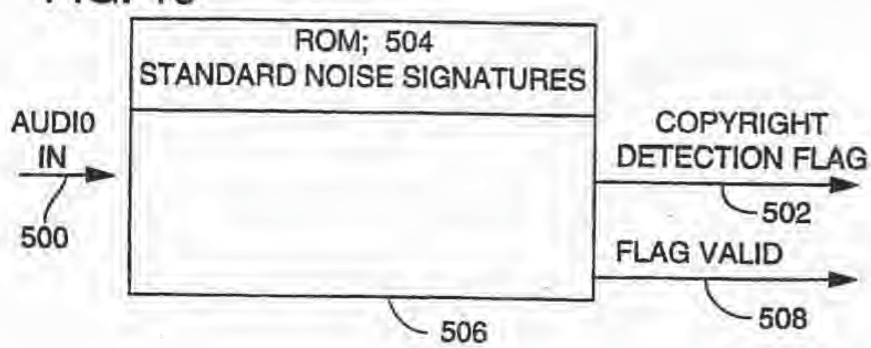


FIG. 11

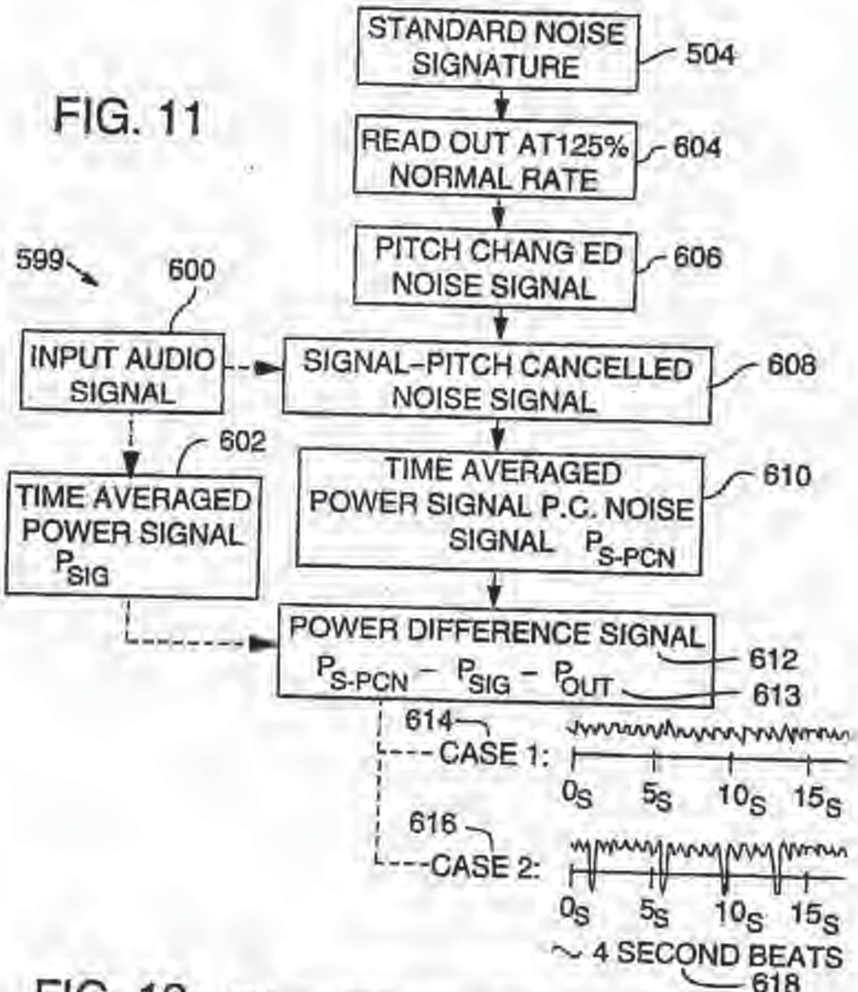
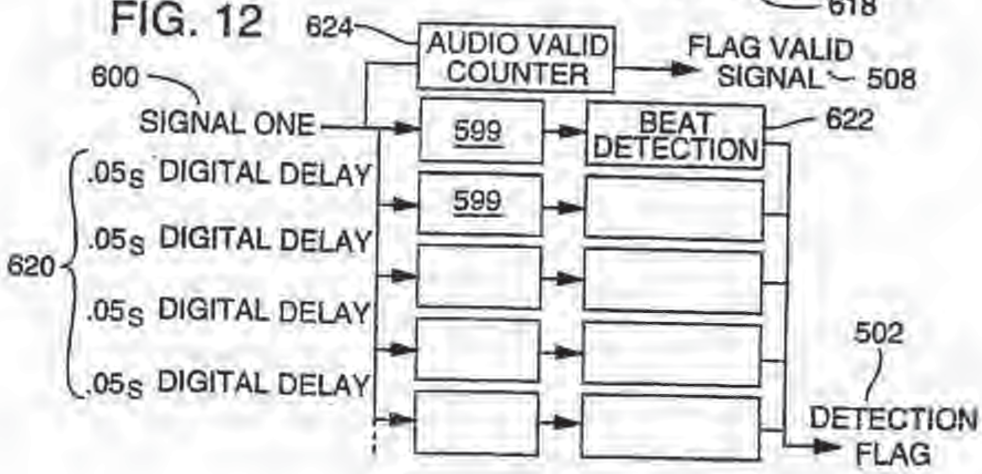

STANDARD NOISE SIGNATURE
504
READ OUT AT125% NORMAL RATE
604
PITCH CHANG ED NOISE SIGNAL
606
599
600
INPUT AUDIO SIGNAL
SIGNAL-PITCH CANCELLED NOISE SIGNAL
608
602
TIME AVERAGED POWER SIGNAL P SIG
TIME AVERAGED POWER SIGNAL P.C. NOISE SIGNAL P S-PCN
610
POWER DIFFERENCE SIGNAL
P S-PCN − P SIG − P OUT
612
613
614
CASE 1:
0S 5S 10S 15S
616
CASE 2:
0S 5S 10S 15S
~ 4 SECOND BEATS
618

FIG. 12


624
AUDIO VALID COUNTER
FLAG VALID SIGNAL
508
600
SIGNAL ONE
599
BEAT DETECTION
622
.05S DIGITAL DELAY
599
.05S DIGITAL DELAY
620
.05S DIGITAL DELAY
.05S DIGITAL DELAY
502
DETECTION FLAG

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04B 1/66, G11B 20/00	A3	(11) International Publication Number: WO 95/14289 (43) International Publication Date: 26 May 1995 (26.05.95)

(21) International Application Number: PCT/US94/13366

(22) International Filing Date: 16 November 1994 (16.11.94)

(30) Priority Data:

154,866	18 November 1993 (18.11.93)	US
215,289	17 March 1994 (17.03.94)	US
327,426	21 October 1994 (21.10.94)	US

(60) Parent Application or Grant
(63) Related by Continuation
US 08/327,426 (CIP)
Filed on 21 October 1994 (21.10.94)

(71) Applicant (*for all designated States except US*): PINECONE IMAGING CORPORATION [US/US]; 363 S.W. Tualatin Loop, West Linn, OR 97068 (US).

(72) Inventor; and
(75) Inventor/Applicant (*for US only*): RHOADS, Geoffrey, B. [US/US]; 363 S.W. Tualatin Loop, West Linn, OR 97068 (US).

(74) Agent: CONWELL, William, Y.; Klarquist, Sparkman, Campbell, Leigh & Whinston, One World Trade Center, Suite 1600, 121 S.W. Salmon Street, Portland, OR 97204 (US).

(81) Designated States: CA, JP, US, European patent (AT, BE, CH, DE, DK, ES, 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.

(88) Date of publication of the international search report: 29 June 1995 (29.06.95)

(54) Title: IDENTIFICATION/AUTHENTICATION CODING METHOD AND APPARATUS

(57) Abstract

An identification code signal is impressed on a carrier to be identified (such as an electronic data signal or a physical medium) in a manner that permits the identification signal later to be discerned and the carrier thereby identified. The method and apparatus are characterized by robustness despite degradation of the encoded carrier, and by holographic permeation of the identification signal throughout the carrier. An exemplary embodiment is a processor that embeds the identification signal onto a carrier signal in real time.

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.

AT	Austria	GB	United Kingdom	MR	Mauritania
AU	Australia	GE	Georgia	MW	Malawi
BB	Barbados	GN	Guinea	NE	Niger
BE	Belgium	GR	Greece	NL	Netherlands
BF	Burkina Faso	HU	Hungary	NO	Norway
BG	Bulgaria	IE	Ireland	NZ	New Zealand
BJ	Benin	IT	Italy	PL	Poland
BR	Brazil	JP	Japan	PT	Portugal
BY	Belarus	KE	Kenya	RO	Romania
CA	Canada	KG	Kyrgystan	RU	Russian Federation
CF	Central African Republic	KP	Democratic People's Republic of Korea	SD	Sudan
CG	Congo	KR	Republic of Korea	SE	Sweden
CH	Switzerland	KZ	Kazakhstan	SI	Slovenia
CI	Côte d'Ivoire	LI	Liechtenstein	SK	Slovakia
CM	Cameroon	LK	Sri Lanka	SN	Senegal
CN	China	LU	Luxembourg	TD	Chad
CS	Czechoslovakia	LV	Latvia	TG	Togo
CZ	Czech Republic	MC	Monaco	TJ	Tajikistan
DE	Germany	MD	Republic of Moldova	TT	Trinidad and Tobago
DK	Denmark	MG	Madagascar	UA	Ukraine
ES	Spain	ML	Mali	US	United States of America
FI	Finland	MN	Mongolia	UZ	Uzbekistan
FR	France			VN	Viet Nam
GA	Gabon				

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 94/13366

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04B1/66 G11B20/00

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)
IPC 6 H04B G11B G06K

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X Y A	GB,A,2 196 167 (THORN EMI) 20 April 1988 see page 1, line 35 - page 2, line 35 ---	1,2,5, 21,22 3 4,9
Y	EP,A,0 411 232 (IBM) 6 February 1991 see page 4, line 7 - line 12 see page 5, line 28 - line 35 ---	3
A	EP,A,0 372 601 (PHILIPS) 13 June 1990 see column 3, line 47 - column 4, line 12 see column 7, line 3 - line 17 ---	1
A	DE,A,38 06 411 (DEUTSCHE THOMSON-BRANDT) 7 September 1989 see column 3, line 5 - column 4, line 25 -----	1

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"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)
"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

"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
"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
"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.
"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
16 May 1995	24.05.95
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Holper, G

Form PCT/ISA/210 (second sheet) (July 1992)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: 0 581 317 A2

(12) # EUROPEAN PATENT APPLICATION

(21) Application number: 93112290.7

(51) Int. Cl.⁵: G07D 7/00, G07F 7/12

(22) Date of filing: 30.07.93

(30) Priority: 31.07.92 US 923841

(43) Date of publication of application:
02.02.94 Bulletin 94/05

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(71) Applicant: INTERACTIVE HOME SYSTEMS
17950 N.E. 65th Street
Redmond, Washington 98052(US)

(72) Inventor: Powell, Robert D.
13720 - 246th Avenue Southeast
Issaquah, Washington 98027(US)
Inventor: Nitzberg, Mark J.
20A Prescott Street No.3B
Cambridge, Massachusetts 02138(US)

(74) Representative: Patentanwälte Grünecker, Kinkeldey, Stockmair & Partner
Maximilianstrasse 58
D-80538 München (DE)

(54) **Method and system for digital image signatures.**

(57) A method and system for embedding signatures within visual images in both digital representation and print or film. A signature is inseparably embedded within the visible image, the signature persisting through image transforms that include resizing as well as conversion to print or film and back to digital form. Signature points are selected from among the pixels of an original image. The pixel values of the signature points and surrounding pixels are adjusted by an amount detectable by a digital scanner. The adjusted signature points form a digital signature which is stored for future identification of subject images derived from the image. In one embodiment, a signature is embedded within an image by locating relative extrema in the continuous space of pixel values and selecting the signature points from among the extrema. Preferably, the signature is redundantly embedded in the image such that any of the redundant representations can be used to identify the signature. Identification of a subject image includes ensuring that the subject image is normalized with respect to the original image or the signed image. Preferably, the normalized subject image is compared with the stored digital signature.

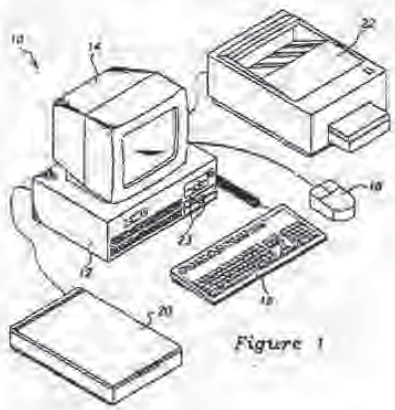


Figure 1

EP 0 581 317 A2

Rank Xerox (UK) Business Services
(3. 10/3.09/3.5.4)

Technical Field

This invention relates to a method of and system for encoding a signature into a digital image and auditing a digital subject image to determine if it was derived from the encoded image.

Background of the Invention

Various images in traditional print or photographic media are commonly distributed to many users. Examples include the distribution of prints of paintings to the general public and photographs and film clips to and among the media. Owners may wish to audit usage of their images in print and electronic media, and so require a method to analyze print, film and digital images to determine if they were obtained directly from the owners or derived from their images. For example, the owner of an image may desire to limit access or use of the image. To monitor and enforce such a limitation, it would be beneficial to have a method of verifying that a subject image is copied or derived from the owner's image. The method of proof should be accurate and incapable of being circumvented. Further, the method should be able to detect unauthorized copies that have been resized, rotated, cropped, or otherwise altered slightly.

In the computer field, digital signatures have been applied to non-image digital data in order to identify the origin of the data. For various reasons these prior art digital signatures have not been applied to digital image data One reason is that these prior art digital signatures are lost if the data to which they are applied are modified. Digital images are often modified each time they are printed, scanned, copied, or photographed due to unintentional "noise" created by the mechanical reproduction equipment used. Further, it is often desired to resize, rotate, crop or otherwise intentionally modify the image. Accordingly, the existing digital signatures are unacceptable for use with digital images.

Summary of the Invention

The invention includes a method and system for embedding image signatures within visual images, applicable in the preferred embodiments described herein to digital representations as well as other media such as print or film. The signatures identify the source or ownership of images and distinguish between different copies of a single image. In preferred embodiments, these signatures persist through image transforms such as resizing and conversion to or from print or film and so provide a method to track subsequent use of digital images including derivative images in print or other form.

In a preferred embodiment described herein, a plurality of signature points are selected that are positioned within an original image having pixels with pixel values. The pixel values of the signature points are adjusted by an amount detectable by a digital scanner. The adjusted signature points form a digital signature that is stored for future identification of subject images derived from the image.

The preferred embodiment of the invention described herein embeds a signature within the original image by locating candidate points such as relative extrema in the pixel values. Signature points are selected from among the candidate points and a data bit is encoded at each signature point by adjusting the pixel value at and surrounding each point. Preferably, the signature is redundantly embedded in the image such that any of the redundant representations can be used to identify the signature. The signature is stored for later use in identifying a subject image.

According to a preferred embodiment, the identification of a subject image includes ensuring that the subject image is normalized, i.e., of the same size, rotation, and brightness level as the original image. If not already normalized, the subject image is normalized by aligning and adjusting the luminance values of subsets of the pixels in the subject image to match corresponding subsets in the original image. The normalized subject image is then subtracted from the original image and the result is compared with the stored digital signature. In an alternate embodiment, the normalized subject image is compared directly with the signed image.

Brief Description of the Drawings

Figure 1 is a diagram of a computer system used in a preferred embodiment of the present invention.

Figure 2 is a sample digital image upon which a preferred embodiment of the present invention is employed.

Figure 3 is a representation of a digital image in the form of an array of pixels with pixel values.

Figure 4 is graphical representation of pixel values showing relative minima and maxima pixel values.

Figure 5 is a digital subject image that is compared to the image of Figure 2 according to a preferred embodiment of the present invention.

Detailed Description of the Invention

The present invention includes a method and system for embedding a signature into an original image to create a signed image. A preferred embodiment includes selecting a large number of candidate points in the original image and selecting a number of signature points from among the candidate points. The signature points are altered slightly to form the signature. The signature points are stored for later use in auditing a subject image to determine whether the subject image is derived from the signed image.

The signatures are encoded in the visible domain of the image and so become part of the image and cannot be detected or removed without prior knowledge of the signature. A key point is that while the changes manifested by the signature are too slight to be visible to the human eye, they are easily and consistently recognizable by a common digital image scanner, after which the signature is extracted, interpreted and verified by a software algorithm.

In contrast to prior art signature methods used on non-image data, the signatures persist through significant image transformations that preserve the visible image but may completely change the digital data. The specific transforms allowed include resizing the image larger or smaller, rotating the image, uniformly adjusting color, brightness and/or contrast, and limited cropping. Significantly, the signatures persist through the process of printing the image to paper or film and rescanning it into digital form.

Shown in Figure 1 is a computer system 10 that is used to carry out an embodiment of the present invention. The computer system 10 includes a computer 12 having the usual complement of memory and logic circuits, a display monitor 14, a keyboard 16, and a mouse 18 or other pointing device. The computer system also includes a digital scanner 20 that is used to create a digital image representative of an original image such as a photograph or painting. Typically, delicate images, such as paintings, are converted to print or film before being scanned into digital form. In one embodiment a printer 22 is connected to the computer 12 to print digital images output from the processor. In addition, digital images can be output in a data format to a storage medium 23 such as a floppy disk for displaying later at a remote site. Any digital display device may be used, such a common computer printer, X-Y plotter, or a display screen.

An example of the output of the scanner 20 to the computer 12 is a digital image 24 shown in Figure 2. More accurately, the scanner outputs data representative of the digital image and the computer causes the digital image 24 to be displayed on the display monitor 14. As used herein "digital image" refers to the digital data representative of the digital image, the digital image displayed on the monitor or other display screen, and the digital image printed by the printer 22 or a remote printer.

The digital image 24 is depicted using numerous pixels 24 having various pixel values. In the gray-scale image 24 the pixel values are luminance values representing a brightness level varying from black to white. In a color image the pixels have color values and luminance values, both of which being pixel values. The color values can include the values of any components in a representation of the color by a vector. Figure 3 shows digital image 24A in the form of an array of pixels 26. Each pixel is associated with one or more pixel values, which in the example shown in Figure 3 are luminance values from 0 to 15.

The digital image 24 shown in Figure 2 includes thousands of pixels. The digital image 24A represented in Figure 3 includes 225 pixels. The invention preferably is used for images having pixels numbering in the millions. Therefore, the description herein is necessarily a simplistic discussion of the utility of the invention.

According to a preferred embodiment of the invention numerous candidate points are located within the original image. Signature points are selected from among the candidate points and are altered to form a signature. The signature is a pattern of any number of signature points. In a preferred embodiment, the signature is a binary number between 16 and 32 bits in length. The signature points may be anywhere within an image, but are preferably chosen to be as inconspicuous as possible. Preferably, the number of signature points is much greater than the number of bits in a signature. This allows the signature to be redundantly encoded in the image. Using a 16 to 32 bit signature, 50-200 signature points are preferable to obtain multiple signatures for the image.

A preferred embodiment of the invention locates candidate points by finding relative maxima and minima, collectively referred to as extrema, in the image. The extrema represent local extremes of luminance or color. Figure 4 shows what is meant by relative extrema. Figure 4 is a graphical representation of the pixel values of a small portion of a digital image. The vertical axis of the graph shows pixel values while the horizontal axis shows pixel positions along a single line of the digital image. Small undulations in pixel values, indicated at 32, represent portions of the digital image where only small changes in luminance or color occur between pixels. A relative maximum 34 represents a pixel that has the highest pixel value for a given area of the image. Similarly, a relative minimum 36 represents a pixel that has the lowest pixel value for a given area of the image.

Relative extrema are preferred signature points for two major reasons. First, they are easily located by simple, well known processing. Second, they allow signature points to be encoded very inconspicuously.

One of the simplest methods to determine relative extrema is to use a "Difference of Averages" technique. This technique employs predetermined neighborhoods around each pixel 26; a small neighborhood 28 and a large neighborhood 30, as shown in Figures 2 and 3. In the present example the neighborhoods are square for simplicity, but a preferred embodiment employs circular neighborhoods. The technique determines the difference between the average pixel value in the small neighborhood and the average pixel value of the large neighborhood. If the difference is large compared to the difference for surrounding pixels then the first pixel value is a relative maxima or minima.

Using the image of Figure 3 as an example, the Difference of Averages for the pixel 26A is determined as follows. The pixel values within the 3x3 pixel small neighborhood 28A add up to 69; dividing by 9 pixels gives an average of 7.67. The pixel values within the 5x5 pixel large neighborhood 30A add up to 219; dividing by 25 pixels gives an average of 8.76 and a Difference of Averages of -1.09. Similarly, the average in small neighborhood 28G is 10.0; the average in large neighborhood 30G is 9.8; the Difference of Averages for pixel 26G is therefore 0.2. Similar computations on pixels 26B-26F produce the following table:

	26A	26B	26C	26D	26E	26F	26G
Small Neighborhood	7.67	10.56	12.89	14.11	13.11	11.56	10.0
Large Neighborhood	8.76	10.56	12.0	12.52	12.52	11.36	9.8
Difference of Averages	-1.09	0.0	0.89	1.59	0.59	0.2	0.2

Based on pixels 26A-26G, there may be a relative maximum at pixel 26D, whose Difference of Averages of 1.59 is greater than the Difference of Averages for the other examined pixels in the row. To determine whether pixel 26D is a relative maximum rather than merely a small undulation, its Difference of Averages must be compared with the Difference of Averages for the pixels surrounding it in a larger area.

Preferably, extrema within 10% of the image size of any side are not used as signature points. This protects against loss of signature points caused by the practice of cropping the border area of an image. It is also preferable that relative extrema that are randomly and widely spaced are used rather than those that appear in regular patterns.

Using the Difference of Averages technique or other known techniques, a large number of extrema are obtained, the number depending on the pixel density and contrast of the image. Of the total number of extrema found, a preferred embodiment chooses 50 to 200 signature points. This may be done manually by a user choosing with the keyboard 16, mouse 18, or other pointing device each signature point from among the extrema displayed on the display monitor 14. The extrema may be displayed as a digital image with each point chosen by using the mouse or other pointing device to point to a pixel or they may be displayed as a list of coordinates which are chosen by keyboard, mouse, or other pointing device. Alternatively, the computer 12 can be programmed to choose signature points randomly or according to a preprogrammed pattern.

One bit of binary data is encoded in each signature point in the image by adjusting the pixel values at and surrounding the point. The image is modified by making a small, preferably 2%-10% positive or negative adjustment in the pixel value at the exact signature point, to represent a binary zero or one. The pixels surrounding each signature point, in approximately a 5 x 5 to 10 x 10 grid, are preferably adjusted proportionally to ensure a continuous transition to the new value at the signature point. A number of bits are encoded in the signature points to form a pattern which is the signature for the image.

In a preferred embodiment, the signature is a pattern of all of the signature points. When auditing a subject image, if a statistically significant number of potential signature points in the subject image match corresponding signature points in the signed image, then the subject image is deemed to be derived from the signed image. A statistically significant number is somewhat less than 100%, but enough to be reasonably confident that the subject image was derived from the signed image.

In an alternate embodiment, the signature is encoded using a redundant pattern that distributes it among the signature points in a manner that can be reliably retrieved using only a subset of the points. One embodiment simply encodes a predetermined number of exact duplicates of the signature. Other redundant representation methods, such as an error-correcting code, may also be used.

In order to allow future auditing of images to determine whether they match the signed image, the signature is stored in a database in which it is associated with the original image. The signature can be stored by associating the bit value of each signature point together with x-y coordinates of the signature point. The signature may be stored separately or as part of the signed image. The signed image is then distributed in digital form.

As discussed above, the signed image may be transformed and manipulated to form a derived image. The derived image is derived from the signed image by various transformations, such as resizing, rotating, adjusting color, brightness and/or contrast, cropping and converting to print or film. The derivation may take place in multiple steps or processes or may simply be the copying of the signed image directly.

It is assumed that derivations of these images that an owner wishes to track include only applications which substantially preserve the resolution and general quality of the image. While a size reduction by 90%, a significant color alteration or distinct-pixel-value reduction may destroy the signature, they also reduce the image's significance and value such that no auditing is desired.

In order to audit a subject image according to a preferred embodiment, a user identifies the original image of which the subject image is suspected of being a duplicate. For a print or film image, the subject image is scanned to create a digital image file. For a digital image, no scanning is necessary. The subject digital image is normalized using techniques as described below to the same size, and same overall brightness, contrast and color profile as the unmodified original image. The subject image is analyzed by the method described below to extract the signature, if present, and compare it to any signatures stored for that image.

The normalization process involves a sequence of steps to undo transformations previously made to the subject image, to return it as close as possible to the resolution and appearance of the original image. It is assumed that the subject image has been manipulated and transformed as described above. To align the subject image with the original image, a preferred embodiment chooses three or more points from the subject image which correspond to points in the original image. The three or more points of the subject image are aligned with the corresponding points in the original image. The points of the subject image not selected are rotated and resized as necessary to accommodate the alignment of the points selected.

For example, Figure 5 shows a digital subject image 38 that is smaller than the original image 24 shown in Figure 2. To resize the subject image, a user points to three points such as the mouth 40B, ear 42B and eye 44B of the subject image using the mouse 18 or other pointer. Since it is usually difficult to accurately point to a single pixel, the computer selects the nearest extreme to the pixel pointed to by the user. The user points to the mouth 40A, ear 42A, and eye 44A of the original image. The computer 12 resizes and rotates the subject image as necessary to ensure that points 40B, 42B and 44B are positioned with respect to each other in the same way that points 40A, 42A, and 44A are positioned with respect to each other in the original image. The remaining pixels are repositioned in proportion to the repositioning of points 40B, 42B and 44B. By aligning three points the entire subject image is aligned with the original image without having to align each pixel independently.

After the subject image is aligned, the next step is to normalize the brightness, contrast and/or color of the subject image. Normalizing involves adjusting pixel values of the subject image to match the value-distribution profile of the original image. This is accomplished by a technique analogous to that used to align the subject image. A subset of the pixels in the subject image are adjusted to equal corresponding pixels in the original image. The pixels not in the subset are adjusted in proportion to the adjustments made to the pixels in the subset. The pixels of the subject image corresponding to the signature points should not be among the pixels in the subset. Otherwise any signature points in the subject image will be hidden from detection when they are adjusted to equal corresponding pixels in the original image.

In a preferred embodiment, the subset includes the brightest and darkest pixels of the subject image. These pixels are adjusted to have luminance values equal to the luminance values of corresponding pixels in the original image. To ensure that any signature points can be detected, no signature points should be selected during the signature embedding process described above that are among the brightest and darkest pixels of the original image. For example, one could use pixels among the brightest and darkest 3% for the adjusting subset, after selecting signature points among less than the brightest and darkest 5% to ensure that there is no overlap.

When the subject image is fully normalized, it is preferably compared to the original image. One way to compare images is to subtract one image from the other. The result of the subtraction is a digital image that includes any signature points that were present in the subject image. These signature points, if any, are compared to the stored signature points for the signed image. If the signature points do not match, then the subject image is not an image derived from the signed image, unless the subject image was changed substantially from the signed image.

In an alternative embodiment, the normalized subject image is compared directly with the signed image instead of subtracting the subject image from the original image. This comparison involves subtracting the subject image from the signed image. If there is little or no image resulting from the subtraction then the subject image equals to the signed image, and therefore has been derived from the signed image.

In another alternate embodiment instead of normalizing the entire subject image, only a section of the subject image surrounding each potential signature point is normalized to be of the same general resolution and appearance as a corresponding section of the original image. This is accomplished by selecting each potential signature point of the subject image and selecting sections surrounding each potential signature point. The normalization of each selected section proceeds according to methods similar to those disclosed above for normalizing the entire subject image.

Normalizing each selected section individually allows each potential signature point of the subject image to be compared directly with a corresponding signature point of the signed image. Preferably, an average is computed for each potential signature point by averaging the pixel value of the potential signature point with the pixel values of a plurality of pixels surrounding the potential signature point. The average computed for each signature is compared directly with a corresponding signature point of the signed image.

While the methods of normalizing and extracting a signature from a subject image as described above are directed to luminance values, similar methods may be used for color values. Instead of or in addition to normalizing by altering luminance values, the color values of the subject image can also be adjusted to equal corresponding color values in an original color image. However, it is not necessary to adjust color values in order to encode a signature in or extract a signature from a color image. Color images use pixels having pixel values that include luminance values and color values. A digital signature can be encoded in any pixel values regardless of whether the pixel values are luminance values, color values, or any other type of pixel values. Luminance values are preferred because alterations may be made more easily to luminance values without the alterations being visible to the human eye.

From the foregoing it will be appreciated that, although specific embodiments of the invention have been described herein for purposes of illustration, various modifications may be made without deviating from the spirit and scope of the invention. Accordingly, the invention is not limited except as by the appended claims.

Claims

1. A method of image signature processing of an original image having pixels with luminance values, comprising:

   locating a plurality of candidate points from among the pixels of the original image;

   selecting a first plurality of signature points from among the candidate points;

   adjusting the pixel values of the signature points to form a signed image, the adjusted signature point pixel values forming a signature for the signed image; and

   storing the signature for future identification.

2. The method according to claim 1 wherein the candidate points are located by locating relative extrema in the original image and wherein the selecting step includes selecting the signature points from among the extrema.

3. The method according to claim 2 wherein the extrema are relative minima or maxima of luminance values of the pixels of the original image.

4. The method according to claim 1, further comprising adjusting a plurality of pixel values surrounding the signature points to provide smooth transitions to the adjusted pixel values at the signature points.

5. The method according to claim 1, further comprising:

   selecting a second plurality of signature points from among the candidate points; and

   adjusting the pixel values of the second plurality of signature points to form a redundant signature for the signed image.

6. A method of image signature processing of an original image having pixels with pixel values, comprising:

   selecting a first plurality of signature points from among the pixels of the original image;

   adjusting the pixel values of the signature points, the adjusted signature point pixel values forming a signature for the image; and storing the signature for future identification.

7. The method according to claim 6, further comprising locating relative extrema in the original image and wherein the selecting step includes selecting the signature points from among the extrema.

8. The method according to claim 7 wherein the extrema are relative minima or maxima of luminance values of the pixels of the original image.

9. The method according to claim 6 further comprising:
selecting a second plurality of signature points from among the candidate points; and
adjusting the pixel values of the second plurality of signature points to form a redundant signature for the signed image.

10. The method according to claim 6 wherein the digital image has a border surrounding the image and the pixel values adjusted are selected so as not to be within a predetermined distance from the border.

11. The method according to claim 6, further comprising adjusting a plurality of pixel values surrounding the signature points to provide smooth transitions to the adjusted pixel values at the signature points.

12. The method according to claim 6 wherein the pixel values adjusted are luminance values.

13. The method according to claim 6 wherein the pixel values adjusted are color values.

14. The method according to claim 6, further comprising analyzing whether a digital subject image constitutes or is derived from a signed image having pixel values that were adjusted to form a signature according to claim 6.

15. The method according to claim 14 wherein the analyzing step includes normalizing the subject image.

16. The method according to claim 15 wherein the normalizing step includes aligning the subject image with the signed image or the original image.

17. The method according to claim 16 wherein the aligning step includes selecting three or more pixels in the subject image and aligning the three or more peels with corresponding pixels in the original or the signed image.

18. The method according to claim 15 wherein the pixel values of the subject image and the original image include luminance values and the normalizing step includes adjusting the luminance values of a subset of the pixels in the subject image to equal the luminance values of a corresponding subset of pixels in the original image.

19. The method according to claim 14 wherein the analyzing step includes subtracting the subject image from the original image to obtain a resulting image and comparing the resulting image with the stored signature.

20. The method according to claim 14 wherein the analyzing step includes comparing the subject image with the signed image.

21. The method according to claim 14 wherein the analyzing step includes selecting a potential signature point in the subject image corresponding to a signature point of the signed image and comparing the pixel value of the selected point to the pixel value of the corresponding signature point of the signed image.

22. The method according to claim 14 wherein the analyzing step includes selecting a potential signature point in the subject image corresponding to a signature point of the signed image, computing an average of pixel values of the potential signature point and a plurality of pixels surrounding the potential signature point, and comparing the average to the pixel value of the corresponding signature point of the signed image.

23. A method of determining whether a subject image having pixels with pixel values constitutes or is derived from a signed image having pixels with pixel values that have been adjusted to collectively form a signature, comprising:
ensuring that the subject image is normalized with respect to an original image or the signal image;
comparing the signature of the signed image with potential signature points of the subject image corresponding to the pixels of the signature.

24. The method according to claim 23 wherein the ensuring step includes normalizing the subject image with respect to the original image or the signed image.

25. The method according to claim 24 wherein the normalizing step includes aligning the subject image with the signal image or the original image.

26. The method according to claim 25 wherein the aligning step includes selecting three or more pixels in the subject image and aligning the three or more pixels with a like number of pixels in the original or signed image.

27. The method according to claim 24 wherein the pixel values of the subject image and the original image include luminance values and the normalizing step includes adjusting the luminance values of a subset of the pixels in the subject image to equal the luminance value of a corresponding subset of pixels in the original image.

28. The method according to claim 23 wherein the comparing step includes subtracting the subject image from the original image to obtain a resulting image and comparing the resulting image with the stored digital signature.

29. The method according to claim 23 wherein the comparing step includes comparing the subject image with the signed image.

30. The method according to claim 23 wherein the comparing step includes selecting the potential signature points corresponding to pixels of the signature, computing an average of the pixel values of each potential signature point and a plurality of pixels surrounding each signature point, and comparing each average to the pixel value of the corresponding signature point of the signed image.

31. A system for image signature processing of an original image having pixels with pixel values, comprising:
a display device for displaying digital images to a user;
selection means for selecting a plurality of signature points from among the pixels of the original image;
a computing device in communication with the display device and the selection means, the computing device adjusting the pixel values of the signature points to form a signed image, the adjusted signature point pixel values forming a signature associated with the signed image; and
memory in communication with the computing device, the memory receiving the signature from the computing device and storing the signature for future identification.

32. The system according to claim 31 wherein the computing device includes location means for locating candidate points from among the pixels in the original image and the selecting means selects signature points from among the candidate points.

33. The system according to claim 32 wherein the selection means includes a pointer operatively connected to the display device and the computing device such that a user can select signature points from among the candidate points displayed on the display device and the computing device alters the signature points selected to form a signature associated with the signed image.

34. The system according to claim 32 wherein the location means includes means for locating pixel value extrema in the original image, the extrema being the candidate points.

35. The system according to claim 31 wherein the computing device includes means for identifying a subject image derived from the signed image.

36. The system according to claim 35, further comprising normalizing means for normalizing the subject image with the original image or the signed image.

37. The system according to claim 36 wherein the normalizing means includes a pointer operatively connected to the display device and the computing device such that a user can select alignment points from among the pixels of the subject image displayed on the display device and the computing device receives the alignment points selected and aligns the subject image with the original image or the signed image in response thereto.

38. The system according to claim 36 wherein the computing device includes comparing means for comparing the normalized subject image with the original image or the signed image.

39. The system according to claim 36 wherein the computing device includes:
subject selection means for selecting a potential signature point on the subject image corresponding to a signature point of the signed image;
averaging means for computing an average of the pixel values of the potential signature point and a plurality of pixels surrounding the potential signature point; and
comparing means for comparing the average to a pixel value of the corresponding signature point of the signed image.

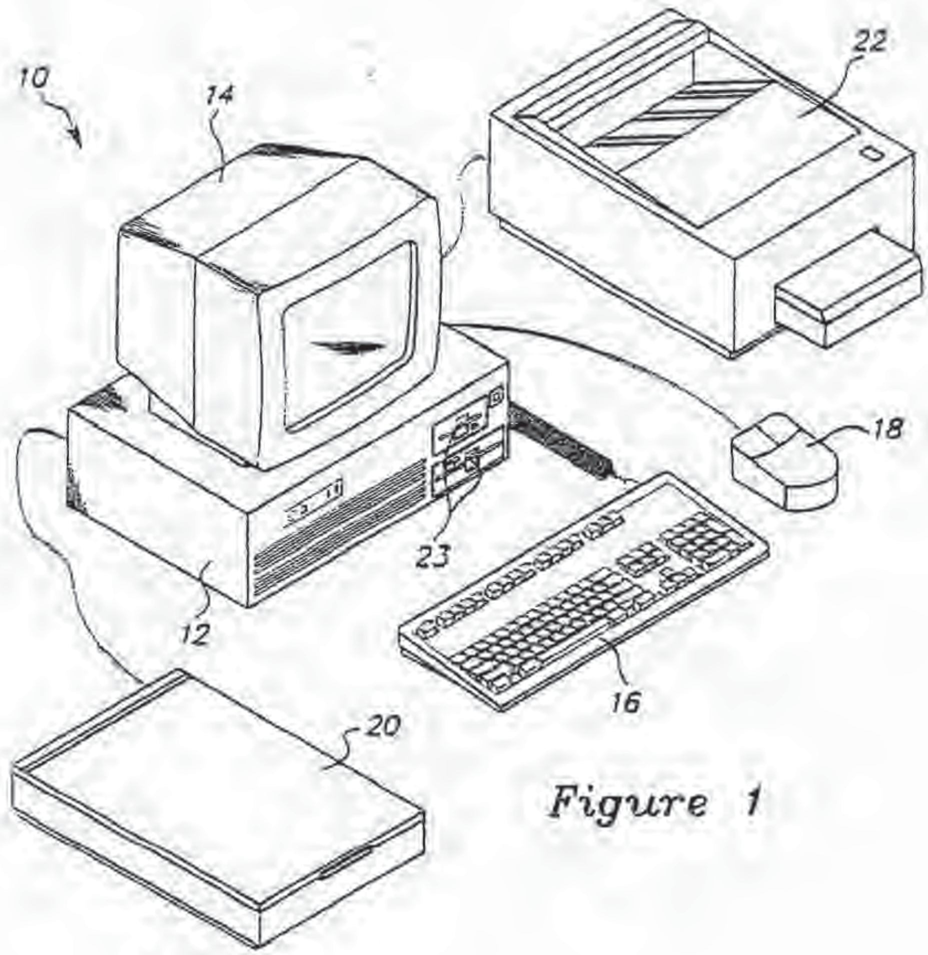


Figure 1

Figure 4

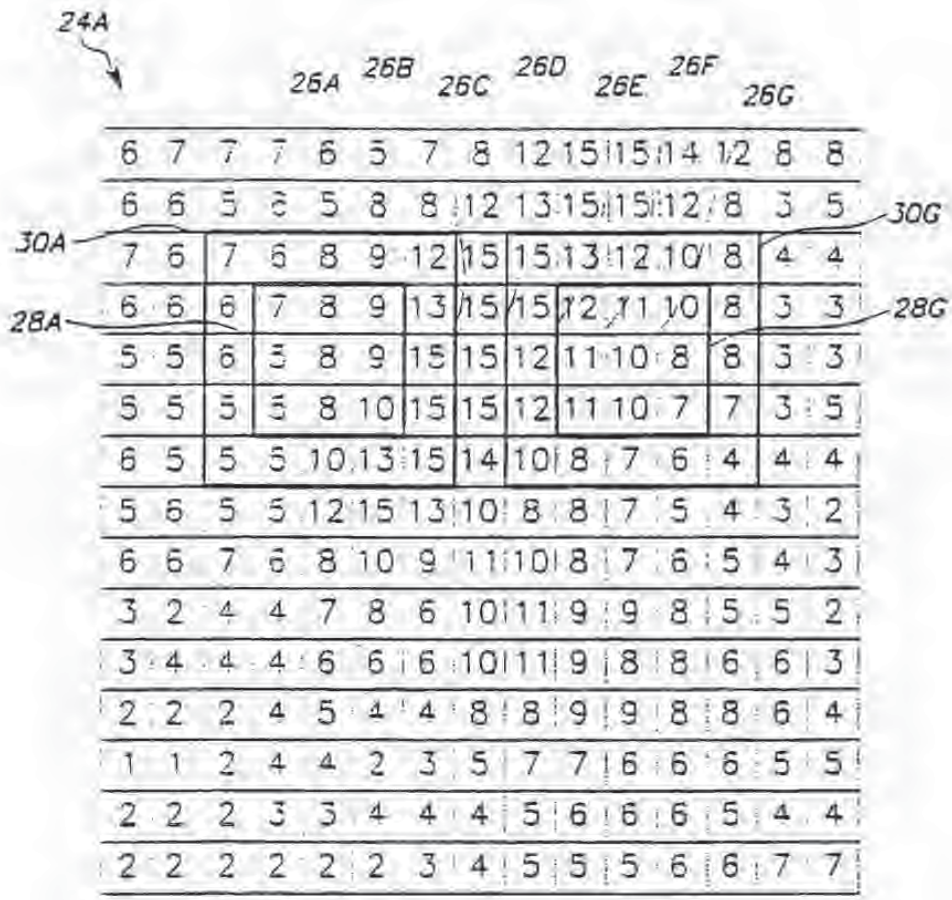

24A
26A
26B
26C
26D
26E
26F
26G
30A
30G
28A
28G
6 7 7 7 6 5 7 8 12 15 15 14 12 8 8
6 6 5 6 5 8 8 12 13 15 15 12 8 3 5
7 6 7 6 8 9 12 15 15 13 12 10 8 4 4
6 6 6 7 8 9 13 15 15 12 11 10 8 3 3
5 5 6 5 8 9 15 15 12 11 10 8 8 3 3
5 5 5 5 8 10 15 15 12 11 10 7 7 3 5
6 5 5 5 10 13 15 14 10 8 7 6 4 4 4
5 6 5 5 12 15 13 10 8 8 7 5 4 3 2
6 6 7 6 8 10 9 11 10 8 7 6 5 4 3
3 2 4 4 7 8 6 10 11 9 9 8 5 5 2
3 4 4 4 6 6 6 10 11 9 8 8 6 6 3
2 2 2 4 5 4 4 8 8 9 9 8 8 6 4
1 1 2 4 4 2 3 5 7 7 6 6 6 5 5
2 2 2 3 3 4 4 4 5 6 6 6 5 4 4
2 2 2 2 2 2 3 4 5 5 5 6 6 7 7

Figure 3

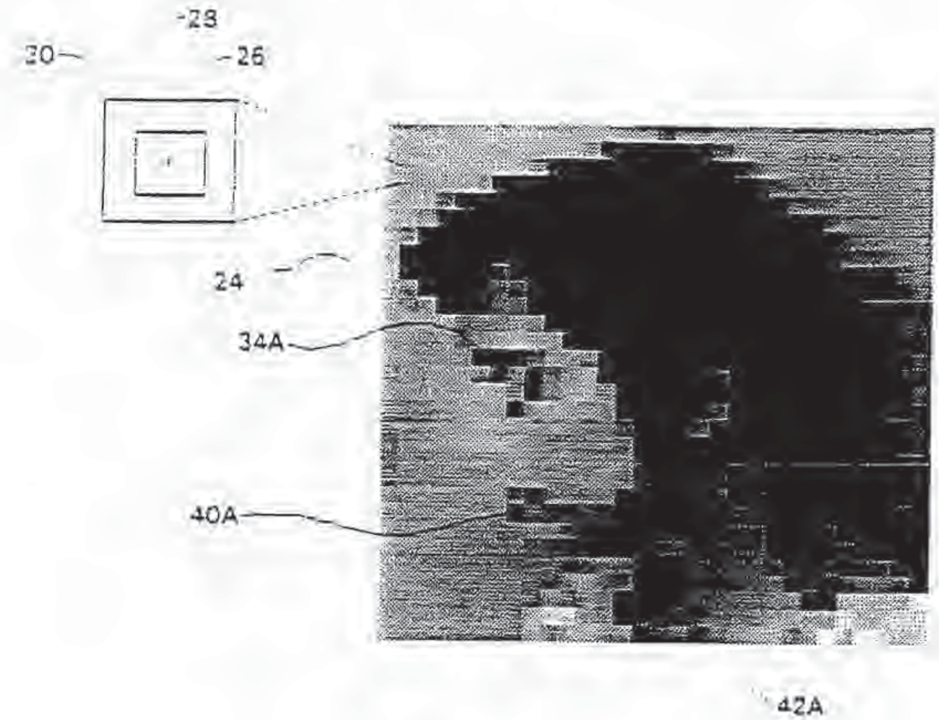


Figure 2

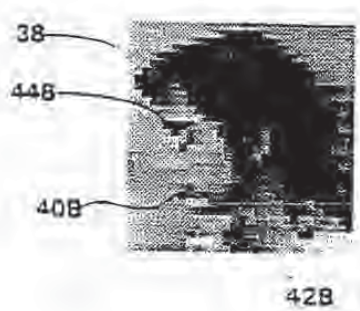


Figure 5

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 581 317 A3

(12) EUROPEAN PATENT APPLICATION

(88) Date of publication A3:
01.05.1996 Bulletin 1996/18

(51) Int. Cl.[6] G07D 7/00, G07F 7/12

(43) Date of publication A2:
02.02.1994 Bulletin 1994/05

(21) Application number: 93112290.7

(22) Date of filing: 30.07.1993

(84) Designated Contracting States:
AT BE CH DE DK ES FR GB GR IE IT LI LU MC NL PT SE

(30) Priority: 31.07.1992 US 923641

(71) Applicant: CORBIS CORPORATION
Bellevue, Washington 98007-6537 (US)

(72) Inventors:
- Powell, Robert D.
Issaquah, Washington 98027 (US)
- Nitzberg, Mark J.
D-50677 Köln (DE)

(74) Representative: Grünecker, Kinkeldey,
Stockmair & Schwanhäusser
Anwaltssozietät
Maximilianstrasse 58
D-80538 München (DE)

(54) **Method and system for digital image signatures**

(57) A method and system for embedding signatures within visual images in both digital representation and print or film. A signature is inseparably embedded within the visible image, the signature persisting through image transforms that include resizing as well as conversion to print or film and back to digital form. Signature points are selected from among the pixels of an original image. The pixel values of the signature points and surrounding pixels are adjusted by an amount detectable by a digital scanner. The adjusted signature points form a digital signature which is stored for future identification of subject images derived from the image. In one embodiment, a signature is embedded within an image by locating relative extrema in the continuous space of pixel values and selecting the signature points from among the extrema. Preferably, the signature is redundantly embedded in the image such that any of the redundant representations can be used to identify the signature. Identification of a subject image includes ensuring that the subject image is normalized with respect to the original image or the signed image. Preferably, the normalized subject image is compared with the stored digital signature.

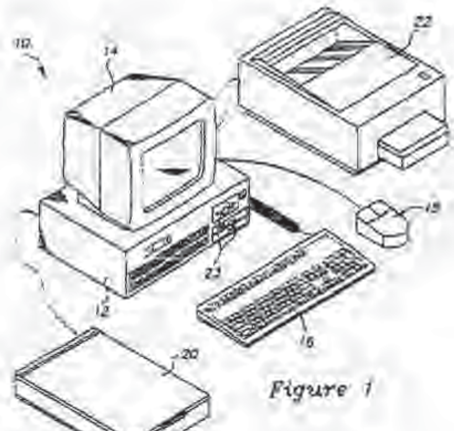


Figure 1

EP 0 581 317 A3

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 93 11 2290

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.5)
X	1979 CARNAHAN CONFERENCE ON CRIME COUNTERMEASURES, 16 - 18 May 1979 UNIVERSITY OF KENTUCKY, LEXINGTON, KENTUCKY USA, pages 101-109, SZEPANSKI, WOLFRAM 'A Signal Theoretic method for creating Forgery-proof Documents for Automatic Verification.' * page 103 - page 104; figures 3.4 , 4 * ---	1-39	G07D7/00 G07F7/12
X	DE-A-29 43 436 (SZEPANSKI WOLFRAM DR ING) 7 May 1981 * page 8, paragraph 3; figure 3 * ---	1-39	
A	US-A-3 914 877 (HINES MARION E) 28 October 1975 * claim 1; figure 2 * ---	1-39	
A	US-A-4 488 245 (DALKE GEORGE W ET AL) 11 December 1984 * claim 1; figure 6 * ---	1-39	TECHNICAL FIELDS SEARCHED (Int.Cl.5)
A	US-A-4 310 180 (MOWRY JR WILLIAM H ET AL) 12 January 1982 * claim 1; figure 1 * -----	1-39	G07D G07F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	7 March 1996	Kirsten, K

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

EPO FORM 1503 03.82 (P04C01)

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number: 0 372 601 B1

(12) # EUROPEAN PATENT SPECIFICATION

(45) Date of publication of patent specification: 22.02.95 Bulletin 95/08

(51) Int. Cl.[5]: H04B 1/66

(21) Application number: 89202823.4

(22) Date of filing: 08.11.89

(54) **Coder for incorporating extra information in a digital audio signal having a predetermined format, decoder for extracting such extra information from a digital signal, device for recording a digital signal on a record carrier, comprising such a coder, and record carrier obtained by means of such a device.**

(30) Priority: 10.11.88 NL 8802769
25.04.89 NL 8901032

(43) Date of publication of application: 13.06.90 Bulletin 90/24

(45) Publication of the grant of the patent: 22.02.95 Bulletin 95/08

(84) Designated Contracting States: AT BE DE ES FR GB IT SE

(56) References cited:
EP-A- 0 145 332
EP-A- 0 289 080

(73) Proprietor: Philips Electronics N.V.
Groenewoudseweg 1
NL-5621 BA Eindhoven (NL)

(72) Inventor: Druyvesteyn, Willem Frederik
c/o INT. OCTROOIBUREAU B.V.
Prof. Holstlaan 6
NL-5656 AA Eindhoven (NL)
Inventor: Hoogendoorn, Abraham
c/o INT. OCTROOIBUREAU B.V.
Prof. Holstlaan 6
NL-5656 AA Eindhoven (NL)
Inventor: Van de Kerkhof, Leon Maria
c/o INT. OCTROOIBUREAU B.V.
Prof. Holstlaan 6
NL-5656 AA Eindhoven (NL)
Inventor: Veldhuis, Raymond Nicolaas Johan
c/o INT. OCTROOIBUREAU B.V.
Prof. Holstlaan 6
NL-5656 AA Eindhoven (NL)

(74) Representative: van der Kruk, Willem Leonardus et al
INTERNATIONAAL OCTROOIBUREAU B.V.,
Prof. Holstlaan 6
NL-5656 AA Eindhoven (NL)

EP 0 372 601 B1

Jouve, 18, rue Saint-Denis, 75001 PARIS

Description

The invention relates to a coder for incorporating extra information in the form of an auxiliary signal in a digital audio signal having a predetermined format, to a decoder for extracting this extra information from digital signal, to a device for recording a digital signal on a record carrier and to a record carrier obtained by means of such a device.

In digital sound transmission and recording systems, such as CD players, future television systems, such as D2MAC, and so on, the format, i.e. the sampling rate and the number of bits per sample, in which the digital sound signal is recorded or transmitted, is generally predetermined, for example, in connection with international agreements. Sometimes, however, there is a need for recording or transmitting more information than possible on the basis of the available number of channels. For example, on the basis of international agreements, not more than two high-quality digital audio channels, for example, each channel for 14-bit digital signals, can be available in specific future television systems. These channels are used for transmitting audio information for the respective left and right-hand channels. However, there is a wish to transmit information for rear channels too, for example, a left-hand and a right-hand rear channel for so-called surround sound. Also in other cases it may be very useful if extra information can be added to existing channels for digital signals having a predetermined format, without the need for extending the number of channels for this purpose. In this context one may think of adding music signals containing music information without vocals, which is commonly referred to as Karaoke, so that the user himself can provide the vocals; or adding music signals in which a specific instrument is omitted, so that the user can play this instrument along with the rest of the recording. One may also think of adding extra information by way of data signals, such as, for example, for Ceefax information.

It will be evident that in all these cases the system is desired to be compatible with state of the art systems, that is to say, it should be possible to reproduce the original signal information in an undisturbed manner with equipment not comprising a specific decoder for extracting the extra information from the signal. If, for example, there is a television signal containing surround-sound information, in a television set not equipped for producing surround sound, it should be possible to reproduce the information for the left and right-hand channels without this reproduction being disturbed in any audible way by the "masked" information for extracting the signal from the rear channels.

It is an object of the invention to provide a system presenting this feature and it thereto provides a system of the above type wherein the coder comprises means for analysing the digital signal, means for quantizing the analysed digital signal in an unequivocal manner and means for determining, on the basis of the acoustic properties of the human auditory system, the amount of extra information that can be added to the quantized digital signal without this extra information being audible with unmodified detection; means for combining the extra information and the quantized digital signal to a compound signal. The coder may further comprise means for reconverting the compound signal into a digital signal having the predetermined format.

According to a preferred embodiment of the invention the psychoacoustic property of the human auditory system is exploited that when the audio frequency band is divided into a number of sub-bands, whose bandwidths approximately correspond with the bandwidths of the critical bands of the human auditory system, the quantizing noise in such a sub-band is optimally masked by the signals of this sub-band.

It should be noted in this respect that a coder for generating subband signals is known from EP-A-0 289 080.

In an embodiment in which this masking principle is implemented the means for analysing the digital signal comprise analysis filter means for generating a number of P sub-band signals in response to the digital signal, which analysis filter means divide the frequency band of the digital signal into consecutive sub-bands having band numbers p ($1 \leq p \leq P$) according to a filter method with sample frequency reduction, while the bandwidths of the sub-bands preferably approximately correspond to the critical bandwidths of the human auditory system in the respective frequency ranges although it is likewise possible to use a smaller number of sub-bands, whereas, if the auxiliary signal is a digital audio signal, analysis filter means are preferably also provided for generating a number of P sub-band signals in response to the auxiliary signal, which analysis filter means divide the frequency band of the auxiliary signal into consecutive sub-bands with band numbers p($1 \leq p \leq P$), according to a filter method with sample frequency reduction, while the bandwidths of the sub-bands again preferably approximately correspond with the critical bandwidths of the human auditory system in the respective frequency ranges, whereas for each of the respective sub-bands means are provided for quantizing the digital signal in an unequivocal manner and means for combining the respective quantized sub-band signals and the corresponding sub-band signals. Preferably, the coder further comprises the auxiliary signal for constituting P compound sub-band signals, and synthesis filter means for constructing a replica of the compound signal in response to the compound sub-band signals, which synthesis filter means combine the subbands according to a filter

DISH - Blue Spike-408
Exhibit 1010, Page 2160

method with sample frequency enhancement corresponding to the sub-division in the analysis filter means.

For extracting the auxiliary signal incorporated in such a compound signal there are provided a decoder, comprising analysis filter means for generating a number of compound sub-band signals in response to the compound signal, these analysis filter means subdividing the frequency band of the compound signal into consecutive sub-bands having band numbers p ($1 \le p \le P$) according to a filter method with sample frequency reduction, the bandwidths of the sub-bands corresponding with those of the analysis filter means in the transmitter; means for quantizing in an unequivocal way the compound subband signals; means for subtracting the respective quantized sub-band signals from the corresponding sub-band signals of the compound signal in order to form sub-band difference signals, and synthesis filter means for constructing a replica of the auxiliary signal in response to subband difference signals, which synthesis filter means combine the subbands according to a filter method with sample frequency enhancement corresponding with the sub-division in the analysis filter means. The analysis filter means and the synthesis filter means together constitute a perfect reconstruction filter both in the coder and the decoder.

Although the invention can be applied to recording digital information on, for example, a compact disc or a video tape, as well as reproducing same, and also applied to transmitting and receiving digital information as is done in, for example, television, transmission and reception will be mentioned in the sequel for brevity, whereas recording and subsequent reproduction are also implicitly referred to.

The invention is based on the recognition of the fact that quantizing the digital audio signal in a predetermined manner enables to mask in resultant quantizing noise extra information in the form of an auxiliary signal, in the form of a discrete time signal, generally a digital signal, or in the form of a data signal, and that this re-quantized digital audio signal with the incorporated auxiliary signal can subsequently be reconverted into a compound digital signal again having the predetermined format, while when receiving this compound digital signal in a receiver that does not comprise a specific decoder, the audio information incorporated in the original digital audio signal can be extracted from this compound signal in the customary fashion, without the auxiliary signal affecting this signal to an audible level because this auxiliary signal lies below the masking threshold of the audio signal and remains masked in the quantizing noise. In a receiver that does comprise a decoder, however, the information relating to the auxiliary signal can be derived from the difference between the compound digital signal and the compound digital signal quantized in the predetermined manner.

The recognition on which the invention is based enables in a relatively simple manner to add extra information, in the form of an auxiliary signal, to an existing digital audio signal having a fixed format, to be called the main signal hereinafter and, subsequently, extract same again, without affecting to an audible extent the original information, whereas this original information can be reproduced even without any modification of the receiving equipment.

The recognition underlying this invention can only be applied if a number of requirements are fulfilled, which are the following:

1) The quantization method for the main signal is to be selected such that the quantization methods implemented both during transmission and reception is always the same,

2) The amplitude of the auxiliary signal to be added is to be smaller than half the quantization step of the main signal; and

3) The quantization of the main signal is to be performed such that the quantization noise is not audibly enhanced.

Condition 1) can be fulfilled in a simple manner when a choice is made in favour of a fixed quantization step, whose size is thus independent of the amplitude of the main signal. When quantization is effected both at the transmit end and the receive end the quantization step is fixed and no problems will occur. In practice, however, an adaptive quantization step is preferably used because it will then be possible to realise a maximum amplitude range for the auxiliary signal. With such an adaptive quantization special measures are to be taken so as to decide always unequivocally on the same quantization during transmission and reception, both at the transmit end and at the receive end, irrespective of the signal amplitude of the main signal.

According to a preferred embodiment of the invention the magnitude of the quantization step per sub-band depends on the amplitude of the main signal, whilst there is an exponential relationship with a predetermined basic number between any consecutive steps. Thus it is possible to obtain adaptive quantization which accommodates itself to the amplitude of the main signal and can be derived in an unequivocal manner from the compound signal at the receive end, so as to reclaim thus the main signal. The matter will be further explained hereinbelow.

The above condition 2) can be fulfilled by attenuating by a specific factor the auxiliary signal per sub-band at the transmit end and amplifying this signal again by the same factor at the receive end, whilst the magnitude of this factor can be selected in dependence on the magnitude of the quantization step used for quantizing the main signal. If the auxiliary signal is a data signal, no attenuation is required because in that case it can be determined for each quantized sample of the main signal how many bits form a half quantization step and, consequently, how many data per sample can be added.

Condition 3) can basically be fulfilled by choosing the quantization steps small enough so that the quantization noise can be maintained at a very low level. However, this will lead to a conflict with condition 2). For, if a small quantization step is concerned, the amplitude available to the auxiliary signal, which amplitude, for that matter, should be smaller than this half quantization step, is also very small, which will lead to problems in connection with noise and reproducibility of the auxiliary signal. Therefore, a rather coarse quantization of the main signal is preferably used in combination with measures to make the resultant quantization noise inaudible to the human auditory system. Such measures are known per se.

A first measure is based on the phenomenon that when the audio signal band is divided into a plurality of sub-bands, whose bandwidths approximately correspond with the bandwidths of the critical bands of the human auditory system in the respective frequency ranges, it may be expected on grounds of psychoacoustic experiments that the quantization noise in such a sub-band will be optimally masked by the signals in this sub-band when the noise masking curve of the human auditory system is taken into account when the quantization is effected. This curve indicates the threshold value for masking noise in a critical band by a single tone in the middle of the critical band. If a high-quality digital music signal, represented, for example, in accordance with the compact disc standard, by 16 bits per signal sample with a sampling rate of 1/T = 44.1 kHz, it turns out that the use of this prior-art sub-band encoding with a suitably chosen bandwidth and a suitably chosen quantization for the respective sub-bands results in quantized transmitter output signals which can be represented by an average number of approximately 2.5 bits per signal sample, whilst the quality of the replica of the music signal does not perceptually differ from that of the original music signal in virtually all passages of virtually all sorts of music signals. For a further explanation of this phenomenon reference is made to the article entitled "THE CRITICAL BAND CODER -- DIGITAL ENCODING OF SPEECH SIGNALS BASED ON THE PERCEPTUAL REQUIREMENTS OF THE AUDITORY SYSTEM" by M.E. Krasner in proceedings IEEE ICASSP 80, Vol. 1, pp. 327-331, April 9-11, 1980. By implementing this so-called simultaneous masking in frequency sub-bands the main signal can yet be quantized with a minimum loss of quality despite a coarse quantization, as a result of which the maximum quantization range for the auxiliary signal, that is to say, the range smaller than a half quantization step, is relatively large, so that this signal too can be reconstructed with a minimum loss of quality.

A further measure known per se utilizes the psychoacoustic effect of temporal masking, that is to say, the property of the human auditory system that the threshold value for perceiving signals shortly before and shortly after the occurrence of another signal having a relatively high signal energy appears to be temporarily higher than during the absence of the latter signal. In the period of time before and after such a signal having a high signal energy, extra information of the auxiliary signal can now be recorded. It is also possible to combine temporal masking with frequency sub-band masking. A first possibility in this respect according to the invention is the implementation of the knowledge about the amplitude of one or more preceding digital signal samples. If there is a decreasing amplitude the quantization step can, in the case of adaptive quantization, be chosen to be larger than would be permissible on the basis of the actual signal amplitude and the selected quantization criterion, because the resultant extra quantization noise at this relatively low amplitude is masked by the preceding larger amplitude(s). Since a coarser quantization can be chosen, more extra information can be masked in the digital signal samples following a large signal amplitude, which favourably affects the signal-to-noise ratio when the auxiliary signal is received. A great advantage of this manner of temporal masking is the fact that no additional delay occurs when the samples are taken in which it is permitted to quantize more coarsely on the basis of temporal masking.

A further possibility is storing the samples of the main signal in blocks and deciding to come to a single quantization step which holds for all samples in that block on the basis of the maximum signal amplitude in that block, whilst assuming that owing to temporal masking the actually too coarse quantization of the samples having a lower sample amplitude is inaudible. However, a block signal sample is invariably to be stored before a quantization step can be determined.

A special use of the coder is in a device for recording a digital signal on a record carrier, for example a magnetic record carrier. The auxiliary signal which is then also recorded may now serve as a copy inhibit code. Said device will be used by the software industry to generate prerecorded record carriers provided with a copy-inhibit code. When such record carriers are played the analog signal obtained after D/A conversion still contains the auxiliary signal which, however, as stated above, is not audible. Every subsequent recording via said analog path, can now be inhibited if a recording device intended for the consumer market comprises a detection unit which is capable of detecting said auxiliary signal.

Such a device for recording a digital audio signal on record carrier comprising a coder for sub-band coding of the digital audio signal of given sample frequency 1/T, the coder comprising: analysis filter means responsive to the audio signal to generate a plurality of P sub-band signals, which analysis filter means divide the frequencyband of the audio signal in accordance with a filter method with sample frequency reduction into consecutive sub-bands having band numbers p(1 ≤ p ≤ P), which analysis filter means are further adapted to apply the P sub-band signals to P outputs, which outputs are coupled to P corresponding inputs of a

- recording unit which is constructed to record the P sub-band signals on the record carrier,

is therefor characterized in that the device further comprises a detection unit coupled to the analysis filter means, in that the detection unit is adapted to detect the presence of an auxiliary signal in one or more sub-band signals and to generate a control signal upon detection of the auxiliary signal and to apply the control signal to an output, in that said output is coupled to a control signal input of the recording unit, and in that the recording unit is adapted to inhibit recording of the audio signal in the presence of the control signal and to record the audio signal in the absence of the control signal. When the auxiliary signal is detected recording is inhibited, or the signal to be recorded is distorted on purpose before it is recorded. It is obvious that reproducing devices should comprise a decoder with which during reproduction the digital audio signal is read together with the auxiliary signal, without the two signals being separated from one another. During a subsequent recording the auxiliary signal in the audio signal can then be detected, if present, so that it is possible to inhibit unauthorized copying of copy-protected audio information.

It is alternatively possible not to inhibit copy-protected information but merely to detect that the audio signal to be copied comprises an auxiliary signal, and to signal that in the relevant case the information is protected and should not be copied.

Such a device, which is also intended for the consumer market, for recording a digital audio signal on the record carrier, comprising a coder for sub-band coding of the digital audio signal of given sample frequency 1/T, wherein the coder comprises:

- analysis filter means responsive to the audio signal to generate a plurality of P sub-band signals, which analysis filter means divide the frequency band of the audio signal into consecutive sub-bands having band numbers p(1 ≤ p ≤ P) in accordance with a filter method using sample frequency reduction, which analysis filter means are further adapted to apply the P sub-band signals to P outputs, which outputs are coupled to P corresponding inputs of a
- recording unit which is constructed to record the P sub-band signals on the record carrier, which device is capable of realizing this, is characterized in that the device further comprises a detection unit coupled to the analysis filter means, in that the detection unit is adapted to detect the presence of an auxiliary signal in one or more of the sub-band signals and to generate a control signal upon detection of the auxiliary signal and to apply the control signal to an output, in that said output is coupled to a signalling unit, and in that the signalling unit is constructed to signal that the audio signal to be recorded, when a control signal is present, is an audio signal containing an auxiliary signal.

The above recording devices, which are intended for the consumer market, may be characterized further in that the coder further comprises signal combination means coupled to the analysis filter means, in that the signal combination means are adapted to selectively add the auxiliary signal, in the absence of a control signal, to one or more of the sub-band signals to form P composite sub-band signals and to apply said P composite sub-band signals to P outputs, which P outputs are coupled to the P corresponding inputs of the recording unit. This enables a user of the device to provide his recordings, if desired, with a copy inhibit code, in order to ensure that no copies can be made of record carriers made by the user and provided with his own recordings.

The devices intended for the consumer market may alternatively be characterized in that the coder further comprises signal combination means coupled to the analysis filter means, in that the signal combination means are adapted to add the auxiliary signal, in the absence of the control signal, to one or more of the sub-band signals to form P composite sub-band signals and to apply said P composite sub-band signals to P outputs, which P outputs are coupled to the P corresponding inputs of the recording unit. In that case there is no longer a selection possibility and in all cases an auxiliary signal will be added to the audio signal to be recorded, which does not yet contain the auxiliary signal. This enables original recordings (not provided with the auxiliary signal) or prerecorded tapes (neither provided with the auxiliary signal) to be copied, while it is not possible to make copies of the recordings thus copied.

Embodiments of the invention will now be described in more detail, by way of example, with reference to the drawings in which:

Fig. 1 shows a block diagram of a preferred embodiment of a transmit-receive system comprising a coder and a decoder in accordance with the invention,

Fig. 2 illustrates diagrammatically the quantization method in the coder,

Fig. 3 shows a device for recording a digital audio signal on a record carrier,

Fig. 4 shows a device for reproducing the signal recorded on the record carrier by means of the device shown in Fig. 3,

Fig. 5 shows another embodiment,

Fig. 6 shows a further embodiment,

Fig. 7 shows still another embodiment, and

Fig. 8 shows yet another embodiment of a device for recording a digital audio signal.

Fig. 1 diagrammatically shows a system comprising a transmitter 1 and a receiver 2 for adding and extracting respectively, extra information to and from a digital audio signal having a predetermined format, which information is transferred via or stored in medium 3. This medium can be a transmission channel but, for example, also a compact disc or a magnetic tape or disc.

The transmitter comprises a coder in the form of a processor 7 having an input terminal 4 for the digital signal u(k) having the predetermined format and an input terminal 5 for the additional digital auxiliary signal v(k) and having an output terminal 6. The output terminal 6 of the processor circuit 7 is coupled to the medium 3.

The receiver 2 comprises a delay circuit 9 having a delay τ, as well as a decoder in the form of a processor circuit 10. The input terminals of these two circuits are connected to one another and arranged for receiving the digital compound signal produced by the medium 3. At the output terminal of the delay circuit 9 the main signal is available again, as will be explained hereinafter, in the form of a signal u'(k) and at the output terminal of processor circuit 10 the auxiliary signal is available in the form of a signal v'(k).

The operation of the system according to Fig. 1 is as follows. At the input terminal of the transmitter 1 consecutive samples of the signal u(k) are presented. For example, in the case of an audio signal formed in accordance with the compact disc standard, each signal sample comprises 16 bits and the sampling rate is 44.1 kHz. In the processor circuit 7 it is determined how much information of the signal v(k) can be added to each sample of the signal u(k) on the basis of the chosen method according to which the auxiliary signal v(k) is added, that is, by means of temporal masking or simultaneous frequency sub-band masking or by means of a combination of the two. If temporal masking is used, this may be done in the time intervals shortly before and/or shortly after a loud passage in the signal u(k) and if simultaneous masking is chosen, it will be possible to add information about the signal v(k) to each signal sample of the signal u(k) by means of the subdivision into frequency sub-bands. As stated earlier, a combination of the two types of masking is possible. The combined output signal of the processor circuit 7 is reconverted in a converter 29 into the predetermined format of the digital main signal and applied to the medium 3.

In the receiver 2 the received signal is subjected to a decoding operation in the processor circuit 10 in order to split up the signals u(k) and v(k), so that at the output of circuit 10 the signal v'(k) is available, whereas through delay circuit 9, whose delay is equal to that which is produced by the processor circuit 10, the signal u'(k) is available in synchronism with the signal v'(k).

In the sequel the structure of the processor circuits 7 and 10 will be explained.

The processor circuit 7 comprises filter banks 22 and 23 for splitting up through sample frequency reduction the respective signals u(k) and v(k) into P consecutive sub-bands, whose bandwidths approximately correspond with the critical bandwidths of the human hearing in the respective frequency bands. The use and structure of such filter banks is known from, for example, the above article by Krasner and the chapter of "Sub-band coding" in the book entitled "Digital coding of waveforms" by N.S. Jayant and P. Noll, Prentice Hall Inc., Englewood Cliffs, New Jersey, 1984, pp. 486-509. Each of the p sub-band signals of filter bank 22 is applied to an adaptive quantizer 24(p), with $1 \leq p \leq P$, whereas each sub-band output signal of filter bank 23 is applied to an attenuator 25(p), with $1 \leq p \leq P$. The output signals of summing circuit 26(p) are now applied to a synthesis filter bank 27 in which the P sub-bands are combined to a signal having the same bandwidth as the original signals u(k) and v(k). The output signal of the synthesis filter bank 27 is encoded in a converter 29 into a digital signal having a predetermined format, for example, 16 bits, and applied to the medium 3 as a compound signal s(k).

If the number of quantization levels per frequency band in the transmitter 2 is chosen in the right way, nothing can be perceived in the digital signal applied to medium 3 of the addition of the signal v(k), provided that the condition is fulfilled that the amplitude of an auxiliary signal sample to be added is smaller than q/2 in each frequency sub-band for each sample of $u_p(k)$ where q is the quantization step of that sample.

At the receive end the original signal u(k) can now be reproduced directly without any adaptation by means of a non-adapted device, because in the compound digital signal s(k) the extra information of the signal v(k) is not audible, because it is masked by the signal u(k).

A receiver which is indeed suitable for receiving both the signal u(k) and the signal v(k), for example, a D2MAC television receiver with surround-sound reproduction features comprises, however, a filter bank 31 which is arranged in the same way as the filter bank 22. This filter bank 31 splits up again the received compound signal s(k) into P sub-bands having the same bandwidths and central frequencies as the sub-bands of the filter bank 22. Each of these sub-band signals is applied to an adaptive quantizer 33(p), with $1 \leq p \leq P$. A proper dimensioning of this quantizer provides that for each sub-band the signal $u_p(k)$ is again obtained from each of the P sub-bands after quantization. By subtracting each of these sub-band signals $u_p(k)$ from the compound sub-band signal $s_p(k)$ in a subtracting circuit 34(p), the signal $v_p(k)$ is obtained for each sub-band p. Each of these signals

$v_p(k)$ is amplified in an amplifier 35(p), with $1 \leq p \leq P$, by a factor G which is the same as that which is used in the coder for attenuating the relevant sub-band and, subsequently, these scaled signals $v_p(k)$ are applied to a synthesis filter bank 36 which reconstructs the signal v'(k) from the individual sub-bands $v_p(k)$. The signal u'(k) can be extracted directly, as observed hereinbefore, from the compound signal s(k) and needs only to be delayed in a delay circuit 9 over a time which is equal to the delay time introduced by the processor 10, if the main signal and the auxiliary signal are desired to be synchronous.

In the case of a television transmit-receive system with surround-sound reproduction facilities, in the left channel the signals u(k) and v(k) may be the digital reproduction of, for example, the signal LV + LA and the signal LA respectively. An unmodified receiver will receive the complete sound signal LV + LA and can reproduce this without complications, whereas in a modified receiver, the signals LA and LV can be applied separately to the relevant reproduction channels after u(k) and v(k) have been split up by means of a subtracting circuit.

In the sequel it will be discussed in what way the adaptive quantizers 24(p) and 33(p) can be arranged in the transmitter and receiver of the system according to Fig. 1 so as to obtain in an unequivocal manner an adaptive quantization for each of the sub-band signals. For this purpose the number of quantization steps desired for each of the sub-bands is determined beforehand, which this number I(p) is constant for each of the sub-bands.

In view of the wish that quantization be adaptive, the quantization steps are to be chosen approximately in proportion to the signal size. For this purpose the amplitude axis is subdivided into sections T_i whilst, if the amplitude of a sample of the signal u(k) is situated in a specific section T_n, where n is an integer, the quantization steps for that sample have a specific magnitude which is equal to the magnitude of the section T_n. The quantization level is positioned in the centre of said section, so as to allow the auxiliary signal v(k) to have equal amplitude ranges on either one of the two sides of this section relative to the quantization level, without the compound signal $s_p(k)$ being situated in another quantization section.

Since one wishes to choose the quantization steps in proportion to the maximum signal size, and the number of quantization steps is fixed, the magnitudes of the sections T which always determine the magnitude of the quantization step, have to enhance in proportion to the amplitude. Therefore, the variation of the section magnitudes is preferably exponential, each section varying from $a^{(n-1/2)}$ to $a^{(n+1/2)}$ where a is a constant and n an integer. The quantization level belonging to a specific section T_n is then $1/2(a^{n-1/2} + a^{n+1/2})$.

Fig. 2 shows an amplitude axis on which the division of the quantization levels according to the embodiment is shown. Depending on the absolute value of the maximum amplitude $\hat{u}(k)$ of the signal u(k) the quantization step is equal to the size of the section in which $\hat{u}(k)$ is located and thus equal to $a^{(n+1/2)} - a^{(n-1/2)}$. In this case the choice of the value of the factor a is free. However, it is often desired that also the value 0 is a quantization level, because it does not matter then whether the maximum signal level of u(k) is positive or negative, whereas relatively small signal amplitudes are also avoided to be quantized at a considerably higher quantization level. This provides the additional requirement that the chosen quantization level is an integer number of times the quantization step. This requirement limits the choice of the constant a to a = (2k + 1)/(2k - 1) with k = 1, 2 ...; that is to say, a = 3; a = 5/3; a = 7/5 ... and so on.

The consequence of the choice of the quantization steps according to this preferred embodiment is the fact that in the decoding arrangement the signal $v_p(k)$ can always be extracted from the compound signal s(k) in an unequivocal manner, because with a specific signal amplitude, always the same quantization level is decided on. When this quantization level and thus $u_p(k)$ is determined, $u_p(k)$ can be subtracted from the compound signal so as to thus determine the signal $v_p(k)$.

For controlling the respective quantizers 24(p) and 32(p), the processor circuit 7 comprises quantization step determining circuits 28(p) and processor circuit 10 the quantization step determining circuits 32 respectively, the structure of these circuits being basically identical. The circuits 28(p) and 32(p) comprise memory sections 28'(p) and 32'(p) respectively, in which for each sub-band the predetermined value for the basic number a is stored, which may be different for each sub-band. The circuits 28(p) and 32(p) compute for each sample of $u_p(k)$ and $s_p(k)$ respectively, the size of the quantization step on the basis of the above-described quantization procedure and apply through outputs the values of these steps to the respective quantizers 24(p) and 33(p). A value derived from the value a in the respective memory sections 28'(p) and 32'(p) is also applied to a control input of the respective attenuators 25(p) and the respective amplifiers 35(p) so as to attenuate and amplify respectively, the signals $v_p(k)$ by a factor G. The attenuation factor or gain factor G respectively, derived from the value a is 2a/(a - 1). It is known that $\hat{u}(k)$, the maximum amplitude of the signal u(k), is equal to $a^{(n+1/2)}$ as a maximum whereas the maximum permissible amplitude $\hat{v}(k)$ of the auxiliary signal v(k) is then equal to $1/2[a^{(n+1/2)} - a^{(n-1/2)}]$. Now $\hat{u}(k)/\hat{v}(k) = 2a/(a-1)$. If it is provided beforehand that always $\hat{v}(k) < \hat{u}(k)$, which in practice can be realised without any problems, it is always certain that $\hat{v}(k) < q/2$ if for the factor G is chosen G = 2a/(a - 1). In practical cases the condition $\hat{v}(k) < \hat{u}(k)$ has often been fulfilled automatically because of the relationship which exists between these two signals.

In order to avoid $\hat{v}(k)$ nevertheless exceeding the value q/2 in any way, the output line of each attenuator 25(p) can comprise the limiter 30(p) shown in a dashed line in Fig. 1, which limiter receives information about the limitation value to be set from the circuits 28(p) and limits the output signal of the attenuator 25(p) to a maximum of q/2.

If a choice is made in favour of simultaneous masking combined with temporal masking, the circuits 28(p) and 32(p) comprise the circuits necessary for comparing the current sample of $u_p(k)$ to one or more previous samples so as to decide to a larger quantization step on the basis of pre-stored information about the variation of the temporal masking curve belonging to a specific maximum amplitude of $u_p(k)$, if the current sample has a lower amplitude than the amplitude of one or more of the previous samples.

In the case of block quantization, a buffer circuit is to be provided between each of the P outputs of the filter bank 22 and the input of the relevant quantizer 24(p), which circuit constantly stores a block of M signal samples, determines the maximum block amplitude and uses this value for determining the quantization step for the entire block.

Finally, it is observed that additional room can be found for adding v(k) in a sub-band p by also considering the amplitude variations in adjacent sub-bands. If, in an adjacent sub-band, a large amplitude of u(k) occurs, whereas in the p sub-band amplitude of u(k) is very small or even zero, one may decide, on the basis of the masking properties of the signal in this adjacent sub-band, yet to allow a specific amount of the signal v(k) to enter the sub-band p.

It is further pointed out that at the output of the quantizers 33(p) a signal $u_p(k)$ is available which basically has less quantization noise than the signal s(k) so that in a receiver comprising a decoder a better replica of the signal u(k) can be derived from these output signals by means of an additional synthesis filter.

Fig. 3 shows a device for recording a digital audio signal, such as the digital audio signal u(k) in Fig. 1, on a record carrier. The device comprises a coder 7' which bears much resemblance to the coder shown in Fig. 1. The only difference is that the synthesis filter bank 27 has been dispensed with. Instead, the outputs of the summing circuit 26(p) are coupled to a recording unit 47. This recording unit is constructed to record the P sub-band signals applied to its inputs on a record carrier 48. Averaged over all sub-bands this enables such a data reduction to be achieved that the information to be recorded on the record carrier is recorded with, for example, 4 bits per sample, while the information applied to the input 4 comprises, for example, 16 bits per sample.

The auxiliary signal V(k) is generated in an auxiliary signal generator 40 which has an output coupled to the input 5, to apply the auxiliary signal to the coder 7'. By means of the coder 7' the auxiliary signal is inserted in the audio signal in the manner described hereinbefore. The auxiliary signal can thus be inserted into one or more of the sub-band signals into which the audio signal (k) has been divided.

Preferably, the auxiliary signal is accommodated in one or more of the lower sub-bands (of low frequency). In the sub-bands which are situated in the low-frequency range the signal content of the audio signal is generally maximal. This means that the masking threshold in said sub-band(s) is also high. This enables an auxiliary signal of large amplitude to be inserted in the audio signal. This simplifies detection of the auxiliary signal.

Thus, by means of the device shown in Fig. 3 record carriers 48 are obtained on which the audio signal including the auxiliary signal is recorded. The method of recording on the record carrier 48, as is effected in the recording unit 47, is not relevant to the present invention. It is possible, for example, to employ a recording method as known in RDAT or SDAT recorders. The operation of RDAT and SDAT recorders is known per se and is described comprehensively inter alia in the book "The art of digital audio" by J. Watkinson, Focal Press (London) 1988. Obviously, the recording unit 47 should be capable of converting the parallel data stream of the P sub-band signals into a signal stream which can be recorded by means of an RDAT or SDAT recorder.

Fig. 4 shows diagrammatically a device for reproducing the audio signal as recorded on the record carrier 48 by means of the device shown in Fig. 3. For this purpose the device comprises a read unit 41 which is constructed to read the data stream from the record carrier 48 and to supply the P sub-band signals via P outputs. These P sub-band signals are then applied to P inputs of a synthesis filter bak 27', having the same function as the filter bank 27 in Fig. 1. This means that the P sub-band signals are recombined to form a digital signal of a predetermined format of, for example, 16 bits. After D/A conversion in the D/A converter 42 the audio signal is then available again on the output terminal 43.

The audio signal, then still contains the auxiliary signal. However, this auxiliary signal is not audible because it is masked by the audio signal.

Fig. 5 shows a device for recording an audio signal, for example the audio signal reproduced by the device shown in Fig. 4. Such a device is intended for example for the consumer market. The device is capable of normally recording audio information not containing a copy inhibit code on a record carrier. However, the device comprises a detector unit to detect a copy inhibit code inserted in the audio signal to inhibit recording of this audio signal.

The device shown in Fig. 5 bears much resemblance to the device shown in Fig. 3, the difference being that the device shown in Fig. 5 is not capable of inserting a copy inhibit code into an audio signal. This means that the elements bearing the reference numerals 23, 25(1) to 25(P), 28(1) to 28(P) and 26(1) to 26(P) are dispensed with. The device shown in Fig. 5 further comprises subtractor circuits 34(1) to 34(P), amplifiers 35(1) to 35(P), a synthesis filter bank 36, and a detector unit 50. The section 10' of the device shown in Fig. 5, indicated by means of a solid line, is in fact identical to the decoder 10 in Fig. 1. This means that the section 10' is adapted to filter out the auxiliary signal which, if present in the digital audio signal applied to the input 51, then becomes available on the output 52. The detector unit 50, which has an input 53 coupled to the output 52, is constructed to detect said auxiliary signal and to generate the control signal which is then applied to the control signal input 55 of the recording unit 47' via the output 54.

The recording unit 47' is constructed in such a way that if a control signal appears on the control signal input 55 the recording unit 47' does not record the sub-band signals applied to its inputs or seriously distorts these sub-band signals before they are recorded. In the absence of a control signal on the control signal input 55 the recording unit 47' will record the sub-band signals applied to its inputs.

In this way an audio signal containing a copy-inhibit code in the form of the auxiliary signal inserted in the audio signal is prevented from being recorded on the record carrier 48' by the device.

In the device shown in Fig. 5 it is assumed that the auxiliary signal is accommodated in a number of sub-band signals. However, as already stated, the auxiliary signal may also be inserted in only one sub-band signal. In that case only one subtractor circuit 34 and one amplifier 35 are required and the filter bank 36 comprises only one input. In the synthesis filter bank 36 the auxiliary signal is converted into a digital signal of, for example, 16 bits.

The detector unit 50 may be a detector unit which can directly detect the presence or absence of a digital signal. Another possibility is the use of an analog detector unit 50. In that case the output signal of the filter bank is first converted into an analog signal. The detector unit 50 then comprises a narrow band band-pass filter, a rectifier and a threshold detector. If the input signal of the device is an analog signal an A/D converter is arranged between the terminal 51 and the input of the filter bank 22.

It is now assumed that the auxiliary signal is inserted in only one sub-band, for example the lower sub-band. In that case it may be adequate to use a simpler detection circuit in the form of a digital filter coupled to the output P = 1 of the analysis filter means 22. This filter may be for example a recursive filter having a sharp filter characteristic, the maximum in the filter characteristic coinciding with the frequency of the auxiliary signal. The output of the digital filter may then be coupled to the input 53 of the detector unit 50. In that case the elements 34(1) to 34(P), 35(1) to 35(P) and 36 may be dispensed with.

The embodiment shown in Fig. 6 bears much resemblance to that shown in Fig. 5. The output of the detector unit 50 is now coupled to an input of a signalling unit 56, for example in the form of a light-emitting diode. The auxiliary signal in the audio signal then does not function as a copy inhibit code but merely as a signalling code to signal that it is, in fact, not allowed to copy the relevant audio signal. In this case the decision whether the audio signal is subsequently copied depends on the user himself.

If the presence of the auxiliary signal in the audio signal to be recorded is detected the detector unit 50 generates a control signal upon which the signalling unit 56 (the diode) lights up. The user may now decide to discontinue recording.

From Fig. 6 it is evident that the inputs of the recording unit 57' are now coupled to the outputs of the analysis filter means 22, so that if the user should decide to continue recording, the audio signal, including the auxiliary signal, will be recorded.

Fig. 7 shows another embodiment of the device. The device shown in Fig. 6 is an extension of the device shown in Fig. 5. The controllable amplifiers 35(1) to 35(P) are not shown for simplicity. The device shown in Fig. 6 is in addition adapted to selectively insert a copy inhibit code to the signal to be recorded, assuming that the signal applied to the input 4 does not yet contain a copy inhibit code. In that case recording will be inhibited by means of the control signal applied to the control signal input 55 of the recording unit 47'.

The circuit bearing the reference numeral 7" is substantially identical to the circuit 7' in Fig. 3, the difference being that it comprises an additional control signal input 60 via which a control signal can be applied to switches S_1 to S_p arranged in the lines to the summing circuit 26(1) to 26(P).

If the signal u(k) applied to the input 4 does not contain a copy inhibit code the signal can be recorded on the record carrier 48'. If a control signal is applied to the switches S_1 to S_p via the input 60 the switches will be in the position shown. This means that the auxiliary signal V(k) is added to the signal to be recorded via the summing circuits 26(1) to 26(P), to inhibit further copying. If another control signal is applied to the input 60, the switches S_1 to S_p will be in the position not shown. This means that the value "0" is applied to all the summing circuits 26, so that merely the signal u(k), without auxiliary signal, is recorded on the record carrier 48'.

Again it is obvious that if the auxiliary signal is recorded in only one sub-band only one summing circuit 26(P) is provided and the control signal is applied to only one switch S_p via the terminal 60.

Fig. 8 shows an embodiment which bears much resemblance to the embodiment shown in Fig. 7. The embodiment shown in Fig. 8 excludes the possibility of making a choice whether the audio signal which does not contain a copy inhibit code will be provided with such an inhibit code. This means that if the detector unit 50 detects that the signal to be recorded does not contain an auxiliary signal, this auxiliary signal will be inserted automatically. Fig. 8 shows that interconnections are now arranged between the outputs of the amplifiers 25(1) to 25(P) and the (second) inputs of the signal combination units 26(1) to 26(P). The switches S_1 to S_p and the control signal input 60 in Fig. 7 are consequently dispensed with.

Such a device is very useful if it has been decided to allow copies to be made only of prerecorded record carriers (which are not provided with said auxiliary signal) and original recordings (which neither contain said auxiliary signal), copying of these copies, however, being inhibited. A prerecorded record carrier can now be copied normally. However, the resulting copy is provided with an auxiliary signal and cannot be copied again.

It is to be noted that all the embodiments have been described for devices for recording a digital audio signal on a magnetic record carrier. However, this should not be regarded as a limitation to magnetic record carriers only. The invention likewise relates to devices which record the audio signal on an optical record carrier. In the future this possibility will become available to the consumer. With the advent of the CD erasable and the CD write-once and magnetooptical recording technologies.

Claims

1. A coder for incorporating extra information in the form of an auxiliary signal v(k) in a digital audio signal u(k) having a predetermined format, characterised in that the coder (1) comprises means (22, 28) for analysing the digital signal, means (24) for quantizing the analysed digital signal in an unequivocal manner and means (28') for determining, on the basis of the acoustic properties of the human auditory system, the amount of extra information that can be added to the quantized digital signal without this extra information being audible with unmodified detection; means (26) for combining the extra information and the quantized digital signal to a compound signal.

2. A coder as claimed in Claim 1, characterized in that it comprises means (29) for reconverting the compound signal into a digital signal having the predetermined format.

3. A coder as claimed in Claim 1 or 2, characterised in that the means for analysing the digital signal comprise analysis filter means (22) for generating a number of P sub-band signals in response to the digital signal, which analysis filter means divide the frequency band of the digital signal into consecutive sub-bands having band numbers p ($1 \le p \le P$), whereas for each of the respective sub-bands (P) means (24(p)) are provided for quantizing the digital signal in an unequivocal manner and means (26) for combining the respective quantized sub-band signals and the auxiliary signal for constituting P compound sub-band signals.

4. A coder as claimed in Claim 3, where dependent on Claim 2, characterized in that synthesis filter means (27) are provided for constructing a replica of the compound signal in response to the compound sub-band signals, which synthesis filter means combine the sub-bands according to a filter method with sample frequency enhancement corresponding to the sub-division in the analysis filter means (22).

5. A coder as claimed in Claim 4, characterised in that the auxiliary signal v(k) is a digital audio signal and in that analysis filter means (23) are provided for generating a number of P sub-band signals in response to the auxiliary signal v(k), which analysis filter means divide the frequency band of the auxiliary signal into consecutive sub-bands having band numbers p ($1 \le p \le P$) according to a filter method with sample frequency reduction.

6. A coder as claimed in Claim 4 or 5, characterised in that the bandwidths of the sub-bands approximately correspond to the critical bandwidths of the human auditory system in the respective frequency ranges.

7. A coder as claimed in Claims 4, 5 or 6, characterised in that the means (24) for quantizing the digital signal in an unequivocal manner are arranged for adaptively quantizing this signal and in that for each sub-band the size of the quantization step depends on the amplitude of the digital signal sample, while there is an exponential relationship with a preset basic number a between the possible successive steps.

8. A coder as claimed in Claim 7, characterised in that the size of the quantization step of a sample to be quantized also depends on the size of at least a previous sample.

9. A coder as claimed in Claim 7 or 8, characterised in that means (25) are provided for attenuating each sub-band signal of the auxiliary signal by a

factor G, for which holds G = 2a/(a - 1).

10. A decoder to be used in combination with a coder (7) as claimed in Claims 5 to 9, characterised in that the decoder (10) comprises analysis filter means (31) for generating a number of compound sub-band signals in response to the compound signal, which analysis filter means divide the frequency band of the compound signal into consecutive sub-bands having band numbers p (1 ≤ p ≤ P) according to a filter method with sample frequency reduction, while the bandwidths of the sub-bands correspond with those of the analysis filter means (22) in the coder; means (33) for quantizing compound sub-band signals in an unequivocal manner; means (34) for subtracting the respective quantized sub-band signals from the corresponding sub-band signals of the compound signals for constituting sub-band difference signals, and synthesis filter means (36) for constructing a replica of the auxiliary signal v'(k) in response to the sub-band difference signals, which synthesis filter means combine the sub-bands according to a filter method with sample frequency enhancement corresponding to the sub-division in the analysis filter means.

11. A decoder as claimed in Claim 10, characterised in that the means (33) for quantizing the digital signal in an unequivocal manner are arranged for adaptively quantizing this signal and in that per sub-band the size of the quantization step depends on the amplitude of the sample of the digital signal, whilst between the possible successive steps there is an exponential relationship with a predetermined basic number a.

12. A decoder as claimed in Claim 9, characterised in that means (35) are provided for amplifying each sub-band difference signal by a factor G, which complies with G = 2a/(a - 1).

13. A device for recording a digital audio signal on a record carrier (48), comprising a coder (7) as claimed in any one of the claims 1 to 9.

14. A device for recording a digital audio signal on a record carrier (48'), comprising a coder for sub-band coding of the digital audio signal of given sample frequency 1/T, the coder comprising:

- analysis filter means (22) responsive to the audio signal to generate a plurality of P sub-band signals, which analysis filter means divide the frequency band of the audio signal in conformity with a filter method with sample frequency reduction into consecutive sub-bands having band numbers p(1 ≤ p ≤ P), which analysis filter means are further adapted to apply the P sub-band signals to P outputs, which outputs are coupled to P corresponding inputs of a
- recording unit (47') which is adapted to record the P sub-band signals on the record carrier,

characterized in that the device further comprises a detection unit (50) coupled to the analysis filter means (22), in that the detection unit is adapted to detect the presence of an auxiliary signal in one or more of the sub-band signals and to generate a control signal upon detection of the auxiliary signal and to apply the control signal to an output (54), in that said output is coupled to a control signal input (55) of the recording unit (47'), and in that the recording unit is adapted to inhibit recording of the audio signal in the presence of the control signal and to record the audio signal in the absence of the control signal.

15. A device for recording a digital audio signal on a record carrier (48'), comprising a coder for sub-band coding of the digital audio signal of given sample frequency 1/T, wherein the coder comprises:

- analysis filter means (22) responsive to the audio signal to generate a plurality of P sub-band signals, which analysis filter means divide the frequency band of the audio signal into consecutive sub-bands having band numbers p(1 ≤ p ≤ P) in accordance with a filter method using sample frequency reduction, which analysis filter means are further adapted to apply the P sub-band signals to P outputs, which outputs are coupled to P corresponding inputs of a
- recording unit (47') which is adapted to record the P sub-band signals on the record carrier,

characterized in that the device further comprises a detection unit (50) which is coupled to the analysis filter means (22), in that the detection unit is adapted to detect the presence of an auxiliary signal in one or more of the sub-band signals and to generate a control signal upon detection of the auxiliary signal and to apply the control signal to an output (54), in that said output is coupled to a signalling unit (56), and in that the signalling unit is constructed to signal that the audio signal to be recorded, when the control signal is present, is an audio signal containing an auxiliary signal.

16. A device as claimed in Claim 14 or 15, characterized in that the coder further comprises signal combination means (26, S1 to Sp) coupled to the analysis filter means, in that the signal combination means are adapted to selectively (via 60) add

the auxiliary signal, in the absence of the control signal, to one or more of the sub-band signals to form P composite sub-band signals and to apply said P composite sub-band signals to P outputs, which P outputs are coupled to the P corresponding inputs of the recording unit (47') (Fig 7).

17. A device as claimed in Claim 14 or 15, characterized in that the coder further comprises signal combination means (26) coupled to the analysis filter means (22), in that the signal combination means are adapted to add the auxiliary signal, in the absence of the control signal, to one or more of the sub-band signals to form P composite sub-band signals and to apply said P composite sub-band signals to P outputs, which P outputs are coupled to the P corresponding inputs of the recording unit (Fig 8).

18. A device as claimed in Claim 14, characterized in that the coder forms part of a coder as claimed in any one of the Claims 1 to 9.

19. A record carrier on which a digital audio signal has been recorded by means of a device as claimed in any one of the Claims 13, 16, 17 or 18, characterized in that the audio signal is divided into P sub-band signals and in that the audio signal is combined with an auxiliary signal in one or more of the sub-bands in order to obtain P composite sub-band signals recorded on the record carrier (48), and in that the auxiliary signal is selected in such a way that during reproduction of the composite audio signal recorded on the record carrier via a loudspeaker device said auxiliary signal is substantially imperceptable to a listener.

Patentansprüche

1. Kodierer zum Aufnehmen zusätzlicher Information in Form eines Hilfssignals v(k) in ein digitales Audiosignal u(k) eines vorbestimmten Formats, dadurch gekennzeichnet, daß der Kodierer (7) mit Mitteln (22, 28) zum Analysieren des digitalen Signals, mit Mitteln (24) zum auf eindeutige Art und Weise Quantisieren des analysierten Signals, sowie mit Mitteln (28') zum auf Grund der akustischen Eigenschaften des menschlichen Ohres Bestimmen der Menge zusätzlicher Information, die dem quantisierten digitalen Signal zugefügt werden kann, ohne daß diese zusätzliche Information bei einer unmodifizierten Detektion hörbar ist, und mit Mitteln (26) zum Kombinieren der zusätzlichen Information und des quantisierten digitalen Signals zu einem zusammengesetzten Signal versehen ist.

2. Kodierer nach Anspruch 1, dadurch gekennzeichnet, daß dieser mit Mitteln (29) versehen ist, zum Umwandeln des zusammengesetzten Signals in ein digitales Signal des vorbestimmten Formats.

3. Kodierer nach Anspruch 1 oder 2, dadurch gekennzeichnet, daß die Mittel zum Analysieren des digitalen Signals Analysenfiltermittel (22) aufweisen zum in Antwort auf das digitale Signal Erzeugen von P Teilbandsignalen, wobei diese Analysenfiltermittel das Frequenzband des digitalen Signals nach einem Filterverfahren mit Abtastfrequenzwertverringerung in Aufeinanderfolgende Teilbänder mit Bandnummern p (1 ≤ p ≤ P), wobei für jedes der betreffenden Teilbänder (P) Mittel (24(p)) vorgesehen sind zum auf eindeutige Weise Quantisieren des digitalen Signals und Mittel (26) zum Kombinieren der betreffenden quantisierten Teilbandsignale und der entsprechenden Teilbandsignale des Hilfssignals zum Bilden von P zusammengesetzten Teilbandsignalen.

4. Kodierer nach Anspruch 3 insofern abhängig von Anspruch 2, dadurch gekennzeichnet, daß der Kodierer weiterhin mit Synthesefiltermitteln (27) versehen ist zum in Antwort auf die zusammengesetzten Teilbandsignale Bilden einer Replik des zusammengesetzten Signals, wobei das Synthesefiltermittel die Teilbänder nach einem der Aufteilung in den Analysenfiltermitteln entsprechenden Filterverfahren mit Abtastfrequenzwerterhöhung zusammenfügen.

5. Kodierer nach Anspruch 4, dadurch gekennzeichnet, daß das Hilfssignal v(k) ein digitales Audiosignal ist und daß Analysenfiltermittel (23) vorgesehen sind zum in Antwort auf das Hilfssignal Erzeugen einer Anzahl von P Teilbandsignalen, wobei die Analysenfiltermittel das Frequenzband des Hilfssignals v(k) nach einem Filterverfahren mit Abtastfrequenzwertverringerung in aufeinanderfolgende Teilbänder mit Bandnummern p (1 ≤ p ≤ P) aufteilen.

6. Kodierer nach Anspruch 4 oder 5, dadurch gekennzeichnet, daß die Bandbreiten der Teilbänder den kritischen Bandbreiten des menschlichen Ohres in den betreffenden Frequenzbereichen annähernd entsprechen.

7. Kodierer nach Anspruch 4, 5 oder 6, dadurch gekennzeichnet, daß die Mittel (24) zum auf eindeutige Weise Quantisieren des digitalen Signals zum adaptiven Quantisieren dieses Signals eingerichtet sind und je Teilband die Größe des Quantisierungsschrittes von der Amplitude eines Abtastwertes des digitalen Signals abhängig ist,

wobei es zwischen den möglichen aufeinanderfolgenden Schritten einen exponentiellen Zusammenhang mit einer orbestimmten Grundzahl a gibt.

8. Kodierer nach Anspruch 7, dadurch gekennzeichnet, daß die Größe des Quantisierungsschrittes eines zu quantisierenden Abtastwertes zugleich von der Größe mindestens eines vorhergehenden Abtastwertes abhängig st.

9. Kodierer nach Anspruch 7 oder 8, dadurch gekennzeichnet, daß Mittel (25) vorgesehen sind um jedes Teilbandsignal des Hilfssignals um einen Faktor G zu dämpfen, wobei gilt: G = 2a / (a - 1).

10. Dekoder zum Gebrauch zusammen mit einem Kodierer (7) nach den Ansprüchen 5 bis 9, dadurch gekennzeichnet, daß der Dekoder (10) mit Analysenfiltermitteln (31) versehen ist zum in Antwort auf das zusammengesetzte Signal Erzeugen einer Anzahl zusammengesetzter Teilbandsignale, wobei die Analysenfiltermittel das Frequenzband des zusammengesetzten Signals nach einem Filterverfahren mit Abtastfrequenzwertverringerung in aufeinanderfolgende Teilbänder mit Bandnummern p (1 ≤ p ≤ P) aufteilen, wobei die Bandbreiten der Teilbänder denen der Analysenfiltermittel (22) in dem Kodierer entsprechen, mit Mitteln (33) zum auf eindeutige Weise Quantisieren der zusammengesetzten Teilbandsignale, mit Mitteln (34) zum Subtrahieren der betreffenden quantisierten Teilbandsignale von den entsprechenden Teilbandsignalen des zusammengesetzten Signals zum Bilden von Teilbanddifferenzsignalen und mit Synthesefiltermitteln (36) zum in Antwort auf die Teilbanddifferenzsignale Bilden einer Replik des Hilfssignals v'(k), wobei die Synthesemittel die Teilbänder nach einem der Aufteilung in den Analysenfiltermitteln entsprechenden Filterverfahren mit Abtastfrequenzwerterhöhung zusammenfügen.

11. Dekoder nach Anspruch 10, dadurch gekennzeichnet, daß die Mittel (33) zum auf eindeutige Weise Quantisieren des digitalen Signals zum adaptiven Quantisieren dieses Signals eingerichtet sind und je Teilband die Größe des Quantisierungsschrittes von der Amplitude eines Abtastwertes des digitalen Signals abhängig ist, wobei es zwischen den möglichen aufeinanderfolgenden Schritten einen exponentiellen Zusammenhang mit einer vorbestimmten Grundzahl a gibt.

12. Dekoder nach Anspruch 11, dadurch gekennzeichnet, daß Mittel (35) vorgesehen sind um jedes Teilbanddifferenzsignal um einen Faktor G zu verstärken, wobei gilt: G = 2a / (a - 1).

13. Anordnung zum Aufzeichnen eines digitalen Audiosignals auf einem Aufzeichnungsträger (48) mit einem Kodierer (7) nach einem der Ansprüche 1 bis 9.

14. Anordnung zum Aufzeichnen eines digitalen Audiosignals auf einem Aufzeichnungsträger (48) mit einem Kodierer zur Teilbandkodierung des digitalen Audiosignals einer bestimmten Abtastfrequenzwert 1/T, wobei der Kodierer mit den folgenden Elementen versehen ist:

- Analysenfiltermitteln (22) zum in Antwort auf das Audiosignal Erzeugen einer Anzahl von P Teilbandsignalen, wobei diese Analysenfiltermittel das Frequenzband des Audiosignals nach einem Filterverfahren mit Abtastfrequenzwertverringerung in aufeinanderfolgende Teilbänder mit Bandnummern p (1 ≤ p ≤ P) aufteilen, wobei diese Analysenfiltermittel weiterhin dazu eingerichtet sind, P Ausgängen die P Teilbandsignale zuzuführen, wobei diese Ausgänge gekoppelt sind mit P entsprechenden Eingängen,
- einer Aufzeichnungseinheit (47'), die zum Aufzeichnen der P Teilbandsignale auf dem Aufzeichnungsträger eingerichtet ist,

dadurch gekennzeichnet, daß die Anordnung weiterhin eine mit den Analysenfiltermitteln (22) gekoppelte Detektionseinheit (50) aufweist, daß die Detektionseinheit zum Detektieren des Vorhandenseins eines Hilfssignals in einem oder mehreren der Teilbandsignale sowie zum Erzeugen eines Steuersignals bei Detektion des Hilfssignals und zum Zuführen dieses Steuersignals zu einem Ausgang (54) eingerichtet ist, daß dieser Ausgang mit einem Steuersignaleingang (55) der Aufzeichnungseinheit (47') gekoppelt ist und daß die Aufzeichnungseinheit zum Sperren der Aufnahme des Audiosignals beim Vorhandensein des Steuersignals und zum Aufzeichnen des Audiosignals beim Fehlen des Steuersignals eingerichtet ist.

15. Anordnung zum Aufzeichnen eines digitalen Audiosignals auf einem Aufzeichnungsträger (48') mit einem Kodierer zur Teilbandkodierung des digitalen Audiosignals mit der bestimmten Abtastfrequenz 1/T, wobei der Kodierer mit den folgenden Elementen versehen ist:

- Analysenfiltermitteln (22) zum in Antwort auf das Audiosignal Erzeugen einer Anzahl von P Teilbandsignalen, wobei diese Analysenfiltermittel das Frequenzband des Audiosignals nach einem Filterverfahren mit Abtastfrequenzwertverringerung in aufeinanderfolgende Teilbänder mit Bandnummern p (1 ≤ p ≤ P) aufteilen, wobei diese Analysenfiltermittel weiterhin dazu eingerichtet sind, P Ausgängen die P Teilbandsignale zuzuführen, wobei diese Ausgänge gekoppelt sind mit P entsprechenden Eingängen,

- einer Aufzeichnungseinheit (47'), die zum Aufzeichnen der P Teilbandsignale auf dem Aufzeichnungsträger eingerichtet ist,

dadurch gekennzeichnet, daß die Anordnung weiterhin eine mit den Analysenfiltermitteln (22) gekoppelte Detektionseinheit (50) aufweist, daß die Detektionseinheit zum Detektieren des Vorhandenseins eines Hilfssignals in einem oder mehreren der Teilbandsignale sowie zum Erzeugen eines Steuersignals bei Detektion des Hilfssignals und zum Zuführen dieses Steuersignals zu einem Ausgang (54) eingerichtet ist, daß dieser Ausgang mit einer Anzeigeeinheit (56) gekoppelt ist, die dazu eingerichtet ist, beim Vorhandensein des Steuersignals anzuzeigen, daß das aufzuzeichnende Audiosignal ein mit einem Hilfssignal versehenes Audiosignal ist.

16. Anordnung nach Anspruch 14 oder 15, dadurch gekennzeichnet, daß der Kodierer weiterhin mit Signalkombiniermitteln (26, S1 bis Sp) versehen ist, die mit den Analysenfiltermitteln gekoppelt sind, daß die Signalkombiniermittel dazu eingerichtet sind, beim Fehlen des Steuersignals das Hilfssignal nach Wunsch (über 60) einem oder mehreren der Teilbandsignale hinzuzufügen zur Bildung von P zusammengesetzten Teilbandsignalen und zum Zuführen dieser P zusammengesetzten Teilbandsignale zu P Ausgängen, die mit den P entsprechenden Eingängen der Aufzeichnungseinheit (47') gekoppelt sind (Fig. 7).

17. Anordnung nach Anspruch 14 oder 15, dadurch gekennzeichnet, daß der Kodierer weiterhin mit Signalkombiniermitteln (26) versehen ist, die mit den Analysenfiltermitteln (22) gekoppelt sind, daß die Signalkombiniermittel dazu eingerichtet sind, beim Fehlen des Steuersignals das Hilfssignal einem oder mehreren der Teilbandsignale hinzuzufügen zur Bildung von P zusammengesetzten Teilbandsignalen und zum Zuführen dieser P zusammengesetzten Teilbandsignale zu P Ausgängen, die mit den P entsprechenden Eingängen der Aufzeichnungseinheit gekoppelt sind (Fig.8).

18. Anordnung nach Anspruch 14, dadurch gekennzeichnet, daß der Kodierer einen Teil des Kodierers nach einem der Ansprüche 1 bis 8 bildet.

19. Aufzeichnungsträger, auf dem mittels der Anordnung nach einem der Ansprüche 13, 16, 17 oder 18 ein digitales Audiosignal aufgezeichnet ist, dadurch gekennzeichnet, daß das Audiosignal in P Teilbandsignale aufgeteilt ist und daß zum Erhalten von P zusammengesetzten Teilbandsignalen, die auf dem Aufzeichnungsträger (48) aufgezeichnet sind, dem Audiosignal in einem oder mehreren der Teilbänder ein Hilfssignal zugefügt worden ist und daß das Hilfssignal derart gewählt worden ist, daß dieses Hilfssignal bei Wiedergabe des auf dem Aufzeichnungsträger aufgezeichneten zusammengesetzten Audiosignals über die Lautsprecheranordnung für einen Zuhörer im wesentlichen nicht wahrnehmbar ist.

Revendications

1. Codeur pour incorporer des informations supplémentaires sous la forme d'un signal auxiliaire v(k) dans un signal audionumérique u(k) ayant un format prédéterminé, caractérisé en ce que le codeur (7) comprend des moyens (22, 28) pour analyser le signal numérique, des moyens (24) pour quantifier le signal numérique analysé de manière non équivoque et des moyens (28') pour déterminer, sur la base des propriétés acoustiques du système auditif humain, la quantité d'informations supplémentaires que l'on peut ajouter au signal numérique quantifié sans que ces informations numériques supplémentaires soient audibles avec une détection non modifiée, des moyens (26) étant prévus pour combiner les informations supplémentaires et le signal numérique quantifié en un signal composite.

2. Codeur selon la revendication 1, caractérisé en ce qu'il comprend des moyens (29) pour reconvertir le signal composite en un signal numérique ayant le format prédéterminé.

3. Codeur selon la revendication 1 ou 2, caractérisé en ce que les moyens d'analyse du signal numérique comprennent des moyens de filtrage analytique (22) pour générer un nombre de P signaux de sous-bandes en réaction au signal numérique, ces moyens de filtrage analytique divisent la bande de fréquences du signal numérique en des sous-bandes consécutives ayant des nombres de bandes p (1 ≤ p ≤ P), tandis que, pour chacune des sous-bandes respectives (p), des moyens (24(p)) sont prévus pour quantifier le signal numérique de manière non équivoque et des moyens (26) sont prévus pour combiner les signaux de sous-bandes quantifiés respectifs et le signal auxiliaire pour constituer P signaux de sous-bandes composites.

4. Codeur selon la revendication 3, découlant de la revendication 2, caractérisé en ce que des moyens de filtrage synthétique (27) sont prévus pour construire une réplique du signal composite en réaction aux signaux de sous-bandes composites, ces moyens de filtrage synthétique combinent les sous-bandes selon un procédé de filtrage avec augmentation de la fréquence d'échantillonnage correspondant à la subdivision dans les moyens de filtrage analytique (22).

5. Codeur selon la revendication 4, caractérisé en ce que le signal auxiliaire v(k) est un signal audionumérique et des moyens de filtrage analytique (23) sont prévus pour générer un nombre P de signaux de sous-bandes en réaction au signal auxiliaire v(k), ces moyens de filtrage analytique divisant la bande de fréquence du signal auxiliaire en des sous-bandes consécutives ayant des nombres de bandes p ($1 \leq p \leq P$) selon un procédé de filtrage avec réduction de la fréquence d'échantillonnage.

6. Codeur selon la revendication 4 ou 5, caractérisé en ce que les largeurs des sous-bandes correspondent approximativement aux largeurs de bande critiques du système auditif humain dans les plages de fréquences respectives.

7. Codeur selon la revendication 4, 5 ou 6, caractérisé en ce que les moyens (24) pour quantifier le signal numérique de manière non équivoque sont conçus pour quantifier ce signal de manière adaptative et que, pour chaque sous-bande, la grandeur du pas de quantification dépend de l'amplitude de l'échantillon de signal numérique, une relation exponentielle avec un nombre de base préréglé a existant entre les pas successifs possibles.

8. Codeur selon la revendication 7, caractérisé en ce que la grandeur du pas de quantification d'un échantillon à quantifier dépend également de la grandeur d'au moins un échantillon précédent.

9. Codeur selon la revendication 7 ou 8, caractérisé en ce que les moyens (25) sont prévus pour atténuer chaque signal de sous-bande du signal auxiliaire d'un facteur G, qui répond à la relation $G = 2a/(a - 1)$.

10. Décodeur à utiliser en combinaison avec un codeur (7) selon les revendications 5 à 9, caractérisé en ce que le décodeur (10) comprend des moyens de filtrage analytique (31) pour générer un certain nombre de signaux de sous-bandes composites en réaction au signal composite, ces moyens de filtrage analytique subdivisant la bande de fréquences du signal composite en des sous-bandes consécutives ayant des nombres de bandes p ($1 \leq p \leq P$) selon un procédé de filtrage avec réduction de la fréquence d'échantillonnage, tandis que les largeurs des sous-bandes correspondent à celles des moyens de filtrage analytique (22) dans le codeur, des moyens (33) pour quantifier de manière non équivoque les signaux de sous-bandes composites, des moyens (34) pour soustraire les signaux de sous-bandes quantifiés respectifs des signaux de sous-bandes correspondants des signaux composites pour former des signaux de différences de sous-bandes, et des moyens de filtrage synthétique (36) pour construire une réplique du signal auxiliaire v'(k) en réaction aux signaux de différence de sous-bandes, lesdits moyens de filtrage synthétique combinent les sous-bandes selon un procédé de filtrage avec augmentation de la fréquence d'échantillonnage correspondant à la subdivision dans les moyens de filtrage analytique.

11. Décodeur selon la revendication 10, caractérisé en ce que les moyens (33) pour quantifier le signal numérique de manière non équivoque sont agencés pour quantifier de manière adaptative ce signal et que, par sous-bande, la grandeur du pas de quantification dépend de l'amplitude de l'échantillon du signal numérique, tandis qu'entre les pas successifs possibles, il y a une relation exponentielle avec un nombre de base prédéterminé a.

12. Décodeur selon la revendication 9, caractérisé en ce que des moyens (35) sont prévus pour amplifier chaque signal de différence de sous-bande d'un facteur G qui répond à la formule $G = 2a/(a - 1)$.

13. Dispositif pour enregistrer un signal audionumérique sur un support d'enregistrement (48), comprenant un codeur (7) selon l'une quelconque des revendications 1 à 9.

14. Dispositif d'enregistrement d'un signal audionumérique sur un support d'enregistrement (48), comprenant un codeur pour le codage de sous-bandes du signal audionumérique de fréquence d'échantillon donnée 1/T, ce codeur comprenant :

- des moyens de filtrage analytique (22) réagissant au signal audio pour générer une pluralité de P signaux de sous-bandes, ces moyens de filtrage analytique divisant la bande de fréquences du signal audio selon un procédé de filtrage avec réduction de la fréquence d'échantillonnage en des sous-bandes consécutives ayant des nombres de bandes p (1 ≤ p ≤ P), ces moyens de filtrage analytique étant, en outre, à même d'appliquer les P signaux de sous-bandes à P sorties, lesdites sorties étant couplées à P entrées correspondantes

- d'une unité d'enregistrement (47') qui est conçue pour enregistrer les P signaux de sous-bandes sur le support d'enregistrement,

caractérisé en ce que le dispositif comprend, en outre, une unité de détection (50) reliée aux moyens de filtrage analytique (22), que l'unité de détection est à même de détecter la présence d'un signal auxiliaire dans un ou plusieurs signaux de sous-bandes, de générer un signal de commande lors de la détection du signal auxiliaire et d'appliquer le signal de commande à une sortie (54), que ladite sortie est reliée à une entrée de signal de commande (55) de l'unité d'enregistrement (47') et que l'unité d'enregistrement est à même d'empêcher l'enregistrement du signal audio en présence du signal de commande et d'enregistrer le signal audio en l'absence du signal de commande.

15. Dispositif d'enregistrement d'un signal audionumérique sur un support d'enregistrement (48'), comprenant un codeur pour le codage en sous-bandes du signal audionumérique de fréquence d'échantillonnage donnée 1/T, dans lequel le codeur comprend :

- des moyens de filtrage analytique (22) réagissant au signal audio pour générer un pluralité de P signaux de sous-bandes, ces moyens de filtrage analytique divisant la bande de fréquence du signal audio en des sous-bandes consécutives ayant des nombres de bandes p (1 ≤ p ≤ P) selon un procédé de filtrage avec réduction de la fréquence d'échantillonnage, lesdits moyens de filtrage analytique étant, en outre, à même d'appliquer les P signaux de sous-bandes à P sorties, lesquelles sont couplées à P entrées correspondantes
- d'une unité d'enregistrement (47') qui est conçue pour enregistrer les P signaux de sous-bandes sur le support d'enregistrement,

caractérisé en ce que le dispositif comprend, en outre, une unité de détection (50) reliée aux moyens de filtrage analytique (22), que l'unité de détection est à même de détecter la présence d'un signal auxiliaire dans un ou plusieurs des signaux de sous-bandes, de générer un signal de commande par détection du signal auxiliaire et d'appliquer le signal de commande à une sortie (54), que ladite sortie est reliée à une unité de signalisation (56) et que l'unité de signalisation est conçue pour signaler que le signal audio à enregistrer, lorsqu'un signal de commande est présent, est un signal audio contenant un signal auxiliaire.

16. Dispositif selon la revendication 14 ou 15, caractérisé en ce que le codeur comprend, en outre, des moyens de combinaison de signaux (26 S_1 à S_p) reliés aux moyens de filtrage analytique, les moyens de combinaison de signaux sont à même d'ajouter sélectivement (via 60) le signal auxiliaire, en l'absence de signal de commande, à un ou plusieurs des signaux de sous-bandes pour former P signaux de sous-bandes composites et d'appliquer lesdits P signaux de sous-bandes composites à P sorties, lesquelles sont couplées aux P entrées correspondantes de l'unité d'enregistrement (47')(Fig. 7).

17. Dispositif selon la revendication 14 ou 15, caractérisé en ce que le codeur comprend, en outre, des moyens de combinaison de signaux (26) reliés aux moyens de filtrage analytique (22), que les moyens de combinaison de signaux sont à même d'ajouter le signal auxiliaire, en l'absence du signal de commande, à un ou plusieurs des signaux de sous-bandes pour former P signaux de sous-bandes composites et d'appliquer lesdits P signaux de sous-bandes composites à P sorties, lesquelles sont couplées aux P entrées correspondantes de l'unité d'enregistrement (Fig. 8).

18. Dispositif selon la revendication 14, caractérisé en ce que le codeur fait partie d'un codeur selon l'une quelconque des revendications 1 à 9.

19. Support d'enregistrement sur lequel un signal audionumérique a été enregistré à l'aide d'un dispositif selon l'une quelconque des revendications 13, 16, 17 ou 18, caractérisé en ce que le signal audio est divisé en P signaux de sous-bandes et que le signal audio est combiné avec un signal auxiliaire dans une ou plusieurs de sous-bandes de manière à obtenir P signaux de sous-bandes composites enregistrés sur le support d'enregistrement (48) et que le signal auxiliaire est sélectionné de telle manière qu'au cours de la reproduction du signal audio composite enregistré sur le support d'enregistrement via un dispositif à haut-parleur, ledit signal auxiliaire soit sensiblement imperceptible à un auditeur.

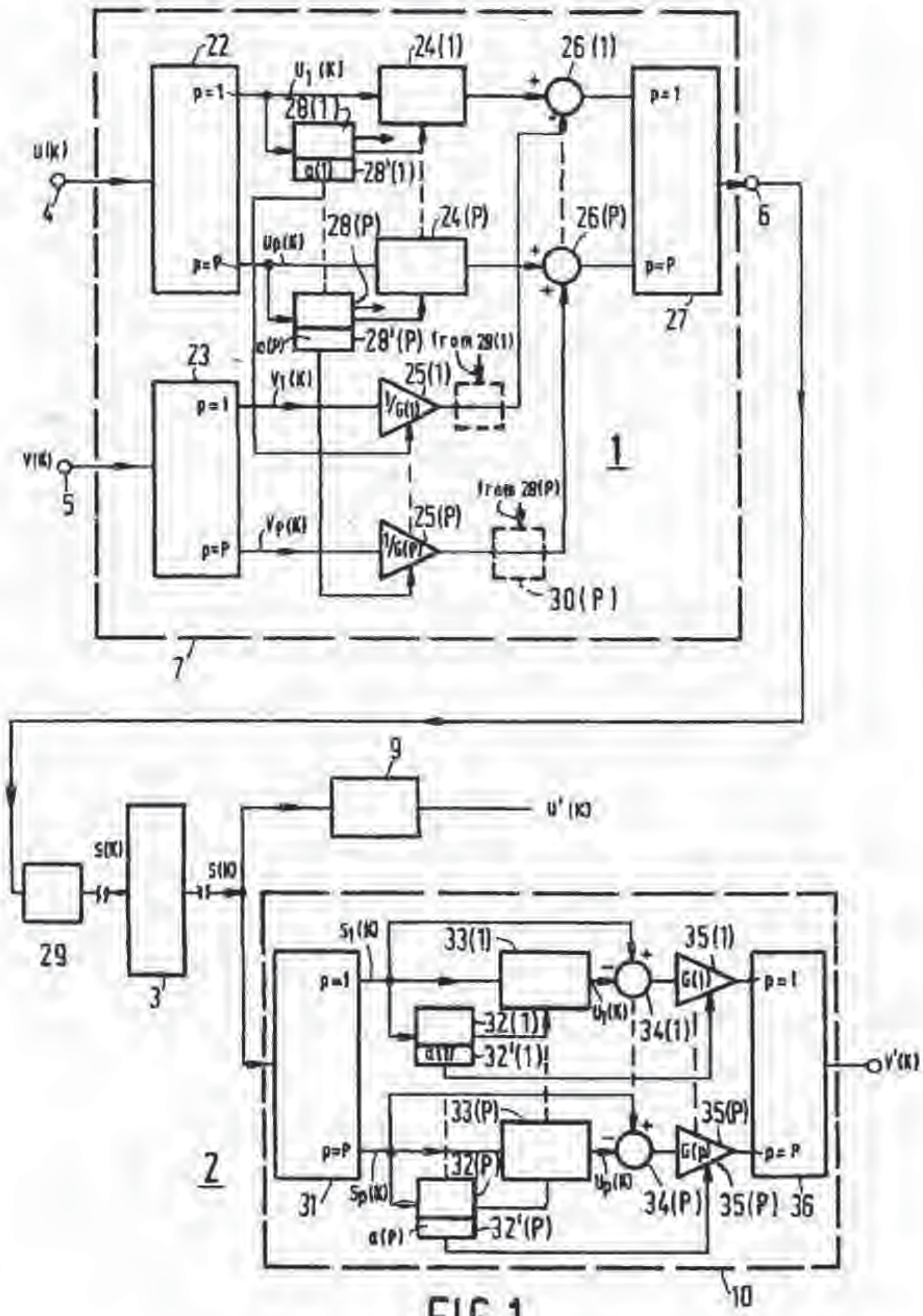

22
24(1)
26(1)
p=1
U_1(K)
28(1)
u(K)
4
a(1)
28'(1)
6
28(P)
24(P)
26(P)
U_p(K)
p=P
27
a(P)
28'(P)
from 29(1)
23
V_1(K)
25(1)
1/G(1)
V(K)
1
5
from 28(P)
V_p(K)
25(P)
1/G(P)
30(P)
7
9
U'(K)
S(K)
29
3
10
S_1(K)
33(1)
35(1)
G(1)
U_1(K)
32(1)
34(1)
32'(1)
V'(K)
33(P)
35(P)
G(P)
32(P)
2
31
S_p(K)
U_p(K)
34(P)
36
a(P)
32'(P)

FIG.1

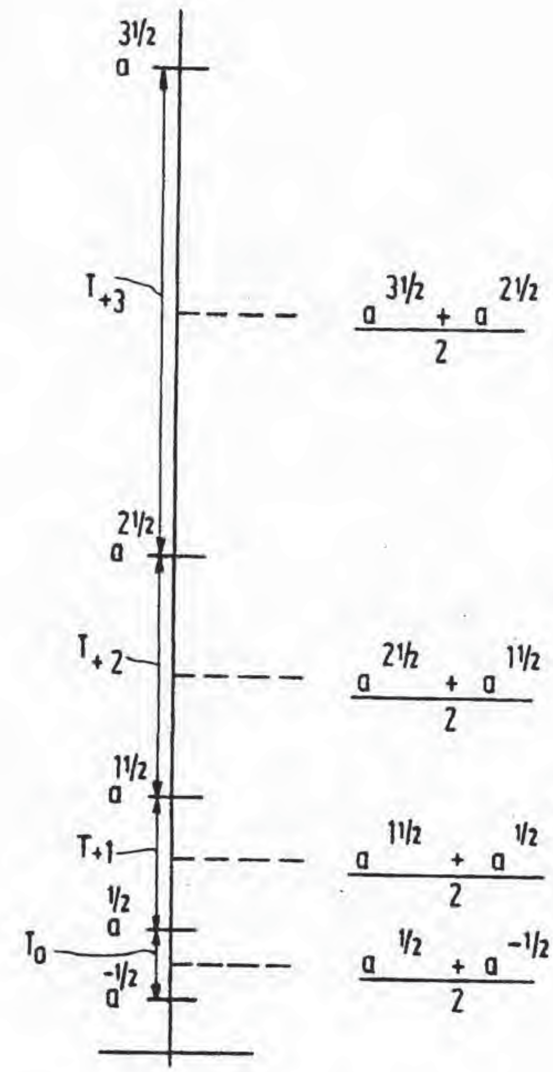
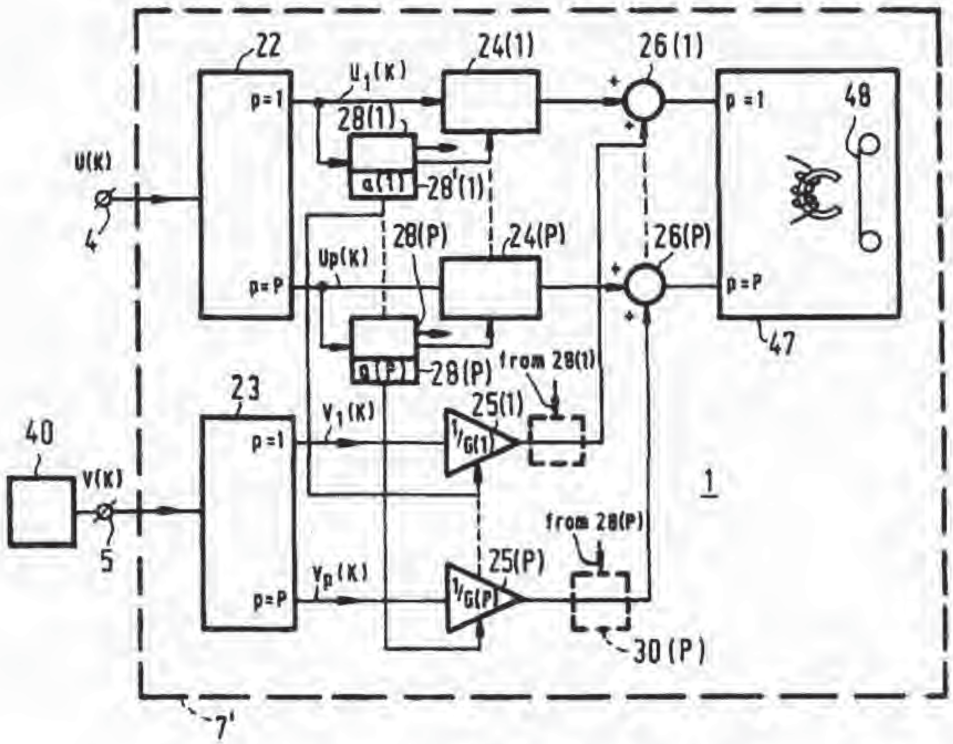
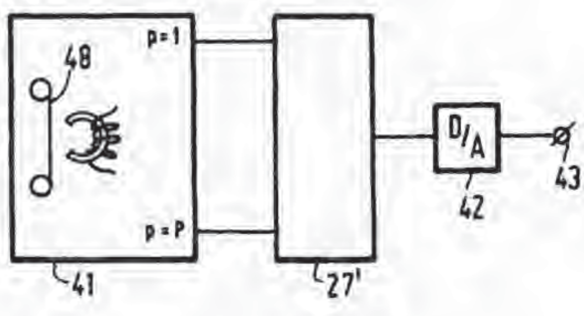

$a^{3\frac{1}{2}}$
T_{+3}
$\frac{a^{3\frac{1}{2}} + a^{2\frac{1}{2}}}{2}$
$a^{2\frac{1}{2}}$
T_{+2}
$\frac{a^{2\frac{1}{2}} + a^{1\frac{1}{2}}}{2}$
$a^{1\frac{1}{2}}$
T_{+1}
$\frac{a^{1\frac{1}{2}} + a^{\frac{1}{2}}}{2}$
$a^{\frac{1}{2}}$
T_0
$a^{-\frac{1}{2}}$
$\frac{a^{\frac{1}{2}} + a^{-\frac{1}{2}}}{2}$

FIG. 2



22
24(1)
26(1)
U(K)
p=1
U1(K)
28(1)
a(1)
28'(1)
28(P)
24(P)
26(P)
Up(K)
p=P
a(P)
28'(P)
from 28(1)
48
47
4
23
40
V(K)
V1(K)
25(1)
1/G(1)
1
from 28(P)
5
Vp(K)
25(P)
1/G(P)
30(P)
7'

FIG. 3



48
p=1
p=P
41
27'
D/A
42
43

FIG. 4

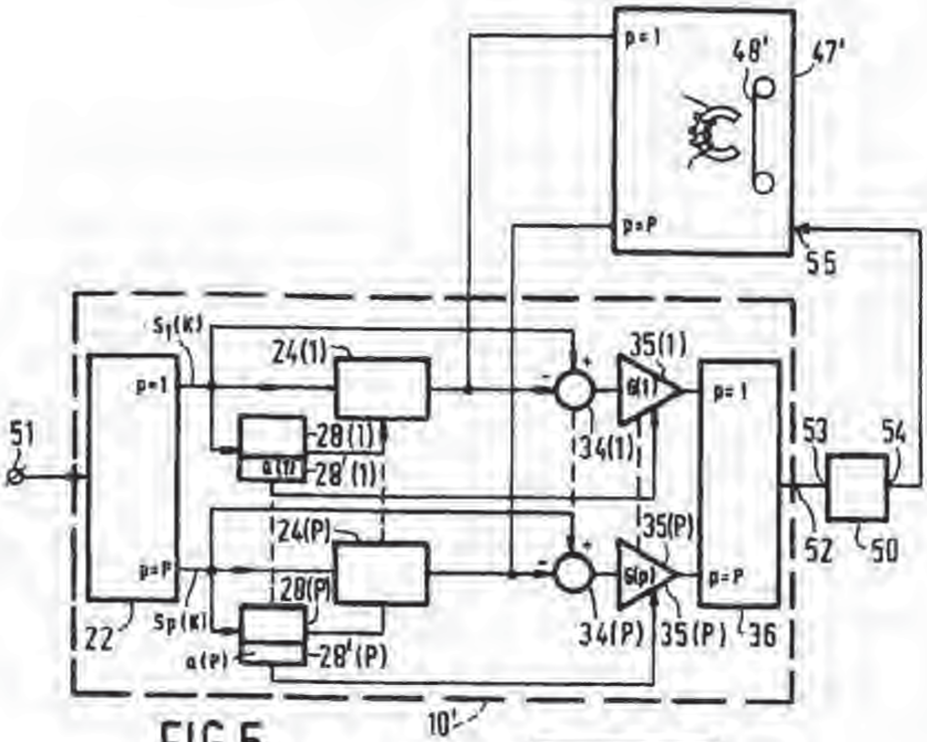

p=1
48'
47'
p=P
55
S1(K)
24(1)
35(1)
p=1
G(1)
p=1
51
28(1)
q(1)
28'(1)
34(1)
53
54
24(P)
35(P)
p=P
28(P)
G(p)
p=P
52
50
Sp(K)
22
q(P)
28'(P)
34(P)
35(P)
36
10'

FIG.5

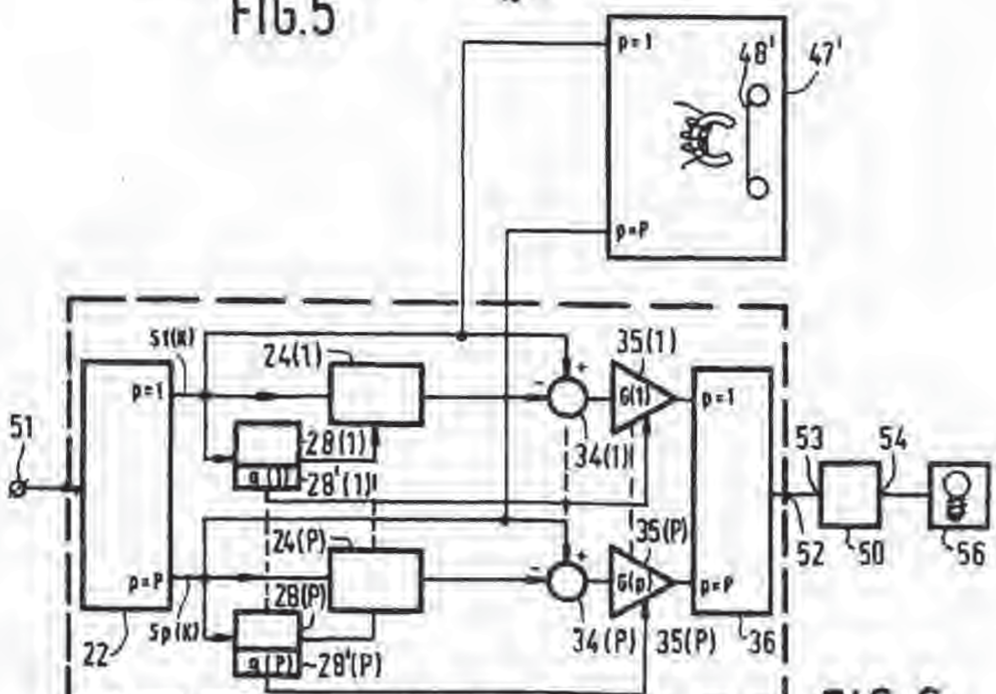

p=1
48'
47'
p=P
S1(K)
24(1)
35(1)
p=1
G(1)
p=1
51
28(1)
q(1)
28'(1)
34(1)
53
54
24(P)
35(P)
52
50
56
p=P
28(P)
G(p)
p=P
Sp(K)
22
q(P)
28'(P)
34(P)
35(P)
36
10'

FIG. 6

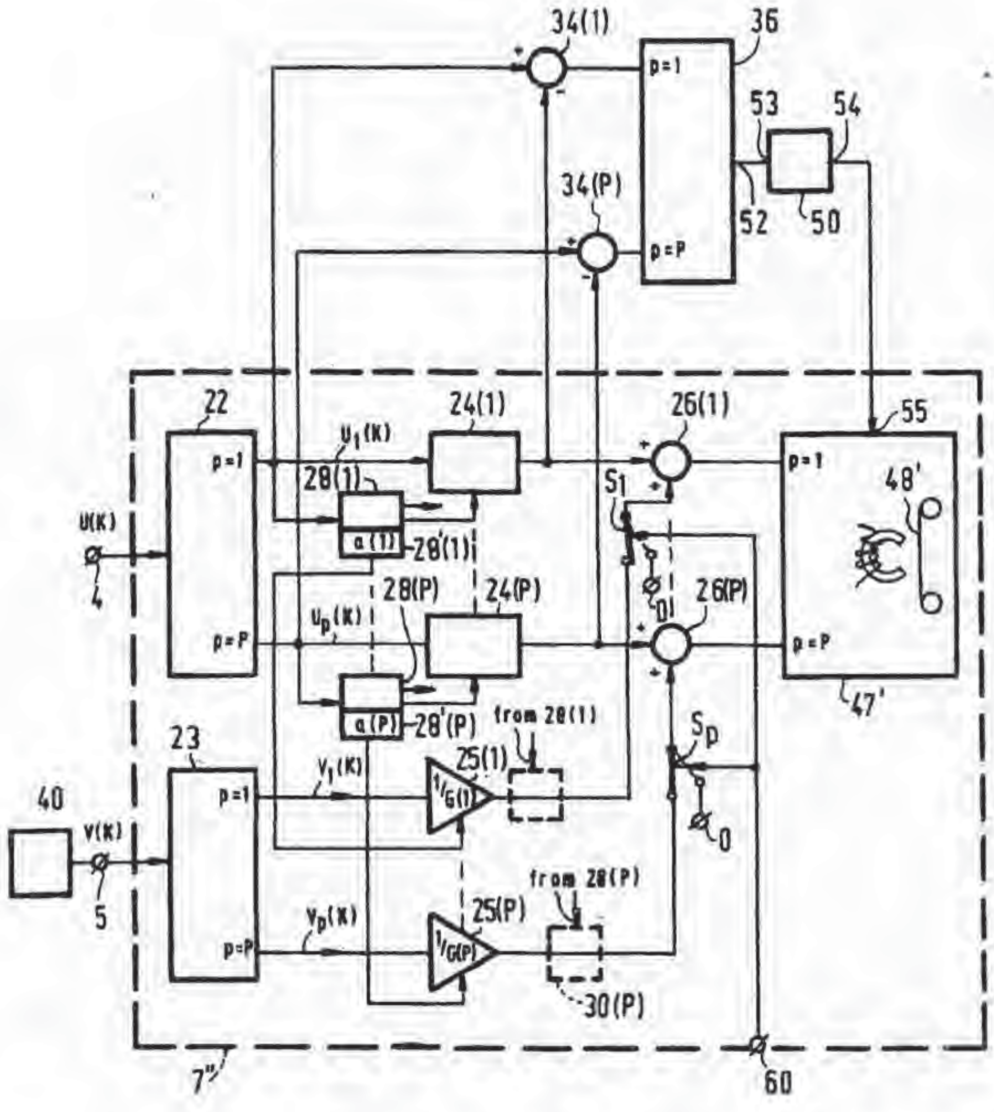

34(1)
36
p=1
53
54
34(P)
52
50
p=P
22
24(1)
26(1)
55
p=1
U1(K)
28(1)
S1
p=1
48'
U(K)
α(1)
28'(1)
4
28(P)
24(P)
26(P)
Up(K)
p=P
p=P
47'
α(P)
28'(P)
from 28(1)
23
Sp
V1(K)
25(1)
40
p=1
1/G(1)
V(K)
0
5
from 28(P)
Vp(K)
25(P)
p=P
1/G(P)
30(P)
7"
60

FIG.7

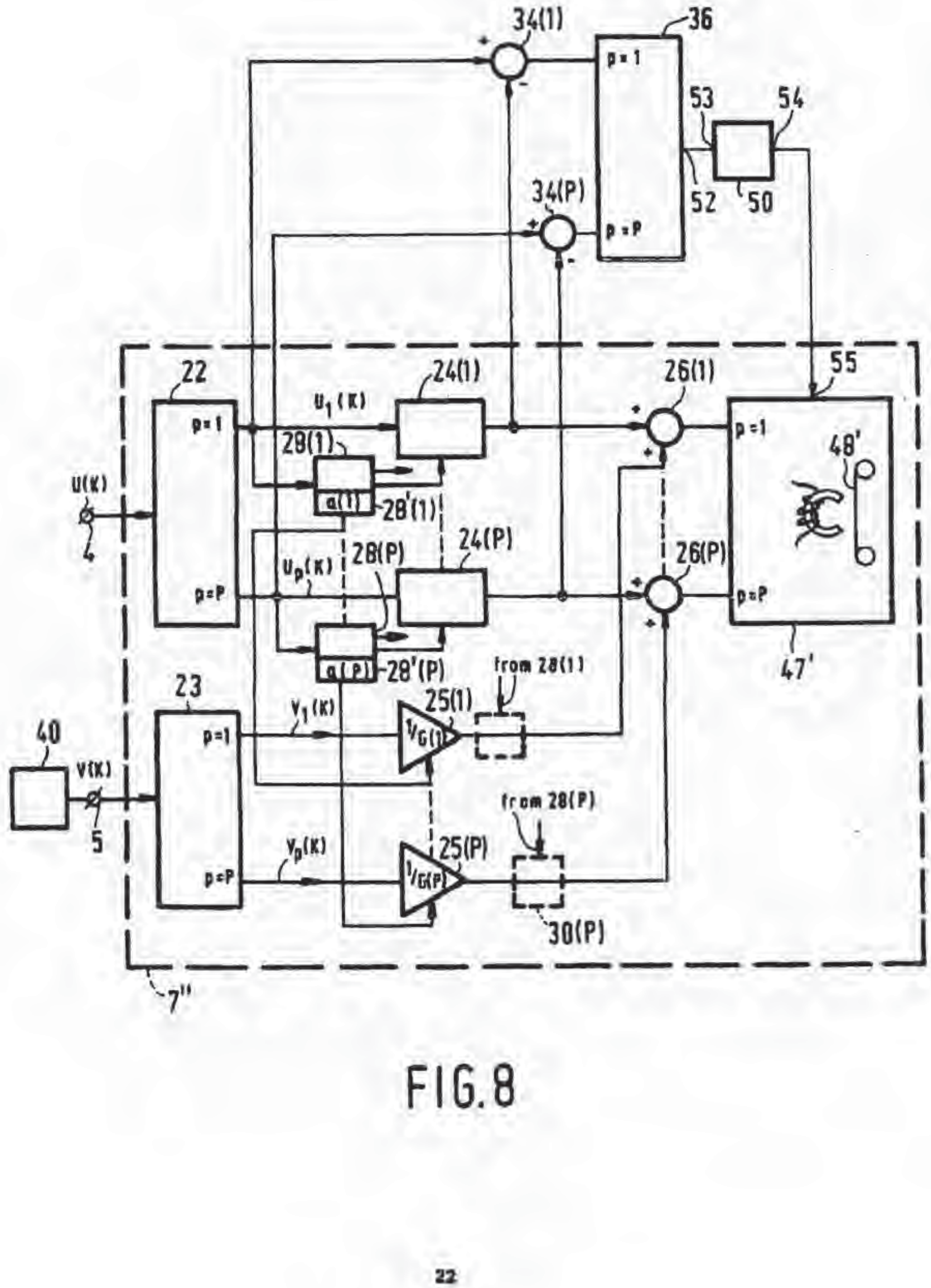

34(1)
36
p=1
53
54
52
50
34(P)
p=P
22
24(1)
26(1)
55
u1(K)
p=1
28(1)
p=1
48'
u(K)
a(1)
28'(1)
4
24(P)
up(K)
28(P)
26(P)
p=P
p=P
a(P)
28'(P)
from 28(1)
47'
23
y1(K)
25(1)
40
p=1
1/G(1)
v(K)
5
from 28(P)
yP(K)
25(P)
p=P
1/G(P)
30(P)
7''

FIG.8

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06K 19/08, 19/10, H04L 9/00 — A1

(11) International Publication Number: WO 98/37513

(43) International Publication Date: 27 August 1998 (27.08.98)

(21) International Application Number: PCT/AU98/00106

(22) International Filing Date: 20 February 1998 (20.02.98)

(30) Priority Data:
PO 5218 — 20 February 1997 (20.02.97) — AU

(71) Applicant (for all designated States except US): TELSTRA R & D MANAGEMENT PTY. LTD. [AU/AU]; 242 Exhibition Street, Melbourne, VIC (AU).

(72) Inventors; and
(75) Inventors/Applicants (for US only): JOHNSON, Andrew [AU/AU]; 21 Sunbury Crescent, Surrey Hills, VIC 3127 (AU). BIGGAR, Michael [AU/AU]; 24 Kalbar Road, Research, VIC 3095 (AU).

(74) Agents: LESLIE, Keith et al.; Davies Collison Cave, 1 Little Collins Street, Melbourne, VIC 3000 (AU).

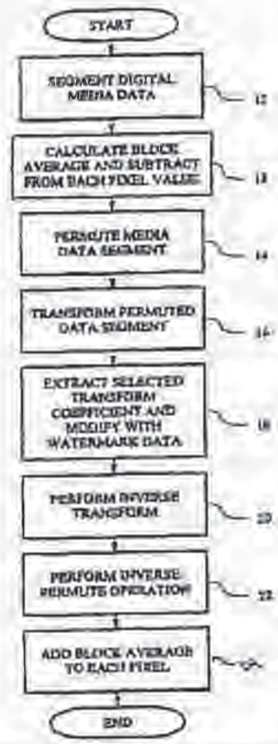
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, GW, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: INVISIBLE DIGITAL WATERMARKS

(57) Abstract

A method and system of insertion and extraction of identification or authentication (watermark) data in digital media data such as video. The video data is divided into blocks and a pseudo-random function, such as a permutation, is applied thereto. The permuted data block is then transformed using an orthogonal transform such as a Walsh Hadamard Transform or a Discrete Cosine Transform. One or more of the ac coefficients generated by the transform are selected and the watermark data is inserted or extracted therefrom. An inverse permutation and inverse transform can then be used to return the video to the unencoded spatial domain. The inserted watermark data is substantially invisible in the reconstructed video since it is spread over the pixels in the block by virtue of the permute and transform.



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		

INVISIBLE DIGITAL WATERMARKS

This invention relates to the provision of identification or authentication data, sometimes referred to as a watermark or signature, in digital media data such as digital image or audio data. In particular, the present invention relates to a method and apparatus for incorporating a watermark in digital media data, and a method and apparatus for retrieving or extracting a watermark from digital media data in which a watermark has been previously incorporated.

In this specification the term "watermark" is used to refer to any distinctive or distinguishing data which may be used for identification or authentication of the digital media data associated therewith, or of some attribute of the media data such as the source thereof. A watermark may comprise image data, such as pixel data forming a logo or the like, or may be in the form of coded text and/or binary numbers, for example, which represent a message. In some applications the watermark data may include error correction coding techniques to improve the robustness of the watermark to image manipulation. The format of the signal that is to be watermarked is not restricted to a multi dimensional representation. It is also possible for audio information to be watermarked. This method of encoding data is not restricted to information associated with copyright and could be used to convey any suitable information in a hidden manner.

Watermarks are utilised in media data for a number of reasons, one being to prevent or discourage copying of the media data if it is subject to copyright, or to at least allow for identification of the media data even if it is copied. Visible watermarks have been employed for many years in varying applications including banknotes and photographs, but have significant disadvantages because of their visible nature. Although a visible watermark may be quite effective in discouraging copying of an associated image, in general it is considered disadvantageous for a watermark to be obtrusive upon the original image.

Besides the issue of whether or not the watermark is visible in an associated image (or audible in the case of watermarked audio media), several other factors are also considered important.

For one, the watermark should be robust to manipulation of the watermarked media, and should be secure so as to not be easily removable by a malicious user. Before the advent of digital media processing and manipulation, a degree of robustness and security was inherent in a visible watermark, because a copy of the watermarked image would generally bring with it the visible watermark itself which would be difficult to remove. However, digital processing makes it possible to perform many sophisticated manipulative operations on watermarked media, which may degrade the visible watermark or be utilised to alter an image to at least substantially remove the watermark. In this case, therefore, the properties of a visible watermark count against the security thereof since it is clearly visible what must be removed or altered in the watermarked image. A paper entitled "Protecting publicly-available images with a visible image watermark" (Gordon Braudaway, Karen Magerlein & Fred Mintzer; SPIE Vol. 2659, pp 126-133) discusses robustness and security in visible image watermarks.

Visible watermarks are considered unsuitable for many modern applications because of the intrusive effect of the watermark on the original media. Watermarking schemes have been developed in which the watermark is substantially invisible on an original image but readily visible on a copy thereof. However, such schemes generally rely upon characteristics of photocopying or electronic scanning apparatus, and so are only suitable for a limited range of applications, such as in images or text on paper documents. In any event, these watermarking schemes are also subject to security difficulties arising from digital processing and manipulation.

In media involving a sequence of images, such as video media, it is particularly undesirable for a watermark to be intrusively visible, since considerable effort is expended in providing the image data to the user in a form which is as visually clear as possible, and a visible watermark may significantly detract from the original image. Visible watermarks are presently used in some video applications, particularly television coverage of live sporting events where a relatively small and faint logo or the like is superimposed on the television picture, typically near one corner thereof. This is not completely satisfactory, besides the visual intrusion, because the logo can be easily cropped from the picture in a copy thereof, or could be relatively easily removed, at least substantially, with digital processing techniques. To make the visible watermark more secure it should be placed over the visually most important part of the image, which also makes the watermark more intrusive and thus less desirable.

Invisible watermarking techniques, particularly for digital media data, have been developed, and one is described in an article entitled "Watermarking Digital Images for Copyright Protection" (J.J.K. O'Ruanaidh, F.M. Boland & O. Sinnen). This article discloses a method of embedding a watermark in a digital image which is said to be invisible and quite robust. The image data is divided into rectangular blocks, and each block is then transformed using either a Walsh transform, discrete cosine transform (DCT) or wavelet transform. The bits defining the watermark graphic are inserted in the digital image by incrementing or decrementing a selected coefficient in the transform domain of the data block. Coefficients are selected according to a criterion based on energy content. Another algorithm described in the article relates to insertion of watermark data based on the use of the discrete Fourier transform (DFT). This method differs fundamentally from the transform domain technique outlined above. The DFT is a complex transform that generates complex transform domain coefficients given a real valued input. The watermark is placed in the phase component of generated transform coefficients when using this transform.

Another article which addresses the difficult issues of digital watermarking is "Secure Spread Spectrum Watermarking for Multimedia" (Ingemar J Cox, Joe Kilian, Tom Leighton & Talal Shamoon; NEC Research Institute, Technical Report 95-10). This article describes an invisible digital watermarking method for use in audio, image, video and multimedia data. The method described in this article also involves a frequency domain transform of the image data and insertion of the watermark data whilst in the transform domain. In practice, in order to place a length n watermark into an N x N image, the discrete cosine transform of the image is computed, and the watermark data encoded into the n highest magnitude coefficients of the transform matrix, excluding the dc component. In other words, the watermark data is placed in transform domain components of greatest perceptual significance, which enables the watermark to be robust to image distortion and unauthorised removal without serious degradation of the image itself. This watermarking algorithm employs an energy compacting transform, which makes the selection of transform coefficients for encoding of the watermark data very important. For most images the coefficients selected will be the ones corresponding to the low spatial frequencies, with the result that significant tampering of the image at those frequencies would destroy the image fidelity before the encoded watermark. The watermarking techniques of J.J.K O'Ruanaidh et al and Ingemar J. Cox et al require the original image when performing the watermark extraction operation. As a consequence, proof of ownership is accomplished only if the original image is certified as being the original by a trusted third party, and the particular segment of the original image must be first identified and found before ownership is verified.

The present invention addresses some of the difficulties identified in the prior art, and embodiments of the invention aim to provide a digital watermarking process in which:

1. the presence of the watermark is invisible (i.e. the watermarked visual or audio material is visually or auditorially substantially indistinguishable from the original);

2. the watermark is robust to signal manipulation and distortion;

3. the watermark is secure;

4. the original media data is not required in order to extract the watermark; and

5. the watermark can be inserted and/or extracted by a simple computational procedure which can be done in real time.

In accordance with the present invention, there is provided a method for inserting identification or authentication data into digital media data, including the steps of:

segmenting the digital media data into data blocks;

applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block;

applying an orthogonal transform on the modified data block to obtain transform domain data;

modifying at least one selected transform domain data coefficient in accordance with identification or authentication data;

inverse transforming the transform domain data having the at least one modified coefficient; and

applying an inverse pseudo-random function to obtain watermarked digital media data.

The present invention also provides a method for extracting identification or authentication data from watermarked digital media data, including the steps of:

segmenting the digital media data into data blocks;

applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block;

applying an orthogonal transform to the modified data block to obtain transform domain data; and

extracting identification or authentication data from at least one coefficient of the transform domain data.

Preferably, the pseudo-random reversible function has the property of flattening the power spectral density of the data block (i.e. the function performs a spectral whitening operation), such that each coefficient then generated by the transform contributes substantially equally to the total energy of the block. This allows the watermarking process to be less sensitive, with regard to the introduced distortion, to the selection of the transform coefficient which is modified in the watermark insertion operation.

The insertion and/or extraction method can be performed in real time, which is particularly advantageous when the digital media data has presentation timing restrictions, such as in the case of real time video and/or audio data.

It is preferred for optimal performance that the average (dc) component of the transformed media data be restricted to a single known transform coefficient and that this transform coefficient is not available for modification by the watermark insertion operation. It is also preferred that the pseudo-random reversible function be tolerant to the introduction of noise resulting from signal processing that could subsequently be performed on the watermarked media data. Many different pseudo-random functions could be used for this application. One pseudo-random function that offers good performance in terms of its noise rejection capability, spectral flattening performance and simplicity of implementation is a permutation of the data block based upon a keyed random number generator. In that case, the user should ensure that a permutation is selected that exhibits the desired spectral whitening characteristics as this is not guaranteed by all permutations.

A number of different transforms exist that could be used as the orthogonal transform operation in the preferred method. These include the Walsh Hadamard Transform (WHT), Discrete Cosine Transform (DCT), Discrete Sine Transform (DST) and Fast Fourier Transform (FFT). The Walsh Hadamard Transform is the preferred choice due in part to its low implementation complexity. The AC transform coefficients generated with such a transform in conjunction with an appropriate pseudo-random function, using real image data as input, are characterised by all possessing approximately equal energy. The selection of transform coefficient(s) for modification can thus be based on a random keyed operation to further enhance the security of the watermark.

For functions and transforms that do not restrict the average value of the data block to a single transform coefficient, it is preferred (to minimise watermark visibility) that the average (dc) value for the data block is calculated, stored, and subtracted from each data value in the data block prior to the application of the of the pseudo-random function. The average value is subsequently retrieved and added to each data value making up the watermarked data block immediately after the application of the inverse pseudo-random function.

The application of the pseudo-random function and the application of the orthogonal transform can be combined into a single operation. Similarly with respect to the inverse pseudo-random function and inverse transform. A combined data permutation and transform operation can be considered equivalent to, in the one dimensional case, performing a permutation upon the columns making up the basis matrix of the transform in question. Each permutation will yield an orthogonal transform, hence the number of transforms contained in the set is equal to the number of available permutations. Using this interpretation, the security of the watermark relies not just on which transform coefficient has been modified to contain the watermark data, but also on which member of the set of available transforms has been used.

The present invention further provides apparatus for inserting or extracting watermark data in digital media data, comprising:

segmenting means for segmenting the digital media data into data blocks;

processing means for applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block and performing a transform on the modified data block to obtain transform domain data; and

means for inserting or extracting watermark data in at least one coefficient of the transform domain data.

Preferably, in the case where watermark data is to be inserted in the digital media data the processing means is also adapted to perform an inverse transformation and inverse pseudo-random function on the transform domain data containing the watermark data so as to obtain watermarked digital media data.

In practice, the segmenting of the digital media data into data blocks might comprise forming blocks of 64x64 pixels of image luminance pixel data, where the watermark is to be inserted into a still image or image sequence. The block size need not be restricted to being square and of dimension 64x64 pixels, both smaller and larger block sizes are possible depending upon application requirements. In practice, the identification/authentication data which is inserted into a data block of digital media data might comprise a pixel from a binary graphic, or data in the form of bits used to represent text and binary numbers, for example. The watermark data is inserted into the data block that has undergone a block transform operation. The distortion introduced due to the insertion of watermark data is dependent upon the block size, the number of transform coefficients modified by the insertion operation and the magnitude of the modification. The watermark data density per block is arbitrary depending upon application requirements. In general, however, the higher the density the more visually noticeable is the inserted watermark in the image. A series of data blocks may be contained in a single image frame or spread over a number of image frames.

The invention is described in greater detail hereinafter, by way of example only, with reference to the accompanying drawings, wherein:

Figure 1 is a flowchart illustrating operations for inserting watermark data into digital media data;

Figure 2 is a flowchart illustrating operations for extracting watermark data from digital media data;

Figure 3 is a diagram of the watermark insertion process of a preferred embodiment of the present invention;

Figure 4 is a flowchart illustrating the operations for a particular implementation of the watermarking insertion procedure;

Figure 5 is a block diagram of watermarking apparatus for real-time video; and

Figure 6 is a block diagram of a media monitoring system.

This invention relates to the insertion and extraction of identification or authentication data for use as a watermark in digital media data, such as digital image data, still or sequential, digital audio data or the like. A watermark provided in digital media data may provide a means for identification of the source or some other attribute of the media data as may be required to prove copyright ownership, for example. As mentioned above, embodiments of the present invention are designed to have a number of advantageous properties, including:

the watermark presence being at least substantially invisible (ie the watermarked visual or audio material is visually or auditorially substantially indistinguishable from the original);

the watermark can be inserted and/or extracted by a simple computational procedure which can be done in real time for audio and/or video media data; and

the original media data not being required in order to extract the watermark from the watermarked media data.

Additionally, as also discussed above, it is desirable for watermarks in digital media data to also be both secure in that a malicious user cannot easily remove or disguise the watermark so as to prevent extraction, and robust to enable the inserted watermark to survive manipulation of the watermarked media data. Digital images and image sequences, for example, are seldom stored or transported over a communications link in their raw format. Frequently some form of compression may be applied to the media data, and it is therefore important that the signal processing associated with the compression algorithm does not remove or wash out the associated watermark inserted in the media data.

Although the following description of embodiments of the present invention refer primarily to still or sequential image data, it is to be understood that the invention is equally applicable to other forms of digital media data, such as digitised audio data.

In an embodiment of the invention, image pixel data is subdivided into 64 x 64 pixel spatial domain blocks in order to provide a manageable data segment in which to insert watermark data. For example, a digital image comprising 1,024 x 768 pixels may be nominally divided into blocks of 64 x 64 pixels so that the entire image is contained in an array of 16 x 12 image data blocks (a total of 192 data blocks). Different watermark data may then be inserted into each data block, so that the watermark data is spread over the entire image. For example, the watermark might comprise a 16 x 12 pixel logo or the like, so that a value representing each pixel of the logo is inserted in a respective data block of the digital image. Alternatively, the watermark may comprise a text message formed in ASCII code and/or binary numbers. A message comprising of 192 bits could be inserted in the digital image if a watermark density of 1/ 4096 (one bit per 64x64 block) was employed.

The invisibility and robustness of the watermark are aided by dividing the image into blocks and distributing the watermark data throughout the data blocks, and are further facilitated by the insertion procedure utilised to insert the watermark data into each data block. The following steps are used to insert a watermark data bit or binary pixel graphic into a 64 x 64 spatial domain luminance data block.

(i) Permute the 64x64 data block using a predetermined random permutation. There exist 4096 factorial different ways in which this permutation can be performed. To minimise the distortion introduced by the watermark modification, a permutation should be selected that performs a spectral whitening operation on a signal that has a predominant low pass power spectral density. The permutation is generated from a keyed pseudo-random operation.

(ii) Transform the permuted data using a Walsh Hadamard Transform. This transform can be implemented as a 4096-point one dimensional fast transform operation.

(iii) Watermark data is inserted into the data block by modification of selected transform coefficient(s). The coefficient selection process is based on a keyed-pseudo random operation, and does not include the dc coefficient in set of coefficients available for modification. To maximise security of the watermarking process, different coefficients are selected via the pseudo-random operation for each data block.

A watermark data bit can be represented by the sign of a selected transform coefficient. A transform coefficient value greater than or equal to zero could represent logic zero and the negative values logic one. Transform coefficient(s) need only be modified if necessary, to ensure that the sign (+/-) corresponds the digital bit to be embedded (1/0).

(iv) An inverse transform is then applied to reconstruct an approximation of the original

64x64 spatial domain data block. In the transform domain, the watermark data is completely contained by one transform coefficient when using a watermark data density 1/4096. In the spatial domain, however, the watermark data is distributed over each of the pixels making up the 64x64 data block.

The watermark read operation is accomplished by repeating steps (i) and (ii) above. The original image or image sequence is not required for the reading operation. The watermark data can be extracted with the knowledge of the permutation applied to the data block, the transform operation, and which of the transform coefficient(s) modified to contain the watermark data. The permutation employed is preferably kept secret by the owner of the image or image sequence. The permutation could be represented by a secret seed number to a well defined pseudo random number generator.

Block transforms such as the classic Walsh Hadamard Transform (WHT), Discrete Cosine Transform (DCT), Discrete Sine Transform (DST) and the Haar Transform (HT) can be employed in the watermarking process in embodiments of the invention. For transforms that isolate the average block value or dc value into one coefficient, that coefficient should not be used to contain watermark data. The WHT is the preferred choice for the transform operation due to its low implementation complexity. Fast transform implementations of the WHT exist that require only summing and one scaling operation, and the transform basis vector contains only +1 and -1 elements. The analysis and synthesis transforms are identical.

Figure 1 illustrates a flow chart of operation involved in insertion of watermark data into digital media data, according to an embodiment of the invention. Beginning at step 12, the digital media data is first segmented into manageable data blocks such as blocks of 64x64 pixels or equivalent data elements. Step 13 calculates the average pixel value for the block which is then subtracted from each pixel. Step 13 is unnecessary when using a transform that contains the block average in a single transform coefficient. This is the case with the WHT and the DCT, for example. The resulting dc transform coefficient should not, however, be used to contain watermark data. The media data block or segment is then subjected to a permute operation (step 14) in which the data elements of the block or segment are rearranged in a pseudo random, but repeatable and reversible manner. Next, at step 16, the permuted spatial domain media data segment is subjected to the transform operation. In this embodiment one of the transform coefficients is selected and modified to include watermark data. When watermarking images or image sequences a watermark data bit could be represented by the sign of the selected transform coefficient. A transform coefficient value greater than or equal to zero could represent logic zero and the negative values logic one.

The watermark data density per block in this case is 1/4096. In some applications, densities greater than 1/4096 may be required.

Following insertion of the watermark data into the transform domain of the media data, the spatial domain media data is then reconstructed through steps 20, 22 and 23 by performing an inverse transformation followed by an inverse permute operation and then the previously subtracted block average value added to each pixel making up the block. Again, step 23 is not necessary when using a transform that contains the block average in a single transform coefficient. The resulting digital media data segment contains watermark data which is robust to manipulation thereof, secure from unauthorised removal, and yet the reconstructed, watermarked media data is substantially indistinguishable from the original spatial domain media data when compared in subjective quality testing.

In order to extract the watermark data form digital media data in which watermark data has been previously inserted, the procedure outlined in the flow chart of Figure 2 may be employed. Essentially this involves steps mirroring the first half of the procedure illustrated in Figure 1. The digital media data is first segmented as discussed previously (step 32), the average pixel value for that block is determined and subtracted from each pixel (step 33) if necessary. The resulting data block is then subjected to a permute operation as shown at step 34. The permute operation must be the same as that performed during insertion of the watermark data, and thus if different permute operations are variously employed, some record must be maintained of which of the particular 4096 factorial permutations applies to the particular media data segment in question. This could be in the form of a secret seed to a well defined pseudo random number generator. The permuted media data segment is then transformed with the same transform used by the insertion operation (step 36). Then it is a simple matter to extract the particular coefficient for the transform domain media data and then recover from this the watermark information.

Figure 3 illustrates a block diagram of the watermark insertion process described in connection with the flow chart of Figure 1. As discussed above, in this embodiment only a single watermark data component, eg a data bit or binary graphic pixel, is inserted into each selected digital media data segment or block, and the information required to reconstruct an entire watermark requires the examination of a number of digital media data segments.

Figure 4 is a flow chart illustrating the insertion process of watermark data into digital media data, which has been segmented into data blocks, over a series of data blocks. Where the digital media data comprises a sequence of images, such as in the case of digital video or the like, a complete watermark (eg the total of the identification data) may in fact be distributed over more than one image or image frame. At step 42 the first data block in the image or sequence of images is selected and, if necessary, the average of that block is then calculated and subtracted from each pixel element in step 43. The resulting data block forming the image segment is subjected to a permute operation, as described hereinabove, at step 44. The permuted image data is then transformed using a block transform. At step 47 a particular transform coefficient is selected for possible modification. The selection process is performed in a pseudo random deterministic manner. Transforms that contain the block average (dc) in one transform coefficient, or set of coefficients, must eliminate this coefficient from the selection process. Step 48 performs the modification operation to incorporate the watermark data into the selected transform coefficient(s). The inverse of the transformation and permute operations are then applied at steps 50 and 52 and step 53 adds to each pixel value the average as determined in step 43, if necessary. A test is then applied at step 54 to determine whether the media data has finished, and if so the watermarking procedure ends. Otherwise, the next block of the digital media data is selected at step 56. The watermark data is then incremented, meaning the next component of the watermark data, such as the next data bit or binary pixel element, is selected at step 58. Of course, it will be recognised that it is unnecessary for every data block of a particular digital media data source to be encoded with watermark data, and only a certain selection of data blocks may in fact be encoded with watermark data in practice. To provide copyright protection for the complete image sequence, the watermark can be repeatedly inserted, with the watermark beginning at different frame locations within the sequence and ensuring that watermarks do not overlap. Of course, acquisition of the signal is important. This can be accomplished, by incorporating in the watermark data, synchronisation information that, once acquired informs the watermark reader the location of the beginning of the watermark message data or binary graphic

To increase robustness and ensure readability even in the case where the original video signal is significantly changed, such as through reduced spatial resolution or the case where watermarked interlaced material is later converted to non-interlaced format, the watermark can be distributed across both fields in such a way that the watermark can be independently read from either or both fields and/or restricted to the low spatial frequencies. The latter may be accomplished by the application of a 2x2 WHT on each row of the image to produce low and high spatial frequency components. The watermark is then inserted in only the half horizontal resolution frame corresponding to the low spatial frequencies. The full resolution watermarked frame is produced by performing an inverse 2x2 WHT on the rows making up the low spatial frequency watermarked half horizontal resolution frame and the original high spatial frequency half horizontal resolution frame.

In order to further improve security of the watermarking procedure, it is possible to alter the permute operation periodically (step 60 in Figure 4). As mentioned above, it is nevertheless necessary that the particular permute operation performed on each data block be repeatable at a future time to enable extraction of the watermark.

Figure 5 illustrates a block diagram of watermarking apparatus for encoding real time video with watermark data according to an embodiment of the present invention. Real time video feed is provided to the apparatus at a buffer 80 or the like, which provides an input to real time processing circuitry 82. The circuitry 82 may comprise digital processing circuitry in the form of high speed programmable computer circuitry, for example, which carries out the algorithmic steps described in connection with Figure 4, for example. The watermark data is provided from a buffer 84 which may be in the form, for example, of a ring buffer which cyclically feeds watermark data being a component of watermark text or graphic material to the processing circuitry 82. The reconstructed video data containing the watermark data is then passed to an output buffer 86 which provides the video data for transmission, recording or whatever function the video data is required for.

Embodiments of the invention, operating in real time, can be utilised to add watermark data to media such as video and/or audio during live broadcast or other transmission, whilst recording to storage such as tape or disc, during broadcast or other transmission from storage, and during transferral from one storage device to another, for example. Furthermore, embodiments of the invention operating in real time can be used to monitor media such as television transmissions to detect the presence of watermark data incorporated in the media data. A block diagram of such a system is illustrated in Figure 6. Video data is provided to a buffer 90 from a source such as a broadcast receiver or the like. Real time processing circuitry 93 is coupled to receive the media data from the buffer 90 and perform the algorithmic steps described in connection with Figure 2, for example. This results in the extraction of any watermarking data contained in the media data which was inserted according to a process known to the monitoring apparatus (i.e. watermark data which has been added with a known permutation and transform in transform coefficients selected according to a known scheme). A comparison processor 94 can then be used to compare any watermark data which is retrieved with stored watermark data to determine if the retrieved watermark data corresponds to a known watermark indicating the source of the media data.

It will be appreciated from the foregoing description that the original media data is not required by the watermark extraction process in order to extract the watermark data, and therefore it is not required that the original image be certified by a trusted third party or held in escrow in order to prove the presence of a watermark in the media data. Random accessibility of a watermark within an image sequence is easily achieved, as all that is required to extract the watermark is the image or sequence of images that contains sufficient watermark data to reconstruct the entire watermark or a substantial portion thereof, and the secret keys used to seed the random permutation and the random coefficient selection process.

The watermarking process according to an embodiment of the invention has been tested on still images and image sequences, and has been demonstrated to be near invisible to the naked eye in a comparison between the reconstructed, watermarked media data and the original media data. It has also be found to be secure and robust to compression such as 4 Mbps MPEG coding of image sequences and 20% quality setting for JPEG compressed still images. The described watermarking procedure is also robust to digital-to-analogue and analogue-to-digital conversions. Accordingly, embodiments of the invention can be utilised to insert and extract watermark data in analogue media as well as digital media. For example, watermark data can be inserted and extracted from broadcast or home quality analogue or digital video. Tests have been performed demonstrating a successful read operation for watermarked digital video originally of broadcast studio quality which has been temporarily recorded on an analogue consumer VHS tape. In the case where the media is generated, stored and/or transmitted in an analogue form, an analogue-to-digital conversion using known techniques is used to obtain digital media data before inserting or extracting the watermark data (see 92 in Figure 6). The media data may be returned to analogue form, if desired, using known digital-to-analogue techniques.

It will also be appreciated that the simple nature of the computational processes involved in the watermarking process of the present invention allow it to be applied quite readily to real time video data, for example. This is because the only two computationally complex steps in the watermarking procedure, namely the permute and transformation are still relatively simple. This makes for a watermarking process that is very low in complexity, is easily automated, and requires no human intervention in its application.

The foregoing detailed description of the present invention has been presented by way of example only, and is not intended to be considered limiting to the invention as defined in the claims appended hereto.

Claims.

1. A method for inserting identification or authentication data into digital media data, including the steps of:

segmenting the digital media data into data blocks;

applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block;

applying an orthogonal transform on the modified data block to obtain transform domain data;

modifying at least one selected transform domain data coefficient in accordance with identification or authentication data;

inverse transforming the transform domain data having the at least one modified coefficient; and

applying an inverse pseudo-random function to obtain watermarked digital media data.

2. A method as claimed in claim 1, wherein the pseudo-random function applied to the data block is a keyed function controlled by a cryptographic key.

3. A method as claimed in claim 1 or 2, wherein the pseudo-random function applied to the data block has a property of flattening the power spectral density of the data block.

4. A method as claimed in claim 1, wherein application of the pseudo-random function and application of the orthogonal transform are carried out in the same operation.

5. A method as claimed in claim 1, wherein the at least one transform domain data coefficient selected for modification is selected according to a keyed pseudo-random operation.

6. A method as claimed in claim 1, wherein a plurality of data blocks of the digital media data are modified according to the identification or authentication data.

7. A method as claimed in any one of claims 1 to 6, wherein the digital media data is video data.

8. A method as claimed in any one of claims 1 to 6, wherein the digital media data is audio data.

9. A method as claimed in claim 7 or 8, wherein the identification or authentication data is inserted into the digital media data in real time.

10. A method as claimed in claim 1, wherein at least one coefficient in the transform domain data which represents the average (dc) of the data block is restricted from selection for modification with the identification or authentication data.

11. A method as claimed in claim 1 or 10, wherein the orthogonal transform is a Walsh Hadamard transform.

12. A method as claimed in claim 1 or 10, wherein the orthogonal transform is selected from a discrete cosine transform, a discrete sine transform and a fast Fourier transform.

13. A method as claimed in claim 1, wherein the pseudo-random reversible function is a permutation of the data block based on a keyed pseudo-random number generator.

14. A method as claimed in claim 1, including determining an average of data values in the data block, subtracting the average value from the data values in the data block before applying the pseudo-random function, and adding the average value back to the data values in the data block after applying the inverse pseudo-random function.

15. A method for extracting identification or authentication data from watermarked digital media data, including the steps of:

segmenting the digital media data into data blocks;

applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block;

applying an orthogonal transform to the modified data block to obtain transform domain data; and

extracting identification or authentication data from at least one coefficient of the transform domain data.

16. A method as claimed in claim 15, wherein the pseudo-random function applied to the data block is a keyed function controlled by a cryptographic key.

17. A method as claimed in claim 15 or 16, wherein the pseudo-random function applied to the data block has a property of flattening the power spectral density of the data block.

18. A method as claimed in claim 15, wherein application of the pseudo-random function and application of the orthogonal transform are carried out in the same operation.

19. A method as claimed in claim 15, wherein the extracting step includes selecting at least one transform domain data coefficient from which to extract identification or authentication data according to a keyed pseudo-random operation.

20. A method as claimed in any one of claims 15 to 19, wherein the digital media data comprises video data.

21. A method as claimed in any one of claims 15 to 19, wherein the digital media data comprises audio data.

22. A method as claimed in claim 20 or 21, wherein the identification or authentication data is extracted from the digital media data in real time.

23. A method as claimed in claim 15, wherein the orthogonal transform is a Walsh

Hadamard transform.

24. A method as claimed in claim 15, wherein the orthogonal transform is selected from a discrete cosine transform, a discrete sine transform and a fast Fourier transform.

25. A method as claimed in claim 15, wherein the pseudo-random reversible function is a permutation of the data block based on a keyed pseudo-random number generator.

26. A method as claimed in claim 15, including determining an average of data values in the data block, and subtracting the average value from the data values in the data block before applying the pseudo-random function.

27. An apparatus for inserting or extracting watermark data in digital media data, comprising:

segmenting means for segmenting the digital media data into data blocks;

processing means for applying a pseudo-random reversible function to a block of the digital media data to obtain a modified data block and performing a transform on the modified data block to obtain transform domain data; and

means for inserting or extracting watermark data in at least one coefficient of the transform domain data.

28. An apparatus as claimed in claim 27, wherein the processing means is also adapted to apply an inverse transformation and inverse pseudo-random function of the transform domain data containing the watermark data so as to generate watermarked digital media data.

29. An apparatus as claimed in claim 27 or 28, wherein the apparatus inserts or extracts watermark data in digital media data in real time

30. An apparatus as claimed in claim 29, wherein the digital media data comprises video data.

31. An apparatus as claimed in claim 29, wherein the digital media data comprises audio data.

32. An apparatus as claimed in claim 27, including means for selecting at least one transform domain data coefficient for the insertion or extraction of identification or authentication data according to a keyed pseudo-random operation.

33. A media data monitoring system comprising:

a media data buffer for temporarily storing media data received from a data source;

a real time processor coupled to receive media data from the media data buffer and adapted to extract identification or authentication data according to the method defined in claim 15; and

a comparison processor coupled to the real time processor for comparing extracted identification or authentication data with known identification or authentication data.

34. A media monitoring system as claimed in claim 33, including an analogue-to-digital converter for converting media data into a digital form before processing by the real time processor.

35. A media monitoring system as claimed in claim 33 or 34, wherein the media data comprises video data.

36. A media monitoring system as claimed in claim 35, wherein the data source of the media data is a receiver of video transmissions.

37. A media data monitoring method comprising:

receiving media data from a data source;

extracting identification or authentication data according to the method defined in claim 15; and

comparing extracted identification or authentication data with known identification or authentication data.

38. A media monitoring method as claimed in claim 37, including converting the media data into a digital form before processing by the real time processor.

39. A media monitoring method as claimed in claim 37 or 38, wherein the media data comprises video data.

40. A media monitoring method as claimed in claim 39, wherein the media data is received from a video transmission.

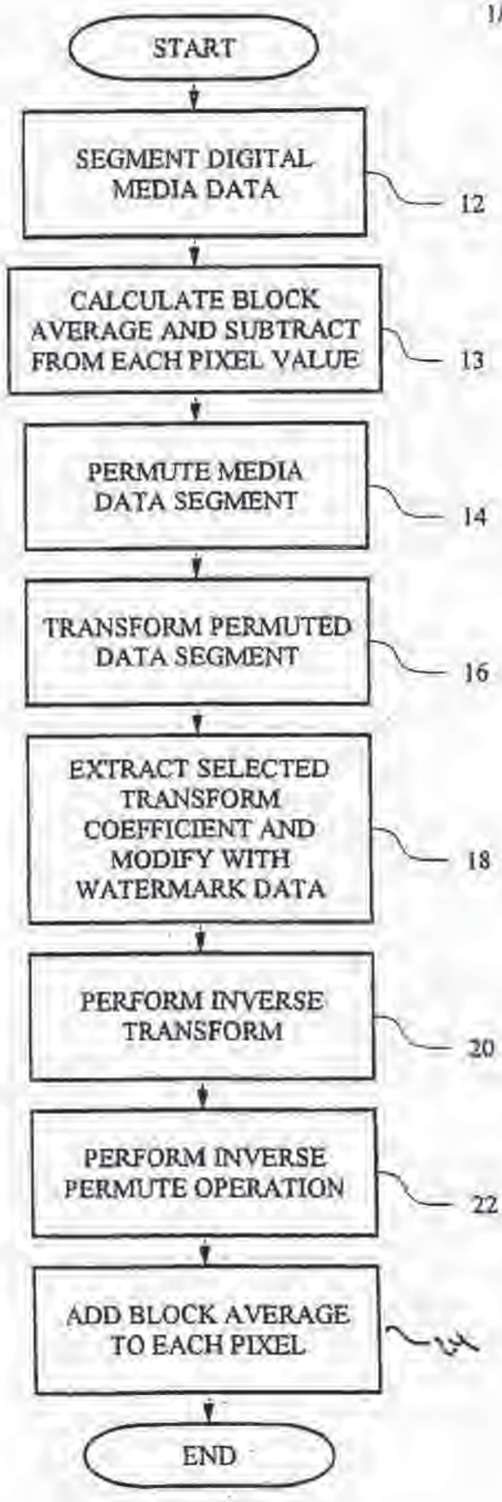


Figure 1.

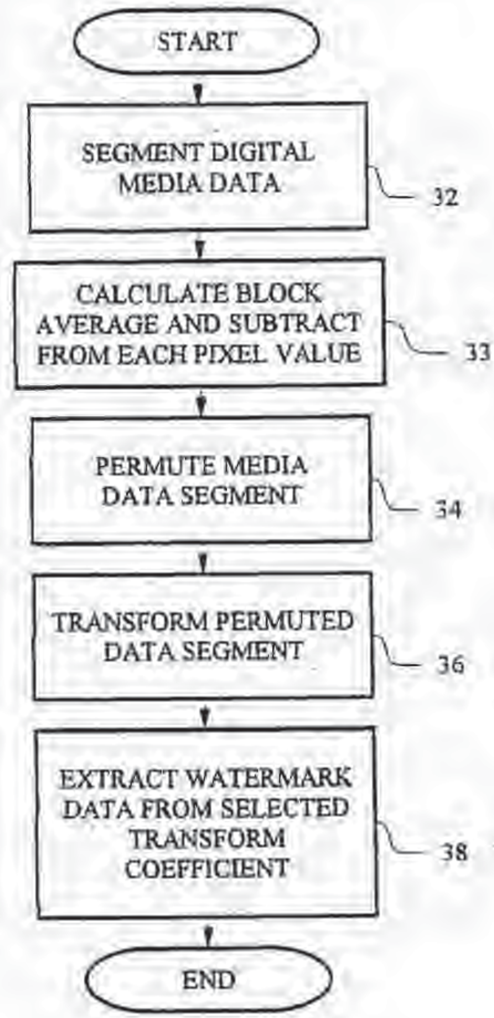


Figure 2.

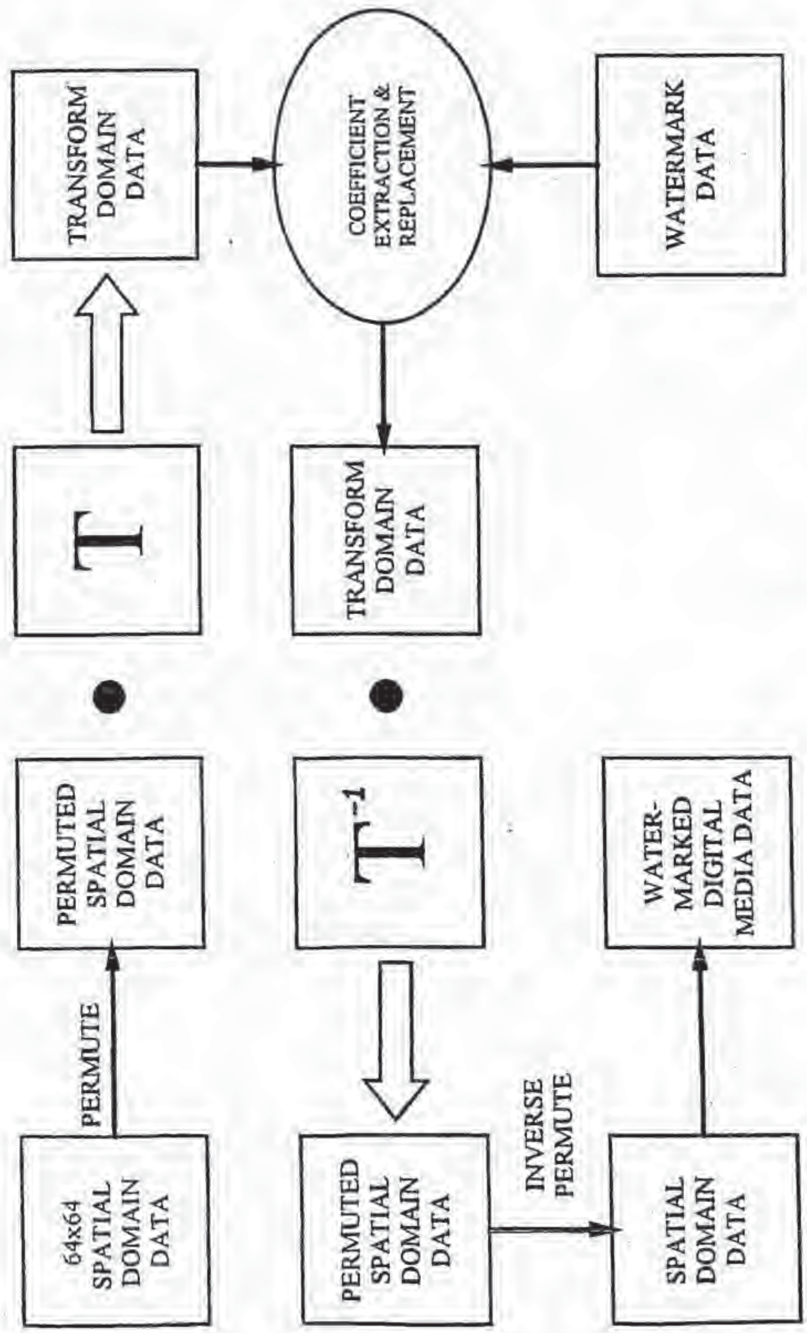

64x64 SPATIAL DOMAIN DATA
PERMUTE
PERMUTED SPATIAL DOMAIN DATA
T
TRANSFORM DOMAIN DATA
COEFFICIENT EXTRACTION & REPLACEMENT
WATERMARK DATA
TRANSFORM DOMAIN DATA
T-1
PERMUTED SPATIAL DOMAIN DATA
INVERSE PERMUTE
SPATIAL DOMAIN DATA
WATER-MARKED DIGITAL MEDIA DATA

Figure 3.

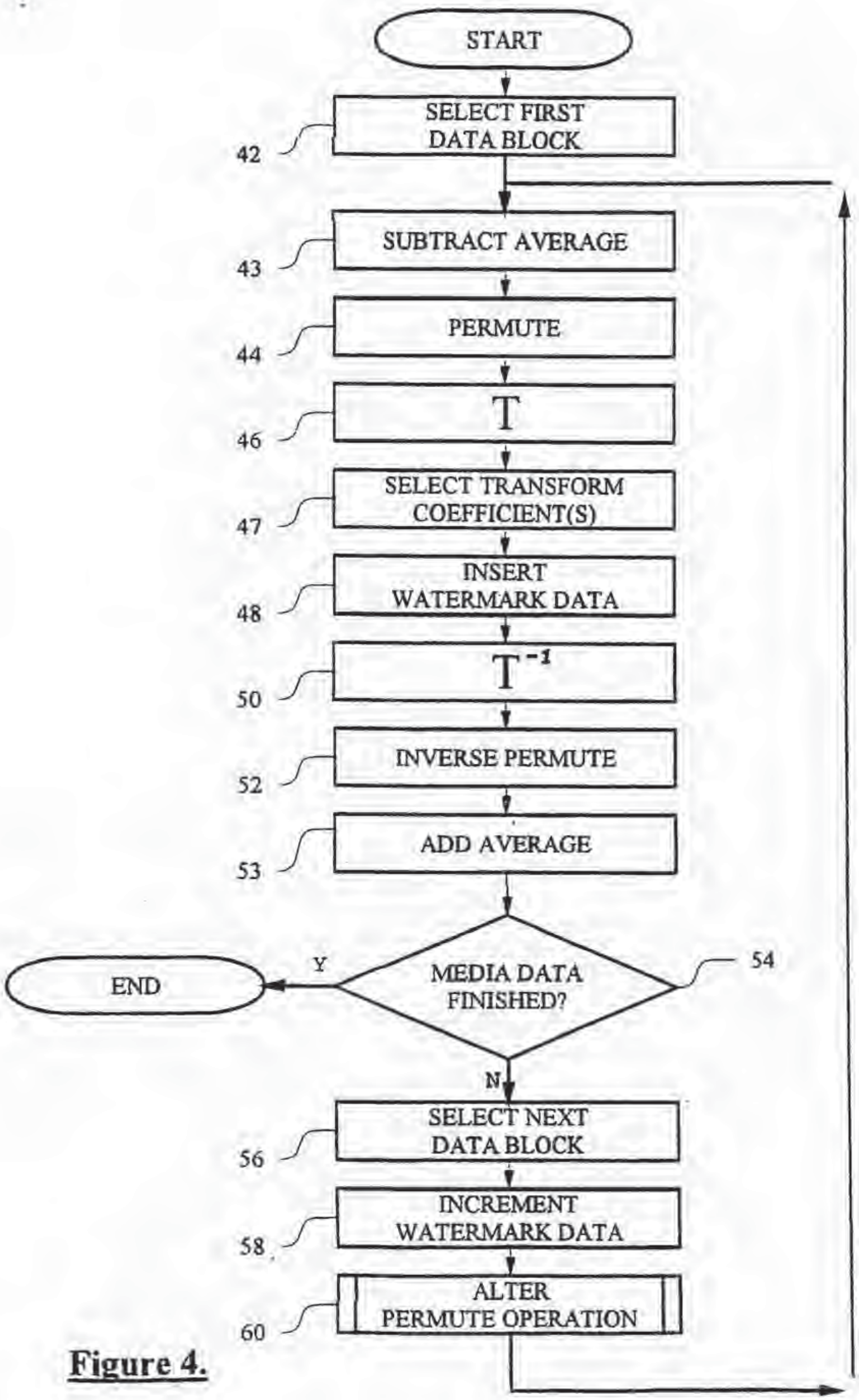

START
SELECT FIRST DATA BLOCK
42
SUBTRACT AVERAGE
43
PERMUTE
44
T
46
SELECT TRANSFORM COEFFICIENT(S)
47
INSERT WATERMARK DATA
48
T^-1
50
INVERSE PERMUTE
52
ADD AVERAGE
53
MEDIA DATA FINISHED?
54
Y
END
N
SELECT NEXT DATA BLOCK
56
INCREMENT WATERMARK DATA
58
ALTER PERMUTE OPERATION
60

Figure 4.

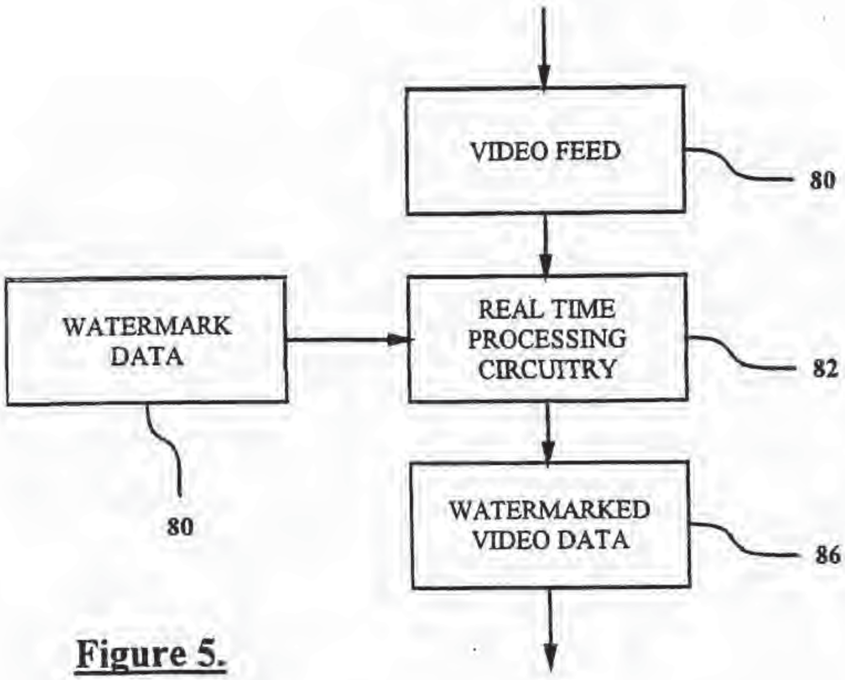


Figure 5.

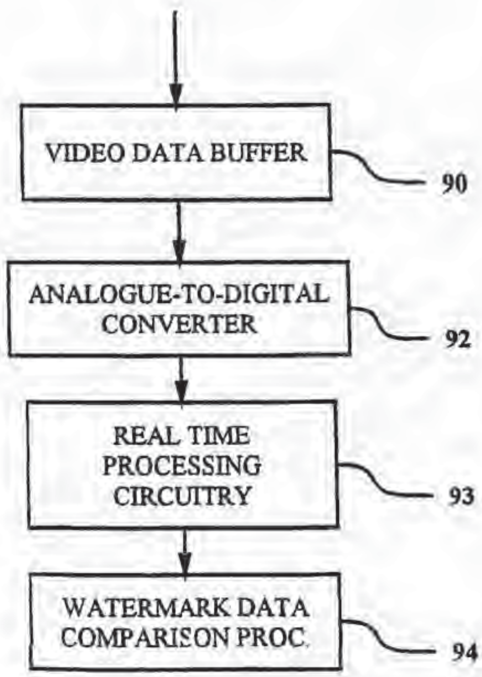


Figure 6.

- INTERNATIONAL SEARCH REPORT

International Application No.
PCT/AU 98/00106

A.	CLASSIFICATION OF SUBJECT MATTER
Int Cl[6]:	G06K 19/08, 19/10, H04L/9/00

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)
IPC:as above

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
AU:IPC as above

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)
IBM Patent Database: Digital, Watermark, Transform
Derwent WPAT:Digital, Watermark.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X, P	EP 766468 (NEC CORPORATION) 2 April 1997	1 to 40
A	BYTE Magazine, January 1997, 'Look, It's Not There', Zhao, J. (INTERNATIONAL FEATURE) page 40is 7-12	1 to 40
X	AU 45073/96 (INTEL CORPORATION) 6 June 1996	33
X, T	AU 26083/97 (V-CAST INC.) 4 December 1997	33

☐ Further documents are listed in the continuation of Box C

☒ See patent family annex

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier document but published on or after the international filing date
"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)
"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
"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
"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
"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
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
17 March 1998	08 APR 1998
Name and mailing address of the ISA/AU AUSTRALIAN PATENT OFFICE PO BOX 200 WODEN ACT 2606 AUSTRALIA Facsimile No.: (02) 6285 3929	Authorized officer J.W.THOMSON Telephone No.: (02) 6283 2214

Form PCT/ISA/210 (second sheet) (July 1992) copfma

INTERNATIONAL SEARCH REPORT
Information on patent family members

International Application No.
PCT/AU 98/00106

This Annex lists the known "A" publication level patent family members relating to the patent documents cited in the above-mentioned international search report. The Australian Patent Office is in no way liable for these particulars which are merely given for the purpose of information.

Patent Document Cited in Search Report		Patent Family Member					
EP	766468	AU	65840/96	CA	2184949	JP	9191394
AU	96/45073	WO	9617292	EP	795154		

END OF ANNEX

Form PCT/ISA/210 (extra sheet) (July 1992) copima

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) Publication number : **0 651 554 A1**

(12) EUROPEAN PATENT APPLICATION

(21) Application number : **94420293.6**

(22) Date of filing : **25.10.94**

(51) Int. Cl.[6] : **H04N 1/21**, G06F 1/00

(30) Priority : **29.10.93 US 146371**

(43) Date of publication of application :
03.05.95 Bulletin 95/18

(84) Designated Contracting States :
DE GB

(71) Applicant : **EASTMAN KODAK COMPANY**
343 State Street
Rochester, New York 14650-2201 (US)

(72) Inventor : **Rabbani, Majid, Eastman Kodak Company**
Patent Legal Staff,
343 State Street
Rochester, New York 14650-2201 (US)

Inventor : **Melnychuck, Paul W., Eastman Kodak Company**
Patent Legal Staff,
343 State Street
Rochester, New York 14650-2201 (US)

Inventor : **Axman, Michael Stuart, Eastman Kodak Company**
Patent Legal Staff,
343 State Street
Rochester, New York 14650-2201 (US)

Inventor : **Baradar, Ali R., Eastman Kodak Company**
Patent Legal Staff,
343 State Street
Rochester, New York 14650-2201 (US)

(74) Representative : **Boulard, Denis et al**
Kodak-Pathé
Département Brevets
CRT-Zone Industrielle
F-71102 Chalon-sur-Saône Cédex (FR)

(54) Method and apparatus for the addition and removal of digital watermarks in a hierarchical image storage and retrieval system.

(57) An image processing technique is described in the context of a hierarchical image storage and retrieval system. The method allows for the controlled addition and removal of digital watermarks from selected image components in the hierarchy. The method adds a digital watermark in a selected image resolution component and the means to remove it in an additional image component termed the watermark removal component. The method employs the encryption of the watermark removal component, and decryption with a special key, or password during authorized retrieval. This technique allows users of a distributed system the convenience of providing the entire image hierarchy on a single storage medium permitting images containing watermarks to be accessed without restriction for browsing and proofing, while the watermark removal requires knowledge and us of a controlled code.

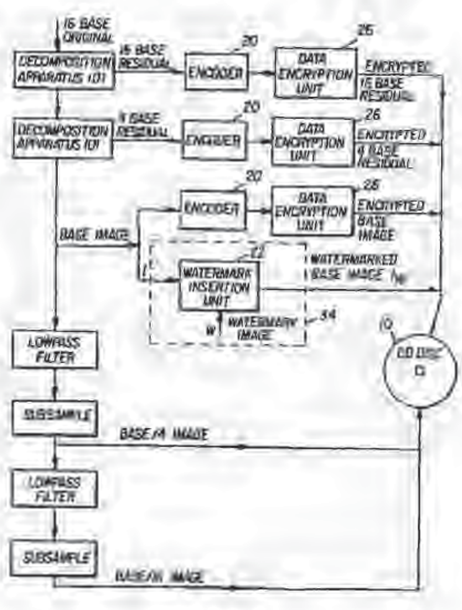


FIG 2

EP 0 651 554 A1

Cross-reference to Related Application:

The present application is related to U.S. Patent Application Serial No. 08/026,726, entitled "Method and Apparatus for Controlling Access to Selected Image Components In An Image Storage and Retrieval System" filed March 5, 1993, by P. W. Melnychuck and assigned to Kodak, the assignee of the present application.

Technical field Of The Invention

The present invention is related to the field of digital image processing and more particularly to methods and associated apparatuses for adding and removing a digital watermark to and from a selected image resolution and the preventing of unauthorized use of associated higher resolution digital image components.

Background Of The Invention

A number of hierarchical techniques for image coding have been described in the open technical literature and in various patents. Of particular relevance to the present invention are the following publications:

P. J. Burt and E. H. Adelson, "The Laplacian Pyramid As A Compact Code," IEEE Trans. Comm., COM-31, 532-540 (1983).

J. Seberry and J. Pieprzyk, "CRYPTOGRAPHY: An introduction to Computer Security" Prentice Hall, 1988 and the following patents:

U.S. Pat No. 4,969,204 entitled "Hybrid Residual-Based Hierarchical Storage And Display Method For High Resolution Digital Images In A Multiuse Environment," by Paul W. Melnychuck and Paul W. Jones, 1990.

U.S. Pat No. 5,048,111 entitled "Hybrid Subband-Based Hierarchical Storage And Display Method For High Resolution Digital Images In A Multiuse Environment," by Paul W. Jones and Paul W. Melnychuck, 1991.

The publication by Burt, et al, teaches an encoding method for images termed the Laplacian pyramid, the Burt pyramid, or the residual pyramid. In this technique, the original image is lowpass filtered, and this lowpass image is subsampled to take advantage of its reduced bandwidth to provide an image of reduced dimension. This process of lowpass filtering and subsampling is repeated three times to generate a hierarchical structure, or pyramid of images of successively smaller dimensions. The total number of resolution levels are created depending on the application. Each lowpass image in this pyramid is then expanded to the dimensions of the next higher level by upsampling (inserting zeros) and filtering to form a prediction image for that level. This prediction image is subtracted from its corresponding lowpass image in a subtractor to generate difference, or residual, images. The residual images corresponding to the levels of the lowpass pyramid form another pyramid which is termed the Laplacian, Burt, or residual pyramid. This technique is motivated by the fact that the residual images have a reduced variance and entropy compared to the original or lowpass images and may be quantized and entropy encoded to provide efficient storage of the data. Reconstruction is performed by interpolating the decoded lowpass image at the bottom of the lowpass pyramid and adding in the corresponding decoded residual to generate the next level in the lowpass pyramid. This process is iterated until the original image size is reached. A progressive improvement in reconstructed image quality and resolution can thus be obtained by displaying the reconstructed lowpass filtered image at each level of the pyramid. Note that errors introduced in the encoding process are propagated from one level to the next higher level in the decoding process.

The patent to Melnychuck and Jones (U. S. Pat. No. 4,969,204) teaches a modification of the Burt pyramid scheme by extending the lowpass pyramid structure to include one or more lowpass filtered images of successively smaller dimensions beyond the set described by Burt, et al. The advancement in the method of Melnychuck and Jones is that the residual pyramid is not extended to include these corresponding extended smaller dimensions. Hence, the Melnychuck and Jones pyramid contains the Burt pyramid plus additional lowpass filtered images of smaller dimensions. In a hierarchical image storage and retrieval system, the additional lowpass filtered images of smaller dimension can be retrieved directly, without interpolation and addition of residual components. In the context of the present invention, the Melnychuck and Jones pyramid provides for low resolution images that can be used for browsing or proofing. The use of these additional low resolution images for browsing and proofing means that the customer may use a simple retrieval mechanism and need not possess a more complex and hence, more expensive retrieval device that would be used to decode the higher resolution components of the pyramid. Of course, higher resolution images requiring interpolation and residual addition may be used for browsing and proofing as well.

A hierarchical image processing method will be described for the addition and removal of digital watermarks in selected image components, and for the restriction of selected high resolution image components from unauthorized use. An image hierarchy is constructed in the context of a multi-resolution environment whereby the user has the option of selecting the type of display medium and the desired resolution of this display medium. In particular, two types of display media are considered: video monitors and color hard copies, although photographic, thermal imaging and other types are also of interest. In Fig. 1 a prior art technique for decomposing, storing, recomposing, and displaying, a digital image using a hierarchical process is shown. An original digital image is decomposed to provide image versions at various resolutions to allow for the display of an HDTV quality image on video, an NTSC quality image with PAL/SECAM compatibility on video, one or more sub-NTSC quality images on video for overviews and browsing, and a very high quality image on color hard copy. Intermediate to the decomposition and recomposition steps, generally are inserted an encoding step, to compress the data for storage which in turn requires a decoding step when the data is read from storage.

Summary Of The Invention

The present invention places a digital watermark in a selected image resolution component and the means to remove it in an additional image component termed a watermark removal component. Encryption of the watermark removal component is used to prevent use of the image for the generation of unauthorized high quality color hard copy. A watermark is a form of graphic overlay that may contain a copyright notice or information regarding the restricted use of the image. In a distributed image system it is common to deliver an image of compromised image quality for purposes of browsing or proofing. A compromised rendition of the image is commonly distributed to prevent full utility or fulfillment of the image without proper payment for the service that generated the image. The term browsing refers to the process of image selection from a plurality of images based on some user-defined criterion. Such is the case when a user may select an image from a catalog of images depicting a particular object. The term proofing refers to the process of image selection based on the degree of desirability of a given image from a plurality of images. Such is the case when a professional portrait photographer distributes a plurality of images to a customer for selection and approval. The terms watermark, browsing and proofing described herein are not limited to the examples described above.

Upon selection of the desired image by the customer, the professional delivers a high quality rendition of the image, most often in the form of a high quality color hard copy. At all times the professional possesses the sole means of generating the high quality hard copy. In a conventional photographic system the means would be the original negatives of the images; in a digital hierarchical system according to the present invention, the means are higher resolution residual components.

In a digital imaging system, and in particular one that includes a hierarchical form of digital storage and retrieval, the professional may use a suitable digital storage medium such as a CD for the distribution of proofs. In an unrestricted environment, the customer may choose a desired image resolution from the hierarchy for the purposes of browsing, proofing, or hard copy fulfillment. In those instances where it is desirable for the professional to deliver the digital storage medium containing the entire image hierarchy to the customer; it is also most economical to record the entire image hierarchy once onto the digital storage medium and avoid having to make a second copy containing only low resolution components for distribution. However, it is also desirable to restrict the use of selected high resolution components for the purpose of full image quality fulfillment until payment has been received. The professional may choose to provide low resolution image components for browsing or proofing, while maintaining restriction of the higher resolution components. Alternatively, he may be required to deliver a proof of high resolution. Such is the case when the image content contains information of small detail and the rendition of this detail is subject to approval via the proof. With traditional photographic prints, the professional may place a stamp, or watermark on a strategic location on the print, so as to render the print useless from a fulfillment point of view. Note with digital images that fulfillment may mean high quality video at NTSC/PAL/SECAM, HDTV, or hard copy. In the present invention, the professional places a digital rendition of the watermark on a selected image component. The removal of the watermark is done through an additional image component containing the reverse of the watermark. The customer, having possession of the digital storage medium CD would possess the means for generating his own high quality hard copy when authorized by the professional. Upon payment to the professional, the professional or his agent provides to the customer the information necessary to remove the watermark for full image quality fulfillment. In the present invention, that information would be an authorization code, key, or password that would be inputted to the image processing system accessing the storage medium, to unlock the restricted high resolution components. An advantage of this technique is that the customer may possess all information pertinent to generating high quality hard copy without the need to physically return to the professional for additional image components.

It may additionally be desirable to use some form of hierarchical image representation for the purpose of browsing or proofing in a distributed system because the hierarchy naturally provides a plurality of resolutions, and hence levels of image quality, from which to choose the proof image. No additional operation of compromising the image is necessary; the professional simply chooses at what resolution level(s) he wants to restrict access.

Systems that use a hierarchical structuring of the image data have not been employed in the past for distribution purposes because of the lack of means to simultaneously provide low resolution components for browsing and proofing, while offering restricted access to the remaining hierarchical components for full quality image copy. Additionally, the means to generate and remove a digital watermark in a hierarchical image structure had not been previously considered.

The present invention permits the advantages of hierarchical image decomposition to create a series of residual components, direct retrieval of the additional low resolution images according to the Melnychuck and Jones pyramid, the addition and removal of a digital watermark in a selected image resolution component, and prior art encryption methods applied to the watermark removal component and the residuals, to provide for a system of browsing, proofing and restriction of the high resolution image components suitable in a distributed image system. It is assumed that the residual components and the watermark removal component are symbol encoded using the encoder box 20 in Figures 2 and 4 into a binary string of 1's and 0's either via fixed-length coding techniques (where a binary code word of a fixed-length is assigned to each symbol) or variable-length encoding techniques such as Huffman coding or arithmetic coding. The residual data may also be quantized prior to encoding, or it may be encoded in a lossless manner, i.e., without quantization. Data encryption box 26 is applied to the watermark removal component and if desired, also to the encoded quantized (or non-quantized) residual data. It is assumed that the encryption process is reversible. Hence, the decryption box 28 provides the exact data prior to data encryption.

In one embodiment of the invention a storage medium is called for having stored therein at least one low resolution digital image and at least one high resolution digital image, with said high resolution digital image encoded with a watermark that requires an authorization code for removal.

From the foregoing, it can be seen that it is a primary object of the present invention to provide a method and associated apparatus for storing and controllably retrieving digital images stored in a hierarchical format on a suitable digital storage distribution medium that allows the originator of the distribution medium to distribute the medium containing the entire image hierarchy and a controllably removable watermark for the purpose of retrieving low resolution images for browsing or proofing without compromising the originator's need to withhold the means for creating hard copies of the images without the watermark.

It is another object of the present invention to provide the means for controllably inserting and removing a watermark for a digital image.

It is another object of the present invention to provide the means for compromising a selected image component of a hierarchical formatted digital image by adding a digital watermark to the selected image component, and recording the selected image component containing the watermark as part of the image hierarchy on a digital storage distribution medium.

In association with a digital image, it is another object of the present invention to provide a means for creating a watermark removal component, and for controllably restricting access to the watermark removal component.

It is another object of the present invention to provide a means for affixing a watermark to a digital image and for controllably removing the watermark.

The above and other objects of the present invention will become more apparent when taken in conjunction with the following description and drawings wherein like characters indicate like parts and which drawings form a part of the present description.

Brief Description Of The Drawings

Fig. 1 is a block diagram illustrating the prior art Melnychuck and Jones hierarchical storage and display method.

Fig. 2 is a functional block diagram illustrating a hierarchical image decomposition technique incorporating a watermark insertion into an image component.

Fig. 3 is a functional block diagram illustrating a reconstruction technique for reconstructing the images decomposed by the system of Fig. 2.

Fig. 4 is a functional block diagram of another hierarchical image decomposition technique incorporating a watermark insertion into an image component.

Fig. 5 is a functional block diagram illustrating a reconstruction technique for reconstructing the images decomposed by the system of Fig. 4.

Detailed Description of the Invention

In the following description of the preferred embodiments, it will be assumed that the highest resolution of the image hierarchy is composed of 3072 x 2048 pixels and that this resolution is adequate to produce photographic quality originals on an appropriate digital output device. It is also assumed that a moderately high resolution level of the hierarchy composed of 1536 x 1024 pixels is adequate to generate a high quality HDTV display, or a small-sized photographic quality print on an appropriate digital output device. It is also assumed that the lowest resolution levels of 192 x 128 pixels, 384 x 256 pixels, and 768 x 512 pixels are generated and stored onto a digital storage medium such as a CD. These resolution levels are provided to give the reader an insight as to the operation of one or more embodiments of the invention with the understanding that other resolutions or arrangements may be chosen to suit specific needs without detracting from the teachings of the present invention.

Referring now to Fig. 2, a hierarchical residual decomposition technique, for decomposing a 16BASE original image to form a 16BASE residual, a 4BASE residual, a BASE, a BASE/4, and a BASE/16 image, incorporating the teachings found substantially in Fig. 7 of the patent to Melnychuck and Jones (U. S. Pat. No. 4,969,204), in combination with the present invention is shown. The BASE image is processed in box 34 to incorporate a watermark and to provide a watermarked BASE image.

An example of a watermark insertion box 34 is given by the watermark insertion unit 22 whereby a watermark image *W* is combined with the input image *I* to create a watermarked image I_W. In this example, it is assumed that the input image *I* and the watermark image *W* are of the same size and the same bit-depth. For example, if the input image *I* is an 8-bit image representing the luminance component of a color image, the watermark image *W* would also be an 8-bit image. Similarly, the watermarked image I_W would have the same size and each pixel value would be represented with 8 bits. An example of a watermark insertion unit 22 is one where the input image *I* and the watermark image *W* are combined according to the following equation to create the watermarked image I_W

$$I_W(i,j) = I(i,j) + \alpha W(i,j)$$

Where (i,j) denotes the two-dimensional location of the pixels in the image and the operation is performed for all the pixels in the input image. The watermark image W is prepared by the originator of the storage medium and may contain the logo of the originator or any other pattern that the originator may wish to use as a watermark. The parameter α, which can be either positive or negative, controls the watermark contrast and is also selected by the originator and can vary from one image to another. Larger magnitudes of α would, in general, create a higher contrast watermark. Also, to guarantee that the watermarked image I_W has the same bit-depth as the input image *I*, the watermarked image I_W is clipped to the same range as the input image. For example, for an 8-bit image with pixel values in the range of 0 to 255, for every pixel location (i,j), the value of $I_W(i,j)$ is clipped to 255 if the result of the above equation exceeds 255 and is set to zero if that result is less than zero. It should be noted that this example illustrates only one method of implementing the watermark insertion box 34 and the originator of the storage medium may incorporate any other method to generate a watermark that creates the desired effect of inhibiting the use of the image.

The BASE/16, BASE/4, and watermarked BASE images are stored on the digital storage medium 10 in direct (unencrypted) form. The BASE image, which in this case serves as the watermark removal record, is encrypted in the data encryption unit 26. The data encryption unit 26 consists of either a private-key data encryption algorithm (also referred to as *symmetric data encryption algorithm*) or a public-key data encryption algorithm (also referred to as asymmetric data encryption algorithm) both of which have been explained in the prior art and in the reference book by Seberry and Pieprzyk cited before. Examples of private-key encryption algorithms that can be used in the data encryption unit 26 are either block ciphers such as the Data Encryption Standard (DES) which uses a 56-bit key and operates on blocks of data of length 64 bits at a time, or a stream cipher algorithm such as RC-4, a commercially available encryption software that uses a 40-bit key component. The encrypted BASE image is also stored on the storage medium 10. The 4BASE and 16BASE residual components are also stored on the digital storage medium 10 either in direct (unencrypted) form or in encrypted form depending on the level of security desired by the application. In the case that the encryption of any or all of the residual data are needed, either the same key used in encrypting the BASE image is used or a separate key is used. The use of multiple encryption keys provides the originator of the storage medium with more flexibility in controlling the access to the various resolutions of the image hierarchy.

For browsing or proofing, a procedure illustrated by Fig. 3 is employed. A user retrieves the BASE/16, BASE/4, or watermarked BASE image directly without decryption from the digital storage medium 10. Upon authorization, the user inputs a decryption key(s) to the data decryption unit 28 to allow the decryption of the original BASE image (and the residuals) to be performed. An example of a data decryption unit 28 is a software implementation of a decryption algorithm corresponding to the reverse operation of the encryption algorithm employed in the data encryption unit 26. One example of a set of encryption/decryption algorithms is the Data Encryption Standard (DES) which has been explained in full detail in the reference book by Seberry *et al* mentioned before. Note that the decryption key(s) must be provided by the originator of the storage medium. Upon the decryption of the BASE image and the residual components, these components can be used to arrive at full image quality fulfillment.

In a second embodiment, illustrated in Fig. 4, the 16BASE image is decomposed by decomposition apparatus 101 into a residual pyramid consisting of the 16BASE, 4BASE, and BASE. The BASE image is further decomposed to create the BASE/4 and BASE/16 images, through low pass filtering and subsampling. BASE/4 and BASE/16 are not part of the residual pyramid and hence they are available directly for display on a monitor.

A watermark, as described in the previous embodiment in Fig. 2, is inserted in the BASE image in box 34 to arrive at a watermarked BASE image. This watermarked BASE image is then interpolated to the size of the 4BASE image using linear interpolation as indicated by the interpolator box 24. A difference is formed in subtractor 32 between the original 4BASE image and the interpolated watermarked BASE image to form a modified 4BASE residual that serves as the watermark removal record. The difference in this embodiment versus the first embodiment is that the watermark removal record is the modified 4BASE residual instead of the BASE image. This modified 4BASE residual is encrypted using the data encryption unit 26 as described before and is then stored on the storage media 10 along with the BASE/16, BASE/4, and watermarked BASE image in direct (unencrypted) form. Finally, the 16BASE residual data is stored on the digital storage medium either in direct or encrypted form depending on the application.

For browsing or proofing, the system of Fig. 5 is employed. The user retrieves the BASE/16, BASE/4, or watermarked BASE image directly without decryption from the digital storage medium 10. Upon authorization, the user inputs the decryption key to the data decryption unit 28 to allow the decryption to be performed to generate the modified 4BASE residual. The watermarked BASE image is interpolated using linear interpolation and is added to the decrypted modified 4BASE residual in the reconstruction apparatus 210 to recover the original 4BASE image. If the residuals have not been quantized, the 4BASE image can be exactly recovered. In the case where the residuals have been quantized, some discrepancy between the original 4BASE image and the 4BASE image recovered according to the above scheme would exist. The degree of this discrepancy would depend on the coarseness of the quantizer employed in the quantization of the residual components. Note that the decryption key must be provided by the originator of the storage medium.

It is to be understood that in some instances it may be desirable to place a watermark upon the low resolution images to control their access.

While there has been shown what are considered to be the preferred embodiments of the invention, it will be manifest that many changes and modifications may be made therein without departing from the essential spirit of the invention. It is intended, therefore, in the annexed claims, to cover all such changes and modifications as may fall within the scope of the invention.

Parts List:

10 Digital storage medium (CD-Disc)

20 Encoder
22 Watermark insertion unit
24 Interpolator
26 Data encryption unit
28 Data decryption unit

30 Decoder
32 Subtractor
34 Watermark insertion box

101 Decomposition apparatus

201 Reconstruction apparatus

Claims

1. A storage medium having stored therein at least one low resolution digital image and at least one high resolution digital image, with said high resolution digital image encoded with a watermark that requires an authorization code for removal.

2. The storage medium according to claim 1 and further having stored thereon at least one additional high resolution digital image that is not encoded with a watermark and is accessed with the authorization code in place of the high resolution digital image encoded with the watermark.

3. A storage medium having stored therein at least one low resolution digital image and at least one high resolution digital image in the form of a BASE image, residual image components and a watermark component, with said low resolution digital image, said BASE image or said high resolution image formed by the combination of the BASE image with said residual image components and a watermark component being accessible without an authorization code.

4. The storage medium of claim 3 in combination with an authorization code to remove the watermark component from an accessed high resolution image.

5. A system for controlling the uncompromised use of a high resolution digital image stored on a storage medium as BASE and residual components, comprising:

means for encrypting the residual components stored on said storage medium using a watermark code;

means for accessing the BASE and encrypted residual components;

means for combining the accessed BASE and residual components to reconstruct the high resolution digital image with the watermark code; and

means for authorizing the removal of the watermark code.

6. A system for controlling the uncompromised use of a high resolution digital image comprising:

means for forming a hierarchy of lower resolution digital images from the high resolution digital image;

means for forming residual images that are a function of differences between adjacent images in the hierarchy of lower resolution digital images;

means for encrypting at least one of the formed residual images with a watermark code;

storage means for storing the formed hierarchy of lower resolution images and the at least one encrypted residual image;

means for reconstructing high resolution images by accessing and combining a lower resolution image with a residual image;

means for displaying of the at least one encrypted residual image with the watermark; and

means for controllably removing the watermark code to permit an uncompromised use of the high resolution digital image.

7. A recording medium having stored thereon a plurality of digital images with each of the digital images being comprised of a low resolution digital image component and at least one residual digital image component which is combinable with the low resolution digital image component to form a higher resolution digital image incorporating a watermark which is removable with an authorization code.

8. A method for controlling the use of a digital image stored on a storage medium in a hierarchical form comprised of a BASE image and at least one residual image component, comprising the steps of:

a) associating a watermark with said at least one residual image component;

b) permitting access to the BASE image for low resolution viewing of the digital image;

c) combining the BASE image with the at least one residual image component and an associated watermark to form the digital image for viewing, printing and/or storing; and

d) controllably providing a watermark removal code to remove the watermark from the formed digital image of step c.

9) A storage medium having stored thereon at least one digital image encoded with a watermark that requires an authorization code for removal.

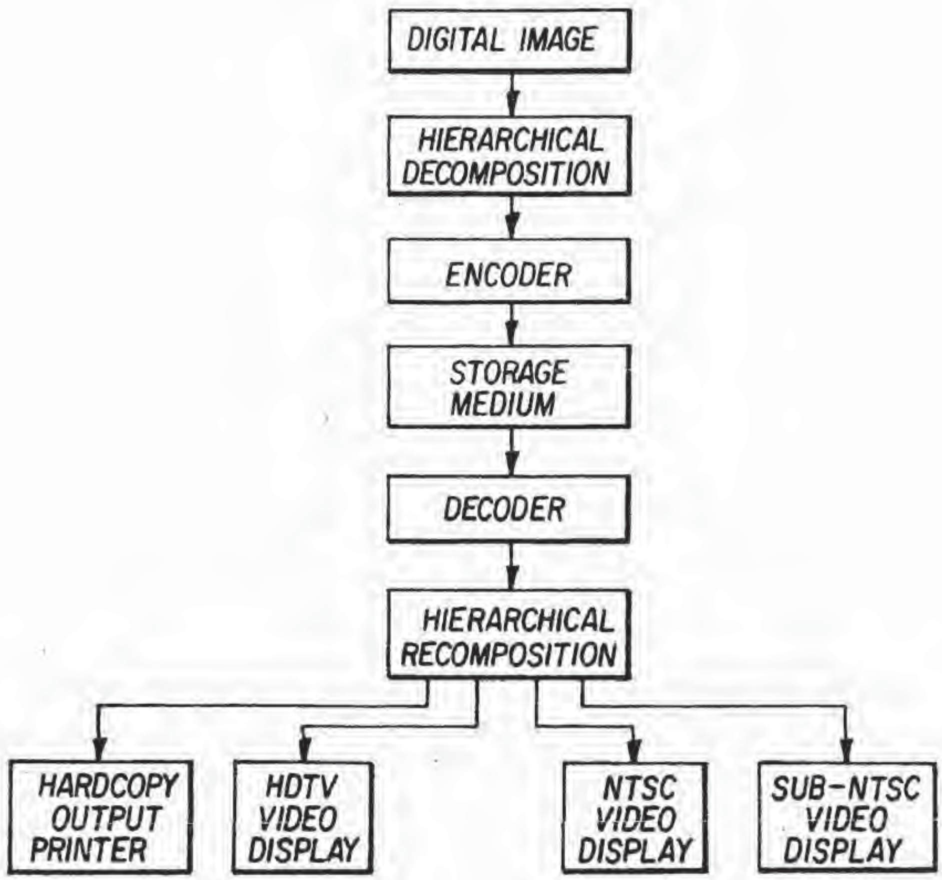


FIG. 1
(prior art)

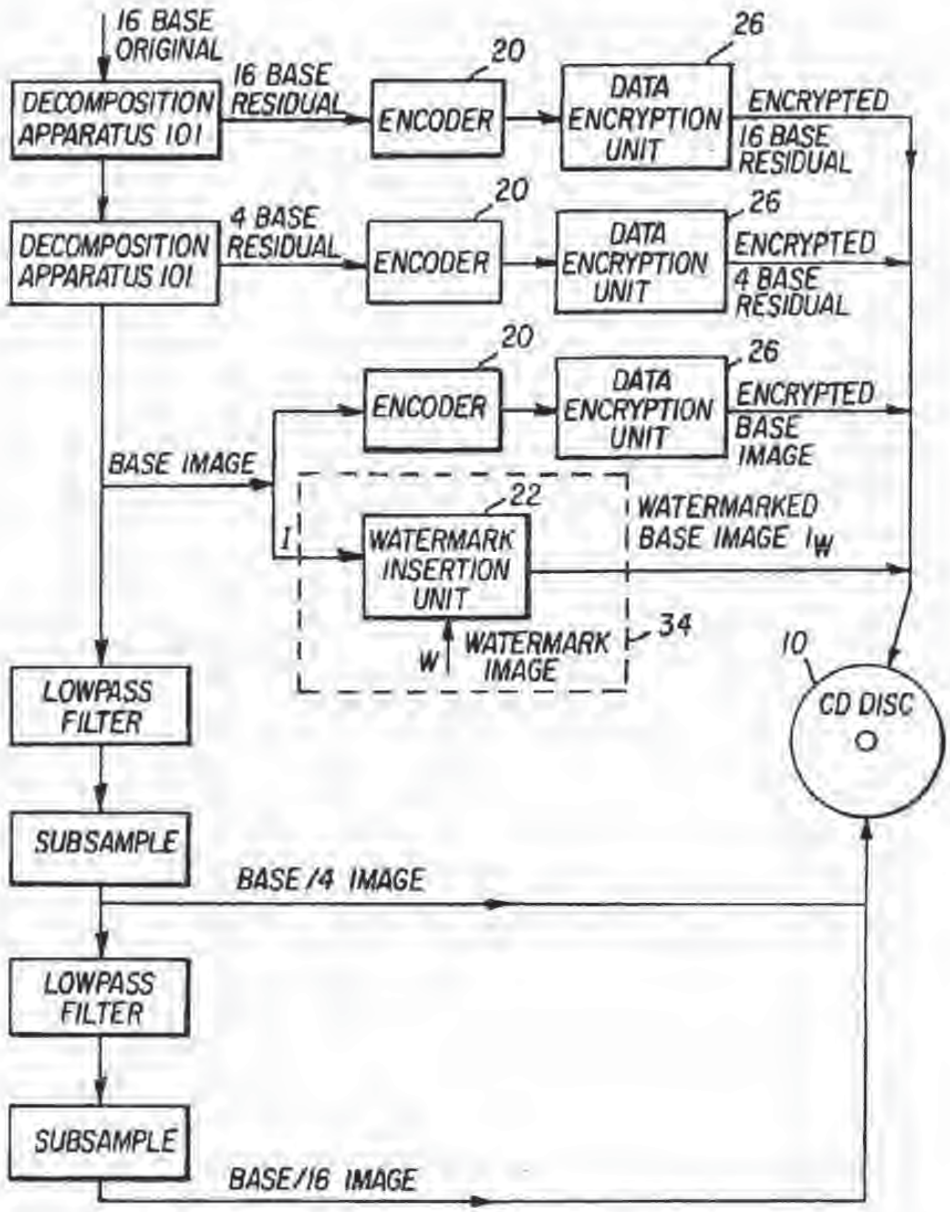

16 BASE ORIGINAL
DECOMPOSITION APPARATUS 101
16 BASE RESIDUAL
20
ENCODER
26
DATA ENCRYPTION UNIT
ENCRYPTED 16 BASE RESIDUAL
DECOMPOSITION APPARATUS 101
4 BASE RESIDUAL
20
ENCODER
26
DATA ENCRYPTION UNIT
ENCRYPTED 4 BASE RESIDUAL
20
ENCODER
26
DATA ENCRYPTION UNIT
ENCRYPTED BASE IMAGE
BASE IMAGE
22
I
WATERMARK INSERTION UNIT
WATERMARKED BASE IMAGE I W
W
WATERMARK IMAGE
34
10
CD DISC
LOWPASS FILTER
SUBSAMPLE
BASE /4 IMAGE
LOWPASS FILTER
SUBSAMPLE
BASE/16 IMAGE

FIG. 2

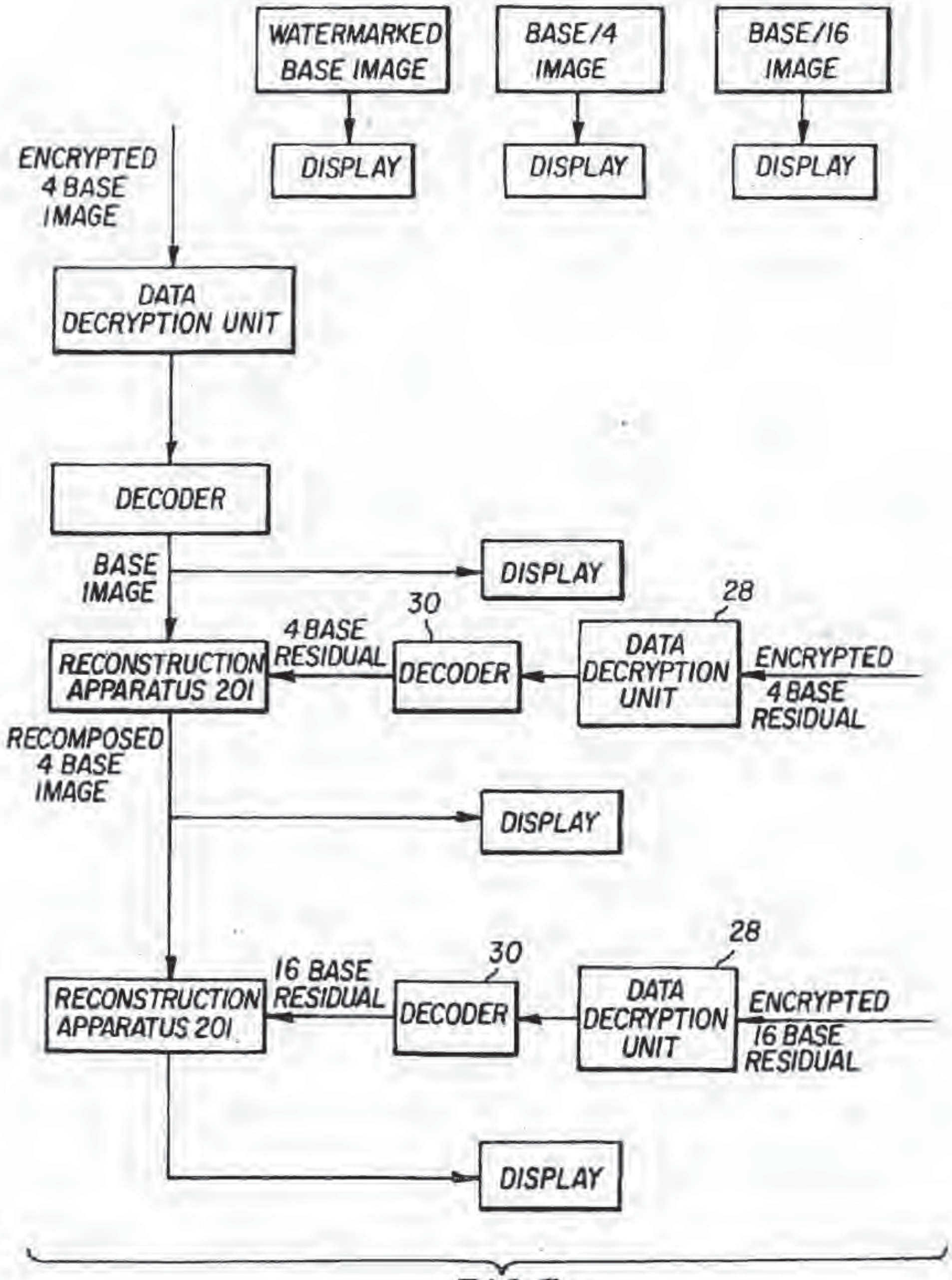

WATERMARKED BASE IMAGE
BASE/4 IMAGE
BASE/16 IMAGE
DISPLAY
DISPLAY
DISPLAY
ENCRYPTED 4 BASE IMAGE
DATA DECRYPTION UNIT
DECODER
BASE IMAGE
DISPLAY
30
28
4 BASE RESIDUAL
RECONSTRUCTION APPARATUS 201
DECODER
DATA DECRYPTION UNIT
ENCRYPTED 4 BASE RESIDUAL
RECOMPOSED 4 BASE IMAGE
DISPLAY
28
30
16 BASE RESIDUAL
RECONSTRUCTION APPARATUS 201
DECODER
DATA DECRYPTION UNIT
ENCRYPTED 16 BASE RESIDUAL
DISPLAY

FIG. 3

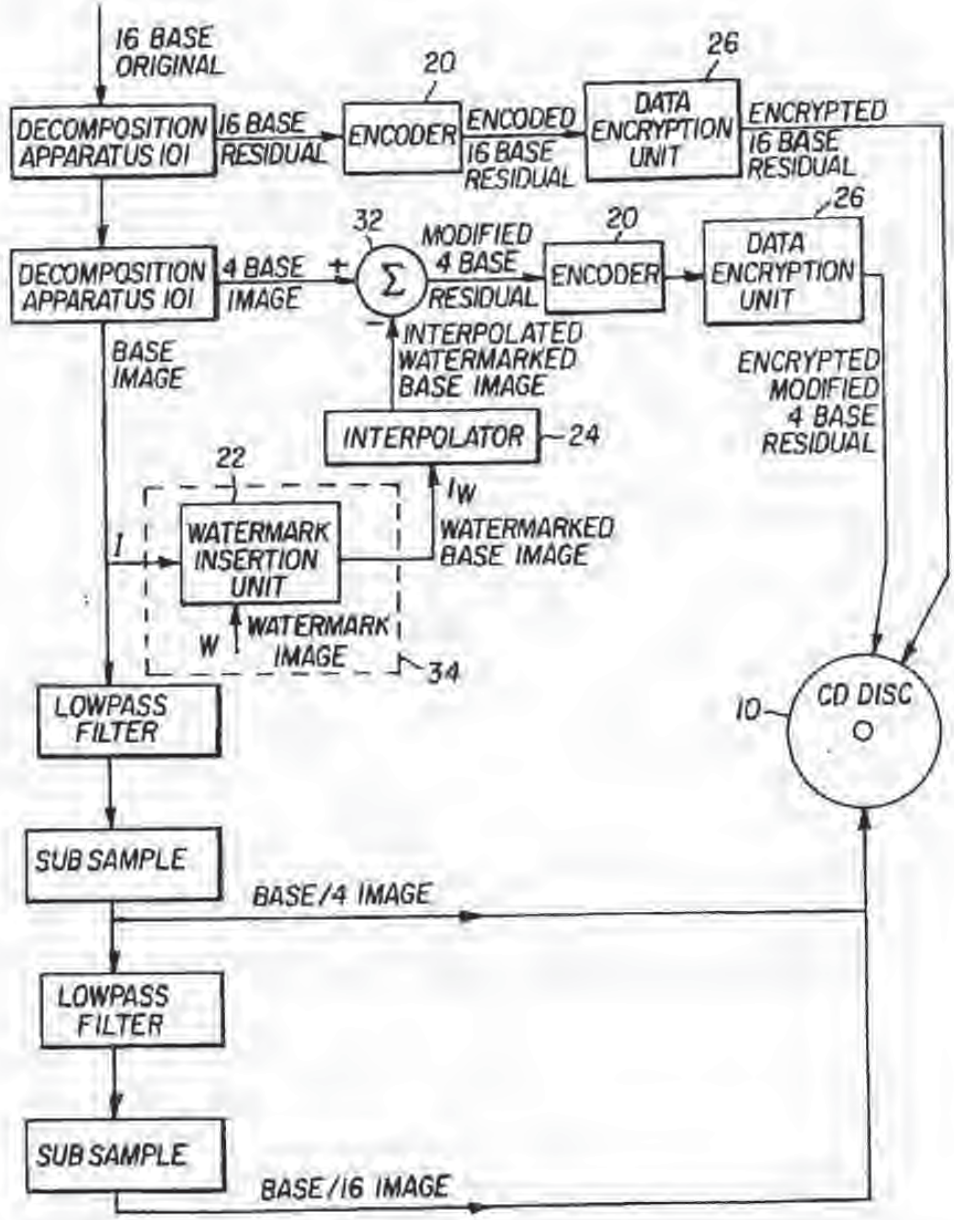

16 BASE ORIGINAL
DECOMPOSITION APPARATUS 101
16 BASE RESIDUAL
20
ENCODER
ENCODED 16 BASE RESIDUAL
26
DATA ENCRYPTION UNIT
ENCRYPTED 16 BASE RESIDUAL
DECOMPOSITION APPARATUS 101
4 BASE IMAGE
32
MODIFIED 4 BASE RESIDUAL
20
ENCODER
26
DATA ENCRYPTION UNIT
INTERPOLATED WATERMARKED BASE IMAGE
BASE IMAGE
ENCRYPTED MODIFIED 4 BASE RESIDUAL
INTERPOLATOR
24
22
I_W
WATERMARKED BASE IMAGE
I
WATERMARK INSERTION UNIT
W
WATERMARK IMAGE
34
LOWPASS FILTER
10
CD DISC
SUB SAMPLE
BASE/4 IMAGE
LOWPASS FILTER
SUB SAMPLE
BASE/16 IMAGE

FIG. 4

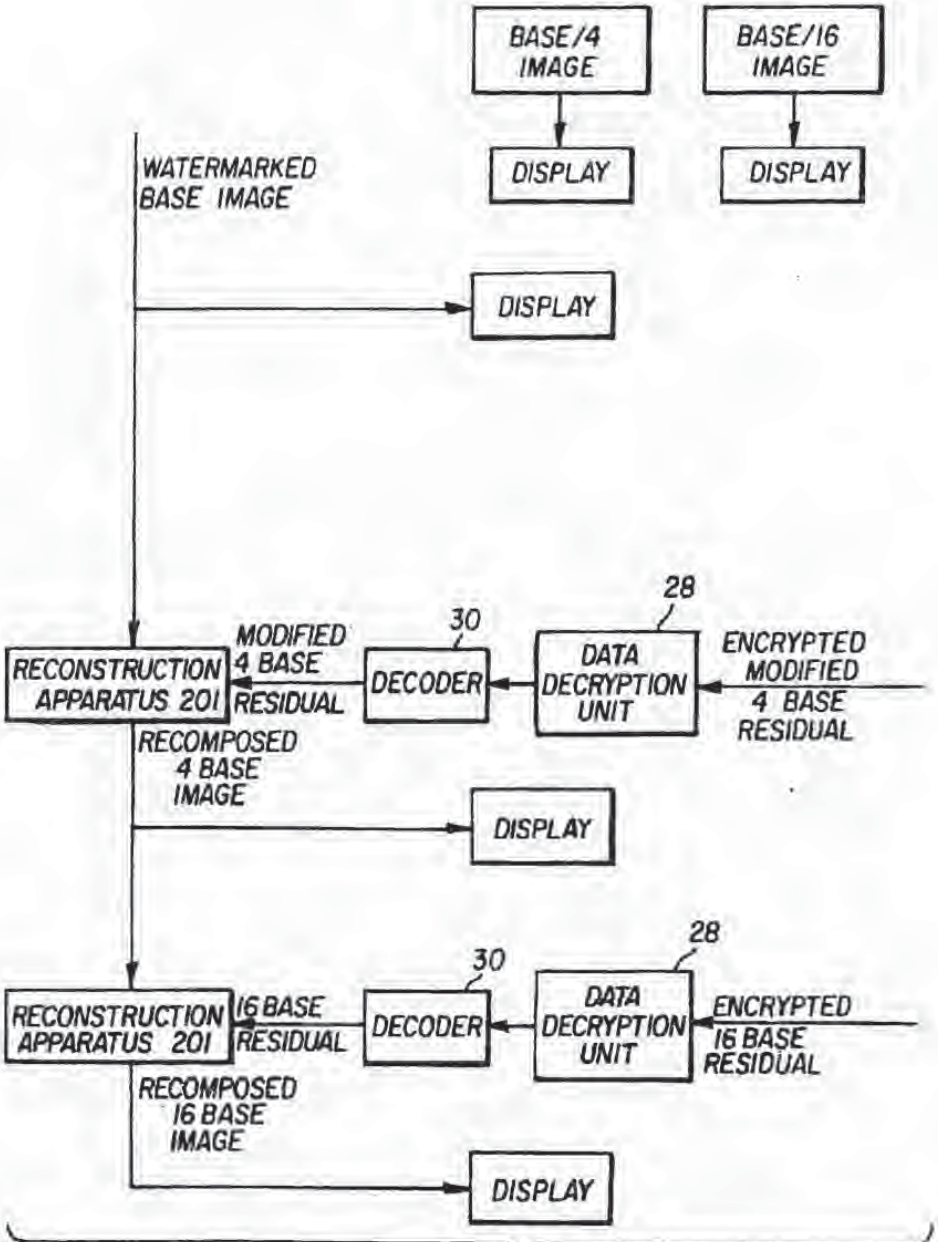

BASE/4
IMAGE
BASE/16
IMAGE
DISPLAY
DISPLAY
WATERMARKED
BASE IMAGE
DISPLAY
28
30
MODIFIED
4 BASE
RESIDUAL
RECONSTRUCTION
APPARATUS 201
DECODER
DATA
DECRYPTION
UNIT
ENCRYPTED
MODIFIED
4 BASE
RESIDUAL
RECOMPOSED
4 BASE
IMAGE
DISPLAY
28
30
RECONSTRUCTION
APPARATUS 201
16 BASE
RESIDUAL
DECODER
DATA
DECRYPTION
UNIT
ENCRYPTED
16 BASE
RESIDUAL
RECOMPOSED
16 BASE
IMAGE
DISPLAY

FIG. 5

European Patent Office

EUROPEAN SEARCH REPORT

Application Number
EP 94 42 0293

DOCUMENTS CONSIDERED TO BE RELEVANT

Category	Citation of document with indication, where appropriate, of relevant passages	Relevant to claim	CLASSIFICATION OF THE APPLICATION (Int.Cl.6)
D,Y	US-A-4 696 204 (MELNYCHUCK ET AL) * the whole document * ---	1-9	H04N1/21 G06F1/00
Y	ELECTRONICS AND COMMUNICATIONS IN JAPAN, vol.73, no.5, May 1990, NEW YORK, US; pages 22 - 33 N.KOMATSU ET AL 'A Proposal on Digital Watermark in Document Image Communication and Its Application to Realizing a Digital Signature' * figures 1-5 * * page 22, left column, line 1 - page 27, left column, line 23 * ---	1-9	
P,Y	EP-A-0 614 308 (EASTMAN KODAK) * abstract; figure 2 * * column 4, line 52 - column 5, line 4 * -----	2	
			TECHNICAL FIELDS SEARCHED (Int.Cl.6)
			H04N G06F

The present search report has been drawn up for all claims

Place of search	Date of completion of the search	Examiner
THE HAGUE	30 January 1995	Powell, D

CATEGORY OF CITED DOCUMENTS

X : particularly relevant if taken alone
Y : particularly relevant if combined with another document of the same category
A : technological background
O : non-written disclosure
P : intermediate document

T : theory or principle underlying the invention
E : earlier patent document, but published on, or after the filing date
D : document cited in the application
L : document cited for other reasons

& : member of the same patent family, corresponding document

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G09C 5/00, H04L 9/00 | A1

(11) International Publication Number: WO 99/62044

(43) International Publication Date: 2 December 1999 (02.12.99)

(21) International Application Number: PCT/US99/09417

(22) International Filing Date: 30 April 1999 (30.04.99)

(30) Priority Data:
09/085,147 26 May 1998 (26.05.98) US

(71) Applicant (*for all designated States except US*): THE REGENTS OF THE UNIVERSITY OF CALIFORNIA [US/US]; Business & Patent Law, Mail Stop D412, Los Alamos, NM 87545 (US).

(72) Inventors; and

(75) Inventors/Applicants (*for US only*): SANDFORD, Maxwell, T., II [US/US]; 160 Monte Rey S., Los Alamos, NM 87544 (US). HANDEL, Theodore, G. [US/US]; 316 Bryce Avenue, Los Alamos, NM 87544 (US).

(74) Agent: WYRICK, Milton, D.; Los Alamos National Laboratory, Mail Stop D412, Los Alamos, NM 87545 (US).

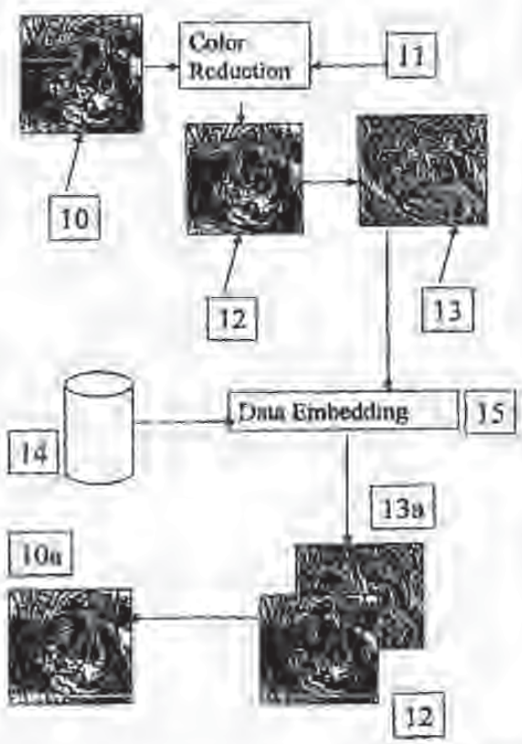
(81) Designated States: AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, GM, HR, HU, ID, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, UA, UG, US, UZ, VN, YU, ZA, ZW, ARIPO patent (GH, GM, KE, LS, MW, SD, SL, SZ, UG, ZW), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG).

Published
With international search report.

(54) Title: REFERENCE PALETTE EMBEDDING

(57) Abstract

A method of embedding auxiliary information (14) into the digital representation of publication quality color-component digital data (10). The method applies to all digital data for which individual values are represented by discrete numerical values, and for which a corresponding approximation known as a digital reference palette image (12) can be made in terms of a lesser number of discrete digital data values. The invention creates an intermediate, digital, color-component difference image (13) that allows steganographic methods (15) to hide or embed (15) the auxiliary data (14). The invention secures the auxiliary data (14) from detection and from unauthorized removal or use by means of the digital reference palette image and a steganographic key. By a substantially reverse process, the embedded auxiliary data can be an authorized user. The invention provides for a means to combine a removable, visible digital watermark with publication quality digital image data.



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

REFERENCE PALETTE EMBEDDING

FIELD OF THE INVENTION

The present invention generally relates to digital manipulation of numerical data. More specifically, the invention relates to the embedding of large amounts of external data into the numerical values used to represent a publication quality digital image without altering the appearance of the digital image. This invention was made with Government support under Contract No. W-7405-ENG-36 awarded by the U.S. Department of Energy. The Government has certain rights in the invention.

Many digital representations of image data have resolutions in intensity and color range greater than is required to represent the meaningful content of the information. Digital representations of publication quality images are ordinarily in Truecolor format using eight or more binary bits of information, for each of the three primary colors (red, green, and blue), for a total of at least 24-bit resolution. An alternative publication quality format for digital images uses primary color complements (cyan, yellow, and magenta), and black to represent the image information. The publication quality of Truecolor digital images insures that the all the information necessary to reproduce the original image in print is present in the alternative electronic form. Truecolor digital images are most often the first-generation image data produced by sensors in scanners or electronic cameras capable of recording the highest quality images.

In many situations, fewer than 24 bits resolve an image adequately to convey its meaning and content. Color reduction methods analyze a Truecolor image to determine a smaller number of colors that can be used to reproduce an approximation to the original publication quality image. Color reductions to 256 or fewer colors are used commonly for digital images intended for display in electronic documents or via the Internet worldwide web (www). Images stored in the Compuserve™ Graphics Interchange Format (GIF), the MICROSOFT® Windows Bitmap™ (BMP), and tagged-image file format (TIFF) formats often use a 256-color palette. The color-reduced palette requires 8-bits per picture element (pixel) to approximate the original 24-bits per pixel Truecolor values.

Reference palette embedding is a new steganographic method for manipulating the information in a 24-bits per pixel Truecolor host image, in order to insert auxiliary data with less error than is caused by methods that replace directly some of the 24-bits with the auxiliary data. Reference palette embedding as taught here provides invisibility of the auxiliary information, in comparison with the method disclosed in U.S. Patent number 5,686,782 issued August 19, 1996 for DATA EMBEDDING, which is included herein by reference for all purposes.

The reference palette embedding invention guarantees that the auxiliary information placed into the image affects only the parts of the Truecolor image that are redundant, and therefore unnecessary for representing the image content. Methods that manipulate the picture element (pixel) values directly by either the methods taught in the aforementioned DATA EMBEDDING patent, or

by the methods taught in U.S. Patent Application Serial No. 08/646,837 filed May 8, 1996, for MODULAR ERROR EMBEDDING, also included herein by reference for all purposes, modify significantly the bit values within the image pixel. Hereinafter, the teachings of the above-described U.S. Patent and the above-described U.S. Patent Application will be referred to as DATA EMBEDDING process and MODULAR ERROR EMBEDDING process, respectively. These alternative steganographic methods necessarily affect the image content to some degree. The present invention, reference palette embedding, utilizes a color-reduced version of the Truecolor image as a template to ensure that the embedding process affects the image quality as little as is possible.

Reference palette embedding uses and extends the DATA EMBEDDING process as taught in the above-mentioned US patent. As disclosed in the DATA EMBEDDING patent, the auxiliary data are embedded in a manner that manipulates the noise component of the host data, and that does not modify directly any host data values. In reference palette embedding, as taught herein, the auxiliary data are embedded into the difference between the original Truecolor image, and a color-reduced version of the original image.

The color-reduced image and the digital key taught in the DATA EMBEDDING patent combine to permit the construction of the auxiliary data from the modified Truecolor image.

Data embedded into the host image with the present reference palette embedding invention are recovered by processing the digital image in machine readable, digital form. Human readable versions of images containing auxiliary data, for example images displayed on a screen or printed from the digital data, cannot be processed to recover the embedded information. In a preferred embodiment of the subject invention, the auxiliary data are compressed and encrypted before beginning the reference palette embedding process, in order to randomize the auxiliary bits, and to minimize the effect of the auxiliary data on the difference between the Truecolor and color-palette images.

It is therefore an object of the present invention to provide apparatus and method for embedding data into a digital information stream so that the meaning and content of the digital information stream is not changed significantly.

It is another object of the present invention to provide apparatus and method for concealing auxiliary data within a digital information stream so that the presence of the auxiliary data is not discernible in the digital information stream.

It is yet another object of the present invention to provide apparatus and method for reducing the error caused by the added information, and for thwarting unauthorized access to the auxiliary data embedded into digital information stream.

It is still another object of the present invention to provide apparatus and method for allowing authorized construction of embedded auxiliary data from a digital information stream.

Additional objects, advantages, and novel features of the invention will be set forth in part in the description which follows, and in part will become apparent to those skilled in the art upon examination of the following, or learned by practice of the invention. The objects and advantages of the following, or learned by practice of the invention.

The objects and advantages of the invention may be realized and attained by means of the instrumentalities and combinations particularly pointed out in the appended claims.

SUMMARY OF THE INVENTION

In accordance with the purposes of the present invention there is provided a method of embedding auxiliary data into publication quality digital image data represented by a quantity of color-component values for each picture element comprising the steps of reducing the quantity of color-component values of the publication quality digital image data to create a digital reference palette, wherein the digital color palette represents the quantity of color-component values of the publication quality digital image data; creating a digital representation of the auxiliary data as a sequence of individual bit values; creating a color-component digital difference image by numerically combining the publication quality digital image with the digital reference palette image; modifying the color-component digital difference image by combining the auxiliary data and the color-component digital difference image through use of a data embedding method; creating a modified publication quality digital image indiscernibly containing the auxiliary data by combining the modified color-component digital difference image and the digital reference palette image; and outputting the modified publication quality digital image into a file format specified for the modified publication quality digital image.

In a still further aspect of the present invention, and in accordance with its objects and purposes, a method of constructing indiscernible auxiliary data from a machine readable publication quality digital image representation of unrelated and uncorrelated data comprising the steps of generating a digital reference palette image from values and properties contained within the publication quality digital image; creating a color-component digital difference image by numerically combining the digital reference palette image and the publication quality digital image; constructing the auxiliary data by processing the color-component digital difference image with a data embedding construction method; interpreting the auxiliary data in order to obtain or remove content, validation or

authentication, or otherwise process the publication quality digital image in order to modify its quality.

BRIEF DESCRIPTION OF THE DRAWINGS

The accompanying drawings, which are incorporated in and form a part of the specification, illustrate the embodiments of the present invention and, together with the description, serve to explain the principles of the invention. In the drawings:

FIGURE 1 is a diagram illustrating the reference palette sequence of calculations.

FIGURE 2 is a partial listing of computer code used for calculating the biased difference image color-component values.

FIGURE 3 is a partial listing of computer code used for calculating modified Truecolor image pixel color-component values.

FIGURE 4 is a diagram illustrating the sequence of calculation for constructing auxiliary data from a modified Truecolor image.

FIGURE 5 is a partial listing of computer code used for constructing modified difference color-component values.

DETAILED DESCRIPTION

The present invention allows auxiliary data to be embedded into a digital Truecolor host image with less error than is caused by modifying the pixel color-components directly. The reduction in error follows from the technique of of the present invention of embedding auxiliary data into the pixel color-component values constructed from the difference between the Truecolor host image and a reference palette image, which has been constructed from the Truecolor host image. The invention can be understood most easily through reference to the drawings.

Refer to Figure 1 for an illustration of the process of the present invention. The images in Figure 1 are printed digital images, and are not copies of photographs. Publication quality digital image data 10, such as a Truecolor-format image is approximated or reduced by one of several commonly known color-reduction methods 11 to produce a palette-format image 12. The palette-format image 12 is denoted hereinafter as reference palette image 12. The palette colors of reference palette image 12 are subtracted from the Truecolor pixel color values of publication quality digital image 10 to create a difference image 13. The difference-image 13 pixel values measure directly the accuracy of the color-reduction method. Auxiliary data 14 are taken as bits from a data source and input to data embedding processor 15, which may contain the DATA EMBEDDING process, the MODULAR ERROR EMBEDDING process, or any other effective steganographic method for combining auxiliary data 14 with difference image 13. A new difference image 13a is created by data embedding processor 15. The color values of the pixels in the new difference image 13a are added to reference palette image 12, and produce a new, modified publication quality digital image 10a, containing auxiliary data 14.

Examples of appropriate publication quality Truecolor format publication quality digital image data 10 include, but are not limited to, publication quality television or motion picture images, X-ray or Magnetic Resonance Imaging data, digital camera images, and personal security and identification data. Other examples of publication quality digital image data 10 include black and white images containing a range of digital levels of brightness, and digitized analog audio signals. For digitized audio signals, a reduced-quality version of the digitized analog audio signals serves as the reference palette 12.

If the steganographic method used in data embedding processor 15 is bitslicing or the above-mentioned MODULAR ERROR EMBEDDING process, the first embodiment of the present invention is implemented. If the steganographic method used in DATA EMBEDDING processor 15 is the above-mentioned DATA EMBEDDING process, the second embodiment of the present invention is implemented.

The difference image 13 is a Truecolor image, and negative pixel values are not permitted. Hence, the difference D between the Truecolor and pallet-color pixel colors is biased in the positive direction, in order to represent the difference as a positive number within the range 0-255 permitted for an 8-bit Truecolor-format image. The difference value is restricted to the range ±127, in order that the biased value remain within the 8-bit range. Pixels that are found to contain differences larger in absolute value than 127 are flagged, in order that the invention can place the original Truecolor value in modified image 10a. Flagged pixels are not used by the invention. Figure 2 is a partial listing of computer code in the C++ language that is used for calculating the biased difference image color-component values. Figure 2 contains two nested loops starting at line 5, over the number of rows in the image, and at line 13, over the number of columns in a row.

The biased color differences are placed into a memory buffer named **buffer**. Data from a row of Truecolor image pixels are placed into a memory buffer named **bufftc** in line 7. The **TCFile** object is an instance of the MICROSOFT® MFC **CFile::** class that accesses the bitmap-format Truecolor image. Data from the picture row in the palette-format image is read into a memory buffer named **buffpal**, from the **CFile::** object named **tape7** at line 10, in Figure 2.

The loop over the columns in the image row that begins at line 13 in Figure 2 processes the buffered pixel data. The three color-components in the Truecolor image pixel are processed sequentially within this loop. The index **k** contains the palette-format pixel value. The palette-format pixel colors are accessed by **k**, into the **colormap[]** array. The Truecolor pixel colors are accessed directly with offsets into the **bufftc** memory buffer. Color differences having a the value 255 are not used in data embedding processor 15. The biased color differences are **b_diff**, **g_diff**, and **r_diff** calculated at lines 17, 21, and 25. The differences are set to a limiting value (255) if the palette color values are greater than the arbitrary value of 250, i.e. the colors are near the top of their color ranges. The biased color differences are tested for range at lines 35, 41, and 47 in Figure 2. If the biased difference does not fit into the range 0-255 that is allowed by an 8-bit unsigned character, the difference buffer is set to a flag value (0x01). Color differences that were set to the limiting value are flagged in this process. The color difference **buffer** becomes the output row in the Truecolor difference image.

Returning to Figure 1, the completed color difference image 13 is combined with auxiliary data 14 by means of data embedding processor 15. In data embedding processor 15 this combination can be accomplished through use of bitslicing techniques, the above-mentioned MODULAR ERROR EMBEDDING process, the above-mentioned DATA EMBEDDING process, or any other effective steganographic algorithm. The color difference image 13 is combined with reference palette image 12 to produce a new, modified Truecolor image 10a.

Figure 3 is a partial listing of computer code used for calculating biased difference Truecolor-image-pixel color-component values. Two nested loops begin at line 5 and line 12 in Figure 3. The output buffer for the new, modified Truecolor image pixel row is named **buffer**. The difference image pixels are read into a memory buffer named **bufftc** at line 7, from the **CFile::** object named **tape6**. The palette-format pixel values are read into a buffer named **buffpal**, from the **CFile::** object named tape7, at line 10.

Construction of the new Truecolor image pixel row proceeds in the loop over image columns that starts at line 12. The output **buffer** is filled with the new color-value data. The statements contained in lines 14 through 16 of Figure 3 process the first row of pixels differently, because the first image row is used to hold the key for the DATA EMBEDDING process. Processing the first row of pixels differently than the rest of the image is not part of the present reference palette embedding invention.

The new Truecolor color-component values are calculated in lines 19, 20, and 21, in Figure 3. Pixels in the difference image that contained flagged values are calculated incorrectly in this loop. The output buffer offsets are set directly to the new color difference values, and the row of pixels is written to the new Truecolor image using the **tape8** file object.

The **tape8** image file object is post-processed to replace the flagged pixels with the original Truecolor color-data pixel values. The flagged pixels, i.e. pixels that were not used to contain auxiliary data 14 (Figure 1), therefore appear without modification in the new Truecolor image 10a (Figure 1).

Constructing (recovering) auxiliary data 14 from new Truecolor image 10a requires the exact reference palette image 12 format version of original Truecolor image 10, and the information necessary to construct auxiliary data 14 from new difference image 13a. Figure 4 is a diagram illustrating the sequence of calculation for constructing auxiliary data 14 from a modified Truecolor image 10a. As in Figure 1, the images in Figure 4 are printed digital images, and are not copies of photographs.

The coding to construct auxiliary data 14, according to the process illustrated in Figure 4, is shown in Figure 5. The color difference image 13a is calculated from modified Truecolor image 10a and the reference palette image 12. The digital key is used with the data construction processor 15a to construct auxiliary data 14. The method named **MakeDifferenceFile()** is executed at line 1 in Figure 5. The **MakeDifferenceFile()** method implements the calculation shown in Figure 2. The **OpenBitmapFile()** method executed at line 3 prepares the difference image 13a for processing by either the above-mentioned MODULAR ERROR EMBEDDING data construction process or the above-mentioned DATA EMBEDDING data construction process. The **ExtractData()** method executed at line 4 in Figure 5 constructs the auxiliary data 14 from the appropriate digital key and the difference image 13a.

As with the DATA EMBEDDING process as taught in the above-mentioned US patent, another way of protecting the pair table key taught in that patent is to remove and encrypt it using public-key or another encryption process. The present invention requires the reference palette image 12, as well as the DATA EMBEDDING process key in order to construct auxiliary data 14. The necessary keys for DATA EMBEDDING process or codes for the steganography used to insert auxiliary data 14 into the difference image can be combined with the reference palette image 12 using known and readily available file formats. The COMPUSERVE® Graphic Interchange Format™, the Tagged Image File Format, and the MICROSOFT® bitmap format enable the addition of additional binary information within the file header fields. Thus, the reference palette image 12 serves as the key to construct auxiliary data 14 from a publication quality Truecolor version of the identical picture indiscernibly containing auxiliary data 14.

The foregoing description of the embodiments of the invention have been presented for purposes of illustration and description. It is not intended to be exhaustive or to limit the invention to the precise form disclosed, and obviously many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in order to best explain the principles of the invention and its practical application to thereby enable others skilled in the art to best utilize the invention in various embodiments and with various modifications as are suited to the particular use contemplated. It is intended that the scope of the invention be defined by the claims appended hereto.

WHAT IS CLAIMED IS:

1. A method of embedding auxiliary data into publication quality digital image data represented by a quantity of color-component values for each picture element comprising the steps of:

reducing said quantity of color-component values of said publication quality digital image data, to create a digital reference palette, wherein said digital color palette represents said quantity of color-component values of said publication quality digital image data;

creating a digital representation of said auxiliary data as a sequence of individual bit values;

creating a color-component digital difference image by numerically combining said publication quality digital image with said digital reference palette image;

modifying said color-component digital difference image by combining said auxiliary data and said color-component digital difference image through use of a data embedding method;

creating a modified publication quality digital image indiscernibly containing said auxiliary data by combining said modified color-component digital difference image and said digital reference palette image; and

outputting said modified publication quality digital image into a file format specified for said modified publication quality digital image.

2. The method as described in Claim 1 further comprising the step of combining said auxiliary data with predetermined information indicative of the presence of said auxiliary data, its file name, and file size, said step to be performed after the step of digitizing said auxiliary data.

3. The method as described in Claim 1 further comprising the step of including an algorithm for removing or hiding a digital watermark signature into said modified publication quality digital image.

4. The method as described in Claim 1, wherein said data embedding method comprises a bitslice process.

5. The method as described in Claim 1, wherein said data embedding method comprises a MODULAR ERROR EMBEDDING process.

6. The method as described in Claim 1, wherein said data embedding method comprises a DATA EMBEDDING process.

7. The method as described in Claim 1, wherein said publication quality digital image originates from a publication quality black and white image containing a range of digital levels of brightness.

8 The method as described in Claim 1, wherein said publication quality digital image originates from a digitized analog audio signal and said reference palette image originates from a reduced-quality version of said digitized audio analog signal.

9. The method as described in Claim 1, wherein said publication quality digital image originates from a television signal or motion picture image.

10. The method as described in Claim 1, wherein said publication quality digital image originates from X-ray or Magnetic Resonance Imaging data.

11. The method as described in Claim 1, wherein said publication quality digital image originates from digitized personal security and identification information.

12. The method as described in Claim 1, wherein said publication quality digital image originates from images made with a camera producing digital images.

13. A method of reconstructing indiscernible auxiliary data from a machine readable publication quality digital image representation of unrelated and uncorrelated data comprising the steps of:

generating a digital reference palette image from values and properties contained within said publication quality digital image;

creating a color-component digital difference image by numerically combining said digital reference palette image and said publication quality digital image;

constructing said auxiliary data by processing said color-component digital difference image with a data embedding construction method;

interpreting said auxiliary data in order to obtain or remove content, validate or authenticate, or otherwise process said publication quality digital image in order to modify auxiliary data quality.

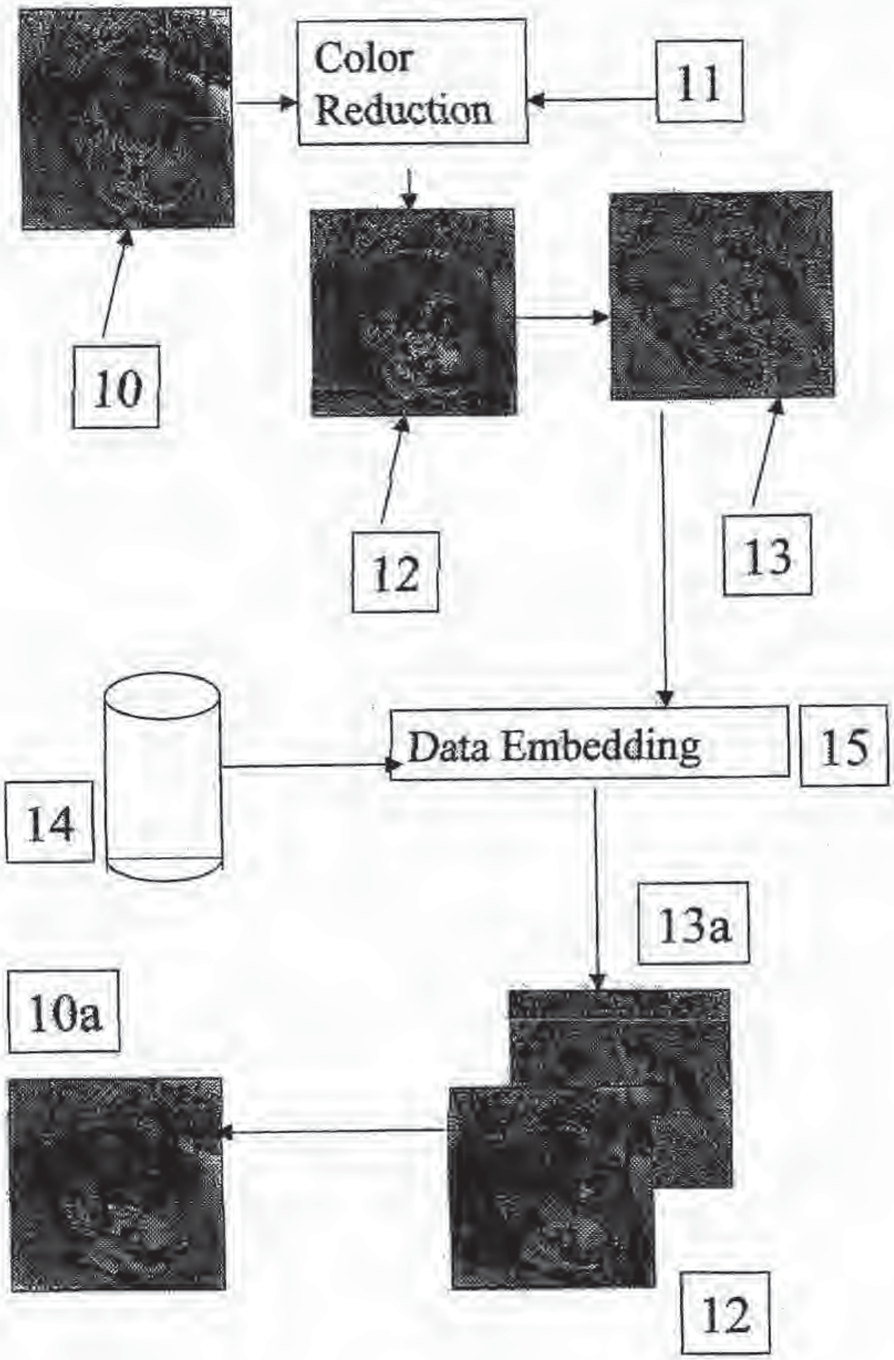


Figure 1

```
// loop to calculate and store the biased-difference of the Truecolor
image
   // difference = 128+(Truecolor - palette)
   // create the Truecolor difference file
   pixelcount = 0L;
   for (i = 0; i < (short)bh.rows; i++)  {
      memset(buffer, 0, BYTES_IN_ROW);
      j = TCFile->Read(buftc, BYTES_IN_ROW);// Truecolor image row
      ASSERT(j == (short)BYTES_IN_ROW);
      bytesread += j;
      j = tape7.Read(buffpal, bytesinrow); // palette-format image row
      ASSERT(j == bytesinrow);

      for (j = 0; j < (short)bh.cols; j++) {
         short b_diff, g_diff, r_diff;
         char pixval[3];
         k = *(buffpal + j);
         b_diff = 128 + (short)*(bufftc + j * 3) - (short)colormap[k].b;
         if (colormap[k].b > 250) {
            b_diff = 255;   // don't use maximum palette values
         }
         g_diff = 128 + (short)*(bufftc + j * 3 + 1) - (short)colormap[k].g;
         if (colormap[k].g > 250) {
            g_diff = 255;    // don't use maximum palette values
         }
         r_diff = 128 + (short)*(bufftc + j * 3 + 2) - (short)colormap[k].r;
         if (colormap[k].r > 250) {
            r_diff = 255;    // don't use maximum palette values
         }
```

FIGURE 2A

```
// set pixel to difference only if it is in range of unsigned char
// otherwise flag with a value that is later removed from the pair-
key
pixval[0] = pixval[1] = pixval[2] = '\0';
if (b_diff < 255 && b_diff > 0) {
    *(buffer + j * 3) = (unsigned char)b_diff;
} else {
    *(buffer + j * 3) = 0x01;    // flag to mark out-of-range pixel
    pixval[0] = 'b';
}
if (g_diff < 255 && g_diff > 0) {
    *(buffer + j * 3 + 1) = (unsigned char)g_diff;
} else  {
    *(buffer + j * 3 + 1) = 0x01;  // flag to mark out-of-range pixel
    pixval[1] = 'g';
}
if (r_diff < 255 && r_diff > 0) {
    *(buffer + j * 3 + 2) = (unsigned char)r_diff;
} else {
    *(buffer + j * 3 + 2) = 0x01;  // flag to mark out-of-range pixel
    pixval[2] = 'r';
}
```

FIGURE 2B

```
// loop to calculate and store the output version of the Truecolor image
   // note:   difference = 128+(Truecolor - palette)
   // hence:  Truecolor  = (difference -128) + palette

for (i = 0; i < (short)bh.rows; i++)  {
      memset(buffer, 0, BYTES_IN_ROW);
      j = tape6.Read(bufftc, BYTES_IN_ROW);   // difference image row
      ASSERT(j == (short)BYTES_IN_ROW);
      bytesread += j;
      j = tape7.Read(buffpal, bytesinrow);   // palette-format image row
      ASSERT(j == bytesinrow);
      for (j = 0; j < (short)bh.cols; j++) {
        unsigned char b_diff, g_diff, r_diff;
        if (i == 0) {
           memcpy(buffer,bufftc,BYTES_IN_ROW);
           break;     // difference embedding key in 1st row
        }
        k = *(buffpal + j);
        b_diff =  *(bufftc + j * 3) -128 + colormap[k].b;
        g_diff =  *(bufftc + j * 3 + 1) -128 + colormap[k].g;
        r_diff =  *(bufftc + j * 3 + 2) -128 + colormap[k].r;
        *(buffer + j * 3) = b_diff;
        *(buffer + j * 3 + 1) = g_diff;
        *(buffer + j * 3 + 2) = r_diff;
       }
       tape8.Write(buffer, BYTES_IN_ROW); // output one Truecolor
       image row
       }
```

FIGURE 3

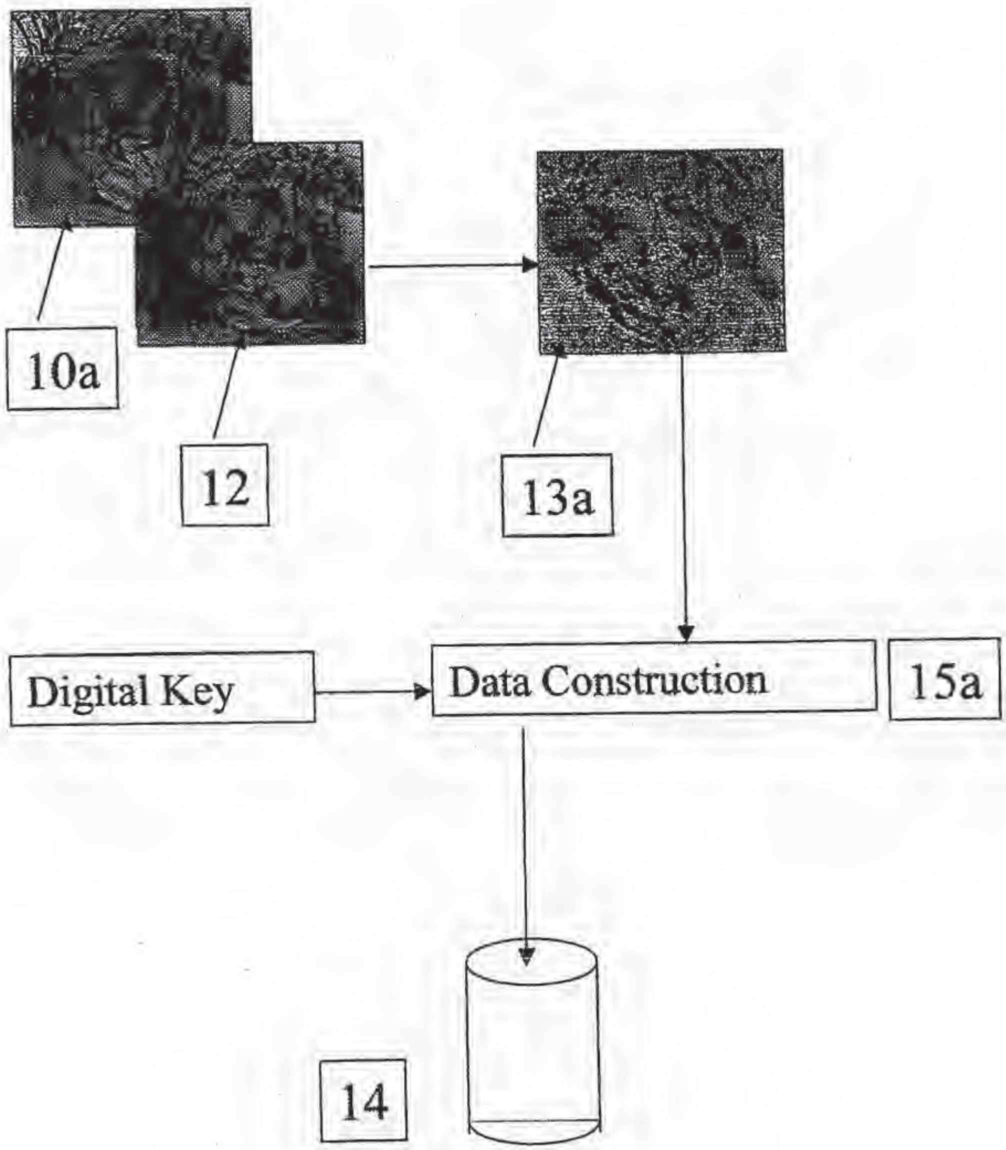


Figure 4

```
MakeDifferenceImage();
// open the difference file and extract the pixel_table information
CImageBitmapFile::OpenBitmapFile(tempstr);
ExtractBitmap();
```

FIGURE 5

WEST (BRS) [illegible]

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,659,726 A (SANDFORD, II et al.) 19 AUGUST 1997, see column column 2, lines 40-56.	1-13
A, P	US 5,819,289 A (SANFORD, II et al.) 06 OCTOBER 1998, col. 4, line 50 thru col. 5, line 16.	1-13
A	US 5,636,292 A (RHOADS) 03 JUNE 1997, see col. 5, lines 46-59.	1-13
A	US 5,652,626 A (KAWAKAMI et al.) 29 JULY 1997, see col. 4, lines 8-64.	1-13
A, E	US 5,930,369 A (COX et al.) 27 JULY 1999, see col. 9, lines 6-44.	1-13
A	US 5,530,759 A (BRAUDAWAY et al.) 25 JUNE 1996, see col. 4, line 52 thru col. 5, line 15.	1-13

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

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
26 AUGUST 1999	09 SEP 1999

Name and mailing address of the ISA/US	Authorized officer
Commissioner of Patents and Trademarks Box PCT Washington, D.C. 20231	GILBERTO BARRÓN JR. Joni Hill
Facsimile No. (703) 305-3230	Telephone No. (703) 305-1830

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/09417

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :G09C 5/00; H04L 9/00
US CL :380/4, 54; 382/232
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. : 380/4, 54; 382/232

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

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

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US99/09417

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5,537,223 A (CURRY) 16 JULY 1996, see column 3, lines 1-36.	1-13

Form PCT/ISA/210 (continuation of second sheet)(July 1992)★

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/30 | A1

(11) International Publication Number: WO 96/29795

(43) International Publication Date: 26 September 1996 (26.09.96)

(21) International Application Number: PCT/US96/03920

(22) International Filing Date: 21 March 1996 (21.03.96)

(30) Priority Data:
08/408,551 21 March 1995 (21.03.95) US

(81) Designated States: CA, JP, European patent (AT, BE, CH, 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.

(71)(72) Applicant and Inventor: MICALI, Silvio [US/US]; 459 Chestnut Hill Avenue, Brookline, MA 02146 (US).

(74) Agent: JUDSON, David, H.; Hughes & Luce, L.L.P., Suite 2800, 1717 Main Street, Dallas, TX 75201 (US).

(54) Title: SIMULTANEOUS ELECTRONIC TRANSACTIONS

(57) Abstract

A communication method between a first and second party, in the presence of a trusted party, that enables a transaction in which the second party receives a first value produced by the first party and unpredictable to the second party if and only if the first party receives a second value produced by the second party and unpredictable to the first party. The method includes two basic steps: exchanging a first set of communications between the first and second parties without participation of the trusted party to attempt completion of the transaction, and if the transaction is not completed using the first set of communications between the first and second parties, having the trusted party take action to complete the transaction.

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.

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

SIMULTANEOUS ELECTRONIC TRANSACTIONS

TECHNICAL FIELD

The present invention relates generally to electronic commerce and transactions and more particularly to techniques for enabling users to effect certified mail, contract signing and other electronic notarization functions.

BACKGROUND OF THE INVENTION

The value of many transactions depends crucially on their simultaneity. Indeed, simultaneity may be so important to certain financial transactions that entities often are willing to incur great inconvenience and expense to achieve it. For example, consider the situation where two parties have negotiated an important contract that they now intend to "close." Often, the parties find it necessary to sign the document simultaneously, and thus they meet in the same place to watch each other's actions. Another example is the process of certified mail, where ideally the sender of a message desires that the recipient get the message simultaneously with the sender's obtaining a "receipt". A common certified mail procedure requires a person who delivers the mail to personally reach the recipient and obtain a signed acknowledgement when the message is delivered. This acknowledgement is then shipped to the sender. Again, this practice is costly and time consuming. Moreover, such acknowledgements do not indicate the content of the message.

In recent years, the cost, efficiency and convenience of many transactions have been improved tremendously by the availability of electronic networks, such as computer, telephone, fax, broadcasting and others. Yet more recently, digital signatures and public-key encryption have added much needed security to these electronic networks, making such communication channels particularly suitable for financial transactions. Nevertheless, while electronic communications provide speed, they do not address simultaneity.

The absence of simultaneity from electronic transactions severally limits electronic commerce. In particular, heretofore there has been no effective way of building so-called *simultaneous electronic transactions* ("SET's"). As used herein, a SET is an electronic transaction that is simultaneous at least in a "logically equivalent" way, namely it is guaranteed that certain actions will take place if and only if certain other actions take place. One desirable SET would be certified mail, however, the prior art has not addressed this problem effectively. This can be seen by the following consideration of a hypothetical example, called *extended certified mail* or "ECM".

In an ECM transaction, there is a sender, Alice, who wishes to deliver a given message to an intended recipient, Bob. This delivery should satisfy three main properties. First, if Bob refuses to receive the message (preferably before learning it), then Alice should not get any receipt. Second, if Bob wishes to receive the message, then he will receive it and Alice will get a receipt for the message. Third, Alice's receipt should not be "generic," but closely related to the message itself. Simultaneity is important in this transaction. For instance, Alice's message could be an electronic payment to Bob, and it is desired that she obtains a simultaneous receipt if possible.

Alice could try to get a receipt from Bob of a message m in the following way. Clearly, sending m to Bob in the clear as her first communication does not work. Should this message be her digital signature of an electronic payment, a malicious Bob may loose any interest in continuing the conversation so as to deprive Alice of her receipt. On the other hand, asking Bob to send first a "blind" receipt may not be acceptable to him.

Another alternative is that Alice first sends Bob an encryption of *m*. Second, Bob sends Alice his digital signature of this ciphertext as an "intermediate" receipt. Third, Alice sends him the decryption key. Fourth, Bob sends Alice a receipt for this key. Unfortunately, even this transaction is not secure, because Bob, after learning the message when receiving Alice's key, may refuse to send her any receipt. (On the other hand, one cannot consider Bob's signature of the encrypted message as a valid receipt, because Alice may never send him the decryption key.)

These problems do not disappear by simply adding a few more rounds of communication, typically consisting of "acknowledgements". Usually, such additional rounds make it more difficult to see where the lack of simultaneity lies, but they do not solve the problems.

Various cryptographic approaches exist in the literature that attempt to solve similar problems, but they are not satisfactory in many respects. Some of these methods applicable to multi-party scenarios propose use of verifiable secret sharing (see, for example, Chor et al), or multi-party protocols (as envisioned by Goldreich et al) for making simultaneous some specific transactions between parties. Unfortunately, these methods require a plurality of parties, the majority of which are honest. Thus, they do not envision simultaneous transactions involving only two parties. Indeed, if the majority of two parties are honest then both parties are honest, and thus simultaneity would not be a problem. Moreover, even in a multi-party situation, the complexity of these prior art methods and their amount and type of communication (typically, they use several rounds of broadcasting), make them generally impractical.

Sophisticated cryptographic transactions between just two parties have been developed but these also are not simultaneous. Indeed, if just two people send each other strings back and forth, and each one of them expects to compute his own result from this conversation, the first to obtain the desired result may stop all communications, thereby depriving the other of his or her result. Nonetheless, attempts at providing simultaneity for two-party transactions have been made, but by using assumptions or methods that are unsatisfactory in various ways.

For example, Blum describes transactions that include contract signing and extended certified mail and that relies on the two parties having roughly equal computing power or knowledge of algorithms. These assumptions, however, do not always hold and are hard to check or enforce anyway. In addition, others have discovered ways to attack this rather complex method. A similar approach to simultaneity has also been proposed by Even Goldreich and Lempel. In another Blum method for achieving simultaneous certified mail, Alice does not know whether she got a valid receipt. She must go to court to determine this, and this is undesirable as well.

A method of Luby et al allows two parties to exchange the decryption of two given ciphertexts in a special way, namely, for both parties the probability that one has to guess correctly the cleartext of the other is slowly increased towards 100%. This method, however, does not enable the parties to achieve guaranteed simultaneity if one party learns the cleartext of the other's ciphertext with absolute probability (e.g., by obtaining the decryption key); then he can deny the other a similar success.

For this reasons several researchers have tried to make simultaneous two-party transactions via the help of one or more external entities, often referred to as "centers", "servers" or "trustees", a notion that appears in a variety of cryptographic contexts (see, for instance, Needham and Schroder and Shamir). A method for simultaneous contract signing and other transactions involving one trustee (called a "judge") has been proposed by Ben-Or et al. Their method relies on an external entity only if one party acts dishonestly, but it does not provide guaranteed simultaneity. In that technique, an honest party is not guaranteed to have a signed contract, even with the help of the external entity. Ben-Or et al only guarantee that the probability that one party gets a signed contract while the other does not is small. The smaller this probability, the more the parties must exchange messages back and forth. In still another method, Rabin envisions transactions with the help of external party that is active at all times (even when no transaction is going on), but also this method does not provide guaranteed simultaneity.

The prior art also suggests abstractly that if one could construct a true simultaneous transaction (e.g., extended certified mail), then the solution thereto might also be useful for constructing other types of electronic transactions (e.g., contract signing). As noted above, however, the art lacks an adequate teaching of how to construct an adequate simultaneous transaction

There has thus been a long-felt need in the art to overcome these and other problems associated with electronic transactions.

BRIEF SUMMARY OF THE INVENTION

It is an object of the invention to provide true simultaneous electronic transactions.

It is a further object of the invention to provide an electronic transaction having guaranteed simultaneity in a two-party scenario and with minimal reliance and support of a third party.

It is another more specific object of the invention to provide simultaneous electronic transactions between two parties that rely on third parties in a minimal and convenient manner. In particular, it is desired to provide electronic transactions between two parties that guarantee simultaneity via the help of an *invisible* third party. A third party is said to be "invisible" because it does not need not to take any action if the transaction occurs with the parties following certain prescribed instructions. Only if one of the original parties deviates from these instructions may the other invoke the intervention of the up-to-then invisible third party, who then can still guarantee the simultaneity of the transaction even though it has not participated from its inception.

These and other objects are provided in a communication method between a first and second party, in the presence of a trusted party, that enables a transaction in which the second party receives a first value produced by the first party and unpredictable to the second party if and only if the first party receives a second value produced by the second party and unpredictable to the first party. The method includes two basic steps: exchanging a first set of communications between the first and second parties without participation of the trusted party to attempt completion of the transaction, and if the transaction is not completed using the first set of communications between the first and second parties, having the trusted party take action to complete the transaction.

Where the first party's value is a message and the second party's value is a receipt, the transaction is a certified transmission of

the first party's message. Alternatively, the first party's value represents a commitment to a contract and the second party's value represents a commitment to the contract, such that the transaction is a contract closing.

Preferably, according to the method the first party can prove that some information it receives is the second value, and the second party can prove that some information it receives is the first value.

According to the more specific aspects of the method, at least one of the first and second parties and the trusted party can encrypt messages, and at least one of the first and second parties and the trusted party can decrypt messages. The first set of communications includes at least one communication of the first party to the second party of a data string generated by a process including encrypting a second data string with an encryption key of the trusted party. The second data string includes a ciphertext generated with an encryption key of one of the parties, as well as information specifying or identifying at least one of the parties. The first set of communications also includes at least one communication of the second party of a data string generated by a process that includes having the second party digitally sign a data string computed from information received from the first party in a prior communication, wherein the data string generated by the second party is the second party's value.

According to further aspects of the method, if the second party does not get the first value in the first set of communications, the second party sends the trusted party, for further processing, a data string that includes at least part of the data received from the first party. The further processing by the trusted party includes decrypting a ciphertext with a secret decryption key. The trusted party then sends the first party information that enables the first party to compute the second value, and the trusted party sends the second party information that enables the second party to compute the first value. In either case, the trusted party also verifies identity information of at least one of the parties but preferably does not learn the first value.

DETAILED DESCRIPTION

In each of the schemes described below, there is a user Alice and a user Bob. The "invisible" third party may be a financial center that facilitates SETs among its customers, including Alice and Bob. For convenience, the following description shows how to make extended certified mail "simultaneous", although the invention is not so limited. In the context of an ECM system, the third party is called the Post Office. As will be seen, however, contrary to ordinary certified mail, the Post Office here is invisible. The inventive scheme is also preferable to ordinary certified mail because the message receipt also guarantees the content of the message. Also, the electronic transaction is faster, more informative and more convenient than traditional certified mail, and its cost should be substantially lower.

In the preferred embodiment, an extended certified mail system is provided using a single "invisible" trustee or "trusted" party. The system is implemented in a computer network, although it should be realized that telephone, fax, broadcast or other communication networks may be used. Thus, without limitation, it is assumed that each user in the system has a computer capable of sending and receiving messages to and from other computers via proper communication channels.

Each user in the system has a unique identifier. Alice's identifier is denoted by A, and Bob's identifier is B. The identifier of the Post Office is denoted by PO. Users and the Post Office can digitally sign messages. Thus, each has a secret signing key and a matching public verification key. If *m* is a message (string), then SIG_A(m) indicates Alice's signature of *m*. (It is assumed, for convenience, that *m* is always retrievable from its signature. This is the case for most signature schemes, and it is otherwise possible to consider a signed message as the pair consisting of the message and its signature.)

Users and the Post Office can encrypt messages by means of a public-key encryption algorithm (e.g., RSA). Thus, each has a public encryption key and a corresponding secret decryption key. $E_A(m)$, $E_B(m)$, and $E_{PO}(m)$ denote, respectively, the encryption of a message *m* with the public key of Alice, Bob, and the Post Office. For simplicity, it is assumed that these schemes are secure in the sense that each of E_A, E_B, and E_{PO} appear to behave as a random function. The system can be suitably modified if these functions are much less secure.

Again, for simplicity these encryption algorithms are deterministic and uniquely decodable. Thus, given a value *y* and a message *m*, all can verify whether *y* is the encryption of *m* with, for example, the Post Office's key, by checking whether $E_{PO}(m)$ equals *y*. (If the encryption scheme is probabilistic, then one may convince another that a string *y* is an encryption of a message m by providing *m* together with the random bits that were used to encrypt *m*.) If *y* is a ciphertext generated by means of the encryption algorithm *E*, $E^{-1}(y)$ denotes the corresponding cleartext, whether or not *E* defines a permutation. (It may also be possible to use encryption algorithms that are not uniquely decodable, for instance, if it is hard to decrypt a given ciphertext in two different ways.) For simplicity, messages are encrypted directly with a public-key algorithm, however, one could first encrypt a message conventionally with some key k, and then encrypt k with a public-key algorithm. (Thus, to decrypt m, one need only just decrypt k).

In one preferred embodiment outlined below, the ECM method requires 5 possible steps of communication: A1 and A2 for user Alice, B1 and B2 for user Bob, and PO for the Post Office. However, at most 3 steps should have to be executed. If Alice and Bob are both honest, only steps A1, B1, and A2 will be executed, and in this order. Step B2 will be executed only if Alice fails to execute Step A2 properly. The execution of Step B2 causes the Post Office to execute its only step, PO. The protocol is as follows:

A1. Given her message m, Alice computes $z = E_{PO}((A, B, E_B(m)))$, the encryption in the Post Office public key of a triplet consisting of identifiers A, B and the message m encrypted in Bob's key, and then sends z to Bob.

B1. Upon receiving z from Alice, Bob digitally signs it and sends it to Alice as the receipt.

A2. If Alice receives the properly signed receipt from Bob, she sends m to Bob.

B2. If, within a given interval of time after having executed Step B1, Bob receives a string m such that $E_{PO}((A, B, E_B(m))) = z$, the value originally received from Alice, then he outputs m as the message and halts. Otherwise, Bob sends the value z

signed by him to the Post Office indicating that Alice is the sender and he is the recipient.

PO. If Bob's signature relative to *z* is correct, the Post Office decrypts *z* with its secret key. If the result is a triplet consisting of A, B and a string *x*, the Post Office (a) sends Alice the value *z* signed by Bob as the receipt, and (b) sends *x* to Bob.

Preferably, Alice sends *z* to Bob digitally signed by her. In addition, Alice may sign *z* in a standard format that indicates *z* is part of an extended certified mail sent from Alice to Bob, e.g., she may sign the tuple *(ECM, A, B, z)*. In this way, Bob is certain that *z* comes from Alice and that, when Alice holds a receipt for *m* signed by Bob, he will have a certified version of *m*. Further, if *z* is digitally signed by Alice, Bob first checks Alice's signature, and then countersign *z* himself. The adoption of a standard format also insures that, by signing *z* as part of an ECM system, Bob does not sign accidently a message that has been prepared by Alice maliciously. Also, the Post Office may also check Alice's signature or any additional formats if these are used.

In analyzing the protocol, it should be noted that Alice, given Bob's signature of *z* as receipt, can prove the content of the message by releasing *m*. Indeed, all can compute $x = E_B(m)$ and then verify that $E_{PO}((A, B, x)) = z$.

Notice also that the Post Office does not understand the message sent via the ECM protocol, whether or not it is called into action. Rather, the Post Office can only obtain $E_B(m)$, but never *m* in the clear (in this embodiment).

Third, notice that m is, by definition, equal to $E'_B(x)$, where $(A, B, x) = E_{PO}^{-1}(z)$, and may be non-sensical. Indeed, nothing prevents Alice from sending Bob a garbled message. However, she can only get a receipt for this same garbled message. It is also noted that, if not every string is an encryption of some message, Alice may choose z so that it is not the encryption of anything. In such case, however, she cannot ever claim to have a receipt for any message. Alternatively, it may be desirable to use cryptosystems for which either every string is an encryption of some other string or such that it can be easily detected whether y encrypts something.

The protocol works for the following reasons. When receiving the value $z = E_{PO}((A, B, E_B(m)))$ from Alice, Bob will have difficulty in computing $E_B(m)$, and thus m, from z without the Post Office's secret key. Thus, if he halts, Alice would not get her receipt, but Bob would not get m either.

Assume now that Bob signs z and sends it to Alice. Because this gives Alice a valid receipt from Bob for her message m, for the simultaneity constraint to hold, it must be shown that Bob easily obtains m. This is certainly true if Alice sends m to Bob in Step A1. Assume therefore that Alice does not send him m. Then, Bob presents z signed by him to the Post Office, essentially asking the Post Office to retrieve (for him) $E_B(m)$ from z. The Post Office complies with this request. In doing so, however, the Post Office also sends Alice z signed by Bob as the receipt. It does so to prevent one last possibility; that Bob, upon receiving z from Alice in Step A1, rather than sending her the receipt in Step B1, goes *directly* to the Post Office in order to have $E_B(m)$ extracted from z.

Summarizing, if Alice sends a message encrypted with the Post Office key to Bob, and Bob does not send Alice a receipt, or if he does not access the Post Office, Bob will never learn *m*. Otherwise, Alice is guaranteed to get her receipt for *m* either from Bob or from the Post Office. On the other hand, upon receiving an encrypted message, Bob is guaranteed that he will understand it, either helped by Alice or helped by the Post Office.

In the preferred embodiment above, the triplet (which includes the ciphertext $E_B(m)$) also includes A and B. The ciphertext is customized in this way so that it can be used by the system only for the purpose of Alice sending a message to Bob. Whether or not this customization is performed, the system is very convenient to use because everyone knows the public key of the Post Office, because everyone can encrypt a value with that key, and because the Post Office can remove this encryption layer for those recipients who claim to have been betrayed by their senders. However, without the above (or an equivalent) customization, this same convenience could be exploited by a malicious recipient, who could learn his messages while denying the senders their legitimate receipts.

In particular, assume that this customization is removed altogether. Then, a malicious Bob, upon receiving $z' = E_{PO}(E_B(m))$ - rather than $z = E_{PO}((A, B, E_B(m)))$ - from Alice in Step A1, may behave as follows. First, he does not send Alice any receipt. Second, he signs z'. Third, he gives this signed value to the Post Office complaining that a sender Chris (an accomplice of his) is refusing to send him the message in the clear. At this point, the Post Office, after verifying Bob's signature and not having any way of checking whether Chris is the real sender, retrieves $E_B(m)$ from z' and sends $E_B(m)$ to Bob, while simultaneously sending the signed z' to Chris as his receipt. Of course, Chris may destroy or hide this receipt. Meanwhile Alice, who does not get any receipt after Step

A1, may think that Bob is away or does not want to receive her message. But she believes that Bob will never be able to read her message in any case.

This violation of the simultaneity constraint (i.e., Bob receiving *m* while Alice having no receipt) may still occur if, without any customization, Alice signs *z* when sending it to Bob in Step A1. Indeed, Bob would have no trouble in removing Alice's signature, asking Chris to sign *z'* and then presenting to the Post Office *z'* signed by Chris and countersigned by himself. The Post Office, after verifying Bob's and Chris's signatures, would still (after removing its encryption layer) send $E_B(m)$ to Bob and the receipt to Chris. This violation of simultaneity, however, does not occur with the customization of the triplet to include A and B. Indeed, assume that Bob gives the Post Office the value $z = E_{PO}((A, B, E_B(m)))$ originally received by Alice and signed by him and Chris, claiming that it was sent to him by Chris. Then, the Post Office, after verifying Bob's (and Chris's) signature and after computing the value $E_{PO}^{-1}(z)$, will notice that this value - i.e. $(A, B, E_B(m))$ - does not specify Chris to be the sender and Bob the receiver.

The benefits of this customization may be implemented in varying ways. For instance, Alice's signature of $(B, E_B(m))$ may be sufficient to indicate that the sender is Alice and the receiver is Bob. More generally, any customization that prevents Bob from obtaining $E_B(m)$ from the Post Office while convincing the Post Office not to send Alice the receipt is within the scope of the invention.

It should be realized that any customization for the purpose of simultaneous electronic transactions is itself within the scope of the present invention, whether or not implemented with an invisible third party. For instance, Alice may send $E_{PO}(A, B, E_B(m))$ directly to the

Post Office, which gives $E_B(m)$ to Bob (if Bob signs the receipt for Alice) after checking that Alice and Bob are, respectively, the sender and the receiver. Alternatively, Alice may send the Post Office $E_{PO}(SIG_A(B,E_B(m)))$ for identifying the sender and the recipient in a way that cannot be decoupled from the transaction. Such approaches may be especially useful with a plurality of trustees as described below. Such an approach, which calls into action the trusted party directly with a proper customization step as described, is also useful for hiding the identity of the sender from the recipient Indeed, the Post Office may solicit a proper receipt from Bob without disclosing Alice's identity (even if the receipt indicates the content of Alice's message).

Although not specified above explicitly, it should be appreciated that all or part of the actions required by the Post Office, Alice or Bob can be realized in software. Some of these actions can also be performed by hardware, or physically secure devices (i.e. devices such as secure chips having at least some portion of which is tamper-proof).

Many variations of the disclosed protocol can be envisioned and are within the scope of the present invention. For instance, while the "receipt" described above witnesses the content of the message sent, the receipt can be made generic, e.g., by having Bob sign a "declaration" (instead of a string including an encrypted version of the message) that he has received an encrypted message from Alice at a given time. Also, if desired, the customization step (i.e. the inclusion of the identifiers A and B in the triplet) can be omitted. This might be advantageous, for example, when no other user may collude with either Alice or Bob to disrupt simultaneity. This may occur where there is no third user, as in the case when certified mail occurs between two predetermined people. In the disclosed system, the Post Office cannot learn the content of the message, but such a restriction can be removed also (e.g., by having Alice compute $z = E_{PO}(A, B, m)$). It may also be convenient to one-way hash strings prior to signing them.

Still another variation would be to impose some temporal element on the transaction. For instance, when Alice sends Bob $z = E_{PO}(A, B, E_B(m))$, she may sign z together with some additional information that specifies a certain time (either absolute or relative to the sending time) after which the Post Office will not help Bob obtain the message. Preferably, Alice specifies this time in a signed manner both outside the Post Office encryption layer as well as within the triplet. In such case, the Post Office must obtain from Bob all necessary information to verify that the time specified outside the PO encryption layer checks with the time specified within the triplet. If it does not, then several possibilities may occur. For example, the Post Office will not help Bob recover the message, or the message is considered unsent (even if Alice obtains a receipt).

Other variations are also possible. Some variations may be used in conjunction or in alternative to the techniques described above. One group of such variants concerns the encryption method used.

For instance, E_B does not need to be interpreted as an encryption algorithm for which Bob has the decryption key. It may just be an encryption algorithm for which Bob can have the message decrypted. For example, and without limitation, the decryption key of E_B may lie with a group of people, each having a piece of the key. These same alternative interpretations apply also to E_A or E_{PO}.

Also, while public-key cryptosystems are quite convenient, it should be realized that conventional cryptosystems could be used for the ECM protocol. For example, *x* may be the conventional encryption of *(A, B, $E_B(m)$)* with a secret key *k* shared between Alice and the Post Office. This key *k* may be released if it is desired that Bob verify *m* to be the genuine message. If, however, it is feared that release of a different key may change the content of the messages, special redundancies could be used. For instance, conventionally a message *M* is encrypted by actually encrypting *(M, H(M))*, where *H* is a one-way function. Thus, if *e* is an encryption of *(M, H(M))* with a key *k*, it is hard to find a second key *K* such that *e* also is an encryption with that key of *(M'H(M'))*. It is preferable that *k*, rather than being a secret key shared by Alice and the Post Office, is a temporary key that Alice may transfer to the Post Office separately by means of a different shared key *K*. This way, divulging *k* (e.g., for the purpose of convincing Bob of the value of *$E_B(m)$)* does not force the Post Office and Alice to agree on another conventional key *k*.

It should also be appreciated that the digital signatures of the ECM system need not be public key signatures. For instance, there may be private key digital signatures or signatures verifiable with the help of other parties, or other suitable forms of message authentication. Thus, as used herein, "digital signatures" and "digital signing" should be broadly construed. Similarly, the notion of encryption with a key of some party should be broadly construed to include encrypting with a public key of that party or encrypting with a secret key shared with that party or known to that party.

There may also be concern that the Post Office will collude with one of the parties. For instance, the Post Office may collude with Bob who, rather than sending the receipt to Alice, goes directly to Post Office, and this enables Bob to understand his message but without giving Alice any receipt. This may occur in ordinary certified mail. Indeed, one who delivers the post may leave a letter with his intended recipient without asking him or her to sign a receipt. Nonetheless, this potential problem may be dealt with effectively and efficiently. For instance, the Post Office may be (or make use of) a physically secure device. Assuming that the Post Office uses such a device in the preferred embodiment, then it will be hard for user Bob to have the Post Office decrypt *(A, B, $E_B(m)$)* for him without sending Alice her receipt. Indeed, the chip can be programmed to perform both operations or none. Although use of physically secure devices might increase the cost of a system, this need not be the case. Indeed, while they may be millions of users, there may be one or much fewer Post Offices. (Each user, of course, may benefit also from being or relying upon physically secure devices.)

While the inventive ECM system is very economical as it requires at most three communication steps, the goals can be accomplished also by more steps. In particular, although the trusted party, upon receiving Bob's communication, can enable Bob to get his message and Alice to get her receipt, without sending messages back and forth, this goal can be accomplished by means of a more complex dialogue. Indeed, more elaborate dialogues, and in particular zero knowledge proofs (see, e.g., Goldwasser et al or Goldreich et al) could be useful (also as an alternative to physically secure devices) to give Bob the message or Alice the receipt so that they learn their respective values, but are not able to "prove" these values to third parties.

A further alternative method envisions a Post Office with a plurality of trustees. A multiplicity of trustees can be beneficial for various aspects, particularly, if the system is set up so that more than one of the trustees must collude for cheating to occur. Presumably, however, each trustee is selected with trustworthiness (or, if it is a device, proper functioning) as a criterion, and thus the possibility that more than one of them is malicious or defective is very small.

A simultaneous ECM system with a multiplicity of trustees may make novel use of prior techniques such as fair cryptography, or secret sharing, verifiable secret sharing or threshold cryptosystems.

In a construction based on fair public cryptosystems, the triplets *(A, B, $E_B(m)$)* are not encrypted with the Post Office's public key, but rather with a user public key. In this embodiment, user Alice computes a pair of public and secret key of a fair public-key cryptosystem, properly shares her secret key with the trustees of the Post Office (e.g., receiving from said trustees a certification that they got legitimate shares of this user key) in some initial phase, and then performs Step A1 of the above ECM protocol. If needed, Bob may turn to the Post Office and instructs the trustees to reconstruct Alice's user key. By doing so, the trustees cannot monitor or cause the Post Office to monitor the message addressed by Alice to Bob, but can reconstruct the triplet *(A, B, E(m))*. To insure that the Post Office trustees do not collude with Bob in depriving Alice of her receipt, it can be arranged that each trustee, when contributing its own piece of a user secret key, also gives a proper acknowledgement to that user. Thus, unless all *n* trustees do not behave properly, Alice would receive at least one receipt.

A possible drawback of this fair-cryptography based system is that Alice must interact with the trustees in order to give them shares of her user key. Thus, the trustees are not fully invisible. This interaction may not even be confined to a single initial phase. This is because Alice may not be able to reuse her key after Bob accesses the Post Office and causes its reconstruction. To alleviate this problem, it might be desirable to use physically secure devices and having the trustees reveal their own pieces to such a device, which would then be able to announce *(A,B,E$_B$(m))* without proof.

A better approach uses the ECM protocol, but involves splitting the secret key of the Post Office rather than the secret user keys. Thus, Alice would continue to encrypt *(A, B, E$_B$(m))* with the help of the Post Office public key, whose corresponding secret key is shared among the n trustees but is not known to any single entity (nor has it been prepared by any single entity). Thus, the n trustees must cooperate, under Bob's proper request, in removing the Post Office's encryption layer. However, they do so without reconstructing the Post Office secret key, not even internally to the Post Office. To this end, a threshold cryptosystem may be used). This solution is now illustrated using the well- known Diffie-Hellman public-key cryptosystem.

In the Diffie-Hellman system, there is a prime p and a generator g common to all users. A user X chooses his own secret key x at random between 1 and p - 1, and sets his public key to be g^x mod p. Let y and g^y mod p, respectively, be the secret and public keys of user Y. Then X and Y essentially share the secret pair key g^{xy} mod p. Indeed, each of X and Y can compute this pair-key by raising the other's public key to his own secret key mod p. On the other hand, without knowledge of x or y, no other user, given the public keys g^x mod p and g^y mod p and based on any known method, can compute the pair-key g^{xy}. Thus X and y can use this key to secure communications between each other (e.g., by using it as the key of a symmetric cipher).

Let now $T_1, \ldots, T_n$ be the trustees of the Post Office. Then, each T_i chooses a secret key xi and a matching public key $g^{x}{}_i$ mod p. Then the public key of the Post Office is set to be the product of these public keys mod p, g^z mod p (i.e., $g^z = g^{x1+\ldots+xn}$ mod p). Thus, each trustee has a share of the corresponding secret key, z. Indeed, the Post Office's secret key would be $z = x1 + \ldots + xn$ mod $p-1$. Assume now that Alice wishes to encrypt $(A, B, E_B(m))$ with the Post Office's key. She selects a (preferably) temporary secret key a and its corresponding public key g^a mod p. She then computes the public pair-key g^{az} mod p, encrypts $(A, B, E_B(m))$ conventionally with the secret pair-key g^{az}, and then sends Bob this ciphertext together with the temporary public-key g^a mod p (all in Step A1). If in Step B1 Bob sends Alice back a receipt, namely, his signature of the received message, then Alice, in Step A2, sends him the secret key a. This enables Bob to compute the pair-key g^{az} mod p (from a and the Post Office's public key), and thus decrypt the conventional ciphertext to obtain $(A, B, E_B(m))$. Thus, if both users behave properly, the Post Office is not involved in the transaction. Assume now that Bob properly asks the Post Office to decrypt Alice's ciphertext. To do this, the trustees cooperate (preferably, with proper notice to Alice and to each other) in computing g^{az} mod p. To this end, each trustee T_i raises Alice's public key g^a mod p to its own secret key. That is, T_i computes g^{axi} mod p. Then these shares of the pair-key are multiplied together mod p to obtain the desired private pair-key. In fact, $g^{ax1} \cdots g^{axn}$ mod $p = g^{ax1+\ldots+axn}$ mod $p = g^{a(x1+\ldots+xn)}$ mod $p = g^{az}$

mod p. This key may be given to Bob, who can thus obtain $E_B(m)$. In this method, it may be useful to have a Post Office representative handle the communications with Bob, while the individual trustees handle directly their sending Alice receipts.

This method can be adjusted so that sufficiently few (alternatively, certain groups of) trustees cannot remove the Post Office's encryption layer, while sufficiently many (alternatively, certain other groups of) trustees can. For instance, there can be kn trustees, and each of the n trustees acting as above can give his own secret key to each of a group of k - 1 other trustees. Thus, each distinct group of k trustees has knowledge of a secret key as above. Further, the above-described modifications to the single invisible-trustee ECM protocol can be applied to embodiments involving multiple trustees.

In the ECM system involving fair cryptography, even a user might be or rely upon a multiplicity of entities. Indeed, in the invention, "user" or "party" or "trusted party" thus should be construed broadly to include this possibility.

It should be appreciated that the inventive ECM systems enable Alice and Bob to exchange simultaneously two special values, the first, produced by Alice, which is (at least reasonably) unpredictable to Bob, and the second, produced by Bob, which is unpredictable to Alice. Indeed, the value produced by Bob and unpredictable to Alice may be Bob's signature of step B1. If the message is not known precisely by Bob, then the message itself may be the value produced by Alice and unpredictable to Bob. Alternatively, if Bob knows the message precisely (but it is desired that he receive it from Alice in an official and certified manner), then the parties may use a customization step so that, for example

$SIG_A(m,E_B(m))$ is the value produced by Alice and unpredictable to Bob.

The inventive system is useful to facilitate other electronic transactions that require the simultaneous exchange of unpredictable values. One such example, not meant to be limiting, involves a contract "closing" wherein a pair of users desire to sign a contract at a particular time and place. The invention thus allows Alice and Bob to sign a contract simultaneously with an invisible third party. Indeed, the first value may be Alice's signature of the contract C and the second value Bob's receipt for a message consisting of Alice's signature of C.

In particular, assume that Alice and Bob have already negotiated a contract C. Then, Alice and Bob agree (in a preliminary agreement) (a) that Alice is committed to C if Bob gets the message consisting of Alice's signature to C, and (b) that Bob is committed to C if Alice gets Bob's receipt of that message. This preliminary agreement can be "sealed" in many ways, for instance by signing, preferably standardized, statements to this effect conventionally or digitally. It does not matter who signs this preliminary agreement first because Bob does not have Alice's message and Alice does not have Bob's receipt. However, after both parties are committed to the preliminary agreement, the inventive ECM system allows the message and the receipt to be exchanged simultaneously, and thus C is signed simultaneously. Those skilled in the art also may realize it may be more convenient to first one-way hash C prior to signing it.

This method may be much more practical than accessing a commonly trusted lawyer particularly, when the contract in question may be very elementary or arises in an "automatic context". Generalizing, one may view a contract C as any arbitrary signal or string of symbols to which the parties wish to commit in a simultaneous way. The inventive solution is very attractive because it can be implemented in software in many contexts, and because the trustee is invisible and need not be called into use if the signatories behave properly. This minimizes cost and time, among other resources. In this application, the trustee, rather than a post office, may be a "financial service center" that facilitates the transactions of its own customers.

Yet another application of the invention is to make simultaneous the result of applying a given function to one or more secret values, some belonging to Alice and some belonging to Bob. For example, the inventive method allows implementation of "blind" negotiations. In this embodiment, assume a seller Alice and a buyer Bob desire to determine whether Alice's (secret) minimum selling price is lower than Bob's (secret) maximum selling price (in a way that both parties will learn the result simultaneously). If the answer is no, then the parties may either try again or terminate the negotiation. Alternatively, if the answer is yes, then preferably the parties also will be committed to the transaction at some value. (For example, the average of the two secret values).

Another useful application of the invention is during a bid process, such as in an auction. For instance, assume that multiple bidders wish that their secret bids be revealed simultaneously. One bidder may also wish that his or her bid be independent of the other bids.

CLAIMS:

What is claimed is:

1. A communication method between a first and second party, in the presence of a trusted party, enabling a transaction in which the second party receives a first value produced by the first party and unpredictable to the second party if and only if the first party receives a second value produced by the second party and unpredictable to the first party, comprising the steps of:

exchanging a first set of communications between the first and second parties without participation of the trusted party to attempt completion of the transaction; and

if the transaction is not completed using the first set of communications between the first and second parties, having the trusted party take action to complete the transaction.

2. The communication method as described in Claim 1 wherein the first party's value is a message and the second party's value is a receipt, such that the transaction is a certified transmission of the first party's message.

3. The communication method as described in Claim 1 wherein the first party can prove that some information it receives is the second value.

4. The communication method as described in Claim 1 wherein the second party can prove that some information it receives is the first value.

5. The communication method as described in Claim 1 wherein the first party can prove that some information it receives is the second value and the second party can prove that some information it receives is the first value.

6. The communication method as described in Claim 1 wherein the first party's value represents a commitment to a contract and the second party's value represents a commitment to the contract, such that the transaction is a contract closing.

7. The communication method as described in Claim 6 wherein the first party can prove that some information it receives is the second value and the second party can prove that some information it receives is the first value.

8. The communication method as described in Claim 1 wherein at least one of the first and second parties and the trusted party can encrypt messages, and at least one of the first and second parties and the trusted party can decrypt messages.

9. The communication method as described in Claim 8 wherein at least one communication of the first party is a data string generated by a process including encrypting a second data string with an encryption key of the trusted party.

10. The communication method as described in Claim 9 wherein the second data string includes a ciphertext generated with an encryption key of one of the parties.

11. The communication method as described in Claim 9 wherein the second data string contains information identifying at least one of the parties.

12. The communication method as described in Claim 8 wherein at least one communication of the second party is a data string generated by a process that includes having the second party digitally sign a data string computed from information received from the first party in a prior communication, wherein the data string generated by the second party is the second party's value.

13. The communication method as described in Claim 8 wherein if the second party does not get the first value in the first set of communications, the second party sends the trusted party for further processing a data string that 5 includes at least part of the data received from the first party.

14. The communication method as described in Claim 13 wherein the further processing by the trusted party includes decrypting a ciphertext with a secret decryption key.

15. The communication method as described in Claim 14 wherein the trusted party sends the first party information that enables the first party to compute the second value, and the trusted party sends the second party information that enables the second party to compute the first value.

16. The communication method as described in Claim 15 wherein the trusted party also verifies identity information of at least one of the parties and does not learn the first value.

17. The communication method as described in Claim 1 wherein the trusted party takes no action to complete the transaction after a specified time.

18. The communication method as described in Claim 17 wherein the specified time is included within the first set of communications.

19. The communication method as described in Claim 17 wherein the specified time is determined by the time at which certain communications occur.

20. A method by which first and second parties and a trusted party effect a certified mail transaction, each of the parties having matching public and secret keys of a public key encryption scheme, and wherein the first party desires to send a message to the second party and obtain a message receipt indicating the content of the message to thereby complete the certified mail transaction, comprising the steps of:

(a) having the first party generate and send to the second party a data string including an encryption, with the trusted party's public key, of information that prevents the trusted party for enabling the second party to obtain the first party's message without the first party obtaining the message receipt;

(b) upon receipt by the second party of the data string, having the second party generate and send to the first party the message receipt;

(c) upon receipt by the first party of the message receipt, having the first party send to the second party information that enables the second party to retrieve the 20message;

(d) upon receipt by the second party of the information, having the second party attempt to verify whether the message was received; and

(e) if the message was not received, having the second party send information to the trusted party for further processing, wherein the information includes a ciphertext encrypted with a public key of the trusted party.

21. The method as described in Claim 20 further including the step of:

(f) having the trusted party, using the information received from the second party, (i) decrypt some information it receives from the second party using the secret key of its public key encryption scheme to thereby generate an encryption of the first party's message using the second party's public key, and (ii) obtain information that identifies at least the first party.

22. The method as described in Claim 21 further including the unordered steps of;

(g) having the trusted party send the first party, as the message receipt, some of the information the trusted party received from the second party; and

(h) having the trusted party send the second party information from which the second party can retrieve the message.

23. The method as described in Claim 20 wherein at least one of the first and second parties and the trusted party includes a physically secure device.

24. The communication method as described in Claim 20 wherein further processing by the trusted party does not occur after a specified time.

25. The communication method as described in Claim 24 wherein the specified time is included within at least communication between the first and second parties.

26. The communication method as described in Claim 24 wherein the specified time is determined by the time at which certain communications occur.

27. A communication method between a first and second party, in the presence of a plurality of trustees, enabling a transaction in which the second party receives a first value produced by the first party and unpredictable to the second party if and only if the first party receives a second value produced by the second party and unpredictable to the first party, comprising the steps of:

exchanging a first set of communications between the first and second parties without participation of any of the trustees to attempt completion of the transaction; and if the transaction is not completed using the first set of communications between the first and second parties, having a given number of the trustees take action to complete the transaction.

28. The communication method as described in Claim 27 wherein the plurality of trustees hold shares of a given secret key.

29. The communication method as described in Claim 27 wherein at least one of the first and second parties and the trusted party can encrypt messages, and at least one of the first and second parties and the trusted party can decrypt messages.

30. The communication method as described in Claim 27 wherein at least one communication of the second party is a data string generated by a process that includes having the second party digitally sign a data string computed from information received from the first party in a prior communication, wherein the data string generated by the second party is the second party's value.

31. The communication method as described in Claim 30 wherein if the second party does not get the first value in the first set of communications, the second party sends the trusted party for further processing a data string that includes at least part of the data received from the first party.

32. The communication method as described in Claim 27 wherein the trusted party takes no action to complete the transaction after a specified time.

33. The communication method as described in Claim 32 wherein the specified time is included within the first set of communications.

34. The communication method as described in Claim 32 wherein the specified time is determined by the time at which certain communications occur.

35. In a communications network wherein first and second parties desire to effect a transaction overseen by a trusted party of the network, each of the first and second parties having a value that cannot be predicted by the other of the first and second parties, and wherein the predetermined transaction is complete when the first party receives the value generated by the second party and the second party receives the value generated by the first party, a communication method comprising the steps of:

exchanging a first set of communications between the first and second parties without participation of the trusted party to attempt completion of the transaction; and

if the transaction is not completed using the first set of communications between the first and second parties, having the trusted party take action to complete the transaction.

36. In the communications network as described in Claim 35 wherein at least one of the first and second parties is a computer.

37. In the communications network as described in Claim 35 wherein the trusted party is a computer.

38. In the communications network as described in Claim 35 wherein at least one of the first and second parties is a secure device.

39. A communication method between a first and second party enabling a transaction in which the second party receives a first value produced by the first party and unpredictable to the second party if and only if the first party receives a second value produced by the second party and unpredictable to the first party, comprising the steps of:

having the first party use a key of a third party to encrypt a string from which the second party can compute the first value; and having the first, second and third parties exchange a set of communications that include the string.

40. The method as described in Claim 39 wherein the string also includes information that is selected from the group consisting of information specifying the first party, information specifying the second party, and information specifying the first and second parties.

41. The method as described in Claim 39 wherein the key of the third party is held by a plurality of trustees.

42. The method as described in Claim 39 wherein the first party comprises a plurality of entities.

43. The method as described in Claim 39 wherein the second party comprises a plurality of entities.

44. The communication method as described in Claim 39 wherein at least one of the parties takes no action to complete the transaction after a specified time.

45. The communication method as described in Claim 44 wherein the specified time is specified by at least one of the parties.

46. The communication method as described in Claim 44 wherein the specified time is determined by the time at which certain communications are received.

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/03920

A. CLASSIFICATION OF SUBJECT MATTER

IPC(6) :HO4L 9/30
US CL :380/30

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. : 380/30

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	US, A, 4,438,824 (MUELLER-SCHLOER) 27 March 1984, See entire document.	9-17, 20-26, 30, 31, 37
Y	US, A, 4,458,109 (MUELLER-SCHLOER) 03 July 1984, See entire document.	9-17, 20-26, 30, 31, 37
Y	US, A, 5,214,700 (PINKAS ET AL) 25 May 1993 See Figs. 2 and 4.	9-17, 20-26, 30, 31, 37
Y	US, A, 5,276,737 (MICALI) 04 January 1994, See Fig. 2.	9-17, 20-26, 30, 31, 37
Y	US, A, 5,315,658 (MICALI) 24 May 1994, See Fig. 2.	9-17, 20-26, 30, 31, 37

☐ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document published on or after the international filing date

"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)

"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

"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

"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

"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

"&" document member of the same patent family

Date of the actual completion of the international search

27 JUNE 1996

Date of mailing of the international search report

02 AUG 1996

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
SALVATORE CANGIALOSI

Telephone No. (703) 305-1837

Form PCT/ISA/210 (second sheet)(July 1992)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US96/03920

Box I Observations where certain claims were found unsearchable (Continuation of item 1 of first sheet)

This international report has not been established in respect of certain claims under Article 17(2)(a) for the following reasons:

1. [X] Claims Nos.: 1-8, 17-19, 27-29, 32-35, 38-46
because they relate to subject matter not required to be searched by this Authority, namely:

They disclose a method of doing business which is not embodied in any specific means.

2. [ ] Claims Nos.:
because they relate to parts of the international application that do not comply with the prescribed requirements to such an extent that no meaningful international search can be carried out, specifically:

3. [ ] Claims Nos.:
because they are dependent claims and are not drafted in accordance with the second and third sentences of Rule 6.4(a).

Box II Observations where unity of invention is lacking (Continuation of item 2 of first sheet)

This International Searching Authority found multiple inventions in this international application, as follows:

1. [ ] As all required additional search fees were timely paid by the applicant, this international search report covers all searchable claims.

2. [ ] As all searchable claims could be searched without effort justifying an additional fee, this Authority did not invite payment of any additional fee.

3. [ ] As only some of the required additional search fees were timely paid by the applicant, this international search report covers only those claims for which fees were paid, specifically claims Nos.:

4. [ ] No required additional search fees were timely paid by the applicant. Consequently, this international search report is restricted to the invention first mentioned in the claims; it is covered by claims Nos.:

Remark on Protest [ ] The additional search fees were accompanied by the applicant's protest.
[ ] No protest accompanied the payment of additional search fees.

Form PCT/ISA/210 (continuation of first sheet(1))(July 1992)*

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04L 9/32

A2

(11) International Publication Number: WO 97/24833

(43) International Publication Date: 10 July 1997 (10.07.97)

(21) International Application Number: PCT/US97/00286

(22) International Filing Date: 3 January 1997 (03.01.97)

(30) Priority Data:
60/009,577 3 January 1996 (03.01.96) US
08/604,870 22 February 1996 (22.02.96) US

(71)(72) Applicant and Inventor: MICALI, Silvio [US/US]; 459 Chestnut Hill Avenue, Brookline, MA 02146 (US).

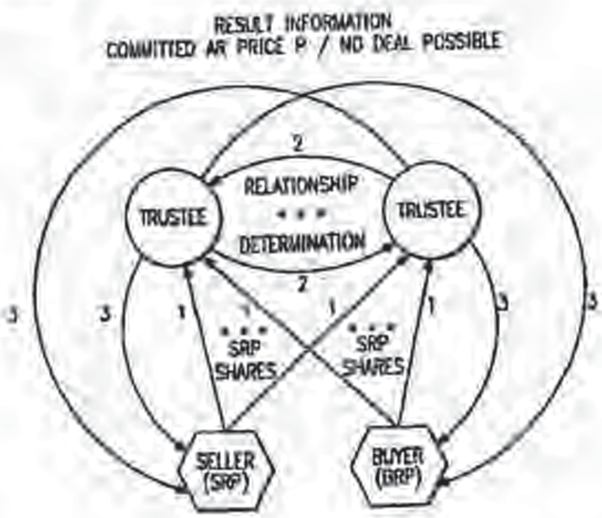
(74) Agents: MUIRHEAD, Donald, W. et al.; Foley, Hoag & Eliot L.L.P., One Post Office Square, Boston, MA 02109-2170 (US).

(81) Designated States: AL, AM, AT, AU, AZ, BB, BG, BR, BY, CA, CH, CN, CZ, DE, DK, EE, ES, FI, GB, GE, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, ARIPO patent (KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

Published
Without international search report and to be republished upon receipt of that report.

(54) Title: IDEAL ELECTRONIC NEGOTIATIONS

(57) Abstract



There is described an electronic communications method between a first party and a second party, with assistance from at least a plurality of trustees, enabling an electronic transaction in which the first party having a selling reservation price (SRP) and the second party having a buying reservation price (BRP) may be commited to a transaction if a predetermined relationship between SRP and BRP is established, but not otherwise. The method begins by having each of the parties transmit shares of their respective reserve prices to the trustees. These shares are such that less than a given number of them does not provide enough useful information for reconstructing the reserve prices while a sufficiently high number of them allows such reconstruction. The trustees then take some action to determine whether the predetermined relationship exists without reconstructing SRP and BRP. If the predetermined relationship exists, then the trustees provide information that allows a determination of the sale price according to a given formula. Otherwise, the trustees determine that no deal is possible. As used herein, "sale" is merely representative as the transaction may be of any type including, without limitation, a sale, lease, license, financing transaction, or other known or hereinafter created financial commercial or legal instrument.

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.

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

IDEAL ELECTRONIC NEGOTIATIONS

TECHNICAL FIELD

The present invention relates generally to secure electronic communications systems and more particularly to cryptographic methods that enable participants in a negotiation to agree on a common price for a given transaction without requiring either participant to reveal certain information about its bargaining position unless a suitable agreement can in fact be reached.

BACKGROUND OF THE INVENTION

In the past two decades, many secure transactions have been devised that compute quantities from certain hidden data without revealing all such data. For instance, Yao (in the Proceedings of Foundations of Computer Science Conference, 1982) presented a solution to the so-called Two-Millionaire problem that involved this approach. In this problem, two millionaires wish to know who is richer without revealing their respective monetary worth. In Yao's solution, the parties engage in cryptographic exchange, each encoding in a special manner the amount of money he/she owns. At the end of the exchange, one of the millionaires is in possession of information indicating which of the two is the richer one and can then, without proof, announce the result to the other.

In another example, Goldreich, Micali, and Widgerson presented the first of a series of cryptographic protocols for secure multi-party computation. This protocol enabled n parties (whose majority is honest), where party I has a secret input x_i, to evaluate f on their private inputs, without revealing these inputs more than absolutely necessary. At the simplest level, the parties compute y = $f(x_1,\ldots,x_n)$ without revealing more about the x_i's that is implicitly revealed by the value y itself. More sophisticated and precise definitions of this protocol were later described, for instance in the work Micali and Rogaway.

In the past, traditional physical proximity has encouraged sellers and buyers to negotiate in good faith. Physical proximity creates enough circumstantial evidence of an enforceable agreement, and also requires a considerable investment of time and effort on both sides, thus reducing the buyer's temptation of negotiating just for "curiosity" without any serious intentions of buying. Such goals, however, are more difficult to achieve where business transactions are carried out more and more at a distance (e.g., over an electronic network). Consider the example of purchasing a house over the Internet. Photographic information of a piece of property is readily available over the Internet, and digital signatures may help in signing a contract. However, in this new setting, it is possible for a seller to negotiate with many potential buyers simultaneously and at a distance so that the various buyers may not be aware of each other. The seller can then use one buyer's offer for obtaining better offers from others, even with stringent time constraints. At the same time, the new setting makes it very convenient for uncommitted buyers just to shop around for a seller's "true" price, and then possibly sell this information to others.

There remains a need in the art to provide cryptographic protocols that enable parties to negotiate and consummate business and other transactions electronically.

BRIEF SUMMARY OF THE INVENTION

It is the primary object of the present invention to describe an entirely new class of electronic cryptographic-based transactions, referred to herein as "blind negotiations."

A "blind negotiation" (sometimes referred to as an "ideal negotiation") according to the present invention is a new electronic transaction wherein a seller S and a buyer B wish to see whether they can agree on a price for a given good or service. It is assumed that the seller has a "reservation" prices, SRP, at which she is willing to sell now (not necessarily the minimum of such prices). Similarly, the buyer has a reservation price, BRP, at which he is ready to buy now (not necessarily the maximum of such price). In a blind negotiation, the current reservation price of each party is a secret of that party.

A blind negotiation is a cryptographic system that guarantees the following two properties (which are NOT readily obtainable even in a physical or face-to-face transaction):

1. *Enforceable Agreement*. Both parties reach an agreement on a price P (between SRP and BRP) whenever SRP < (or equal to) BRP, or else;
2. *Proved Privacy*. Each party is provided a proof that SRP > BRP that does not reveal the other's reservation price.

In a blind negotiation, if seller and buyer learn that no deal is possible (i.e., that SRP > BRP), then they may decide to try another round of negotiating, presumably after changing their reservation prices, or they may decide to quit negotiating. In the latter case, the seller knows that no one has learned her reservation price, and thus that she can participate in future negotiations with her "bargaining power" intact. If, instead, a deal is possible, a blind negotiation may reveal the two reservation prices. Indeed, for instance, assume that the two parties agree to "split in the middle" when a deal is possible (i.e., they adopt P = SRP+BRP/2 as the actual sale price). Then, after reaching agreement on a price P by means of a blind negotiation, each party can, knowing his own reservation price and the average of the two, easily compute the other's reservation price. Indeed, when a blind negotiation system realizes that SRP < (or equal to) BRP, then the system can just reveal SRP and BRP, so that P=SRP+BRP/2 can be easily computed.

It should be noted that in real-life, blind negotiations are not easily obtainable. In fact, if one of the parties (e.g., the seller) makes an offer to sell at a given price, then that offer already provides valuable information about SRP. A similar problem exists when the first offer is made by the buyer. As a result, in a real-life negotiation, sellers and buyers are unwilling to make first offers. This, however, is not a problem in a blind negotiation system.

It is thus an object of the present invention to provide cryptographic techniques and systems for implementing such blind negotiation schemes.

It is a further more specific object of the invention to facilitate blind negotiations using one or more trusted parties who either preferably do not learn BRP or SRP or, if they do, they cannot misuse such information. Such trusted parties may be actively involved in the negotiation or, alternatively, be required only when initial exchanges of communications between buyer and seller leaves one of the parties with uncertainty about the results of the negotiations.

The constraint that a deal is achievable if SRP < (or equal to) BRP is preferable, although other functional relationships between SRP and BRP may be implemented in the blind negotiation system. Thus any reference to the preferred constraint of SRP < (or equal to) BRP should not be taken to limit the present invention. Similarly, the constraint that the actual sale price is in-between SRP and BRP is merely preferable, but not required either.

Thus, in one embodiment, there is described an electronic communications method between a first party and a second party, with assistance from at least a plurality of trustees, enabling an electronic transaction in which the first party having a selling reservation price (SRP) and the second party having a buying reservation price (BRP) may be committed to a transaction if a predetermined relationship between SRP and BRP is established, but not otherwise. The method begins by having each of the parties transmit shares of their respective reserve prices to the trustees. These shares are such that less than a given number of them does not provide enough useful information for reconstructing the reserve prices while a sufficiently high number of them allows such reconstruction. The trustees then take some action to determine whether the predetermined relationship exists without reconstructing SRP and BRP. If the predetermined relationship exists, then the trustees provide information that allows a determination of the sale price according to a given formula. Otherwise, the trustees determine that no deal is possible. As used herein, "sale" is merely representative as the transaction may be of any type including, without limitation, a sale, lease, license, financing transaction, or other known or hereinafter created financial commercial or legal instrument.

In a modification to this embodiment, the actions are taken not only by the trustees alone, but also in conjunction with the first party and the second party.

In an alternate embodiment, the seller and buyer communicate with a single trustee, who can determine whether a deal is possible without learning SRP or BRP. In a still further embodiment, the trusted party may be a secure piece of hardware that receives an encrypted version of SRP and an encrypted version of BRP and determines whether a deal is possible and at what price.

Yet in another embodiment, the blind negotiation is achieved with "invisible" trustees. In such a case, the seller and buyer do not collaborate with any trustee initially and implement a blind negotiation system if they continue collaborating properly. However, if one of the parties stops collaborating, the other party can access one or more trustees who are capable of completing the interrupted blind negotiation.

Of course, in a blind negotiation according to the invention, the parties need not agree on a final price merely by splitting the difference between their respective reserve prices. Indeed, in a blind negotiation the two parties may agree on the actual sale price by any strategy they want. For instance, if a deal occurs in the first blind negotiation, then the parties may agree to split in the middle, but if a deal becomes possible in the next round of blind negotiation, then they may agree on the actual sale price by means of a formula that favors the party who has made the biggest "concession" in the second round. Alternatively, they may decide to favor the party who has varied his reservation price by a smaller degree in the second round, or by some such other approach.

BRIEF DESCRIPTION OF THE DRAWINGS

For a more complete understanding of the present invention and the advantages thereof, reference should now be made to the following Detailed Description taken in conjunction with the drawings in which:

FIGURE 1 illustrates a preferred embodiment of the invention wherein an electronic process having three conceptual steps (as numbered) is effected by first and second parties, with the assistance of a plurality of trustees, in order to achieve an ideal electronic negotiation.

FIGURE 2 illustrates a preferred embodiment of the invention wherein an electronic process having three conceptual steps is effected by first and second parties, with the assistance of a trustee comprising secure hardware, in order to achieve an ideal electronic negotiation.

FIGURE 3 illustrates an embodiment of the invention wherein an electronic process is effected by having first and second parties exchange messages to attempt to complete an ideal negotiation, and the use of the trusted party to complete the action if needed.

FIGURE 4 illustrates a share method embodiment of the invention, involving three numbered steps, wherein seller and buyer are players who, together with at least one other trustee-player(s), take action in determining whether a given relationship exists between SRP and BRP in order to effect the ideal negotiation.

DETAILED DESCRIPTION

Several different types of blind negotiation systems are described below. For each one of these systems there is also presented several variations and modifications. Such variations and modifications also apply to the other blind negotiation systems and not just the particular schemes with which they are described.

Blind Negotiations With Multiple Trustees/Players

In a first embodiment, an *n*-party secure computation (e.g., the protocol of Goldreich, Micali and Widgerson, or that of Ben-Or, Goldwasser and Widgerson, or that of Rabin and Ben-Or, or that of Chaum, Crèpeau and Damgärd) or a "suitable" simplification thereof is used to facilitate a blind negotiation application.

By way of brief background, it is known in the art that secure protocols enable n players (a suitable majority of which is honest) to evaluate a given function f on their private inputs, without revealing these inputs more than absolutely necessary. At the simplest level, the parties compute $y = f(x_1,\ldots,x_n)$ without revealing more about the x_i's that is implicitly revealed by the value y itself. Of course, if each player keeps his own input for himself, the privacy of the inputs x_i is perfectly maintained, but no joint computation of f can occur. Of course too, if a player reveals his input to some other player, this may facilitate some joint computation, but it may not keep the player's input as secret as it should be. Rather, in most secure computation protocols, a player I takes his own secret input x_i and constructs a secret random polynomial $P(x)$ --modulo a prime p, $p > n$, and of degree t, $1 < t < n$ --such that $P(O) = x_i$, his own input. (In other words, the player chooses the last coefficient of the polynomial to be his own input, and all other coefficients at random. If the input of a player is a binary string of at most, say, k bits, then p can be chosen not only $> n$, but also having $k + 1$ bits.)

Then, the player privately gives player a the value $P(a)$, player b the value $P(b)$ and so on. Thus, no single player (other than I), nor any collection of players with less than t members, may know the polynomial $P(x)$, nor the input x_i. However, collectively, the players (indeed any $t+1$ of the players) know $P(x)$. Indeed a t-degree polynomial may be easily obtained by interpolation from its value at $t+1$ different points. Thus, sufficiently many players can easily reconstruct $P(x)$, and thus $P(O) = x_i$, while sufficiently fewer players cannot even guess x_i better than at random.

Each player a thus (1) possesses a share, $P(a)$, of any other player's input, and (2) if the majority of the players want, the input of every player can be revealed, but (3) without the cooperation of the majority of the players, each input remains unpredictable. After sharing each input among all players in such a fashion, a typical secure computation protocol then proceeds to evaluate the given function on the player's inputs, but working on their shares, rather than on the inputs directly. For instance, if the function dictates that the inputs x_i of player i, encoded by a polynomial P (i.e., $P(O) = x_i$), should be added (mod p) to the input x_j of player j, encoded by a polynomial Q (i.e., $Q(0) = x_j$), then each player k, whose share of x_i is $i_k = P(k)$ and whose share of x_j is $j_k = Q(j)$, adds i_k and j_k mod p, thereby computing $(P+Q)(k)$, that is, a share of (x_i+x_j mod p), the sum of the two inputs mod p.

As for another example, if the function dictates that the input x_i of player i (encoded by a polynomial P) should be multiplied modulo p with the input x_j of player j (encoded by polynomial Q), then each player k, whose share of x_i is $i_k = P(k)$ and whose share of x_i is $j_k = Q(j)$, multiplies i_k and j_k modulo p, thereby computing $(PQ)(k)$, that is, a share of x_ix_j (mod p), the product of the two inputs modulo p.[1]

Though not all operations on the inputs translate into operations on the shares in a way that is as simple as in the case of the "addition mod p" operation or of a (single) multiplication modulo p, at the end of the secure computation the players have each his own share of $y=f(x_1,\ldots,X_n)$, that is, each player k has the value $F(k)$, where F is a t-degree polynomial such that $F(O) = y$. Thus all players may release their shares, so as to allow the reconstruction of F by polynomial interpolation, and thus the reconstruction of y without releasing any unwanted information about the inputs x_i's. This reconstruction also works in a simple way (provided that there are sufficiently many honest players) even though some players may be bad and release incorrect shares. This is just the basic background

[1] Note that the product polynomial PQ has degree $2t$, and thus one needs $2t$ points for interpolating it. Therefore, there must by sufficiently many honest players. If one had to execute a chain of several multiplications -- e.g., $((P+Q)QQ+Q)P$--by means of the above method, then the number of honest players needed would become totally impractical. Thus, different (degree-reduction) methods have been devised in the literature. The above method, however, is quite practical if one only needs to compute a single product mod p.

on multi-party secure computations. The reader is directed to the art references for further details.

With this background, it can now be described how one such secure computation protocol is used to facilitate a blind negotiation.

A First Share-Method

As noted above, as indicated in FIGURE 1, a secure-computation protocol assumes that there are n parties, the majority of which are honest. In a blind negotiation there are two parties, the seller and the buyer. It cannot be assumed that both parties are honest, however. Thus, in this embodiment seller and buyer cooperate with one or more *trustees*. These are additional parties that are assumed to be trustworthy (in particular, trusted to follow the prescribed instructions of a secure computation protocol). By means of a system such as described below, the trustees enable seller and buyer to complete their negotiation in a blind way. It is desired, however, that the trustees should not receive much information, nor should they be able to misuse whatever information they do receive.

The following blind negotiation system further makes use of *digital signatures*. In a digital signature scheme, each party X has a secret signing key S_x and a matching public verification key P_x. Party X may obtain its digital signature of a message (string) m, $SIG_x(m)$, by running an algorithm SIG on inputs S_x and m (thus, $SIG_x(m) = SIG(S_x,m)$). The signature of party X on a message m is verified by running a verifying algorithm VER on the signature and X's public key.

The following now describes how to use a multi-party secure computation protocols for building a blind negotiation systems with trustees and digital signatures. For instance, a secure computation with $n=3$ exists by asking one trustee to join the computation. Thus, if either the seller or the buyer is honest, since a trustee is presumably selected with trustworthiness as a prerequisite, an honest majority exists. If desired, larger values of n may be chosen in a secure computation protocol, with the cooperation of more trustees. This way, even if one or more trustees turn out to be malicious, the majority of all players are honest.

Assume now that there are sufficiently many trustees, so that there is a total number of $n > 2$ players, a suitable majority of which are honest. Without loss of generality, the seller is player 1, the buyer player 2, and the trustees players 3,...,*n*. Then, *n* players are used to perform a particular *n*-party secure computation, for an especially selected function *f*, and for especially selected inputs.

Let (S_1,SRP) be the input of player 1, (S_2,BRP) be the input of player 2 and ϵ the input for any other player, where S1 is the secret signing key of the seller, SRP the reserve price of the seller, S2 the secret signing key of the buyer, BRP the reserve price of the buyer, and E; the empty string. Further, let *f* be the function such that $f((S_1,SRP), (S_2,BRP), \epsilon,\ldots,\epsilon) =$

$$(SIG(S_1,(T,SRP+BRP/2)),\ \ SIG(S_2,(T,SRP+BRP/2)))\quad if$$

$SRP \leq BRP$,

and "NO DEAL" otherwise. Here *T* is any string describing the transaction in any sufficient way. For instance, *T* may consist of identifying the seller and the buyer, the negotiated commodity, and/or additional data, such as time data, or an indication of the trustees.

Thus, function *f* outputs a certified commitment for the seller and buyer to trade, at a meet-in-the-middle price, whenever the deal is possible, i.e., whenever *SRP< (or equal to) BRP*. (Of course, within *f*, one could replace *SRP+BRP/2* with any strategy, *g(SRP,BRP)*, to determine the actual trade price.) Therefore, the function *f* only depends on the inputs of seller and buyer, and not on the inputs of the trustees (these could be any value rather than ϵ, because *f* may ignore them anyway).

The above is a "blind negotiation" system because both seller and buyer end up with a signed contract with the right price whenever a deal is possible between them; otherwise they end up with a proof that no deal is possible, but which does not reveal what the two reservation prices may be. In case a deal were possible, preferably the contract is signed by both of them digitally. Indeed, in this case the output of the secure computation is the signature of the buyer and the seller that the transaction T has resulted in a sale at a given *Price*. Thus, the above system satisfies the Enforceable Agreement property. Indeed, whenever SRP is greater to or equal to BRP, seller and buyer end up with a binding contract at an agreed price determined by a given formula.

In case a deal were not possible, then the result of the secure computation is NO DEAL, and this is a proof that SRP > BRP (because of the way the function f is defined, because an honest majority exists among the selected players so that f is correctly computed, and because the result of the computation has been produced by the trustees and can be thus "witnessed by them" if necessary). An alternative proof that no deal is possible can be obtained by modifying the function f so that $SIG_S(T, NO\ DEAL)$ and $SIG_B(T, NO\ DEAL)$ is output instead of just NO DEAL (where the subscript S stands for seller and B for buyer). Either way, the reconstruction of NO DEAL does not reveal what the specific values of SRP and BRP may be, save for the fact that SRP > BRP. Indeed, in a secure computation of a function, only the result of the function evaluation is made known, but not the function's inputs. Thus, if a given computation of f results in outputting NO DEAL, then this output reveals that SRP is greater than BRP but not the specific values thereof. Thus, any other information about SRP, BRP and the seller's and buyer's secret signing key is kept totally secret. The above system thus also satisfies the Proved Privacy property.

A Second Share-Method

The above method, however, may be enhanced by having seller's and buyer's signatures computed outside the share computation phase. Before engaging in any secure computation, buyer and seller sign (preferably digitally) an initial agreement of the kind "in this transaction T, with trustees $T_1, T_2, \ldots$, seller S and buyer B agree to trade commodity C at the average of their reserve prices, if their secure computation of function f is YES." Then, seller, buyer and trustees securely evaluate f on inputs $(SRP, BRP, \epsilon, \ldots, \epsilon)$, making sure that this computation is bound to identifier T. Here, f is the function such that $f(SRP, BRP, \epsilon, \ldots, \epsilon) = YES$ if $SRP \leq BRP$, and NO otherwise. Thus, if the result is YES, the players retrieve SRP and BRP from their shares (alternatively, f may output (SRP, BRP) rather than YES), and seller and buyer can then easily both sign $(T, SRP+BRP/2)$. If one of them refuses to do so despite the result of the computation, then the honest trustees may sign in his or her place, and the signatures of a suitable majority of the trustees may be considered equally binding. If the share computation phase indicates that no deal is possible, then seller and buyer will each sign (T, NO), or the trustees will do it on their behalf. (Notice that it is not important who signs an initial agreement first. Indeed, only after both seller and buyer have signed it will a secure computation of f follow or be completed.)

Of course, many variants of this basic method can be implemented. For instance, different types of initial agreements may be stipulated. Also, in any of the blind negotiation systems, seller and buyer may not participate in as players in the secure computation phase. The players of this phase can just be trustees (so that it is easier to have a suitable honest majority). Thus, each of seller or buyer may just give each trustee his or her proper share of the input, and then the entire computation will be carried over the shares by the trustees, until the final result is produced and handed out to both seller and buyer. Also, the trustees (or seller and buyer) may just sign NO or nothing at all, rather than signing *(T,NO)*. As for *T*, it is preferable that it provides a unique identifier of the current negotiation. For instance, T may include some of S, B, the current date and time, a description of the commodity on sale, as well as encryptions of SRP or BRP, or an indication of the trustees, or a random identifier.

A Third Share-Method

The first alternative embodiment, wherein digital signatures are carried out outside the share computation phase, may also be enhanced. Indeed, a typical secure computation protocol succeeds in securely evaluating a given function by means of securely computing some primitive functions, for instance, modular addition and modular multiplication.

Accordingly, rather than directly applying some ready-made secure computation protocols in the secure computation phase of the inventive blind negotiation protocols, it may preferable to write a new *ad hoc* protocol for this purpose that uses the above primitives in an elementary way. One such protocol is now described.

The new protocol uses as a primitive the share computation of $(a-b)r$ mod p, where a, b, and r are secret values in the multiplicative group mod p, and p is preferably a prime (in which case a, b, and r are between 1 and p-1). In this application, a and b may be specific values (e.g., the private inputs of specific players), while r is a random value, possibly chosen during the computation itself, and it may not belong to any particular player. For instance, r may be chosen as the sum mod p of several random secret values r_i's belonging to different players.[3]

One advantage of the $(a-b)r$ primitive is that its share computation is readily implemented. Indeed, the share computation of a single addition/subtraction and a single multiplication modulo p of secret values (such as a, b and r) is particularly easy to obtain.

A second advantage of the $(a-b)r$ primitive is that it can be used to test whether two given secret inputs a and b are equal without releasing any additional information. In fact, if $a=b$, then $(ab)r=0$ no matter what the actual value of a, b and r may be. Alternatively, if $a \neq b$, $(a-b)$ is a fixed non-zero number. Thus, multiplying modulo p this fixed number by a number r between 1 and p-1, yields a number modulo p different from zero. Moreover, because r is random, this product modulo p is a random number between 1 and p-1, and thus cannot betray what the precise values are of a and b.

These advantages make the $(a-b)r$ primitive especially suitable for constructing a practical and general type of blind negotiation. In particular, assume that the seller's and buyer's reserve prices are in the interval $[M,N]$. That is, M and N are, respectively, agreed (or obvious) lower- and upper-bounds to both SRP and BRP in some given currency. That is, each value between M and N is interpreted as a possible price in dollars, or tens of dollars, or thousands of dollars. (Such M and N can be easily made part of the description, T, of a given negotiation.)

In a particular example, the seller is a car dealer. Buyer and seller are "blindly" negotiating over a new compact car (of a given brand, type, and color) over the Internet. Although dealers should welcome offers from customers outside their own trade area, traditionally they do not like negotiations at a distance because they reveal their reserve prices to someone who may not be serious about any offer discussed (and who may just live a few blocks away). In such a setting,

---

[3] If r is chosen this way, while each r_i may be between 1 and p-1, their sum mod p may be 0. However, if p is suitably large (e.g., 50- or 100-bit long) the probability that the resulting r is 0 when at least one r_i is secretly and randomly chosen, is quite negligible. Thus, from a practical point of view r can be chosen in this matter if desired.

if the players choose thousands of dollars as their currency, they may set $M = 4$ and $N = 40$. (That is, if it is assumed that the car is going to be sold the price will be between $4,000 and $40,000). Alternatively, they may choose $500 or $250 as their basic currency, in which case they may set, respectively, $M = 8$ and $NN = 80$, or $M = 16$ and $N = 160$.

For each price i between M and N, the seller chooses a value S_i as follows. If $i < SRP$, then the seller chooses S_i at random between 1 and p-1 (each such random value is chosen independently from all other such values); else, she sets $S_i = 0$. (Thus, $S_i = 0$ only if price i is acceptable to her.) Symmetrically, for each $I \leq BRP$, the buyer sets $B_i = 0$, and, for each $i > BRP$, he chooses B_i at random between 1 and p-1. (Thus, $B_i = 0$ only if price i is acceptable to him). Then, in the presence of trustees a secure computation of the new primitive is executed for each $i = [M,N]$. That is, for each $i = [M,N]$ the value $(S_i - B_i)R_i$ is computed (without revealing any additional information about S_i and B_i), where each R_i is independently and randomly selected between 1 and p-1. If one of these computations returns a 0, then the deal is possible and agreement if forced. However, if no 0 is obtained, then no agreement is possible and seller and buyer may decide to negotiate again or quit. (Preferably, they had signed an initial agreement prior to executing this procedure indicating their intentions, currency, names, time, etc., and what happens in case of a positive outcome, i.e., in case for some price I the computation of $(S_i - B_i)R_i$ yields zero. This initial agreement can be produced in a standardized manner so as to be more convenient and quite compact.)

How this scheme works can now be explained. Assume first that $SRP \leq BRP$. Then, secure computation of $(S_i - B_i)R_i$ is analyzed in three cases: (1) when $i < SRP \leq BRP$, (2) when $SRP \leq i \leq BRP$, and (3) when $SRP \leq BRP < i$. In Case 1, the secure computation of $(S_i - B_i)R_i$ will return a non-zero random number. Indeed, for each such value of i, $B_i = 0$, thus $(S_i - B_i)R_i$ equals just the product mod p of S_i and R_i. Since each of these numbers is different than 0, so will be their product mod p. (Moreover, this product will be a random number between 1 and P-1 because R_i is random.) In Case 2, $S_i = B_i = 0$. Thus $(S_i - B_i)R_i = 0$ for any possible value of R_i. In Case 3, $S_i = 0$. Thus, the secure computation returns the product mod p of B_i and R_i. Since each of these values is different than 0, so is their product mod p. (Moreover their product will be a random value between 1 and p-1 because so is R_i.).

Assume now that $BRP < SRP$. Again, there are three cases to analyze in the secure computation of $(S_i-B_i)R_i$: (1) $i<BRP<SRP$, (2) $BRP \leq i \leq SRP$, and (3) $BRP \leq SRP < i$. In all three cases, however, what is returned is a random number between 1 and p-1, *independent of what specific values SRP and BRP may have*. Thus, such a result, while proving that no deal is possible (i.e., that $SRP > BRP$), does not reveal any other detail about the specific values of *SRP* and *BRP*.

Therefore, the new primitive shows only the prices i for which both the seller and buyer entered 0 (i.e., all and only those prices at which they are both willing to trade), and thus a sale is possible. Thus, if even a single 0 occurs as the result of the share computation relative to some price i, thanks to their initial agreement, seller and buyer end up with an enforceable agreement to trade at a given price P.

There are several ways to compute price p. For instance if *min* is the minimum value of i for which 0 was returned and *max* the maximum value of i for which a 0 was returned, the initial agreement and the result of the secure computation (as properly witnessed or signed by a suitable number of the players) may be taken to constitute a signed contract to trade the given commodity at price $min + max/2$.

Notice that either the seller or the buyer may enter 0 for some values of i without entering 0 from that point on (i.e., for all values higher than i in the seller's case, and for all values lower than i in the buyer's case).[3] This may indicate that the seller (buyer) is willing to sell (buy) at certain prices only, and not, for whatever reason, at all prices higher (lesser) than a given one. The system may recognize this behavior as legitimate (e.g., the final price may be chosen to coincide with a value i, $min \leq i \leq max$, properly selected among those for which 0 was returned --e.g., $i=min$, or $i=max$, or, preferably as equidistant as possible from *min* and *max*, with a way to break ties). If it is desired to disincentivize this behavior, however, whenever two or more 0's are returned but

---

[3] For instance, the seller may just enter 0 for the single value of i, strictly less than N and strictly greater than M.

the returned 0's do not constitute a contiguous sub-segment of *[M,N]*, all values S_i and B_i relative to any position between the first 0 and the last 0 are recovered (e.g., from the shares in possession of sufficiently many trustees for secure computation purposes), and if the buyer has put 0 consistently in these positions, then some proper action may be taken. For instance, the seller is obliged to sell at a punishingly cheap price (and a punishingly high price for the buyer). If both the seller and buyer have not put their own 0's in a consistent way, then some proper action may be taken. For instance, the trade price will be decided in some other way, or both will be fined.

Although not meant to be limiting, many of the above computations can be effected in secure hardware by persons using such hardware or other known machines including computers. In addition, although the various methods described are conveniently implemented in a general purpose computer selectively activated or reconfigured by software, one of ordinary skill in the art would also recognize that all methods of the present invention may be carried out in hardware, in software, or in more specialized apparatus constructed to perform the required method steps.

Share-Methods with Players

In a modification of the above embodiment, any of our share-methods for blind negotiations can be implemented so that computing actions are taken by the trustee together with players one and two. This yields a share-based blind negotiation system with a plurality of players, where a player may be the first party, a second party or a trustee. In such modifications, one of the two parties may give a share of his reservation price to the other party. Of course, the two parties have enough information to reconstruct both their own reservation prices but, like in the above share-method, any suitably-small subset that does not include both parties does not possess enough information to construct the reservation price of the (missing) party.

Single-Trustee Blind-Negotiation Systems

It may be preferred that a blind negotiation system use only a single trustee in that it be further simplified. One way of achieving this would be to have the seller tell the trustee her own secret value SRP, and have the buyer tell the trustee his own secret BRP, so that the trustee can announce whether a deal is possible, and at what price, without revealing additional information about SRP and BRP. The trustee, however, then learns both SRP and BRP. Even if he may be trusted to keep the received SRP and BRP confidential, he will nonetheless have learned these values, and this may not be acceptable.[4]

It is therefore preferred to implement a blind-negotiation system with just one trustee possessing the following attractive properties: (1) seller and buyer perform their own computations and then they transmit to the trustee some proper piece of information, which the trustee then further processes to conclude the negotiation; and (2) the trustee does not learn any thing about SRP and BRP (except for learning whether a deal has occurred). Thus, such a system has an elementary and convenient interaction among all parties, and yet does not give the trustee the values of SRP and BRP.

To illustrate this system, it is useful to provide a brief background about the known cryptographic notion of a trap-door permutation. This is a function that is computationally easy to evaluate but overwhelmingly hard to invert unless a special secret is known about the function. Thus, any one can, given x in the range of f, compute $f(x)$. However, only he who knows f's secret can feasibly retrieve x from $f(x)$.

The best known (and essentially the only known) examples of trap-door permutations are based on factoring and modular exponentiation. For instance, consider the RSA function. Let n be the product of two large (e.g., 500-bits), secret, and random primes p and q, $n = pq$. Because selecting such primes p and q is easy, and so is multiplying them, one can easily construct such an n. However, since no fast algorithm for factoring is known, finding the prime factorization of such an n will be hard for everyone else. Thus, the prime factorization of n is a secret relative to n. Let us now see how this secret can be used to invert easily the RSA function.

[4] For instance, assume that, after trusting the trustee to this extreme extent, it turned out that no deal was possible between seller and buyer because $SRP > BRP$. Then the seller should be able to negotiate with others the sale of the same commodity, keeping intact her bargaining power. However, the trustee himself would not be able to negotiate blindly with the seller!

The RSA is a permutation over Z^*_n, the multiplicative group mod n obtained as follows. Let e (for exponent) be relatively prime with $(p-1)(q-1)$, and set $f(x)=X^e$ mod n. Then, $f(x)$ is feasibly evaluated. Indeed, if x, the modulus, and the exponent all are at most k-bit long (e.g., 1,000-bit long), then a modular exponentiation can be computed (by the repeated squaring method) with roughly 1,500 modular multiplications without any need to know n's factorization. Moreover, such a $f(x)$ is a permutation. Indeed, it can be inverted as follows: let d be the multiplicative inverse of e mod $(p-1)(q-1)$; that is, ed mod $(p-1)(q-1)=1$. Then, (always operating mod n, and thus mod $(p-1)(q-1)$ at the exponent) we have $(X^e)^d = e^{ed} = x$; that is, the function X^d mod n is the inverse RSA function (with exponent e), x^d mod $n = s^{-1}(x)$.

This proof not only shows that x^e mod n is an invertible function (independently of how much time inverting it may take), but also that it is a trap-door function. Indeed, he who knows p and q, and thus $(p-1)(q-1)$, can easily compute d and thus easily invert the RSA function.[5]

The inventive system makes use of such a trap-door function $f(x)=x^e$ mod n. While the buyer knows n and e (e.g., because the seller gives them to him, or because they are publicly known), preferably only the seller knows n's factorization, (p,q), or, equivalently, d, the multiplicative inverse of e mod $(p-1)(q-1)$.

The system also makes use of preferably a one-way (possibly collision-free hashing) function H. Thus, while it is easy, given x, to compute $y=H(x)$, it is practically impossible, given y, to compute an x such that $H(x) = y$. (In this setting it is not necessary that H be a trap-door permutation. Indeed, it is preferable that H is not trap-door, and that it is a totally different function all together, and not a RSA-like).

Let now M and N, respectively, be lower- and upper-bounds

---

[5] The RSA function can be defined more generally - e.g., for any composite number n and any exponent e relatively prime with $\phi(n)$, where ϕ is Euler's totient function. This more general functions may too be used within our inventive blind-negotiation system. Similarly, one could use Rabin-like trap-door functions, or other function, if so wanted.

for the reserve prices of seller and buyer, and let i be the actual SRP and j the actual BRP (thus, $M \leq i, j \leq N$). The new blind-negotiation system is preferably implemented by means of three steps: a buyer's step, a seller's step, and a trustee's step. Each transmission in the system preferably occurs in a private manner; for instance by encrypting it with a key shared with or owned by the recipient to ensure that no clear text message falls in the wrong hands.

In the buyer's step, the buyer B selects, preferably at random, secret x mod n. Then, he evaluates f, on input x, N-M times, so as to obtain the following sequence of values (presented in reverse order):

$$Z_o = f^{n-m}(x), Z_1 = f^{n-m-1}(x), \ldots, Z_{n-m} = f^0(x) = x.$$

(I.e., Z_1 is the first f-inverse of Z_o, Z_2 is the second f-inverse of Z_o, and so on.) Because his BRP is j, the buyer then computes $H(Z_j)$, and sends this value to the trustee, preferably (digitally) signed together with additional information.[6] To the seller, the buyer instead gives Z_o, preferably signed together with additional information.

In the seller's step, the seller given her knowledge of f's secret information - e.g., n's factorization) may easily compute all the first N-M inverses of Z_o. However, because her SRP is i, she evaluates the one-way function H on the first i such inverses, and then evaluates H on another N-M-i values V_k, each preferably distinct from any of the first N-M f-inverses of Z_o. Thus, she gives the trustee the resulting sequence of N-M values, preferably in random order:

$$H(Z_1), H(Z_2), \ldots, H(Z_i), H(V_1), \ldots, H(V_{N-M-i}).^7$$

In the trustee step, the trustee preferably makes sure (e.g., by using the additional information), that the seller's list and the buyer's value relate to the

---

[6] Such additional information preferably describes the transaction and is taken to be a proof of the buyer's willingness of entering it. For instance, the additional information may include any of the following data: seller's information, buyer's information, transaction information, good-on-sale information, time information, Z_o, any other information, or no information.

[7] The seller may just compute the first i inverses of Z_o *AND* choose the V_k VALUES at random, if the probability that one of these values V_k EQUALS ONE OF THE FIRST N - M INVERSES OF Z_o IS SMALL. Computing all such inverses is desirable, as will be seen.

same negotiation. The trustee checks whether one of the *N-M* values received from the seller equals the value received from the buyer. If so, it announces that a deal is possible; otherwise, it announces that no deal is possible. This announcement is preferably signed by the trustee together with additional information, and sent to both seller and buyer. In case the deal is possible, the dealer preferably includes in his announcement the value of the buyer, $H(Z_j)$, together with the buyer's signature of it, and the seller's list, together with the seller's signature of it.

This scheme works for the following reasons. First, it should be noticed that the trustee does not learn *j* (i.e., the BRP) from the information it receives from the buyer. Indeed, although given Z_o (i.e., within the additional information) the trustee does not know how to invert the RSA function *f*, and thus does not know any of the *N-M* inverses of Z_o. Of course, the trustee could, given Z_j, easily verify that this is the *j*th inverse of Z_o. Indeed, the trustee could evaluate *f* on input Z_j by the buyer, but $H(Z_j)$ should, from a practical point of view, be equivalent to having nothing at all about Z_j. Thus, the trustee has a very hard time determining *j* may be from the buyer's information.

Similarly, the trustee cannot easily learn the value of *i* from the information obtained from the seller. Indeed, the trustee receives from the seller *N-M* items altogether; *i* items obtained by evaluating *H* at inputs that are the first *f*-inverses of Z_o and *N-M* items obtained by evaluating *H* at inputs that are not such *f*-inverses. However, the one-way function H makes it difficult for the trustee to decide whether an individual item is of the first of second type; thus, the trustee cannot count how many type-1 items are there. Indeed, *H* is chosen so that the trustee cannot practically distinguish between a value obtained by evaluating *H* at a *f*-inverse, and one obtained by evaluating *H* at some different input.[8]

[8] Rather than obtaining type-2 values by evaluating *H* at inputs V_k that are not the first *f*-inverses of Z_o, the seller could choose her type-2 values in some other manner (e.g., by choosing *N-M-i* values U_k - of the proper length - at random, because the probability that these chose values happen to be of type 1 is negligible), provided that such values are not easily distinguishable from type-1 values.

Finally, it should be appreciated that, except for the fact of whether or not $i > j$, the trustee may not practically learn anything more about i and j from taking into consideration both the information received from the seller and that received from the buyer.

Indeed, assume first that there is no possible deal (i.e., that $i > j$). Then, the only additional information that the trustee gets from the seller's list and buyer's value taken together is that the buyer's value does not occur in the seller's list. But this does not help the trustee retrieve the precise values of i and j at all.

Assume now that a deal is possible (i.e., that $i \leq j$). Then, the trustee sees that the buyer's value, $H(Z_j)$, is an item in that seller's list, and therefore learns that $H(Z_j)$ has been obtained by evaluating H at one of the first $N - M$ f-inverses of Z_i. However, if the seller's list is presented in random order, the trustee still cannot figure out what the value of j may be, nor the value of i.

In sum, therefore, the single trustee, doing only local and trivial computation, learns whether a deal is possible, but never the values of the reserve

---

Notice also, that one can, within the scope of the invention, use functions H that are not one-way, but more care is needed. For instance, one can choose $H(x)$ to consist of the last - say - 50 bits of x. Now 50 bits of Z_i may not be enough for reconstructing Z_i. This is not so because taking the last 50 bits is a one-way function, but because 50 bits of crisply-clear information about x are just too few to reconstruct a secret long value x, even if $f(Z_i)$, where f is a trap-door or one-way function, is known. Also, the last 50-bits of the RSA inverses (as evidenced by the results of Alexi et al.) may be unpredictable and thus quite random looking. Thus, it would still be hard to distinguish between the last 50 bits of the RSA inverses (the type-1 values) and 50-bit random values (the type-2 values). However, one has to be careful in constructing the blind-negotiation system so that the buyer cannot misuse the system to invert the RSA. Indeed, it is also shown by Goldwasser et al. and Alexi et al. that given an oracle for guessing the last 50 bits of several RSA inverses, one may discover the full RSA inverse on an input of interest. Now, while in general no such oracle is available, the seller herself may, through the mechanism of the blind-negotiation system, provide such an oracle. Indeed, she is called by the system to provide the last 50 bits of several RSA inverses. However, if H is a proper one-way function, such cryptanalitic attacks will become essentially impossible, and the seller may release H evaluated at any RSA inverse without fear.

prices.* The trustee, however, enables the seller and buyer to learn each other's reserve prices - so that they can both, for instance, compute $i + j/2$.

Consider first the seller's situation. Indeed, if the trustee gives the seller the buyer's value $H(z_j)$, she easily learns j, because she knows the value of every single f-inverse of Z_o, and thus can check which inverse, after evaluating H on it, yields the buyer's value. Further, if the buyer's value is given by the trustee to the seller with the buyer's signature, then the seller receives *a proof* of what j is, and thus a proof that he was willing to buy at price j. Similarly, by receiving the seller-signed seller's list, the buyer receives a proof that she was willing to sell at price i. (In fact, the buyer knows at least the first j f-inverses of Z_o, and thus (because $j > i$ when the deal is possible), he can check and prove that the seller's list contains the first f-inverses of Z_o.). These proofs, preferably together with other evidence (e.g., a proper initial agreement between seller and buyer – preferably including Z_o together and with other additional information), can be used to prove in court that $i + j/2$ is the agreed trade price resulting from the negotiation.

The above blind-negotiation system is quite convenient from an interaction point of view (because the parties perform mostly local computations and do not talk back and forth too much). It is also computationally attractive.

Running Time Analysis

The above blind-negotiation system requires little computation because the trustee essentially just checks equality (between the buyer's value and the items of the seller's list). The buyer at most evaluates the trap-door function f and the one-way function H in the forward direction $N - M$ times. This is particularly easy to do. First, H is preferably a non-number theoretic function and plenty of very fast

* In case a deal is possible, however, and the actual trade price is chosen to be $i + j/2$, protecting the secrecy of i and j from the trustee may be deemed to be less crucial. (Indeed, in this case each of the seller and buyer may, from knowledge of his own reserve price and knowledge of the average of their reserve prices, learn readily the other's reserve price.) If this is case, the seller may actually send her list to the trustee in order rather than randomly permuted. This still does not enable the trustee to learn anything additional if no deal is possible, but lets the trustee learn the value of j if the deal is possible. He can in fact easily see that the buyer's value is the jth item in the seller's list.

non-number theoretic functions are known. Second, the exponent e of the RSA function f can be chosen quite small (e.g., equal to 3, if 3 is relatively prime with $p - 1$ and $q - 1$ -and indeed, p and q can be chosen so that this is the case). Thus, rather than requiring a full modular exponentiation, (and thus 1.5k modular multiplications when n, e and x are k-bit long), an RSA evaluation (e.g., a computation of $f(x) = x^e \bmod n$) may require as little as two modular multiplications, and the buyer makes at most $N - M$ such evaluations, and thus at most $2(N - M)$ modular multiplications overall. Moreover, the seller appears instead to perform $N - M$ f-inversions, and thus $N - M$ modular exponentiations, each requiring roughly 1.5k modular multiplications. (Indeed, each such inversion consists of a computation of the type $x^d \bmod n$, where d is the multiplicative inverse of $e \bmod (p-1)(q-1)$; thus, even if e is chosen to be quite short, d may not be short at all.) However, the seller's computation of all required inverses may be accomplished by means of just one modular exponentiation and $N - M$ f-evaluations (each involving two modular multiplications if $e = 3$). Indeed, computing Z_{N-M} requires that the seller inverts f, on input Z_o, $N - M$ times. But this means to compute $(Z^d_0)_{N-M} = Z^d_0{}^{(N-M)} \bmod n$. But because in such a computation the exponents work modulo $(p - 1)(q - 1)$, in effect the seller must compute $x^{d'} \bmod n$, where $d' = d(N - M) \bmod (p - 1)(q - 1)$. Thus the seller may compute d' (which is thus less than $(p - 1)(q - 1)$, and thus less than n, and thus at most k-bit long) with a single modular multiplication, and then $x^{d'} \bmod n$ with just a single modular exponentiation. After she has computed Z_{N-M}, the seller computes all other $N - M - 1$ f-inverses of Z_o by simply evaluating f, on Z_{N-M}, $N - M$ times, and each evaluation requires at most two modular multiplications if e is chosen equal to 3.

It should be noticed also that the value $N - M$ may be quite small. Indeed, in the above blind-negotiations for sale of an automobile, the envisaged values of $N - M$ were, respectively, 36, 72 and 144. Of course, if 144 is an upperbound to the possible reserve prices, so is 1,000. But, independent of other considerations, seller and buyer may have a valid incentive in ensuring that $N - M$ is small. In particular, the trustee of a blind-negotiation (whether of this or another type with lower-and upper-bounds) may actually require payment for his services according to the monetary value of the transaction. Now this value may become clear when a deal occurs, but, because of the very nature of a blind negotiation it will not be revealed otherwise. It is thus desirable that the trustee be paid as a percentage of N or $N - M$, whether or not a deal occurs. It is thus in the interest of seller and buyer that N and $N - M$ be small.

Enhancing Security

The above-described system has been described in the context of a single given blind negotiation. It should be realized, however, that an enemy may also consider attacks that occur outside a single negotiation, possibly setting up a new blind negotiation in order to discover something about an old one. It is thus recommended, in this and other blind negotiation systems as well, that each portion of a negotiation cannot be used in any other negotiation. Thus, if each individual negotiation is secure, all possible negotiations taken together will be secure as well. For instance, it is quite beneficial that the additional information be used so that it fully specifies the negotiation in question, and, if something wrong appears in such specification, then proper security measures can be taken.

For example, it is desirable that messages exchanged within a blind negotiation be *customized*. For instance, the seller first signs the value she sends to the trustee, and then encrypts this signed message with the trustee's key (and not the other way around - though still in the scope of the invention). This way, after the trustee decrypts, he can check that the cleartext message came from the seller (and it is to her - and to the buyer - that he will send his announcement of the outcome of the negotiation, preferably encrypted with her key). This is a practical way to customize messages; that is, to tie messages to their senders so that, in particular, no one else can take the same message and (possibly without *understanding* it) send it as his.

The value of customization can be seen by analyzing what may happen if it is not used. For instance (ignoring additional information and most other details), assume that a seller S gives her list L to the trustee after encrypting it with the trustee's key, and then signing the so obtained ciphertext. That is, assume that she sends $y = SIG_S(E_T(L))$, her own signature of the piece of data $x = E_T(L)$. Assume now that a malicious buyer B has blindly negotiated with S, and that the result announced by the trustee was that no deal was possible. Then, B should learn no more than the fact that the seller's reserve price was bigger than his own one. However, by means of some "outside attacks" he can exactly reconstruct the seller's reserve price as follows.

When S sends y to the trustee, B makes a copy of it (without preventing it from reaching the trustee, and without understanding what he is copying). Then, he strips out S's signature (thus obtaining an unsigned string $x = E_T(L)$ which he cannot understand) and substitutes it with the signature of an accomplice of his, C, thus obtaining the string $y' = SIG_C(E_T(L))$. Then, he pretends that he is blindly negotiating with C several times. Each time he uses the same Z_ω and has C send the trustee the string y'. As for his own messages, the first time he pretends that his reserve price is M (thus he sends the trustee a properly signed and encrypted $H(Z_1)$); the second time he pretends that his reserve price is $M + 1$ (thus he sends the trustee $H(Z_2)$; and so on, until, the kth time, the trustee reports that there is a deal. Thus, B learns that the seller's reserve price was $M + k$.

Notice that each time the trustee notifies B and his accomplice C of the outcome of the negotiation, since, without a proper customization of the messages, he believes that B and C are the parties of these negotiations. (Of course, even if the kth time, the commodity is declared as been sold by C to B, C will ignore such sale. Indeed, C does not own the commodity at hand.) In the mean time, poor S is not even aware that this is going on.

Customizing messages neutralizes this attack. For instance, assume that even a mild form of customization is used, where the seller sends the trustee $y = SIG_S(E_T(L,AI))$, where the additional information AI specifies that the seller is S, the buyer B, and the trustee T. Then, copying y, stripping S's signature, and substituting it with that of accomplice C, and having C send T the string $SIG_C(E_T(L,AI)$ does not help much. In fact, after verifying the signature of C and removing his own encryption layer, the trustee will realize that the additional information identifies S to be the seller and not C. Thus he can take proper measures; for instance, stop the negotiation and alert S of what is going on.

Notice that if S adopts the above customization and the encryption system E_T is properly designed, it would be essentially impossible for B to take the data $x = E_T(L,AI)$ and somehow transform it into another piece of data $x' = E_T(L,AI')$ that happens to be the encryption, with the trustee's key, of the same list L plus additional information AI' indicating that C, rather than S, is the seller. Similar difficulties would be encountered by the above attack if the customization is a bit different; for instance, if the sender communicates her list to the trustee by sending $E_T(SIG_S(L,AI))$, or $SIG_S(E_T(SIG_S((L,AI)))$.

A malicious buyer may steal, however, use the same customized message M_s (whether $M_s = E_T(L,AI)$, or $E_T SIG_S(L,AI))$, or $SIG_S(E_T(SIG_S((L,AI)))$, or another value), and mount the above attack by keeping on sending M_s to the trustee as if coming from the seller, each time pretending that there is a blind negotiation going on. At each such negotiation, he sends a different buyer's value, and possibly tries to prevent that the trustee's announcement reach the genuine seller, so as to keep her in the dark about the attack.

These types of attack can be prevented by inserting in the additional information some time information. For instance, the seller may specify what is the current date and time, in her communication to the trustee. If the trustee when receiving the information notices that the time is sufficiently old may take some proper actions (including, possibly, stop the negotiation and alerting its parties that something is wrong).

A resourceful malicious buyer, however, may do the following. When the seller in a negotiation with him sends the trustee a customized message M_s (e.g., $M_s = SIG_S(E_T(SIG_S(L,AI))))$ that indicates who are seller and buyer as well as what is the time of the transmission, he may copy M_s, and then send it to many different trustees: T_1, T_2, etc. He then behaves as if Trustee T_i is the single trustee of a blind negotiation between Seller S and the buyer B, and his price is i. Thus the first trustees will inform him that no deal is possible, but if $i = SRP$, then trustee T_i will inform him that a deal exists. At the same time the buyer may try to prevent that these announcement reach S. But even if this does not succeed, he will end up with a legitimate purchase at price $i = SRP$, and thus at the minimum possible price at which the seller was ready to sell.

This attack may be prevented if the additional information AI specifies who the trustee of the current blind negotiation is, and thus only his announcement will be regarded as binding, and other trustees receiving a message of a blind negotiation that does not concern them should take proper actions in response. Another way to prevent this attack and other possible attacks consists in adding one or more rounds of communication (in fact, though the fewer these rounds are the more convenient the system is, more interactive systems are within the scope of the invention). Such additional rounds may in particular be used by having the trustee send a randomly selected value so that only responses properly including such values are considered legitimate. This makes it even harder to use portions of a blind negotiation into another blind negotiation.

Blind Negotiations with Invisible Trustees

A blind negotiation system can be implemented with trustees that are *invisible*. This means that an honest seller and buyer can exchange messages so that (for example, and without limitation) the buyer learns whether a deal is possible (e.g., whether $SRP \leq BRP$) without learning the seller's reserve price, and then proves to the seller whether a deal is possible (and at what price). However, if the buyer refuses to "share" with the seller what he has learned, then the seller can go to a trustee, which up to now has been in the background, and have the trustee take action to prove to her the result of the blind negotiation (and/or any other proper action).

Thus, in such a blind negotiation system seller and buyer exchange a first set of messages in an attempt to complete their transaction, and, if the transaction is not completed, a trustee intervenes so as to complete it.

By way of background, cryptographic protocols have been described in the literature that enable two mutually suspicious players, Alice and Bob, the first having a secret input a and the second a secret input b, to evaluate a given function f on their secret inputs so as to compute the value $f(a, b)$ without divulging more information about a and b than is already implicit in the value $f(a, b)$ itself. A variant of such a method due to Yao was discussed in the paper of Goldreich, Micali, and Wigderson. A particular simple cases arises when the function f is the AND function, Alice has a secret bit a, Bob has a secret bit b, and the two parties want to compute the AND of a and b, i.e., $a \wedge b$, without disclosing their bits more than $a \wedge b$ already does. Recall that $a \wedge b = 1$ if and only if both bits are 1. Thus, if the secret bit of one party is 1, then, after learning the value $a \wedge b$, that party will immediately also learn the other party's bit; indeed, that will coincide with $a \wedge b$. For the AND function, therefore, computing it on secret inputs without revealing more about these inputs than already implicit in the result means to meet the following two conditions:

1. *(Bob's privacy:)* If Alice has 0 as her secret bit, then, after learning that $a \wedge b = 0$, she should not learn whether Bob's bit is 1 or 0. Symmetrically,

2. *(Alice's privacy:)* If Bob has 0 as her secret bit, then, after learning that $a \wedge b = 0$, he should not learn whether Alice's bit is 1 or 0.

In the above Yao method, one of the parties (e.g., without limitation Bob) furnishes the other party (e.g., without limitation Alice) with various encrypted data having a special structure, in particular, with two ciphertexts (relative to the output bit): E0 and E1. Ciphertext E0 (encrypting a secret value *V0*) is openly labeled 0 and Cipertext E1 (encrypting a different secret value *V1*) is openly labeled *1*.

Having prepared both ciphertexts, Bob knows their decryptions *V0* and *V1*, but Alice does not, she only knows E0 and E1. If $a \wedge b = 0$, then the special structure of the data given from Bob to Alice guarantees that Alice will be able to retrieve *V0*, (but not *V1*); else, if $a \wedge b = 1$, Alice will be able to retrieve *V1* (but not *V0*). Since the labels of these ciphertexts are known, Alice can thus determine whether $a \wedge b = 0$ or $a \wedge b = 1$.

After learning one of the two secrets relative to the output bit, and thus the value of the bit $a \wedge b$, Alice can tell Bob what the output bit was. If Bob does not trust her, she can prove to him what the result of $a \wedge b$ is by releasing the secret she actually learned (i.e., either *V0* or *V1*).

Besides enabling the computation of $a \wedge b$, the method also guarantees Bob's and Alice's privacy conditions. Note, however, that Alice, after learning the actual value of $a \wedge b$, can deprive Bob of this information by simply telling him nothing, not the result $a \wedge b$, not any *proof* that this is indeed the AND of their secret input bits. It is thus a goal to rectify this weakness as well as derive from any such special computation of the AND function a new blind-negotiation system, one that works with invisible trustees.

<u>A New Blind Negotiation System</u>

In particular, assume that *M* and *N* are, respectively, lower-and upper-bounds to the reserve prices of a given commodity, and that Alice is the seller and Bob the buyer. Then, for each possible price *i* between *M* and *N*, let the bit a_i be

1 if $SRP > i$, and 0 otherwise; similarly, let the bit b_i be 1 if $i < BRP$, and 0 otherwise.

Since SRP is Alice's secret and BRP Bob's secret, each a_i is a secret bit of Alice, and each b_i a secret bit of Bob. Notice that price i is acceptable to both Alice and Bob if and only if $a_i \wedge b_i = 1$. Thus a deal between Alice and Bob is possible (i.e., SRP < BRP) if and only if there exist a value i such that $a_i \wedge b_i = 1$. If this is the case, the actual trade price maybe chosen in various ways, for instance, as the average of l and h, where l is the lowest value of i such that $a_i \wedge b_i = 1$, and h is the highest value of i such that $a_i \wedge b_i = 1$.

Thus, Alice and Bob can conduct a blind negotiation by simply computing, for all i between M and N, $a_i \wedge b_i$, by means of a special AND method such as above. (Since we are using such a special AND computation for each value of I between M and N, we may use the $_{\cdot r}$ to identify the quantities EO, E1, V0 and V1 relative to the Ith computation of the special AND, that is, EO_i, $E1_i$, $V0_i$ and $V1_i$.)

If no deal is possible, then the result will be $a_i \wedge b_i = 0$ for all i. In this case, Alice cannot learn BRP beyond the fact that it must be lower than her own SRP. Indeed, for each $i <$ SRP, $a_i = 0$ and thus $a_i \wedge b_i = 0$, but, because the special AND computation does not release any other knowledge, she will never learn whether $b_i = 1$ or $b_i = 0$ for any $i <$ SRP; thus, she cannot learn which the value of BRP may be beyond knowing that it is less than her own SRP.

If a deal is possible, then $a_i \wedge b_i = 1$ for some i. In this case, the actual trade price can be computed - for instance, by computing l and h and setting the trade price to be $(l + h)/2$.[10]

Of course, like in all blind negotiations explained so far, Alice and Bob preferably make use of digital signatures during the process of evaluating each AND in the special way, so, that each can prove who said what to whom when,

---

[10] Note that also this method allows to avoid certain prices if so wanted. E.g., Bob may choose $b_i = 1$ *and* $b_{i+5} = 1$, but chose $b_{i+3} = 0$. Again, as in one of our prior blind negotiations, this behavior of Bob may be permitted, and interpreted as his wish not to trade at price $1 + 3$, no matter what his reasons may be. Alternatively, as indicated above, it may be agreed that setting $b_i = 1$ and $b_{i+5} = 1$ is tantamount to setting $b_j = 1$ for all j between i and $i + 5$, independent of the actual value of b_j actually entered by Bob in a special gate.

and relative to which negotiation. Indeed, they may preferably sign an initial agreement, preferably specifying proper additional data for the special AND computation relative to each price *i*. In particular, the additional data for the *i*th special AND may include the ciphertext EO_i and EI_i (which respectively encrypt the secret values VO_i and VI_i, which are not part of such additional data). Thus, the release of VO_i *or* VI_i relative to the AND computation of price *i*, does not just prove to Alice or Bob whether *i* is a mutually agreeable price, but, together with other signatures already exchanged, can be part of a provably signed contract of trade between the two parties.

We should now point out that it is (for instance) Alice who finds out the values $a_i \wedge b_i$ first, and she may or may not reveal or prove what these values are to Bob. This is indeed a feature of the above mentioned special AND computation. In our context, this may result in Alice withholding from Bob the result of the negotiation.

To avoid this, the following additional modifications are proposed. First, for each special AND computation, rather than having the encryption of *VO* (denoted by EO) be openly labeled with *0* and the encryption of *VI* (denoted by *EI)* be openly labeled with *1*, the labels of *EO* and *EI* may be encrypted, preferably with a key of a trustee. For instance, Bob (who prepares these two labeled ciphertexts) may label *EO* with $E_T(0)$ and *EI* with $E_T(1)$ (where $E(x)$ is an encryption scheme of which a trusted party, has the decryption key), and make sure that these two cipertext-label pairs are presented in random order. For instance, he may provide Alice with the label-ciphertext pairs $(E_T(1), EI)$ *and* $(E_T(0), EO)$. (The encryptions of the labels *0* and *1* are preferably probabilistic. For instance, $E_T(0)$ may be the encryption, with a trustee's key, of a random even number, and $E_T(1)$ the encryption (with a trustee's key) or a random odd number.[11])

This way, after Alice computes the decryption of *EO* (i.e., *VO*) or the decryption of *EI* (i.e., *VI*), she does not understand whether the result signifies a

---

[11] Of course, one may use the same encryption scheme to encrypt *0* and *1*, or different scheme, such a scheme can be public key, or private key, in which case the ordinary encryption/decryption key can be known to both Bob and the trusted party.

0 or a *1*. (In fact, she can see that *EO* is labeled with $E_{T(0)}$ in that *E1* is labeled with $E_{T(1)}$, but she does not know which of E_{T0} and E_{T1} is an encryption of 0 and which is an encryption of 1.) She thus gives *V0* (respectively *V1*) to Bob, and Bob proves to her whether obtaining this decryption means that the AND computation resulted in a *0* or a *1* by decrypting $E_T(O)$ *or* $E_T(1)$ (or both), that is, Bob may give Alice the very even number used in generating E_TO (0) and/or the very odd number used in generating E_T1 (0).

So far, this additional step does not appear to have accomplished much. Indeed, if before it was Alice who could withhold from Bob the result of their blind negotiation, it now appears that it is Bob who could withhold the result from Alice. Indeed, Bob may refuse to provide Alice with the decryption of $E_{T(0)}$ or $E_{T(1)}$. However, Alice may go to the trusted party (preferably with data signed by Bob and data signed by herself, so as to prove that this is part of a blind negotiation). The trusted party will then provide her with the decryption of the desired $E_T(O)$ *or* $E_T(1)$ value.

Thus, the trustee is not needed and is totally in the background if Bob and Alice are honest (because Bob can decrypt himself what he had previously himself encrypted with the trustee's key). However, if this is not the case (like discussed above), the trustee may intervene to complete the negotiation by decrypting what is necessary for completing the transaction.

It is actually preferable that if Alice asks the trustee to decrypt (for example) an "output ciphertext label" $E_T(O)$ after presenting signed data that include her signature of *V0*, that is, her signature of the learned decryption of *EO*, the ciphertext labeled *E(O)*. This reassures the trustee that indeed the negotiation properly started and that Alice is entitled to learning what the learned *V0* means. In informing or proving to Alice that $E_T(O)$ actually means *0*, it is also preferable that the trustee also informs Bob of the result of negotiation; preferably by providing him with at least Alice's signature of *V0*. This way Bob has a proof of what the output of the corresponding AND gate was. Thus, if the trustee provides Alice with such a proof (or result) it also provides Bob with a corresponding proof (or result).

This "joint-notification" is important because otherwise Alice could withhold the result of the negotiation (or its proof) from Bob as follows. She participates *to the* negotiation *honestly* until she computes the decryption of the output-ciphertext of each special AND gate (i.e., either $V0_i$ *or* $V1_i$, for each gate *i*). Then, she does not tell these learned decryptions to Bob, so as to learn what they mean and inform Bob of the same. Rather, she bypasses Bob altogether, goes to the trustee, and has it *tell her* whether the labels of the output-ciphertexts mean. This way, she learns the result of the negotiation, while keeping Bob in the dark. However, if the trustee also informs Bob whenever it informs Alice, then both Alice and Bob will learn the result. Moreover, if the trustee gives Alice the decryption of each label (e.g., *the* even number whose encryption was the given $E_T(O)$, or the odd number whose encryption equaled $E_T(1)$), and gives Bob the particular decryption learned by Alice signed by her, then not only will both parties learn the result of their negotiation, but they will both have a proof of what their *results* are.

Preferably, the labels *0* and *1* are not encrypted in a key known to just one trustee, but with a key that is split among a plurality of trustees (e.g., like in the systems suggested by Micali), so that the cooperation of sufficiently many of them is required for each $E_T(0)$ *or* $E_T(1)$ value to be decrypted. This way, one or sufficiently few trustees may not conspire with (e.g.) Alice in order to let just her know the result of the negotiation. The idea of replacing a single trustee with a multiplicity of trustees possibly holding shares of a given secret key, also applies to other blind negotiation systems of this invention.

It is preferable that Seller and Buyer exchange messages by means of a method that gives certified return receipts. For instance, when Alice gives the learned *V0* secret of a given AND gate, it is recommended that she sends such a *V0* to Bob by means of a certified mail return receipt method that enables her to prove that indeed that particular value *V0* was sent to Bob. Electronic, secure and practical such methods are presented in a copending patent application.

Actually, the use of return-receipt exchanges between Seller and Verifier also enables one to dismiss invisible trustees in the blind-negotiation systems. For instance, if in the above system with a proper initial agreement Alice learns a value V_i relative to the ith AND computation of a price (i.e., V_i equals either $V0_i$ or $V1_i$), and sends it to Bob by a certified return-receipt method (which preferably shows what the sent value actually was), if Bob does not respond with a proof of the result of the computation, she has enough information to receive justice in some form of court. Such courts, however, could be interpreted as invisible trustees too, though not even their keys have been used in the negotiation.

Making Blind Negotiations Transparent

In practice, a single-trustee blind negotiation system may be quite attractive (given that the trustee does not learn the reserve prices anyway). However, one may still fear that the trustee is not trustworthy. For instance, though a blind negotiation indicates that a deal is possible, the trustee may announce that it is not possible and let the buyer know the items appearing in the seller's list. (Note that these items will reveal the seller's reserve price if the buyer knows $Z_{N,M}$).

Thus, although the seller may not mind if the buyer learns her reserve price when a deal occurs, the trustee might enable the buyer to learn the SRP when there is no deal at all.

Some of this cheating may be prevented or dissuaded as follows. When the trustee declares that there is no deal, rather than just saying so, he also signs an encryption of the information he receives from the seller and the buyer. This signed encryption of the seller's list and the buyer's value may consist of the very encryptions that seller and buyer gave the trustee in their respective steps. Indeed, in order to give the trustee her list in a private way, the seller preferably encrypts it with the trustee's key. Similarly the trustee might enable the buyer to learn the SRP when there is no deal at all.

Similarly, the buyer preferably sends the trustee his own value after encrypting it with a trustee's key. Moreover, each of the seller and buyer signs his own data (preferably together with additional data) prior to encrypting it with the trustee's key. Thus the trustee may release these two encrypted signatures when saying that no deal is possible, preferably signing the whole thing himself also.

The reason for announcing such signed encryption when the deal is not possible is to enable either the seller or the buyer to request that the blind negotiation be made "transparent." In this case, the trustee must remove his own encryption layer, thus revealing in an authenticated way the seller's list and the buyer's value.

If, after decrypting the seller's list and the buyer's value, it appears that indeed there was no deal possible (because the buyer's value does not appear in the seller's list), then proper measures can be taken. For instance, assume that the negotiated commodity is yet unsold and that it is the buyer who called for the blind negotiation to become transparent. Then, after learning the values SRP and BRP, and realizing the $SRP > BRP$, the buyer may be forced to purchase the commodity at price SRP (or N, or $SRP + N/2$, or SRP + a given amount -- either fixed or dependent on N, M etc. --) or at any other price deemed proper.

Thus, the seller may not mind that her SRP value was made known because she will be able to sell at that price or better. (Alternatively, the buyer may be properly fined -- e.g., by a fixed amount, or as a percentage of *SRP*, *N*, etc. -- e.g., by a fixed amount, or as a percentage of *SRP*, *N*, etc. - without forcing a sale of the commodity.)

Assume now that, after the blind negotiation was made transparent at the buyer's request, it appears that indeed no deal was possible, and that the seller has already sold her commodity to someone else. Then, other proper measures may be taken. For instance, the buyer may be obliged to pay the amount of *SRP* to the seller without receiving the commodity in exchange, or he may be fined according to a proper formula, etc. (Alternatively, it may be agreed that after the result of a blind negotiation is negative -- i.e., the outcome is "no deal"-- one has only a prescribed *window* of time to request to make it transparent, and that the seller should not sell the commodity during that time.)

Assume now that, after the negotiation has been made transparent, it appears that the trustee announced the wrong result. Then, other proper measures can be taken. For instance, not only the trustee can be made financially responsible for paying what it is deemed proper, but he can be also criminally prosecuted. Thus, the possibility of having the blind negotiation transparent will add a great incentive for the trustee to remain honest.

Of course, a trustee who has lied within a blind negotiation may not wish to decrypt at all. Thus, measures should be taken that dissuade him from taking this course of action. Alternatively, it may be required that the trustee's key may be shared among many other trustees (e.g., by one of the methods of Micali) so that if the trustee refuse to decrypt, the other trustees may intervene and remove his encryption layer anyone.

Forcing Good Faith in Blind Negotiations

It is desired to ensure that the participants of a blind negotiation act in good faith. By this we mean that, no matter what the reserve price of ones participant, there is at least one choice of reserve value for the other participants so that the deal is possible.

For instance, we want to disallow that a malicious buyer may waste the seller's time and resources by negotiating (without being detected) in a way that guarantees that no deal can be reached. For instance, such a buyer may give the trustee a random number R or $H(R)$ as the buyer's value (rather than the image, under function H, of one of the first $N - M$ f-inverses of Z_0). Herefore, with overwhelming probability, this number will not appear in the seller's list. Accordingly, the trustee will report that no deal is possible.

Engaging in such negotiations with the seller, the buyer may, at least temporarily, prevent that the seller negotiates profitably with others, and in general damage her. Such behavior should thus be made impossible, or easily detected.

Of course, the seller may set $i = M$ in a blind negotiation (i.e., have her SRP to be the minimum possible value). If in these conditions the outcome of the blind negotiation still is that no deal is possible, then clearly the buyer or the trustee are cheating. Thus, appropriate measures can be taken if the seller detects and proves that this is the case. (Some of these measured are discussed in the previous section. For instance, the buyer may be obliged to buy at maximum price, or, if he can prove that his value was properly set, the trustee may be fined or prosecuted.)

However, choosing a minimum SRP may be a too expensive way for the seller to check that the buyer is negotiating in good faith. Indeed, if the buyer happens to act in good faith, the seller will essentially "give away" her commodity. Therefore, better strategies to ensure good faith participation in a blind negotiation should be sought. One of them is described below. Of course, after presenting one such strategy, many others can be easily devised.

In her step, the seller gives the trustee, together with her usual list consisting of $N - M$ items (i of which consist of H evaluated at the first f-inverses of Z_0, and $N - M - i$ of which consist of different values) gives an additional *check list*. The latter consists of another $N - M$ items, preferably in random order: $H(Z_{i+1}), \ldots, H(Z_{N-M})$ -- i.e., H evaluated at the remaining $N - M - i$ f-inverses -- and $H(V_{N-M-i+1}), \ldots, H(V_{N-M})$ -- i.e., H evaluated at i values, preferably different both among themselves and from the first f-inverses of Z_0 as well as from all other V values.

Notice that the trustee, though receiving the seller's list and check list, still does not understand what the value of i may be. Indeed, if H is good, any item in each list may appear as a random number to him. Notice too, however, that the buyer's value $H(Z_j)$ should, if the buyer is honest, appear in one of the two lists. Thus, if this is not the case, the trustee may announce so, preferably in a signed manner. At this point steps can be taken to decide who is right and proper measures can be adopted.

The trustee, rather than just announcing that the buyer's value does not appear in either the primary list nor the check list of the seller, may actually release both the seller's lists and the buyer's value, and since these have been signed by their owners, he will release these signatures too. Thus one can verify in authenticated manner what are the items in the seller's list, the items in the seller's check list, and the buyer's value. If she is right, the seller may further reveal every value Z_k and every value V_k, so that one can verify that her lists were both well constructed (by checking where $H(Z_k)$ *and* $H(V_k)$ appear), and become convinced that the buyer participated to the bind negotiation in bad faith. At this point, though the seller's reserve price may be compromised, proper measures can be adopted, such as those discussed in the previous section. For instance, the commodity may be assigned to the buyer at the maximum possible price, or at price i plus a suitable additional amount.

Blind Negotiations with Duplicate Trustees

As we have seen, blind negotiations with a single trustee who does not learn the SRP nor the BRP are most convenient. However, if the trustee is not trustworthy after all, he may declare that no deal is possible (while instead $i < j$) and give, for instance, the buyer the seller's information (i.e., her list).

This event should be rather improbable if the trustee is properly chosen. In any case, the possibility of making negotiations transparent may be quite effective in deterring even this small chance.

There is, however, another way to prevent this cheating: *duplicate trustees*. That is, we envisage running the above single-trustee system with two or more trustees, treating each trustee essentially as if he were the only one. Thus, while in a general blind-negotiation system with multiple trustees, the trustees may engage in non-trivial message exchanges and computations, these duplicate trustees do not. Indeed, to make life for sellers and buyers easier, duplicate trustees may use the same encryption/decryption keys, and sellers and buyers may use these common trustee-keys when talking privately to the duplicate trustee(s). This way each message needs to be encrypted only once (with the common key of the duplicate trustees) rather than many times (with the key of each of the duplicate trustees). If they wish to use different encryptions with each of the different duplicate trustees, however, a proper encryption scheme should be used.[12]

The main advantage of having two or more duplicate trustees is the following: if a deal is possible, then every honest trustee will say so and preferably prove that this is so, thus enabling the deal to go through at the right price. Therefore, for a deal to be illegitimately declared impossible when it is indeed possible, ALL duplicate trustees must be dishonest. And the possibility of this event is even more remote.

Blind-Negotiation Systems with Secure Hardware

In a single-trustee blind negotiation-system, the problem still exists that the trustee, when the deal really is impossible, may give to one participant information relative to the other participant. For instance, he may give the buyer the seller's list(s). Of course, the trustee does not understand the SRP from this information, but the buyer will. This problem does not go away with duplicate trustees. Indeed, the

---

[12] Indeed, some encryption algorithms (like RSA with small exponents) may be secure if each message is encrypted only with one key. However, if the same message is encrypted with a first key, a second key, a third key and so on, then an enemy who gets hold of these ciphertexts can easily retrieve the message.

other duplicate trustees may just confirm that no deal is possible, but may not be aware that one trustee is tipping off the buyer.

One effective avenue to take care of this problem and others as well is having a trustee consist of or include a secure device, for concreteness purposes only but without loss of generality, a secure chip; that is, a chip a portion of which cannot be read or tampered with from the outside. For instance, because trying to tamper with the chip or trying to read part of its protected areas causes all information in the chip to be destroyed.

One advantage of using secure hardware this way is that once such a chip has been properly manufactured, its input-output behavior cannot be changed. Thus, there is no way to "corrupt" such a trustee an convince him to behave dishonestly.

For instance, the secure chip may be manufactured to correctly perform the following operations. The secure chip receives an input i from the seller and an input j from the buyer (preferably with proper additional information, and having each party properly sign his data and encrypt it with a key known to the chip). The chip then verifies the additional information and compares the values i and j. If the information looks fine and $i > j$, then the chip produces an output indicating that no deal is possible. Else, the chip outputs $g(i, j)$, where g is a function chosen to establish the actual trade price.

In either case, the chip preferably digitally signs its output together with proper additional information. (Again, other features of the above blind negotiation systems can be incorporated here - such as, initial agreement, message customization, time stamping, or having the chip give seller or buyer a random number and demanding that that number be part of future messages in the negotiation.)

<u>Random Checking for Proper Special Structures</u>

As we have mentioned, in the method for computing the AND function so as to satisfy Bob's and Alice's privacy conditions, one of the parties (e.g., Bob) sends Alice various encrypted data having a special structure. If this special structure is different from what it should be, then, rather than computing $a \wedge b$, one may compute a different function (with a one-bit output), or always discover the other party's secret bit.

In the context of the above blind negotiation, it would be in Bob's interest to change the special structure so that the function $f(a, b) = a$ would be computed instead. This way, in a blind negotiation, Bob would never offer more than Alice's SRP, though he would not know the value of SRP before hand.

It is thus important that the parties are convinced that each piece of encrypted data possesses the right special structure that makes it a special AND. In the mentioned paper of Goldreich, Micali, and Wigderson, it is suggested that (as part of the method) Bob proves to Alice that the provided cryptographic data possesses the desired special structure by means of a zero-knowledge proof. We note, however, that other well-known simpler methods can be used within our application.

For instance, assume that N - M = k is the number of possible prices for the negotiated commodity. Then, Bob may present Alice with $2k$ (rather than k) pieces of encrypted data, claiming that all of them possess the special structure for implementing an AND with our privacy constraints. Alice may then choose k of them, and ask Bob to decrypt them, so that she can see that they possess the right structure. If this check is passed, then the remaining k pieces of encrypted are believed to implement correctly our AND, and they are used as in the above blind negotiation system.

This way, Bob may cheat with probability at most one half. Indeed, even if he inserts a single incorrect piece of encrypted data, with probability 1/2 Alice will choose it among the k piece she asks Bob to decrypt. Further, the probability may be decreased (to 1/3, 1/4, etc.) by having Bob present Alice more "trial" pieces of encrypted data (e.g., $3k$, $4k$, etc.), and then have Alice choose all of them except k for decryption. Alternatively, not to increase the amount of computation and transmission too much, we may continue to use a small amount of pieces of encrypted data (e.g., $2k$), but make it counterproductive for Bob to cheat. For instance, relying on a proper initial agreement, it can be arranged that, if Bob is caught cheating or refuses to decrypt the "trial" pieces of encrypted data chosen by Alice, then is obliged to buy the given commodity at price 4N, or is fined for an amount 4N. Therefore, by cheating he expects to lose money. Indeed, if he cheats, he has probability $\leq$ 1/2 of gaining something (e.g., discovering Alice's SRP, or buying at a price that is guaranteed to be equal to

SRP) whose worth is at most $N, but also has probability 1/2 of loosing $4N. (Of course, the probability of 1/2 of being caught in the amount 4N penalty are purely exemplary in that other values could be chosen in their place).

GENERAL PRIVATE-FUNCTION EVALUATIONS WITH INVISIBLE TRUSTEES

It should also be noted that, as we have already mentioned, the above AND method generalizes so as to enable Alice and Bob to compute any function *f(a,b)* of two secret inputs *a* and *b* so as to satisfy both Alice's and Bob's privacy constraints. Again, this more general method involves Bob sending Alice encrypted data with a special structure, and having every possible output-bit variable correspond to two encryptions, E0 and E1, one labeled 0 and the other 1. The actual value of a given output-bit variable (in a given execution of a special circuitry for *f*) is 0 if Alice computes the decryption of the corresponding E0 value, and 1 if she computes the decryption of the corresponding E1 value.

Again, therefore, one of the parties may withhold from the other the result of a given private-computation of *f*. However, we can again apply the same system developed above. That is, rather than openly labeling EO with 0 and E1 with 1, we can label EO with $E_T(O)$ and E1 with $E_T(1)$, where $E_T(x)$ is an encryption function for which an invisible trustee has the decryption key. The trustee, the first party and the second party act therefore, very much like in the case of the AND function, so as to yield a method where two parties A and B, each possessing a secret input, respectively, *a* and *b*, can, with the help of an invisible trustee and without revealing these inputs, privately evaluate any given function *f* on their inputs so that, if one party learns $y = f(a,b)$, then so does the other. Again, by invisible trustee we mean the following: if both parties are honest, both will learn without involving the trustee at all, but if one of the parties dishonestly tries to keep for him/herself the learned value *y*, then the trustee intervenes so as to ensure that both learn *y* (but not the other's secret input, unless that is implicit in *y*).

While this invisible-trustee method for privately evaluating a two-input function *f* is useful in general, it is particularly useful in blind negotiations. Indeed, Alice may be a seller and Bob a buyer, *a* may be the SRP and *b* the BRP, and with a proper initial agreement and use of digital signatures, they may profitably achieve a blind negotiation with an invisible trustee by privately evaluating the following (comparison) function *f*: $f(a,b) = 1$ if a $\leq$ b, and 0 otherwise.

Again, they may use the decryption-penalty method for "checking" that the special structures involved are present in the pieces of encrypted data used.

It is now possible to summarize the important advantages of the disclosed blind negotiations systems and methods.

IN THE CLAIMS

What is claimed is:

1. An electronic process executed by a first party and a second party, with assistance from at least a plurality of trustees, wherein the first party has a selling reservation price (SRP) and the second party has a buying reservation price (BRP) and the parties are committed to a transaction if a predetermined relationship between the reservation prices is established, but not otherwise, comprising the steps of:

initiating the electronic process by having the first and second parties compute data strings encoding their respective reservation prices, wherein at least one of said parties uses an electronic device for such computation;

having each of the first and second parties transmit to the trustees the data strings that encode their respective reservation prices, wherein at least one of these transmissions is carried out electronically, and wherein a subset of trustees containing less than a given number of trustees does not possess any useful information sufficient for reconstructing the reservation prices; and

having the plurality of trustees participate in the electronic process by taking action to thereby determine whether the predetermined relationship exists, wherein the determination is made without reconstructing the reservation prices.

2. The electronic process as described in Claim 1 further including the step of:

if the predetermined relationship exists, having the trustees continue the electronic process by providing information that commits the parties to the transaction at a price according to a given formula.

3. The electronic process as described in Claim 1 further including the step of:

if the predetermined relationship does not exist, having the trustees continue the electronic process by providing information that indicates that the transaction is not possible without indicating a party's respective reservation price to the other party.

4. The electronic process as described in Claim 3 wherein the information does not reveal a party's reservation price to the other party.

5. The electronic process as described in Claim 2 wherein the predetermined relationship is SRP < or equal to BRP.

6. The electronic process as described in Claim 5 wherein the given formula is SRP + BRP/2.

7. The electronic process as described in Claim 1 wherein at least one of the trustees continues the electronic process by taking action with at least one of the parties to thereby determine whether the predetermined relationship exists.

8. The electronic process as described in Claim 1 wherein at least one of the trustees makes use of secure hardware.

9. An electronic process executed by a first party and a second party, with assistance from at least one or more trustees, wherein the first party has a selling reservation price (SRP) and the second party has a buying reservation price (BRP) and the parties are committed to the transaction if a predetermined relationship between the reservation prices is established, but not otherwise, comprising the steps of:

initiating the electronic process by having the first and second parties compute shares of their respective reservation prices, wherein at least one of said parties uses an electronic device for such computation;

having each of the first and second parties transmit shares of their respective reservation prices to a set of players selected from a set comprising the first and second parties and at least one trustee, wherein a subset of players, containing less than a given number of players and not one of the parties, does not possess any useful information for reconstructing the reservation price of that party, and wherein at least one of the transmissions is carried out electronically; and

having the players participate in the electronic process by taking action to thereby determine whether the predetermined relationship exists, wherein the determination is made without reconstructing the reservation prices.

10. The electronic process as described in Claim 9 further including the step of:

if the predetermined relationship exists, having at least some of the players continue the electronic process by providing information that commits the parties to the transaction at a price according to a given formula.

11. The electronic process as described in Claim 9 further including the step of:

if the predetermined relationship does not exist, having at least some of the players continue the electronic process by providing information that indicates that the transaction is not possible, wherein the information does not reveal a party's reservation price to the other party.

12. The electronic process as described in Claim 9 wherein at least one player uses secure hardware.

13. An electronic process executed by a first party and a second party, with assistance from at least one trustee, wherein the first party has a selling reservation price (SRP) and the second party has a buying reservation price (BRP) and the parties are committed to a transaction if a predetermined relationship between the reservation prices is established, but not otherwise, comprising the steps of:

having each of the first and second parties transmit to the at least one trustee data that does not possess any useful information for enabling the trustee to reconstruct the reservation prices, wherein at least one of the transmissions is carried out electronically;

having at least one trustee participate in the electronic process by taking action to determine whether the predetermined relationship exists; and

if the predetermined relationship exists, having at least one trustee continue the electronic process by providing information that commits the parties to the transaction at a price according to a given formula; and

if the predetermined relationship does not exist, having at least one trustee continue the electronic process by providing information that indicates that the transaction is not possible without revealing the reservation prices.

14. The electronic process as described in Claim 13 wherein, if the predetermined relationship does not exist, the information provided by the trustee does not reveal a party's reservation price to the other party.

15. The electronic process as described in Claim 13 wherein the predetermined relationship is SRP < or equal to BRP.

16. The electronic process as described in Claim 15 wherein the given formula is SRP + BRP/2.

17. The electronic process as described in Claim 13 wherein the trustee comprises a secure piece of hardware.

18. The electronic process as described in Claim 13 wherein the trustee comprises a plurality of agents.

19. The electronic process as described in Claim 18 wherein the plurality of agents hold shares of a common secret key.

20. An electronic process executed by a first party and a second party, with assistance from at least one trusted party comprising secure hardware, wherein the first party has a selling reservation price (SRP) and second party has a buying reservation price (BRP) and the parties are committed to a transaction if a predetermined relationship between the reservation prices is established to exist, but not otherwise, comprising the steps of:

generating an encrypted version of each party's reservation price, wherein at least one of the encrypted versions is generated using an electronic device:

having the first party transmit to the trusted party the encrypted version of SRP and having the second party transmit to the trusted party the encrypted version of BRP, wherein at least one of the transmissions is carried out electronically;

having at least one trusted party participate in the electronic process by taking action to determine whether the predetermined relationship exists between the reservation prices without revealing SRP and BRP outside the secure hardware; and having at least one trusted party continue the electronic process by transmitting result-information to each of the first and second parties, wherein the reservation prices are not revealed if the predetermined relationship does not exist.

21. The electronic process as described in Claim 20 wherein the predetermined relationship is SRP < or equal to BRP, and wherein if the trusted party determines that SRP < or equal to BRP, the result-information commits the parties to the transaction at a price determined at a given formula.

22. The electronic process as described in Claim 20 wherein the predetermined relationship is SRP < or equal to BRP, and wherein if the trusted party determines that SRP > BRP, the result-information indicates that the transaction is not possible at that time without revealing the reservation price of one party to the other party.

23. The electronic process as described in Claim 20 wherein in addition to the encrypted version of the SRP, the first party also transmits to the trusted party additional information, wherein the additional information includes information selected from the following: a description of the transaction, a proof of the first party's willingness to enter into the transaction, an agreed transaction price if the predetermined relationship exists, date and time, and other transaction information.

24. The electronic process as described in Claim 23 wherein the encrypted version of the SRP and the additional information are digitally signed prior to transmission by the first party to the trusted party.

25. The electronic process as described in Claim 20 wherein in addition to the encrypted version of the BRP, the second party also transmits to the trusted party additional information, wherein the additional information includes information selected from the following: a description of the transaction, a proof of the

second party's willingness to enter into the transaction, an agreed transaction price if the predetermined relationship exists, date and time, and other transaction information.

26. The electronic process as described in Claim 25 wherein the encrypted version of the BRP and the additional information are digitally signed prior to transmission by the second party to the trusted party.

27. The electronic process as described in Claim 20 wherein at least one of the first and second parties use secure hardware to encrypt their respective reservation price.

28. An electronic process executed by a first party and a second party, with assistance from an invisible trusted party if needed, wherein the first party has a selling reservation price (SRP) and the second party has a buying reservation price (BRP) comprising the steps of:

(1) having the first and second party agree to execute an ideal negotiation that results in (a) a commitment to a transaction if a predetermined relationship exists between the reservation prices or (b) no commitment and the determination that the predetermined relationship does not exist without revealing the reservation prices;

(2) having the first party and the second party exchange messages to attempt completion of the ideal negotiation, wherein at least one of the messages is exchanged electronically and wherein either party can determine whether the predetermined relationship exists; and

(3) if the ideal negotiation is not completed in step (2), having the invisible trustee take action to complete the ideal negotiation.

29. An electronic process executed by a first party and a second party, with assistance from an invisible trusted party if needed, wherein the first party has a selling reservation price (SRP) and the second party has a buying reservation price (BRP), wherein the first and second parties have agreed to an ideal negotiation that results in (a) a commitment to a transaction if a predetermined relationship exists between the reservation prices or (b) no commitment and the determination that the predetermined relationship does not exist without revealing the reservations prices, comprising the steps of:

(1) having the first party and the second party exchange messages to attempt completion of the ideal negotiation, wherein at least one of the messages is exchanged electronically; and

(2) if one party does not complete certain actions required in step (1), having the invisible trustee take action to complete the ideal negotiation; and

wherein the trusted party comprises secure hardware.

30. The electronic process as described in Claims 1, 9 or 13 wherein the transaction is selected from at least one of the following types of transactions: a sale, a lease, a license and a financing transaction.

31. The electronic process as described in Claim 30 wherein the transaction involves a commodity having a value within a predetermined upper and lower range, and wherein the trustee is provided a fee according to the value.

32. An electronic process executed by a first party and a second party, with assistance from an invisible trusted party if needed, wherein the first party has a private value "a" and the second party has a private value "b" and the first and second parties have agreed to compute a given function "f" on their inputs "a" and "b", comprising the steps of:

(1) having the first party and the second party exchange messages to enable each of the parties to obtain f(a,b) without revealing "a" and "b", wherein at least one of the messages is exchanged electronically and wherein either party can determine whether the obtained value f(a,b) is correct; and

(2) if one party has not obtained f(a,b) in step (1), having the invisible trustee take action so that both parties can obtain f(a,b).

33. An electronic process executed by a first party and a second party, with assistance from at least one trustee, wherein the first party has a private first value and the second party has a private second value and the parties are committed to a transaction if a predetermined relationship between the first and second values is established, but not otherwise, and wherein each party's respective value is unknown to the other party, comprising the steps of:

initiating the electronic process by having the first and second parties compute data strings encoding their respective values, wherein at least one of said parties uses an electronic device for such computation;

having each of the first and second parties transmit to at least one trustee the data strings that encode their respective values, wherein at least one of these transmissions is carried out electronically, and wherein at least one trustee does not possess any useful information sufficient for reconstructing the first and second values; and

having at least one trustee participate in the electronic process by taking action to help determine whether the predetermined relationship exists, wherein the determination is made without reconstructing the private values.

34. The electronic process as described in Claim 33 further including the step of:

if the predetermined relationship exists, having at least one trustee continue the electronic process by contributing information that helps commit the parties to the transaction according to a given formula.

35. The electronic process as described in Claim 33 further including the step of:

if the predetermined relationship does not exist, having at least one trustee continue the electronic process by providing information that contributes to indicating that the transaction is not possible without thereby indicating the first and second private values.

36. An electronic process executed by a first party and a second party, with assistance from at least one or more trustees, wherein the first party has a secret first value and the second party has a secret second value and the parties are committed to the transaction if a predetermined relationship between the first and second values is established, but not otherwise, wherein each party's respective private value is unknown to the other party, comprising the steps of:

initiating the electronic process by having the first and second parties compute shares of their respective values, wherein at least one of said parties uses an electronic device for such computation;

having each of the first and second parties transmit shares of their respective values to a set of players selected from a set comprising the first and second parties and at least one trustee, wherein a subset of players, containing less than a given number of players and not one of the parties, does not possess any useful information for reconstructing the value of that party, and wherein at least one of the transmissions is carried out electronically; and

having the players participate in the electronic process by taking action to thereby determine whether the predetermined relationship exists, wherein the determination is made without reconstructing the first and second values.

37. The electronic process as described in Claim 36 further including the step of:

if the predetermined relationship exists, having at least some of the players continue the electronic process by providing information that commits the parties to the transaction according to a given formula.

38. The electronic process as described in Claim 36 further including the step of:

if the predetermined relationship does not exist, having at least some of the players continue the electronic process by providing information that indicates that the transaction is not possible, wherein the information does not reveal a party's private value to the other party.

39. An electronic process executed by a first party and a second party, with assistance from at least one trustee, wherein the first party has a private first value and the second party has a private second value and the parties are committed to a transaction if a predetermined relationship between the first and second values is established, but not otherwise, wherein each party's respective value is unknown to the other party, comprising the steps of:

having each of the first and second parties transmit to at least one trustee data that does not possess any useful information for enabling the trustee to reconstruct the first and second values;

having at least one trustee participate in the electronic process by taking action to determine whether the predetermined relationship exists; and

if the predetermined relationship exists, having at least one trustee continue the electronic process by providing information that commits the parties to the transaction according to a given formula;

if the predetermined relationship does not exist, having at least one trustee continue the electronic process by providing information that indicates that the transaction is not possible without revealing the first and second private values.

40. An electronic process executed by a first party and a second party, with assistance from at least one trusted party comprising secure hardware, wherein the first party has a private first value and second party has a private second value and the parties are committed to a transaction if a predetermined relationship between the first and second values is established to exist, but not otherwise, wherein each party's respective value is unknown to the other party, comprising the steps of:

generating an encrypted version of each party's private value, wherein at least one of the encrypted versions is generated using an electronic device;

having the first party transmit to the trusted party the encrypted version of the private first value and having the second party transmit to the trusted party the encrypted version of the private second value, wherein at least one of the transmissions is carried out electronically;

having the trusted party participate in the electronic process by taking action to determine whether the predetermined relationship exists without revealing the first and second private values outside the secure hardware; and having the trusted party continue the electronic process by transmitting result-information to each of the first and second parties, wherein the private first and second values are not revealed if the predetermined relationship does not exist.

41. An electronic process executed by a first party and a second party, with assistance from an invisible trusted party if needed, wherein the first party has a private first value and the second party has a private second value, comprising the steps of:

(1) having the first and second party agree to execute and electronic negotiation that results in (a) a commitment to a transaction if a predetermined relationship exists between the private first and second values or (b) no commitment and the determination that the predetermined relationship does not exist without revealing the first and second values, and wherein each party's respective private value is unknown to the other party;

(2) having the first party and the second party exchange messages to attempt completion of the electronic negotiation, wherein at least one of the messages is exchanged electronically and wherein either party can determine whether the electronic negotiation is complete; and

(3) if the electronic negotiation cannot be completed in step (2), having the invisible trustee take action to complete the electronic negotiation.

42. An electronic process executed by a first party and a second party, using secure hardware, wherein the first party has a private first value and the second party has a private second value and the parties are committed to a transaction if a predetermined relationship between the first and second values is established to exist, but not otherwise, wherein each party's respective value is unknown to the other party, comprising the steps of:

providing the secure hardware the private first and second values, wherein at least one of the values is provided electronically;

having the secure hardware determine whether the predetermined relationship exists without revealing the first and second private values outside the secure hardware; and

having the secure hardware provide result-information to at least one of the first and second parties, wherein at least one of the private first and second values is not revealed outside the secure hardware if the predetermined relationship does not exist.

43. The electronic process as described in Claim 42 wherein if the predetermined relationship exists, the result-information provided by the secure hardware indicates a transaction price by evaluating a predetermined function of the first and second private values.

44. The electronic process as described in Claim 42 wherein the result-information is digitally signed.

45. The electronic process as described in Claim 42 wherein the result–information is digitally signed with other information.

46. The electronic process as described in Claim 42 wherein an initial agreement occurs between the first and second parties prior to the secure hardware providing the result-information.

47. The electronic process as described in Claim 42 wherein at least one of the first and second private values is provided to the secure hardware unencrypted.

48. The electronic process as described in Claim 41 wherein the first and second parties further agree that a given penalty is imposed on a party that has been found to have deviated from prescribed steps of the electronic negotiation.

FIG. 1

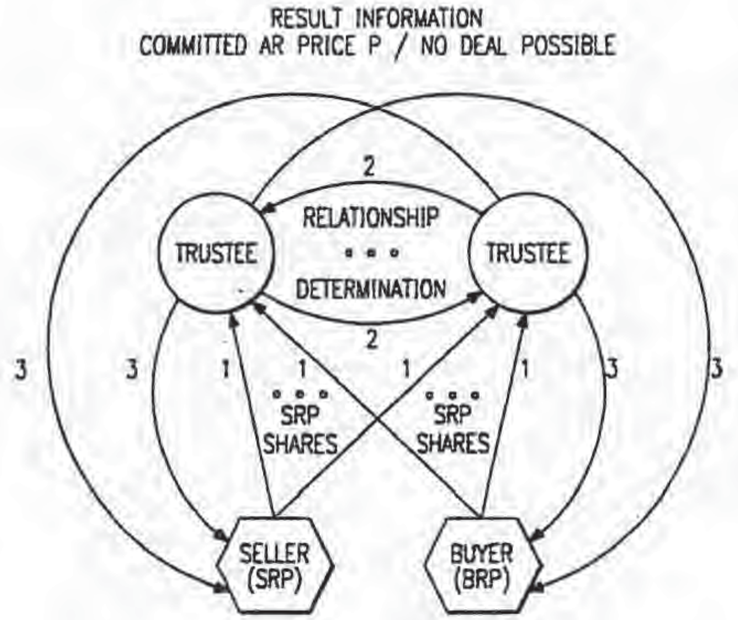

RESULT INFORMATION
COMMITTED AR PRICE P / NO DEAL POSSIBLE
2
RELATIONSHIP
• • •
DETERMINATION
2
TRUSTEE
TRUSTEE
3
3
1
1
1
1
3
3
• • •
SRP
SHARES
• • •
SRP
SHARES
SELLER
(SRP)
BUYER
(BRP)

FIG. 2

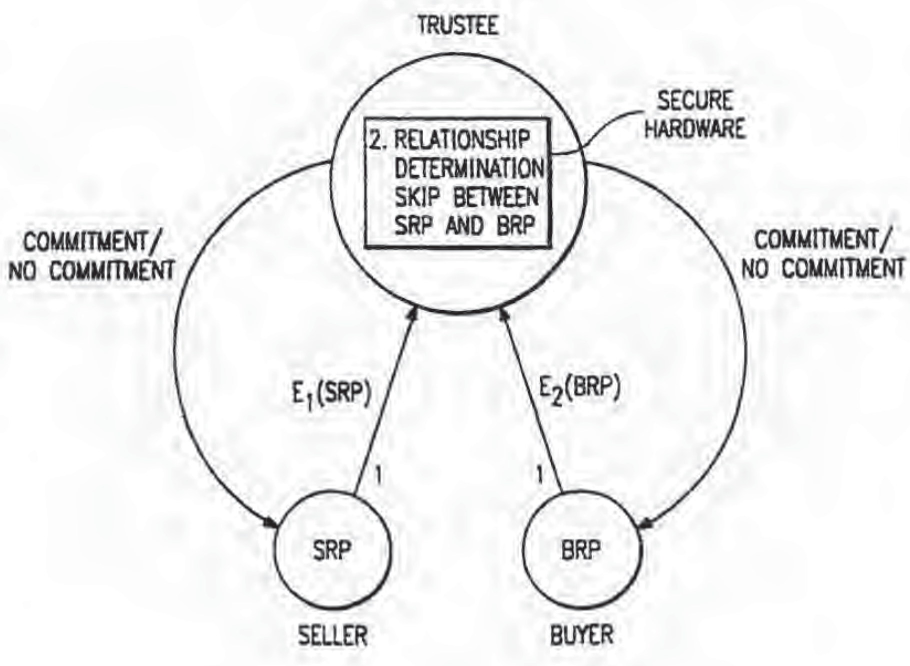

TRUSTEE
2. RELATIONSHIP
DETERMINATION
SKIP BETWEEN
SRP AND BRP
SECURE
HARDWARE
COMMITMENT/
NO COMMITMENT
COMMITMENT/
NO COMMITMENT
E1(SRP)
E2(BRP)
1
1
SRP
BRP
SELLER
BUYER

FIG. 3

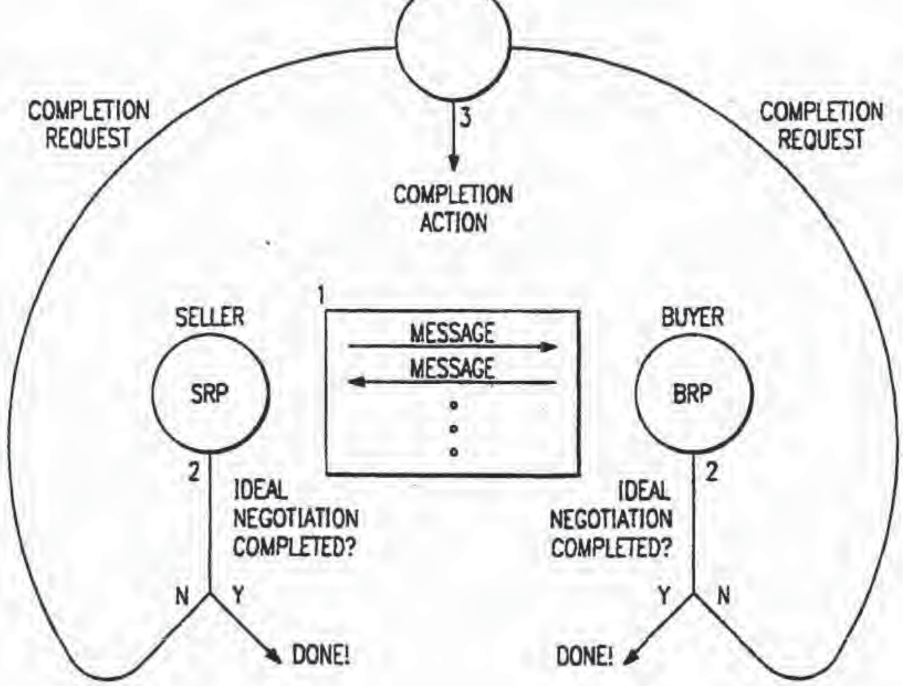
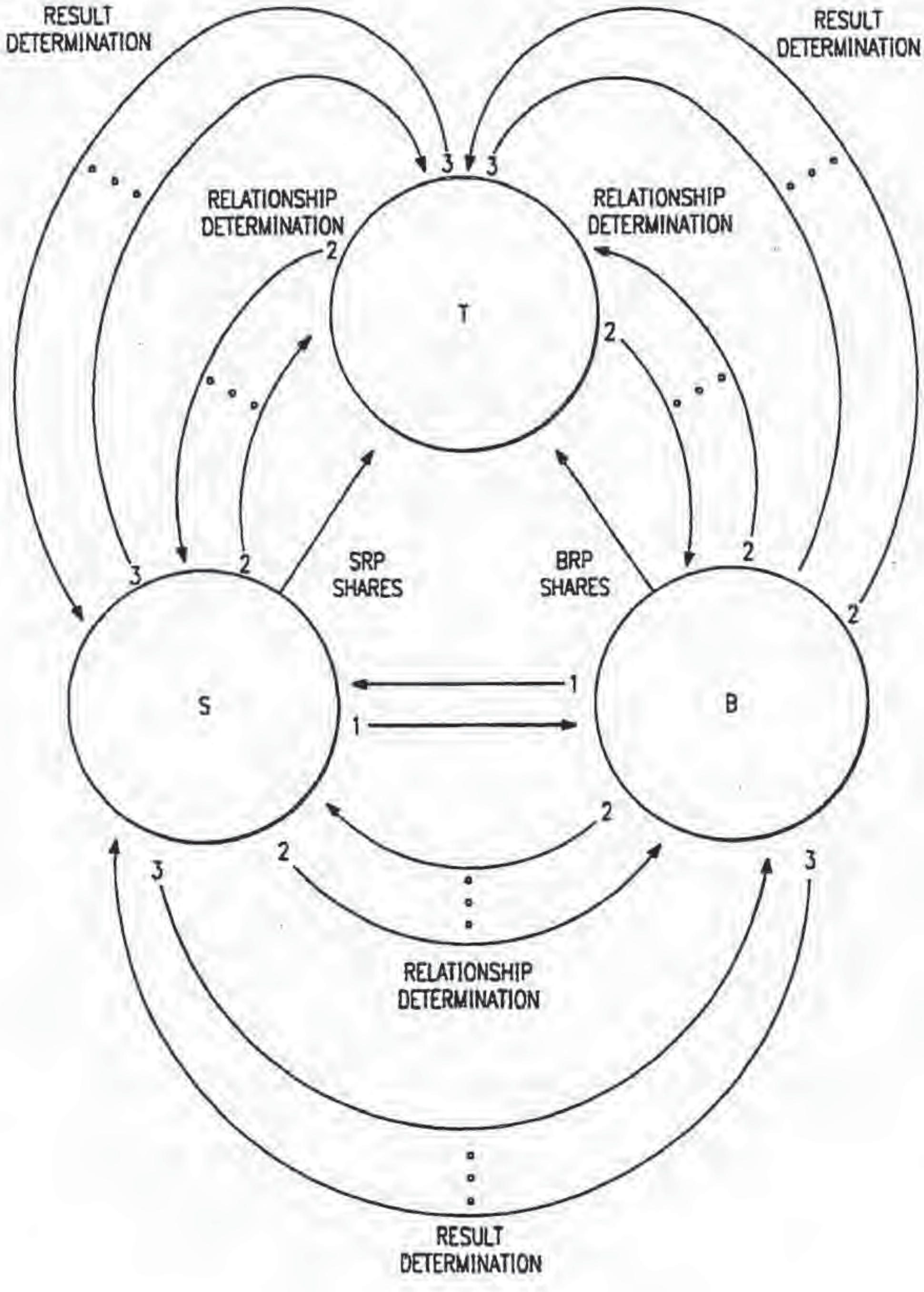

COMPLETION
REQUEST
3
COMPLETION
REQUEST
COMPLETION
ACTION
1
SELLER
MESSAGE
MESSAGE
BUYER
SRP
BRP
2
IDEAL
NEGOTIATION
COMPLETED?
2
IDEAL
NEGOTIATION
COMPLETED?
N
Y
Y
N
DONE!
DONE!

FIG. 4


RESULT
DETERMINATION
RESULT
DETERMINATION
3
3
3
RELATIONSHIP
DETERMINATION
RELATIONSHIP
DETERMINATION
2
2
T
SRP
SHARES
BRP
SHARES
3
2
2
2
S
B
1
1
2
2
3
3
RELATIONSHIP
DETERMINATION
RESULT
DETERMINATION

(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 649 261 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
23.01.2002 Bulletin 2002/04

(51) Int Cl.7: **H04N 7/24**, H04N 7/167

(21) Application number: **94307609.1**

(22) Date of filing: **17.10.1994**

(54) **Image data processing and encrypting apparatus**

Vorrichtung zur Verarbeitung und Verschlüsselung von Bilddaten

Appareil pour le traitement et le chiffrage de données d'images

(84) Designated Contracting States:
DE ES FR GB IT NL

(30) Priority: **18.10.1993 JP 25977093**

(43) Date of publication of application:
19.04.1995 Bulletin 1995/16

(73) Proprietor: **CANON KABUSHIKI KAISHA**
Tokyo (JP)

(72) Inventor: **Enari, Masahiko,**
c/o Canon Kabushiki Kaisha
Ohta-ku, Tokyo (JP)

(74) Representative:
Beresford, Keith Denis Lewis et al
BERESFORD & Co. 2-5 Warwick Court, High Holborn
London WC1R 5DH (GB)

(56) References cited:
EP-A- 0 364 295
EP-A- 0 485 230
EP-A- 0 542 261
EP-A- 0 582 122
EP-A- 0 614 308
EP-A- 0 619 677
WO-A-94/15437

Note: Within nine months from the publication of the mention of the grant of the European patent, any person may give notice to the European Patent Office of opposition to the European patent granted. Notice of opposition shall be filed in a written reasoned statement. It shall not be deemed to have been filed until the opposition fee has been paid. (Art. 99(1) European Patent Convention).

Printed by Jouve, 75001 PARIS (FR)

Description

[0001] The present invention relates to an image processing apparatus, and more particularly to the encryption of image data.

[0002] Fig. 1 shows a block diagram of a configuration of a prior art image encoding apparatus having an encryption function.

[0003] Fig. 2 shows a block diagram of an image decoding apparatus for decoding the image data encoded by the apparatus of Fig. 1.

[0004] In the encoding apparatus shown in Fig. 1, numeral 110 denotes a high resolution analog video signal (hereinafter referred to as an HD signal), which, in the present example, has the number of scan lines of 1,050 and a frame frequency of 30 Hz. Relative to the HD signal, a video signal of an ordinary resolution having the number of scan lines of 525, a frame frequency of 30 Hz and the number of pixels of 858 is referred to as an SD signal.

[0005] An HD A/D conversion circuit 112 samples the video signal 110 at a sampling frequency of 54.054 MHz to convert it to a digital signal. By virtue of the sampling frequency, the number of pixels per line of the digital HD signal is 1,716. A high resolution (HD)/ordinary resolution (SD) conversion circuit 114 reduces the number of pixels to one half in both vertical direction and horizontal direction to output a video signal of the ordinary resolution having the number of scan lines of 525, the frame frequency of 30 Hz and the number of pixels per line of 858.

[0006] An encoding circuit 116 efficiently encodes the digital SD signal outputted from the conversion circuit 114 by an encoding scheme which is a combination of motion compensated adaptive prediction and DCT. A decoding circuit 118 decodes the encoded signal outputted from the decoded circuit 116 to reproduce an SD signal. An SD/HD conversion signal 120 interpolates pixels to the output video data from the decoding circuit 118 by a factor of two in both vertical direction and horizontal direction to convert it to an HD signal. Namely, the SD/HD conversion circuit 120 outputs a signal corresponding to the high resolution video signal having the number of scan lines of 1,050, the number of pixels per line of 1,716 and the frame frequency of 30 Hz.

[0007] A subtractor 122 subtracts the output of the SD/HD conversion circuit 120 from the output of the A/D conversion circuit 112 for each pixel. The output of the subtractor 122 is referred to as an auxiliary video signal. An encoding circuit 124 encodes the output of the subtractor 122 in the same encoding scheme as that for the encoding circuit 116.

[0008] A multiplexing circuit 126 multiplexes the encoded data (the encoded SD signal) outputted from the encoding circuit 116 and the encoded data (the encoded auxiliary video signal) outputted from the encoding circuit 124 and outputs it to an encryption circuit 128. The encryption circuit 128 encrypts the output of the multiplexing circuit 126 in accordance with an encryption key signal of an encryption key output circuit 130, and an output unit 132 outputs the encrypted data outputted from the encryption circuit 128 to a transmission line. As described above, the transmission line may be a communication line or a recording medium.

[0009] The encryption is briefly explained with reference to Figs. 3 and 4. Following encryption techniques are available.

[0010] Fig. 3 shows a flow chart of the encryption by the US Data Encryption Standard (DES) published in the FIPS Publication 46 dated January 15, 1977, and Fig. 4 shows a function of the encryption of Fig. 3. The data encryption algorithm of the DES has been published as the "Data Encryption Standard" as described above. Referring to Figs. 3 and 4, the DES will be explained.

[0011] The DES handles block encryption to binary data comprising 0's and 1's. In the DES, the binary data is grouped into 64-bit blocks and the transposition and the replacement are repeated for each block to encrypt it. An encryption key is a 64-bit signal, of which 8 bits are check bits for detecting an error. Thus, a 56-bit encryption key is actually effective. The replacement of the digit is controlled by the encryption key in each cycle. Fig. 3 shows an encryption process of the DES. Fig. 4 shows a function fK(R) which is a heart of the encryption.

[0012] As shown in Fig. 3, a 64-bit plain text is first transpositioned. This is a fixed transposition independent from the encryption key. Then, the 64 bits are divided into a left half L_0 and a right half R_0. Then, the following operations are repeated over the 16 stages.

$$L_n = R_{n-1}$$

$$R_n = L_{n-1} + fK_n(R_{n-1}) \qquad (1)$$

where + represents a sum of mode 2 for each bit, L_n and R_n represent the left half 32 bits and the right half 32 bit, respectively, at the end of the operation for the n-th stage, and K_n is generated from the encryption key as shown in the right side of Fig. 3. In Fig.3 $s_1, \ldots s_{16}$ are 1 or 2.

[0013] Condensed transposition is defined as the transposition excluding some of the input. In Fig. 3, 8 bits out of the 56 input bits are excluded so that an output comprises 48 bits. The condensed transposition is irrevocable conversion so that the input cannot be perfectly reproduced from the output. This serves to make the estimation of the encryption key difficult.

[0014] Referring to Fig. 4, the function fK(R) in Fig. 3 is specifically explained. In Fig. 4, to generate the function fK(R), augmented transposition is made to R. The augmented transposition is defined as the overlapped transposition of some inputs. In the illustrated example, 16 bits out of the 32 input bits appear in overlap at the output. K composed by the key is mode 2 added to the output. The resulting 48 bits are divided into eight 6-bit blocks and the respective 6 bits are converted to 4 bits by S_1, S_2, ..., S_8, respectively. Assuming that the 6 bits constitute one character, it may be considered as a kind of replacement. However, since the output is compressed to 4 bits, the conversion is irrevocable. Accordingly, the IK(R) is generally an irrevocable function. This, however, does not mean that the conversion of the formula (1) is irrevocable. The formula (1) may be converted as follows:

$$R_{n-1} = L_n$$

$$L_{n-1} = R_n + IK_n(R_{n-1})$$

$$= R_n + IK(L_n) \qquad (2)$$

It is thus seen that L_{n-1} and R_{n-1} can be calculated from L_n and R_n.

[0015] The calculation of the formula (1) is repeated 16 times and when L_{16} and R_{16} are determined, they are finally transpositioned again and the encryption is terminated.

[0016] In a decoding apparatus shown in Fig. 2, a transmission data input unit 140 receives the data from the transmission line and supplies it to a decryption circuit 142. The decryption circuit 142 decrypts it by utilizing the encryption key signal outputted from the encryption key output circuit 144. In order for the decryption to be correctly done, the exactly same encryption key as that outputted from the encryption key output circuit 130 used in the encoding apparatus (see Fig. 1) should be used.

[0017] The decryption is substantially a reverse operation to the encryption. Briefly, the process proceeds from the bottom to the top in Fig. 3. First, a reverse transposition to the last transposition in the encryption is made, and R_{n-1} and L_{n-1} are determined from the formula (2), and when R_0 and L_0 are determined, a reverse transposition to the first transposition in the encryption is made. In this manner, the original 64 bits are reproduced. In order to decrypt the DES encrypted text, there has been no known method other than examining the keys one by one. Assuming that one microsecond is needed to examine if one key is correct one or not, 2,283 years will be needed to examine all of 2^{56} keys.

[0018] The transmission data decrypted by the decryption circuit 142 is separated by a separation circuit 146 to encoded data of the SD signal and encoded data of the auxiliary video signal, which are supplied to decoding circuits 148 and 150, respectively. The decoding circuit 148 outputs the reproduced SD signal and the decoding circuit 150 output the reproduced auxiliary video signal.

[0019] An SD A/D conversion circuit 152 converts the digital SD signal outputted from the decoding circuit 148 to an *analog* signal. The output of the SD A/D conversion circuit 152 is an analog video signal having the number of scan lines of 525 and the frame frequency of 30 Hz. This video signal is applied to a monitor device of an ordinary resolution to display the image.

[0020] An SD/HD conversion circuit 154 converts the digital SD signal outputted from the decoding circuit 148 to a digital HD signal in the same process as that of the SD/HD conversion circuit 120. An adder 156 adds the output of the decoding circuit 150 and the output of the SD/HD conversion circuit 154. The output of the adder 156 is a video signal corresponding to the high resolution video signal. An HD D/A conversion circuit 158 converts the digital output of the adder 156 to an analog signal. The output of the HD D/A converter 158 is a video signal having the number of scan lines of 1,050 and the frame frequency of 30 Hz. The video signal is applied to a high resolution monitor to display the image.

[0021] The above prior art video signal encoding and decoding apparatus has a problem in that the video signal cannot be reproduced for those who do not have the encryption key, for both the low resolution video signal and the high resolution video signal.

[0022] There is a demand that charges to users are discriminated between the low resolution display device having the number of scan lines of 525 and the high resolution display device having the number of scan lines of 1,050, for the same content, but the prior art apparatus does not meet the requirement.

[0023] It is known from EP-A-0364265 to divide a television signal into a number of spatiotemporal components and to perform scrambling on those components containing high frequencies in order to reduce the effects of random noise and interference.

[0024] The following references WO-A-94/15437, EP-A-0582122, EP-A-0614308 and EP-A-0619677 are cited against the present application as prior art only to the extent provided by Articles 54(3) and (4) EPC. WO-A-94/15437 discloses partial unscrambling and decoding of a scrambled television signal by receivers having partial access rights.

[0025] EP-A-0582122 discloses scrambling apparatus for encoded video data.

[0026] EP-A-0614308 discloses key encryption of selected image components such that access to low resolution components is available without decryption.

[0027] EP-A-0619677 discloses scrambling of direct cosine transformation coded blocks of video data, including the scrambling of a DC component.

[0028] According to the present invention there is disclosed an image processing apparatus as set out in claim 1.

[0029] Acording to other aspects of the invention there is also disclosed apparatus and method as set out in claims 6, 13 and 18. Further aspects of the invention are set out in the dependend claims.

[0030] Other aspects features and advantages of the invention will become apparent from the following detailed description taken in conjunction with the accompanying drawings

BRIEF DESCRIPTION OF THE DRAWINGS

[0031]

Fig. 1 shows a block diagram of a prior art image encoding apparatus,
Fig. 2 shows a block diagram of a prior art image decoding apparatus,
Fig. 3 shows a flow of prior art encryption,
Fig. 4 shows a flow of prior art encryption,
Fig. 5 shows a block diagram of a configuration of one embodiment of an image encoding apparatus of the present invention,
Fig. 6 shows a block diagram of a configuration of an embodiment of an image decoding apparatus of the present invention,
Fig. 7 shows a block diagram of a modified portion of a configuration of a modified embodiment of Fig. 6,
Fig. 8 shows a block diagram of a modified portion of a modified embodiment of Fig. 6,
Fig. 9 shows a block diagram of a configuration of a second embodiment of the image encoding apparatus of the present invention,
Fig. 10 shows a block diagram of a configuration of a second embodiment of the image decoding apparatus of the present invention,
Fig. 11 illustrates band division of a space frequency,
Fig. 12 shows a block diagram of a configuration of a modified portion of a modified embodiment of Fig. 10,
Fig. 13 shows a block diagram of a configuration of a modified portion of a modified embodiment of Fig. 10,
Fig. 14 shows a block diagram of a specific encoding circuit of the embodiment, and
Fig. 15 shows a block diagram of a specific decoding circuit of the embodiment.

DETAILED DESCRIPTION OF THE EMBODIMENTS

[0032] Fig. 5 shows a block diagram of a configuration of one embodiment of the encoding apparatus of the present invention, and Fig. 6 shows a block diagram of a configuration of the decoding apparatus.

[0033] The encoding apparatus shown in Fig. 5 is first explained. Numeral 10 denotes a high resolution video signal having the number of scan lines of 1,050 and the frame frequency of 30 Hz as the HD signal 110 does. Numeral 12 denotes an HD A/D conversion circuit for converting the video signal 10 to a digital signal, numeral 14 denotes a high resolution (HD)/ordinary resolution (SD) conversion circuit for converting the digital HD signal outputted from the HD A/D conversion circuit 12 to a video signal of the ordinary resolution, numeral 16 denotes an encoding circuit for efficiently encoding the output of the conversion circuit 14, numeral 18 denotes a decoding circuit for decoding the output of the encoding circuit 16, numeral 20 denotes an SD/HD conversion circuit for interpolating the SD signal output of the decoding circuit 18 to convert it to an HD signal, numeral 22 denotes a subtractor for subtracting the output of the SD/HD conversion circuit 20 from the output of the HD A/D conversion circuit 12 for each pixel, and numeral 24 denotes an encoding circuit for encoding the output of the subtactor 22. The circuits 12 - 24 have the same functions as those of the circuits 112 - 124 of Fig. 1 and operate in the same manner.

[0034] Numeral 26 denotes an encryption circuit for encrypting the output of the encoding circuit 24 in accordance with an encryption signal outputted from an encryption key output circuit 28. As the encryption technique, the one which complies with the DES standard is used.

[0035] Numeral 30 denotes a multiplexing circuit for multiplexing the output of the encoding circuit 16 and the encryption circuit 26, and numeral 32 denotes an output unit for outputting transmission data multiplexed by the multiplexing circuit 30 to a transmission line such as a communication line or a recording medium.

[0036] The encoding apparatus shown in Fig. 5 is explained. The operations of the circuits 12 - 24 are same as those of the prior art apparatus. Namely, the encoding circuit 16 outputs the encoded data of the video signal derived by converting the HD signal 10 to the ordinary resolution, and the encoding circuit 24 outputs the encoded data of the auxiliary video signal to reproduce the high resolution video signal from the transmission video data of the ordinary resolution. In the present embodiment, prior to the multiplexing of the both encoded data, the output encoded data of the encoding circuit 24 is encrypted by the encryption circuit 26 by using the encryption key signal outputted from the encryption key output circuit 28 and it is applied to the multiplexing circuit 30.

[0037] Accordingly, in the present embodiment, the multiplexing circuit 30 multiplexes the encoded data of the video signal of the ordinary resolution (the output of the encoding circuit 16) and the encoded data of the encrypted auxiliary video signal and the output unit 32 outputs the output of the multiplexing circuit 30 to the transmission line. Accordingly, the video signal of the ordinary resolution is transmitted without encryption but the information for reproducing the high resolution video signal (auxiliary video signal) is encrypted so that, in the receiving station, the high resolution video signal cannot be reproduced without the encryption key but the video signal of the ordinary resolution can be reproduced without the encryption key.

[0038] The decoding apparatus shown in Fig. 6 is explained. Numeral 40 denotes a transmission data input unit for receiving data from the transmission line, numeral 42 denotes a separation circuit for separating a set stream from the transmission data input unit 40 to a portion related to the encoded data of the SD signal and a portion related to the encoded data of the auxiliary video signal, and numeral 44 denotes a decryption circuit for decrypting the encoded data of the auxiliary video signal from the separation circuit 42 by referencing the encryption key signal outputted from the encryption key output circuit 46.

[0039] Numeral 48 denotes a decoding circuit for decoding the encoded data of the SD signal from the separation circuit 42, numeral 50 denotes a decoding circuit for decoding the encoded data of the auxiliary video signal from the decryption circuit 44, numeral 52 denotes an SD D/A conversion circuit for converting the digital SD signal outputted from the decoding circuit 48 to an analog signal, numeral 54 denotes an SD/HD conversion circuit for converting the digital SD signal outputted from the decoding circuit 48 to a digital HD signal in the same process as that of the SD/HD conversion circuit 20, numeral 56 denotes an adder for adding the output of the decoding circuit 50 to the output of the SD/HD conversion circuit 54, and numeral 58 denotes an HD D/A conversion circuit for converting the digital output of the adder 56 to an analog signal.

[0040] An operation of the decoding circuit shown in Fig. 6 is explained. The transmission data input unit 40 receives the data from the transmission line and supplies it to the separation circuit 42, and the separation circuit 42 separates it to a portion related to the encoded data of the SD signal and a portion related to the encoded data of the encrypted auxiliary video signal and supplies the former to the decoding circuit 48 and the latter to the decryption circuit 44. The decryption circuit 44 decrypts the encryption applied to the encoded data of the auxiliary video signal by using the same encryption key signal outputted from the encryption key output circuit 46 as the encryption key signal outputted from the encryption key output circuit 28 of the encoding circuit (Fig. 1). The encoded data of the auxiliary video signal decrypted by the decryption circuit 44 is applied to the decoding circuit 50 and decoded thereby.

[0041] Thus, the decoding circuit 48 outputs the reproduced digital SD signal and the decoding circuit 50 outputs the reproduced digital auxiliary video signal.

[0042] The SD D/A conversion circuit 52 converts the digital SD signal outputted from the decoding circuit 48 to an analog signal. The SD D/A conversion circuit 52 may be an analog signal having the number of scan lines of 525 and the frame frequency of 30 Hz and the video signal is applied to a monitor device of the ordinary resolution to display the image.

[0043] The SD/HD conversion circuit 54 converts the digital SD signal outputted from the decoding circuit 48 to a digital signal in the same process as that of the SD/HD conversion circuit 120. The adder 56 adds the output of the decoding circuit 50 to the output of the SD/HD conversion circuit 54 for each pixel. The output of the adder 56 is a video signal corresponding to the high resolution video signal. The HD D/A conversion circuit 58 converts the digital output of the adder 56 to an analog signal. The output of the HD D/A conversion circuit 58 is a high resolution video signal having the number of scan lines of 1,050 and the frame frequency of 30 Hz and it may be applied to a high resolution monitor to display the image.

[0044] In the decoding apparatus shown in Fig. 6, without the encryption key or if the encryption key is not correct (hereinafter collectively referred to as without key or no key state), the decryption circuit 44 outputs quite an unstable data pattern so that the output of the HD D/A conversion circuit 58 is also unstable and an unstable pattern such as a noise image is displayed on the screen of the display device such as a CRT.

[0045] Alternatively, a fixed image may be displayed on the high resolution monitor screen in the no key state. Figs. 7 and 8 show portions of block diagrams of such modified encoding apparatus. The like elements in Figs. 7 and 8 are designated by like numerals.

[0046] In Fig. 7, a switch 60 is provided between the decoding circuit 50 and the adder 56, and when the no key state (no input of the encryption key signal) is detected by the decryption circuit 44, the switch 60 is set to '0' by the detection output so that '0' is applied to the adder 56. When the correct encryption key is inputted to the decryption circuit 44' the decryption circuit 44' connects the switch 60 to the output of the decoding circuit 50.

[0047] In Fig. 8, a switch 62 is provided between the adder 56 and the HD D/A conversion circuit 58 so that in the no key state a predetermined level is inputted to the HD D/A conversion circuit 58. The switch 62 normally selects the output of the adder 56, and when the decryption circuit 44' the no key state (no input of the encryption key signal), the switch is set to the predetermined level input. In this manner, when the correct input is present, the high resolution video signal is outputted but in the no key state, the predetermined level signal is outputted and an image corresponding to the predetermined level is displayed on the monitor screen.

[0048] In Figs. 7 and 8, the switches 60 and 62 are illustrated to facilitate the understanding although it is apparent that the function of such switches 60 and 62 may be incorporated in the decoding circuit 50 and/or HD A/D conversion circuit 58. Alternatively, the output of the decoding circuit 50 or the HD D/A conversion circuit may be forced to a predetermined level (for example, zero output) in response to the detection of the no key state by the decryption circuit 44.

[0049] In Figs. 7 and 8, the no key state is detected by the decryption circuit 44 although it may be detected by error code detection or error correction process.

[0050] A second embodiment of the present invention which is applied to a system in which the image information is transmitted by the band division by the space frequency is now explained. Fig. 9 shows a block diagram of a configuration of an encoding apparatus thereof, and Fig. 10 shows a block diagram of a configuration of a decoding apparatus. Fig. 11 illustrates the band division of the space frequency.

[0051] Numeral 210 denotes an analog HD signal to be encoded. In the present embodiment, it is a video signal having the number of scan lines of 1,050 and the frame frequency of 30 Hz. An HD A/D conversion circuit 212 samples the analog HD signal at a sampling frequency of 54.054 MHz to convert it to a digital signal. The number of pixels per line of the sampled HD signal is 1,716.

[0052] The output of the HD A/D conversion circuit 212 is applied to band division filters 214 and 216 and divided by the filters 214 and 216 to a low frequency component and a high frequency component at a horizontal frequency and the number of pixels is reduced to one half, respectively.

[0053] The output of the band division filter 214 is a low resolution component of the horizontal frequency, which is further separated into a low frequency component and a high frequency component at a vertical frequency by band division filters 218 and 220 to reduce the number of pixels to one half. Similarly, the band division filters 222 and 224 separates the output of the band division filter 216 (the high resolution component at the horizontal frequency) into a low frequency component and a high frequency component at the vertical frequency to reduce the number of pixels to one half.

[0054] In this manner, the high resolution video signal having 1,716 pixels in the horizontal direction and 1,024 pixels in the vertical direction is separated into an LL signal (the output of the band division filter 218), an LH signal (the output of the band division filter 220), an HL signal (the output of the band division filter 222) and an HH signal (the output of the band division filter 224) having one half of the total number of pixels in the horizontal direction and the vertical direction, as shown in Fig. 11. Since only the LL signal has the low-pass data in both the horizontal direction and the vertical direction, it is the video information which can be reproduced for display as the image and corresponds to the video signal of the ordinary resolution having the number of scan lines of 525, the frame frequency of 30 Hz and the number of pixels per line of 858. On the other hand, since the LH signal, the HL signal and the HH signal are high-pass data, they cannot be displayed as the image as they are and they are the auxiliary video signals which form the high resolution video signal in cooperation with the LL signal.

[0055] The encoding circuit 226 efficiently encodes the output of the band division filter 218 (LL signal) by an encoding scheme which is a combination of the motion compensated adaptive prediction known as the CCIR Recommendation 723 and the DCT. Encoding circuit 228, 230 and 232 efficiently encode the outputs of the band division filters 220, 222 and 224 (LH signal, HL signal and HH signal), respectively, by a combination of the DPCM and a zero run length encoded and variable length code. The outputs of the encoding circuits 228 - 232 are multiplexed by a multiplexing circuit 234. An encryption circuit 236 encrypts the output of the multiplexing circuit 234 by using the encryption key outputted from the encryption key output circuit 238 in accordance with the encryption technique of the DES standard described above.

[0056] The multiplexing circuit 240 multiplexes the output of the encoding circuit 226 and the output of the encryption circuit 236 and the output thereof is outputted to the transmission line by the output unit 242.

[0057] In the decoding apparatus shown in Fig. 10, the transmission data input unit 250 receives the transmission data from the transmission line and applies it to the separation circuit 252. The separation circuit 252 separates it into a portion related to the encoded data of the LL signal and a portion related to the other LH, HL and HH signals, and applies the former to the decoding circuit 254 and the latter to the decryption circuit 256. The decryption circuit 256 decrypts the encoded data of the LH, HL and HH signals by using the encryption key signal outputted from the encryption key output circuit 258. In order to correctly decrypt it, the encryption key should be same as that used for encoding the encryption key signal.

[0058] The separation circuit 260 separates the output of the decryption circuit 256 to the encoded data of the LH signal, the encoded data of the HL signal and the encoded data of the HH signal, which are applied to the decoding circuits 262, 264 and 266, respectively.

[0059] The decoding circuits 254, 262, 264 and 266 decode the encoded data inputted thereto, respectively. The output of the decoding circuit 254 is the LL signal. The SD D/A conversion circuit 268 converts the output of the decoding circuit 254 to an analog signal. The output of the SD D/A conversion circuit 268 is an analog video signal having the number of scan lines of 525 and the frame frequency of 30 Hz and it can be displayed as an image by an image display device of the ordinary resolution.

[0060] The reproduced LL signal and LH signal are combined at the vertical frequency by the band synthesization filters 270 and 272 and the number of pixels in the vertical direction is interpolated to two times. Similarly, the reproduced HL signal and HH signal are synthesized at the vertical frequency by the band synthesization filters 274 and 276 and the number of pixels in the vertical direction is interpolated to two times. The synthesized signals are combined at the horizontal frequency by the band synthesization filters 278 and 280 and the number of pixels in the horizontal direction is interpolated to two times.

[0061] By those synthesization processes, the digital high resolution video signal having the number of scan lines of 1,050 and the frame frequency of 30 Hz is reproduced. The HD D/A conversion circuit 282 converts the reproduced digital HD signal to an analog signal.

[0062] In the decoding apparatus shown in Fig. 10, in the no key state, the decryption circuit 256 outputs a quite unstable data pattern so that the output of the HD D/A conversion circuit 282 is also unstable and an unstable pattern such as a noise image is displayed on the screen of the display device such as CRT.

[0063] Alternatively, the image of the low resolution or a still image may be displayed on the high resolution monitor screen in the no key state. Figs. 12 and 13 show portions of block diagrams of such modified decoding apparatus. The like elements to those of Fig. 10 are designated by the like numerals.

[0064] In Fig. 12, an SD/HD conversion circuit 284 for converting the output of the decoding circuit 254 to the HD signal and a selection switch for selecting the output of the SD/HD conversion circuit 284 or the synthesized output by the band synthesization filters 278 and 280 and supplying it to the HD D/A conversion circuit 282 are provided. The SD/HD conversion circuit 284 is identical to the SD/HD conversion circuit 54 of Fig. 6. The switch 286 is normally connected to synthezied output of the band synthesization filters 278 and 280, and when no key state is detected by the decryption circuit, it is switched to the output of the SD/HD conversion circuit 284 by the detection output. Thus, in the no key state, the image can be displayed by the high resolution monitor although the quality of the image is not sufficient for the high resolution monitor.

[0065] When the encryption key signal may not be inputted to the decryption circuit 256', it may be possible that the output of the encryption key output circuit 258 is forcibly stopped or the encryption key output circuit 258 itself is not present.

[0066] For the configuration shown in Fig. 12, the high frequency data of the band synthesization filters 270-280 may be reset by the detection output of the decryption circuit 256' to attain the same effect.

[0067] In Fig. 13, a switch 282 is provided between the synthesized output by the band synthesization filters 278 and 280 and the HD D/A conversion circuit 282 so that in the no key state, a predetermined level is inputted to the HD D/A conversion circuit 282. The switch 288 normally selects the synthesized output by the band synthesization filters 278 and 280, and when the no key state is detected by the decryption circuit 256, it is switched to the predetermined level input by the detection output. In this manner, when the correct encryption key is present, the high resolution video signal is outputted, but in the no key state, the predetermined level signal is outputted and the image corresponding to the predetermined level is displayed on the monitor screen.

[0068] When the encryption key signal is not inputted to the decryption circuit 256', it may be possible that the output of the encryption key output circuit is forcibly stopped or the encryption key output circuit 258 itself is not present.

[0069] For the configuration shown in Fig. 13, the switch 288 may not be provided and the output of the HD D/A conversion circuit 282 may be forced to a constant level (for example, zero output) in accordance with the detection output of the no key state by the decryption circuit 44.

[0070] In Figs. 12 and 13, the no key state is detected by the decryption circuit 256 although it may be detected by an error detection code or error correction process.

[0071] Embodiments of the encoding circuit and the decoding circuit used in the respective embodiments are now explained.

[0072] Fig. 14 shows a block diagram of a specific embodiment of the encoding circuit.

[0073] The encoding circuit shown in Fig. 14 comprises a blocking circuit 301, a DCT circuit 302, a quantization circuit 303, a variable length encoding circuit (VLC) 304, a motion compensation circuit 305, a motion vector detection circuit 306, a rate control circuit 307, a local decoding circuit 308 and a buffer memory 309.

[0074] In Fig. 14, image data to be encoded is grouped into 8 x 8 pixel blocks by the block forming circuit 301 and they are supplied to the DCT (discrete cosine transform) circuit 302 through the switch 310.

[0075] The switch 310 is periodically (for example, for each frame or every several fields) switched to a terminal a to prevent erroneous propagation.

[0076] Namely, when it is connected to the terminal a, an intra-frame or intra-field encoding (intra mode) is conducted.

[0077] In the intra mode, it is DCT-transformed by the DCT circuit 302 and the resulting DCT coefficient is quantized by the quantization circuit 303 and further encoded by the variable length encoding circuit 304 and temporarily stored in the buffer 309.

[0078] On the other hand, in other than the intra mode, the switch 310 is connected to a terminal b to conduct the motion compensated prediction encoding.

[0079] Numerals 311 and 312 denote a de-quantization circuit and a de-DCT circuit which constitute the local decoding circuit 308. The data quantized by the quantization circuit 303 is restored to the original image data by the local decoding circuit 308.

[0080] Numeral 313 denotes an adder, numeral 314 denotes a switch which is closed in other than the intra mode, and numeral 316 denotes a subtractor.

[0081] The locally decoded image data refers the motion vector detected by the motion vector detection circuit 306 to output the corresponding block of the predetermined frame (preceding frame, succeeding frame or interpolated frame).

[0082] The output of the motion compensation circuit 305 is subtracted by the input image data by the subtractor 316 to produce a difference.

[0083] The difference is encoded by the DCT circuit 302, the quantization circuit 303 and the variable length encoding circuit 304 and it is stored in the buffer 309.

[0084] The motion vector detection circuit 306 compares the frame data to be encoded with the predetermined reference frame data to produce the motion vector, and the output of the motion vector detection circuit 306 is supplied to the motion compensation circuit 305 to specify the block to be outputted by the motion compensation circuit 305.

[0085] The rate control circuit 307 controls the quantity of encoding by switching the quantization step of the quantization circuit 303 in accordance with an occupation rate of the encoded data in the buffer 309.

[0086] Finally, the motion vector data detected by the motion vector detection circuit 306, an encoding identification code for identifying the intra mode and quantization step data indicating the quantization step are added by an adding circuit 315 and it is outputted as the encoded data.

[0087] Fig. 15 shows a specific block diagram of the decoding circuit.

[0088] The decoding circuit basically operates in the reverse manner to the encoding circuit shown in Fig. 14.

[0089] The decoding circuit shown in Fig. 15 comprises an input buffer memory 401, a variable length decoding circuit 402, a de-quantization circuit 403, a de-DCT circuit 404, a motion compensation circuit 405 and an output buffer memory 406.

[0090] The encoded data sequentially read from the input buffer memory 401 is processed by the variable length decoding circuit 402, the de-quantization circuit 403 and the de-DCT circuit 404 and converted to the space area data.

[0091] The quantization step of the de-quantization circuit 403 is determined by the quantization step data which is transmitted along with the encoded data.

[0092] Numeral 407 denotes an adder for adding the output of the de-DCT circuit 404 to the difference outputted from the motion compensation circuit 405, and numeral 408 denotes a switch for selecting the output of the de-DCT circuit 404 or the output of the adder 407.

[0093] The switch 408 is connected to the terminal a in the intra mode by the encoding identification code detected by the data detection circuit, not shown, and connected to the terminal b in other mode.

[0094] The decoded data is temporarily stored in the output buffer memory 406 and restored to the original space arrangement and outputted as one-frame or one-field image data.

[0095] As will be readily understood from the above description, in accordance with the present embodiment, the high resolution video signal is not reproduced for those who do not have the encryption key and the reproduction of only the low resolution video signal is permitted. The charges to the users may be discriminated between the display device of the low resolution and the display device of the high resolution of the same content.

[0096] The present invention may be implemented in other various forms.

[0097] For example, while the image signal is divided into four frequency bands in the second embodiment the present invention is not limited thereto.

[0098] In other words, the foregoing description of the embodiments has been given for illustrative purpose only and not to be construed as imposing limitation in every respect.

[0099] The scope of the invention is, therefore, to be determined solely by the following claims and not limited by the text of the specification and alterations made within the scope equivalent to the scope of the claims fall within the scope of the invention.

Claims

1. An image processing apparatus comprising:

   a) input means for inputting an image signal (210);
   b) separation means (214 to 224) for separating said image signal into a low frequency component and a high frequency component in each of horizontal and vertical directions and for producing spatial frequency bands (LL, LH, HL, HH) from said image signal,
   c) encoding means (226 to 232) for high-efficiency encoding the spatial frequency bands (LH, HL, HH) including a highest frequency component and for high-efficiency encoding the spatial frequency band (LL) including a lowest frequency component; and
   d) encryption means (236) for encrypting only the encoded spatial frequency bands including the highest frequency component using an encryption key in accordance with a predetermined encryption algorithm.

2. An apparatus according to claim 1, wherein said separation means is operable to produce a first spatial frequency band (LL) including the low frequency component of the horizontal direction and the low frequency component of the vertical direction, a second spatial frequency band (LH) including the low frequency component of the horizontal direction and the high frequency component of the vertical direction, a third spatial frequency band (HL) including the high frequency component of the horizontal direction and the low frequency component of the vertical direction, and a fourth spatial frequency band (HH) including the high frequency component of the horizontal direction and the high frequency component of the vertical direction.

3. An apparatus according to claim 1 or 2, wherein said encoding means is operable to encode the spatial frequency bands using variable length encoders.

4. An apparatus according to any of claims 1 to 3, fur-

ther comprising:

multiplexing means (234) for multiplexing the spatial frequency bands to be encrypted, and wherein said encryption means is operable to encrypt an output of said multiplexing means.

5. An apparatus according to any of claims 1 to 4, further comprising second multiplexing means (240) for multiplexing the encoded spatial frequency bands encrypted by said encryption means and the encoded spatial frequency band not encrypted by said encryption means.

6. An image processing apparatus comprising:

a) input means (250) for inputting spatial frequency bands (LH, HL, HH) including a highest frequency component and spatial frequency band (LL) including a lowest frequency component, the spatial frequency bands including the highest frequency component are encrypted;
b) decryption means (256 or 256') for decrypting the spatial frequency bands including the highest frequency component using a decryption key in accordance with a predetermined decryption algorithm; and
c) decoding means (254 to 266) for decoding the decrypted spatial frequency bands including the highest frequency component and for decoding the spatial frequency band including the lowest frequency component.

7. An apparatus according to claim 6, wherein said input means inputs a first spatial frequency band (LL) including the low frequency component of the horizontal direction and the low frequency component of the vertical direction, a second spatial frequency band (LH) including the low frequency component in the horizontal direction and the high frequency component in the vertical direction, a third spatial frequency band (HL) including the high frequency component of the horizontal direction and the low frequency component of the vertical direction and a fourth spatial frequency band (HH) including the high frequency component of the horizontal direction and the high frequency component in the vertical direction.

8. An apparatus according to any of claims 6 and 7, further comprising:

synthesizing means (270 to 280) for synthesizing the decrypted spatial frequency bands with other spatial frequency bands.

9. An apparatus according to any of claims 6 to 8, further comprising demultiplexing means (260) for demultiplexing the decrypted spatial frequency bands, and said decoding means is operable to decode an output of said demultiplexing means.

10. An apparatus according to any of claims 6 to 9, wherein said decoding means is operable to decode the spatial frequency bands using variable length decoders.

11. An apparatus according to any of claims 6 to 10, further comprising inhibiting means (286) operable to inhibit an output of said decryption means when said decryption means cannot decrypt the encrypted spatial frequency band.

12. An apparatus according to any of claims 6 to 11, further comprising means (288) for producing a predetermined signal in lieu of the encrypted spatial frequency band when said decryption means cannot decrypt the encrypted spatial frequency band.

13. An image processing method comprising:

a) an input step of inputting an image signal (210);
b) a separation step of separating said image signal into a low frequency component and a high frequency component in each of horizontal and vertical directions and of producing spatial frequency bands (LL, LH, HL, HH) from said image signal;
c) an encoding step of high-efficiency encoding the spatial frequency bands (LH, HL, HH) including a highest frequency component and of high-efficiency encoding the spatial frequency band (LL) including a lowest frequency component; and
d) an encryption step of encrypting only the encoded spatial frequency bands including the highest frequency component using an encryption key in accordance with a predetermined encryption algorithm.

14. A method as claimed in claim 13, wherein said separation step produces a first spatial frequency band (LL) including the low frequency component of the horizontal direction and the low frequency component of the vertical direction, a second spatial frequency band (LH) including the low frequency component of the horizontal direction and the high frequency component of the vertical direction, a third spatial frequency band (HL) including the high frequency component of the horizontal direction and the low frequency component of the vertical direction, and a fourth spatial frequency band (HH) including the high frequency component of the horizontal direction and the high frequency component of the vertical direction.

15. A method as claimed in any of claims 13 and 14 wherein said encoding step encode the spatial frequency bands using variable length encoders.

16. A method as claimed in any of claims 13 to 15, further comprising;

a multiplexing step of multiplexing the spatial frequency bands to be encrypted, and wherein said encryption step encrypts an output of said multiplexing step.

17. A method as claimed in any of claims 13 to 16, further comprising a second multiplexing step of multiplexing the encoded spatial frequency bands encrypted by said encryption step and the encoded spatial frequency band not encrypted by said encryption step.

18. An image processing method comprising:

a) an input step inputting spatial frequency bands (LH, HL, HH) including a highest frequency component and spatial frequency band (LL) including a lowest frequency component, the spatial frequency bands including the highest frequency component are encrypted;
b) a decryption step of decrypting the spatial frequency bands including the highest frequency component using a decryption key in accordance with a predetermined decryption algorithm; and
c) a decoding step of decoding the decrypted spatial frequency bands including the highest frequency component and of decoding the spatial frequency band including the lowest frequency component.

19. A method as claimed in claim 18, wherein said input step inputs a first spatial frequency band (LL) including the low frequency component of the horizontal direction and the low frequency component of the vertical direction, a second spatial frequency band (LH) including the low frequency component of the horizontal direction and the high frequency component of the vertical direction, a third spatial frequency band (HL) including the high frequency component of the horizontal direction and the low frequency component of the vertical direction and a fourth spatial frequency band (HH) including the high frequency component of the horizontal direction and the high frequency component of the vertical direction.

20. A method as claimed in any of claims 18 and 19, further comprising:

a synthesizing step of synthesizing the decrypted spatial frequency bands with other spatial frequency bands.

21. A method as claimed in any of claims 18 to 20, further comprising a demultiplexing step of demultiplexing the decrypted spatial frequency bands, and said decoding means is operable to decode an output of said demultiplexing means.

22. A method as claimed in any of claims 18 to 21, wherein said decoding means is operable to decode the spatial frequency bands using variable length decoders.

23. A method as claimed in any of claims 18 to 22, further comprising an inhibiting step of inhibiting an output of said decryption step when said decryption step cannot decrypt the encrypted spatial frequency band.

24. A method as claimed in any of claims 18 to 23, further comprising a step of producing a predetermined signal in lieu of the encrypted spatial frequency band when said decryption step cannot decrypt the encrypted spatial frequency band.

Patentansprüche

1. Vorrichtung zur Bildverarbeitung, mit

a) einem Eingabemittel zur Eingeben eines Bildsignals (210);
b) einem Trennmittel (214 bis 224) zum Trennen des Bildsignals in eine niederfrequente Komponente und in eine hochfrequente Komponente sowohl in Horizontal- als auch in Vertikalrichtung, um aus dem Bildsignal ein Ortsfrequenzband (LL, LH, HL, HH) zu erzeugen;
c) einem Codiermittel (226 bis 232) zum hocheffizienten Codieren der eine Höchstfrequenzkomponente enthaltenden Ortsfrequenzbänder (LH, HL, HH) und des eine Niedrigstfrequenzkomponente enthaltenden Ortsfrequenzbandes (LL); und mit
d) einem Verschlüsselungsmittel (236) zum Verschlüsseln nur der die Höchstfrequenzkomponente enthaltenden codierten Ortsfrequenzbänder unter Verwendung eines Schlüssels gemäß einem vorbestimmten Verschlüsselungsalgorithmus.

2. Vorrichtung nach Anspruch 1, bei der das Trennmittel betriebsbereit ist zum Erzeugen eines ersten Ortsfrequenzbandes (LL) mit der Niederfrequenzkomponente der Horizontalrichtung unter der Niederfrequenzkomponente der Vertikalrichtung, eines zweiten Ortsfrequenzbandes (LH) mit der Nie-

derfrequenzkomponente der Horizontalrichtung und der Hochfrequenzkomponente der Vertikalrichtung, eines dritten Ortsfrequenzbandes (HL) mit der Hochfrequenzkomponente der Horizontalrichtung und der Niederfrequenzkomponente der Vertikalrichtung, und zum Erzeugen eines vierten Ortsfrequenzbandes (HH) mit der Hochfrequenzkomponente der Horizontalrichtung und der Hochfrequenzkomponente der Vertikalrichtung.

3. Vorrichtung nach Anspruch 1 oder 2, bei der das Codiermittel betriebsbereit ist, die Ortsfrequenzbänder unter Verwendung eines längenvariabel codierenden Codierers zu codieren.

4. Vorrichtung nach einem der Ansprüche 1 bis 3, die des weiteren ausgestattet ist mit:

   einem Multiplexmittel (234) zum Multiplexieren der zu verschlüsselnden Ortsfrequenzbänder,

   wobei das Verschlüsselungsmittel betriebsbereit ist, ein Ausgangssignal des Multiplexmittels zu verschlüsseln.

5. Vorrichtung nach einem der Ansprüche 1 bis 4, die des weiteren über ein zweites Multiplexmittel (240) verfügt, um die vom Verschlüsselungsmittel verschlüsselten codierten Ortsfrequenzbänder und das nicht vom Verschlüsselungsmittel verschlüsselte codierte Ortsfrequenzband zu multiplexieren.

6. Vorrichtung zur Bildverarbeitung, mit:

   a) einem Eingabemittel (25) zur Eingabe von Ortsfrequenzbändern (LH, HL, HH) mit einer Höchstfrequenzkomponente und einem Ortsfrequenzband (LL) mit einer Niedrigstfrequenzkomponente, wobei die die Höchstfrequenzkomponente enthaltenden Ortsfrequenzbänder verschlüsselt sind;
   b) einem Verschlüsselungsmittel (256 oder 256') zum Verschlüsseln der Ortsfrequenzbänder, die die Höchstfrequenzkomponente enthalten, unter Verwendung eines Schlüssels gemäß einem vorbestimmten Verschlüsselungsalgorithmus; und mit
   c) einem Codiermittel (254 bis 266) zum Decodieren der verschlüsselten Ortsfrequenzbänder, die die Höchstfrequenzkomponente enthalten, und zum Decodieren des Ortsfrequenzbandes, das die Niedrigstfrequenzkomponente enthält.

7. Vorrichtung nach Anspruch 6, bei der das Eingabemittel ein erstes Ortsfrequenzband (LL), das die Niederfrequenzkomponente der Horizontalrichtung und die Niederfrequenzkomponente der Vertikalrichtung enthält, ein zweites Ortsfrequenzband (LH), das die Niederfrequenzkomponente in Horizontalrichtung und die Hochfrequenzkomponente in Vertikalrichtung enthält, ein drittes Ortsfrequenzband (HL), das die Hochfrequenzkomponente der Horizontalrichtung und die Niederfrequenzkomponente der Vertikalrichtung enthält, und ein viertes Ortsfrequenzband (HH) eingibt, das die Hochfrequenzkomponente der Horizontalrichtung und die Hochfrequenzkomponente der Vertikalrichtung enthält.

8. Vorrichtung nach einem der der Ansprüche 6 bis 8, die des weiteren ausgestattet ist mit:

   einem Synthetisiermittel (270 bis 280) zum Zusammensetzen der entschlüsselten Ortsfrequenzbänder mit anderen Ortsfrequenzbändern.

9. Vorrichtung nach einem der Ansprüche 6 bis 8, die des weiteren über ein Demultiplexmittel (260) verfügt, um die verschlüsselten Ortsfrequenzbänder zu demultiplexieren, und wobei das Decodiermittel betriebsbereit ist, ein Ausgangssignal vom Demultiplexmittel zu decodieren.

10. Vorrichtung nach einem der Ansprüche 6 bis 9, bei der das Decodiermittel betriebsbereit ist, die Ortsfrequenzbänder unter Verwendung von längenvariabel decodierenden Decodierern zu decodieren.

11. Vorrichtung nach einem der Ansprüche 6 bis 10, die des weiteren über ein Sperrmittel (286) verfügt, das betriebsbereit ist zum Sperren eines Ausgangssignals vom Entschlüsselungsmittel, wenn das Entschlüsselungsmittel das verschlüsselte Ortsfrequenzband nicht entschlüsseln kann.

12. Vorrichtung nach einem der Ansprüche 6 bis 11, mit einem weiteren Mittel (286) zum Erzeugen eines vorbestimmten Signals anstelle des verschlüsselten Ortsfrequenzbandes, wenn das Verschlüsselungsmittel das verschlüsselte Ortsfrequenzband nicht entschlüsseln kann.

13. Verfahren zur Bildverarbeitung, mit den Verfahrensschritten:

   a) Eingeben eines Bildsignals (210);
   b) Trennen des Bildsignals in eine Niederfrequenzkomponente und eine Hochfrequenzkomponente jeweils in Horizontal- und Vertikalrichtung und Erzeugen von Ortsfrequenzbändern (LL, LH, HL, HH) aus dem Bildsignal;
   c) hocheffizientes Codieren der Ortsfrequenzbänder (LH, HL, HH), die eine Höchstfrequenzkomponente enthalten, und des Ortsfrequenz-

bandes (LL), das eine Niedrigstfrequenzkomponente enthält; und

d) Verschlüsseln nur der codierten Ortfrequenzbänder, die die Hochstfrequenzkomponente enthalten, unter Verwendung eines Schlüssels gemäß einem vorbestimmten Verschlüsselungsalgorithmus.

14. Verfahren nach Anspruch 13, bei dem der Verfahrensschritt des Trennens ein erstes Ortsfrequenzband (LL), das die Niederfrequenzkomponente der Horizontalrichtung und die Niederfrequenzkomponente der Vertikalrichtung enthält, ein zweites Ortsfrequenzband (LH), das die Niederfrequenzkomponente der Horizontalrichtung und die Hochfrequenzkomponente der Vertikalrichtung enthält, ein drittes Ortsfrequenzband (HL), das die Hochfrequenzkomponente der Horizontalrichtung und die Niederfrequenzkomponente der Vertikalrichtung enthält, und ein viertes Ortsfrequenzband (HH) erzeugt, das die Hochfrequenzkomponente der Horizontalrichtung und die Hochfrequenzkomponente der Vertikalrichtung enthält.

15. Verfahren nach einem der Ansprüche 13 und 14, bei dem der Verfahrensschritt des Codierens die Ortsfrequenzbänder unter Verwendung eines längenvariabel codierenden Codierers codiert.

16. Verfahren nach einem der Ansprüche 13 bis 15, mit den weiteren Verfahrensschritten:

Multiplexieren der zu verschlüsselnden Ortsfrequenzbänder und

wobei der Verfahrensschritt des Verschlüsselns ein beim Multiplexieren abgegebenes Signal verschlüsselt.

17. Verfahren nach einem der Ansprüche 13 bis 16, mit dem weiteren Verfahrensschritt eines zweiten Multiplexierens der im Verfahrensschritt des Verschlüsselns verschlüsselten codierten Ortsfrequenzbänder und dem im Verfahrensschritt des Verschlüsselns nicht verschlüsselten codierten Ortsfrequenzband.

18. Verfahren zur Bildverarbeitung, mit den Verfahrensschritten:

a) Eingeben von eine Höchstfrequenzkomponente enthaltende Ortsfrequenzbändern (LH, HL, HH) und von einem eine Niedrigstfrequenzkomponente enthaltenden Ortsfrequenzband (LL), wobei die die Hochstfrequenzkomponente enthaltende Ortsfrequenzbänder verschlüsselt sind;

b) Entschlüsseln der Ortsfrequenzbänder, die die Höchstfrequenzkomponente enthalten, unter Verwendung eines Schlüssels gemäß einem vorbestimmten Entschlüsselungsalgorithmus; und

c) Decodieren der die Höchstfrequenzkomponente enthaltenden verschlüsselten Ortsfrequenzbänder und des die Niedrigstfrequenzkomponente enthaltenden Ortsfrequenzbandes.

19. Verfahren nach Anspruch 18, bei dem der Verfahrensschritt des Eingebens folgende Eingaben umfaßt: ein erstes Ortsfrequenzband (LL), das die Niederfrequenzkomponente der Horizontalrichtung und die Niederfrequenzkomponente der Vertikalrichtung enthält, ein zweites Ortsfrequenzband (LH), das die Niederfrequenzkomponente der Horizontalrichtung und die Hochfrequenzkomponente der Vertikalrichtung enthält, ein drittes Ortsfrequenzband (HL), das die Hochfrequenzkomponente der Vertikalrichtung und die Niederfrequenzkomponente der Vertikalrichtung enthält, und ein viertes Ortsfrequenzband (HH), das die Hochfrequenzkomponente der Horizontalrichtung und die Hochfrequenzkomponente der Vertikalrichtung enthält.

20. Verfahren nach einem der Ansprüche 18 und 19, mit dem weiteren Verfahrensschritt:

Synthetisieren der entschlüsselten Ortsfrequenzbänder mit anderen Ortsfrequenzbändern.

21. Verfahren nach einem der Ansprüche 18 bis 20, mit den weiteren Verfahrensschritt des Demultiplexierens der entschlüsselten Ortsfrequenzbänder, wobei das Decodiermittel betriebsbereit ist, das Ausgangssignal vom Demultiplexer zu decodieren.

22. Verfahren nach einem der Ansprüche 18 bis 21, bei dem das Decodiermittel betriebsbereit ist, die Ortsfrequenzbänder mit längenvariabel decodierenden Codierern zu decodieren.

23. Verfahren nach einem der Ansprüche 18 bis 22, mit dem weiteren Verfahrensschritt des Sperrens eines beim Entschlüsseln ausgegebenen Signals, wenn der Verfahrensschritt des Entschlüsselns das verschlüsselte Ortsfrequenzband nicht entschlüsseln kann.

24. Verfahren nach einem der Ansprüche 18 bis 23, mit dem weiteren Verfahrensschritt des Erzeugens eines vorbestimmten Signals anstelle des verschlüsselten Ortsfrequenzbandes, wenn der Verfahrensschritt des Entschlüsselns das verschlüsselte Ortsfrequenzband nicht entschlüsseln kann.

Revendications

1. Appareil de traitement d'image, comprenant :

a) un moyen d'entrée pour introduction d'un signal (210) d'image ;
b) un moyen (214 à 224) de séparation pour séparer ledit signal d'image en une composante basse fréquence et une composante haute fréquence dans chacune de directions horizontale et verticale et pour produire des bandes (LL, LH, HL, HH) de fréquence spatiale à partir dudit signal d'image ;
c) un moyen (226 à 232) de codage pour un codage de grande efficacité des bandes (LH, HL, HH) de fréquence spatiale comportant une composante de fréquence supérieure et pour un codage de grande efficacité de la bande (LL) de fréquence spatiale comportant une composante de fréquence inférieure ; et
d) un moyen (236) de cryptage pour crypter uniquement les bandes codées de fréquence spatiale comportant la composante de fréquence supérieure en utilisant une clé de cryptage en fonction d'un algorithme prédéterminé de cryptage.

2. Appareil selon la revendication 1, dans lequel ledit moyen de séparation peut fonctionner pour produire une première bande (LL) de fréquence spatiale comportant la composante basse fréquence de la direction horizontale et la composante basse fréquence de la direction verticale, une deuxième bande (LH) de fréquence spatiale comportant la composante basse fréquence de la direction horizontale et la composante haute fréquence de la direction verticale, une troisième bande (HL) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante basse fréquence de la direction verticale, et une quatrième bande (HH) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante haute fréquence de la direction verticale.

3. Appareil selon la revendication 1 ou 2, dans lequel ledit moyen de codage peut fonctionner pour coder les bandes de fréquence spatiale en utilisant des codeurs de longueur variable.

4. Appareil selon l'une quelconque des revendications 1 à 3, comprenant en outre :

un moyen (234) de multiplexage pour multiplexer les bandes de fréquence spatiale à crypter,
et dans lequel ledit moyen de cryptage peut fonctionner pour crypter une sortie dudit moyen de multiplexage.

5. Appareil selon l'une quelconque des revendications 1 à 4, comprenant en outre un deuxième moyen (240) de multiplexage pour multiplexer les bandes codées de fréquence spatiale cryptées par ledit moyen de cryptage et la bande codée de fréquence spatiale non cryptée par ledit moyen de cryptage.

6. Appareil de traitement d'image, comprenant :

a) un moyen (250) d'entrée pour introduction de bandes (LH, HL, HH) de fréquence spatiale comportant une composante de fréquence supérieure et une bande (LL) de fréquence spatiale comportant une composante de fréquence inférieure, les bandes de fréquence spatiale comportant la composante de fréquence supérieure étant cryptées ;
b) un moyen (256 ou 256') de décryptage pour décrypter les bandes de fréquence spatiale comportant la composante de fréquence supérieure en utilisant une clé de décryptage en fonction d'un algorithme prédéterminé de décryptage ; et
c) un moyen (254 à 266) de décodage pour décoder les bandes décryptées de fréquence spatiale comportant la composante de fréquence supérieure et pour décoder la bande de fréquence spatiale comportant la composante de fréquence inférieure.

7. Appareil selon la revendication 6, dans lequel ledit moyen d'entrée introduit une première bande (LL) de fréquence spatiale comportant la composante basse fréquence de la direction horizontale et la composante basse fréquence de la direction verticale, une deuxième bande (LH) de fréquence spatiale comportant la composante basse fréquence dans la direction horizontale et la composante haute fréquence dans la direction verticale, une troisième bande (HL) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante basse fréquence de la direction verticale et une quatrième bande (HH) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante haute fréquence dans la direction verticale.

8. Appareil selon l'une quelconque des revendications 6 et 7, comprenant en outre :

un moyen (270 à 280) de synthèse pour synthétiser les bandes décryptées de fréquence spatiale avec d'autres bandes de fréquence spatiale.

9. Appareil selon l'une quelconque des revendications

6 à 8, comprenant en outre un moyen (260) de démultiplexage pour démultiplexer les bandes décryptées de fréquence spatiale, et ledit moyen de décodage pouvant fonctionner pour décoder une sortie dudit moyen de démultiplexage.

10. Appareil selon l'une quelconque des revendications 6 à 9, dans lequel ledit moyen de décodage peut fonctionner pour décoder les bandes de fréquence spatiale en utilisant des décodeurs de longueur variable.

11. Appareil selon l'une quelconque des revendications 6 à 10, comprenant en outre un moyen (286) d'invalidation pouvant fonctionner pour invalider une sortie dudit moyen de décryptage lorsque ledit moyen de décryptage ne peut pas décrypter la bande cryptée de fréquence spatiale.

12. Appareil selon l'une quelconque des revendications 6 à 11, comprenant en outre un moyen (288) pour produire un signal prédéterminé au lieu de la bande cryptée de fréquence spatiale lorsque ledit moyen de décryptage ne peut pas décrypter la bande cryptée de fréquence spatiale.

13. Procédé de traitement d'image, comprenant :

a) une étape d'entrée, d'introduction d'un signal (210) d'image ;
b) une étape de séparation, de séparation dudit signal d'image en une composante basse fréquence et une composante haute fréquence dans chacune de directions horizontale et verticale et de production de bandes (LL, LH, HL, HH) de fréquence spatiale à partir dudit signal d'image ;
c) une étape de codage, de codage de grande efficacité des bandes (LH, HL, HH) de fréquence spatiale comportant une composante de fréquence supérieure et de codage de grande efficacité de la bande (LL) de fréquence spatiale comportant une composante de fréquence inférieure ; et
d) une étape de cryptage, de cryptage uniquement des bandes codées de fréquence spatiale comportant la composante de fréquence supérieure en utilisant une clé de cryptage en fonction d'un algorithme prédéterminé de cryptage.

14. Procédé selon la revendication 13, dans lequel ladite étape de séparation produit une première bande (LL) de fréquence spatiale comportant la composante basse fréquence de la direction horizontale et la composante basse fréquence de la direction verticale, une deuxième bande (LH) de fréquence spatiale comportant la composante basse fréquence de la direction horizontale et la composante haute fréquence de la direction verticale, une troisième bande (HL) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante basse fréquence de la direction verticale, et une quatrième bande (HH) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante haute fréquence de la direction verticale.

15. Procédé selon l'une quelconque des revendications 13 et 14, dans lequel ladite étape de codage code les bandes de fréquence spatiale en utilisant des codeurs de longueur variable.

16. Procédé selon l'une quelconque des revendications 13 à 15, comprenant en outre :

une étape de multiplexage, de multiplexage des bandes de fréquence spatiale à crypter, et dans lequel ladite étape de cryptage crypte une sortie de ladite étape de multiplexage.

17. Procédé selon l'une quelconque des revendications 13 à 16, comprenant en outre une deuxième étape de multiplexage, de multiplexage des bandes codées de fréquence spatiale cryptées par ladite étape de cryptage et de la bande codée de fréquence spatiale non cryptée par ladite étape de cryptage.

18. Procédé de traitement d'image, comprenant :

a) une étape d'entrée introduisant des bandes (LH, HL, HH) de fréquence spatiale comportant une composante de fréquence supérieure et une bande (LL) de fréquence spatiale comportant la composante de fréquence inférieure, les bandes de fréquence spatiale comportant la composante de fréquence supérieure étant cryptées ;
b) une étape de décryptage, de décryptage des bandes de fréquence spatiale comportant la composante de fréquence supérieure en utilisant une clé de décryptage en fonction d'un algorithme prédéterminé de décryptage ; et
c) une étape de décodage, de décodage des bandes décryptées de fréquence spatiale comportant la composante de fréquence supérieure et de décodage de la bande de fréquence spatiale comportant la composante de fréquence inférieure.

19. Procédé selon la revendication 18, dans lequel ladite étape d'entrée introduit une première bande (LL) de fréquence spatiale comportant la composante basse fréquence de la direction horizontale et la composante basse fréquence de la direction verticale, une deuxième bande (LH) de fréquence spatiale comportant la composante basse fréquen-

ce de la direction horizontale et la composante haute fréquence de la direction verticale, une troisième bande (HL) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante basse fréquence de la direction verticale et une quatrième bande (HH) de fréquence spatiale comportant la composante haute fréquence de la direction horizontale et la composante haute fréquence de la direction verticale.

20. Procédé selon l'une quelconque des revendications 16 et 19, comprenant en outre :

> une étape de synthèse, de synthèse des bandes décryptées de fréquence spatiale avec d'autres bandes de fréquence spatiale.

21. Procédé selon l'une quelconque des revendications 18 à 20, comprenant en outre une étape de démultiplexage, de démultiplexage des bandes décryptées de fréquence spatiale, et ledit moyen de décodage peut fonctionner pour décoder une sortie dudit moyen de démultiplexage.

22. Procédé selon l'une quelconque des revendications 18 à 21, dans lequel ledit moyen de décodage peut fonctionner pour décoder les bandes de fréquence spatiale en utilisant des décodeurs de longueur variable.

23. Procédé selon l'une quelconque des revendications 18 à 22, comprenant en outre une étape d'invalidation, d'invalidation d'une sortie de ladite étape de décryptage lorsque ladite étape de décryptage ne peut pas décrypter la bande cryptée de fréquence spatiale.

24. Procédé selon l'une quelconque des revendications 18 à 23, comprenant en outre une étape de production d'un signal prédéterminé au lieu de la bande cryptée de fréquence spatiale lorsque ladite étape de décryptage ne peut pas décrypter la bande cryptée de fréquence spatiale.

FIG. 1

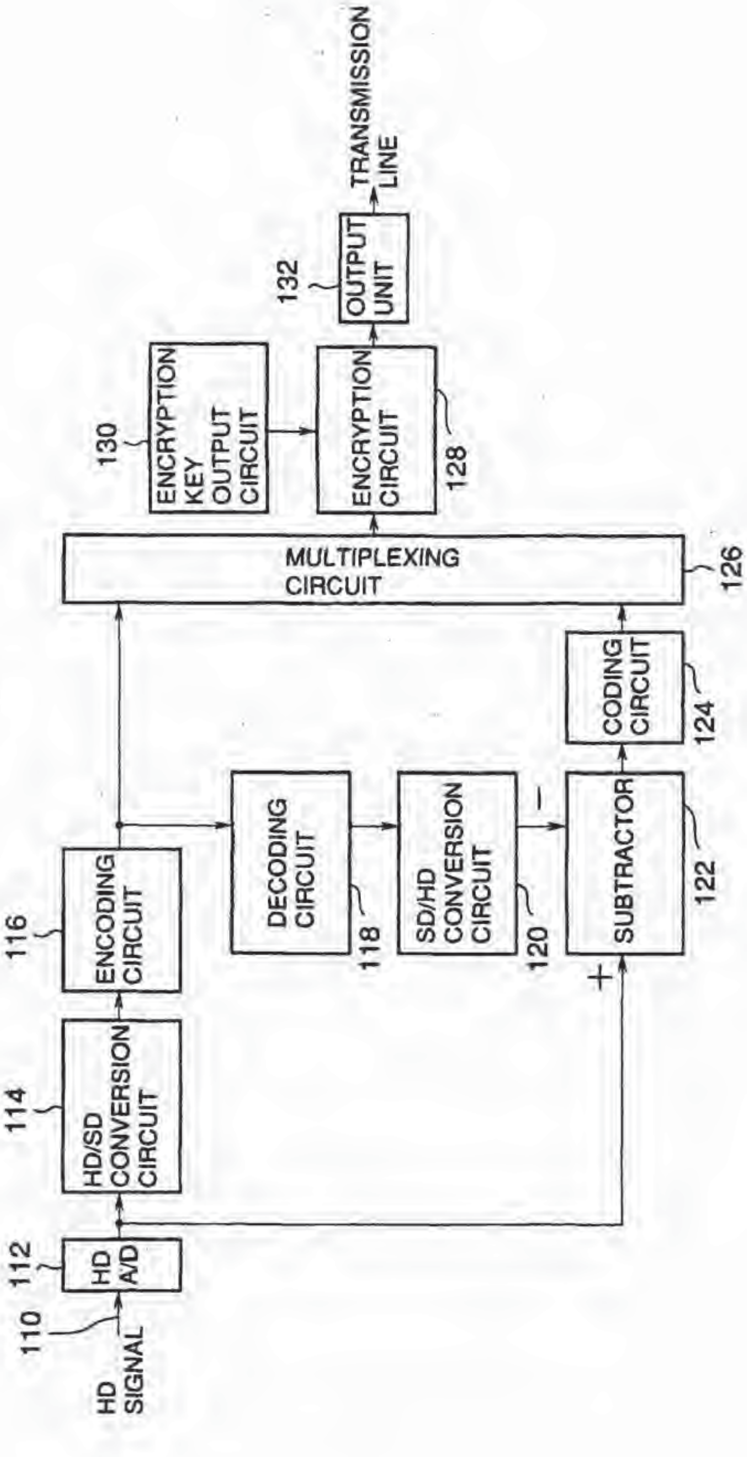

HD SIGNAL
110
112
HD A/D
114
HD/SD CONVERSION CIRCUIT
116
ENCODING CIRCUIT
DECODING CIRCUIT
118
SD/HD CONVERSION CIRCUIT
120
+
−
SUBTRACTOR
122
CODING CIRCUIT
124
MULTIPLEXING CIRCUIT
126
130
ENCRYPTION KEY OUTPUT CIRCUIT
ENCRYPTION CIRCUIT
128
132
OUTPUT UNIT
TRANSMISSION LINE

FIG. 2

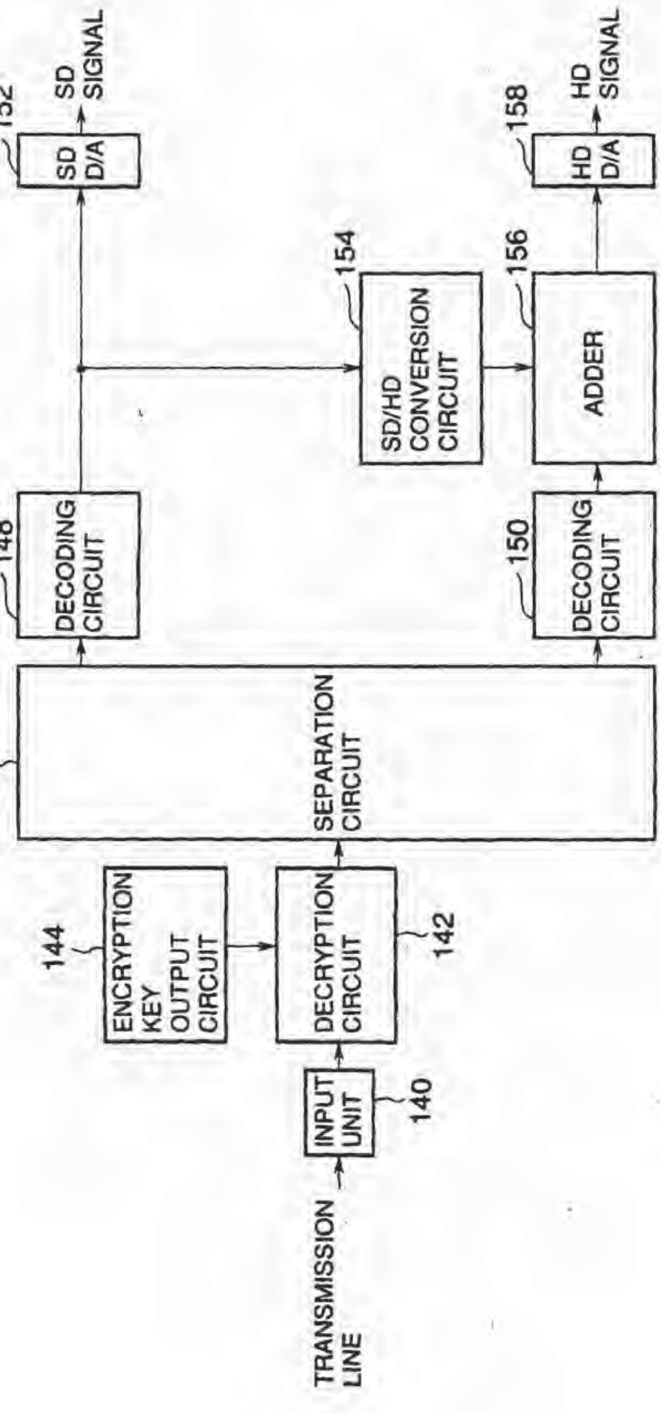

TRANSMISSION LINE
INPUT UNIT
140
ENCRYPTION KEY OUTPUT CIRCUIT
144
DECRYPTION CIRCUIT
142
SEPARATION CIRCUIT
146
DECODING CIRCUIT
148
DECODING CIRCUIT
150
SD/HD CONVERSION CIRCUIT
154
ADDER
156
SD D/A
152
SD SIGNAL
HD D/A
158
HD SIGNAL

FIG. 3

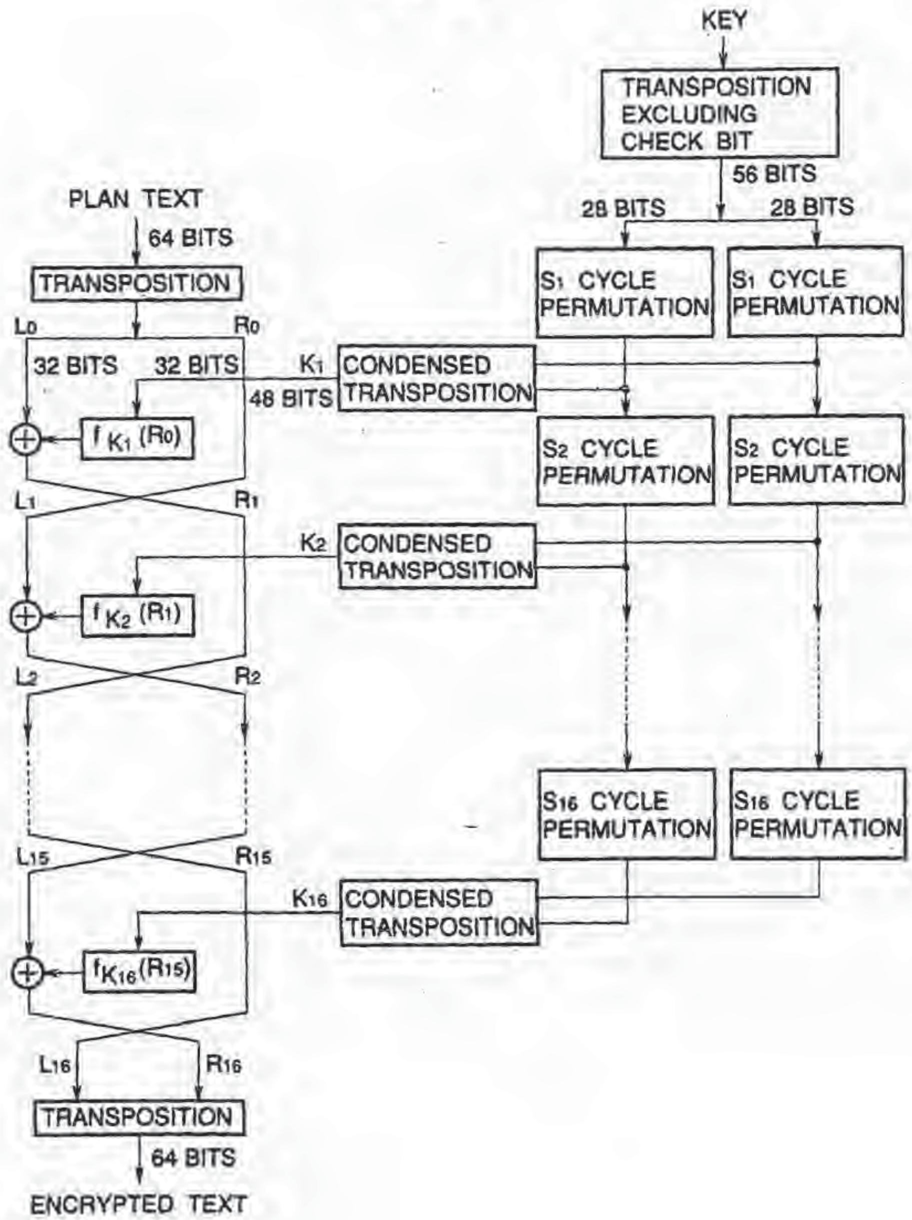

KEY
TRANSPOSITION EXCLUDING CHECK BIT
56 BITS
28 BITS
28 BITS
PLAN TEXT
64 BITS
TRANSPOSITION
L0
R0
32 BITS
32 BITS
S1 CYCLE PERMUTATION
S1 CYCLE PERMUTATION
K1
CONDENSED TRANSPOSITION
48 BITS
f K1 (R0)
S2 CYCLE PERMUTATION
S2 CYCLE PERMUTATION
L1
R1
K2
CONDENSED TRANSPOSITION
f K2 (R1)
L2
R2
S16 CYCLE PERMUTATION
S16 CYCLE PERMUTATION
L15
R15
K16
CONDENSED TRANSPOSITION
fK16(R15)
L16
R16
TRANSPOSITION
64 BITS
ENCRYPTED TEXT

FIG. 4

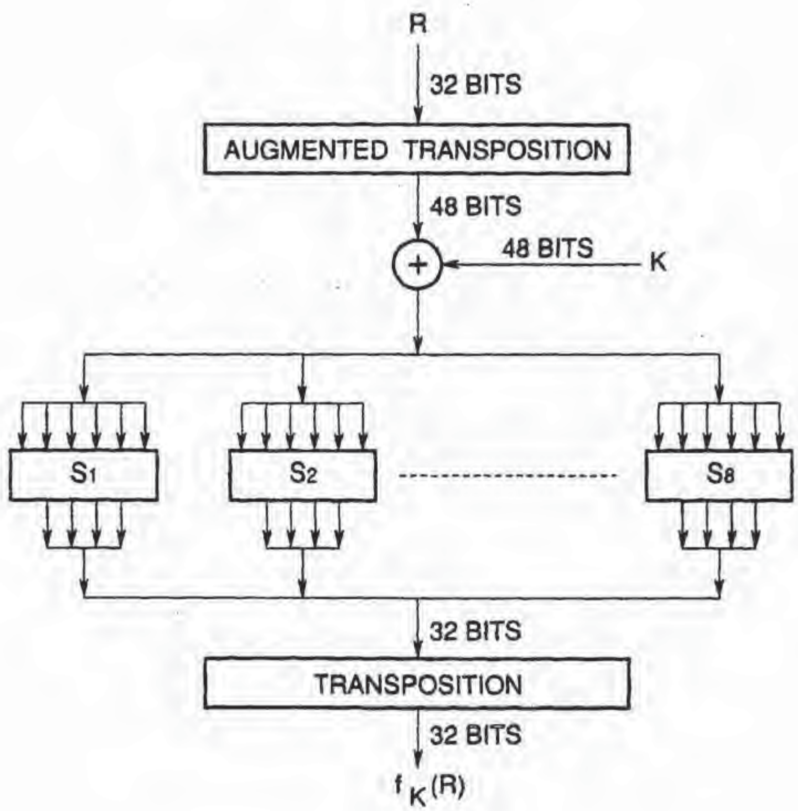

R
32 BITS
AUGMENTED TRANSPOSITION
48 BITS
48 BITS
K
S1
S2
S8
32 BITS
TRANSPOSITION
32 BITS
f K(R)

FIG. 5

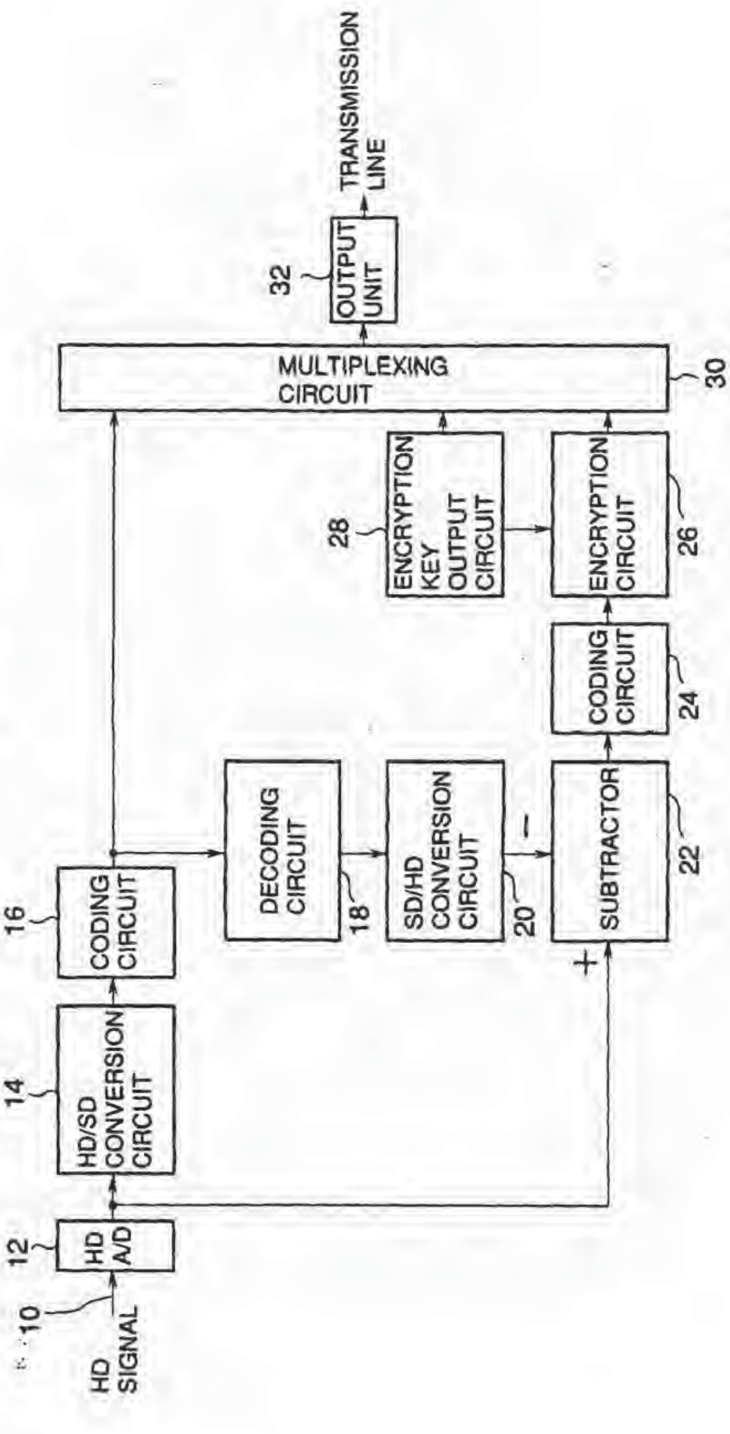

HD SIGNAL
10
12
HD A/D
14
HD/SD CONVERSION CIRCUIT
16
CODING CIRCUIT
DECODING CIRCUIT
18
SD/HD CONVERSION CIRCUIT
20
SUBTRACTOR
22
+
−
CODING CIRCUIT
24
ENCRYPTION CIRCUIT
26
28
ENCRYPTION KEY OUTPUT CIRCUIT
MULTIPLEXING CIRCUIT
30
32
OUTPUT UNIT
TRANSMISSION LINE

FIG. 6

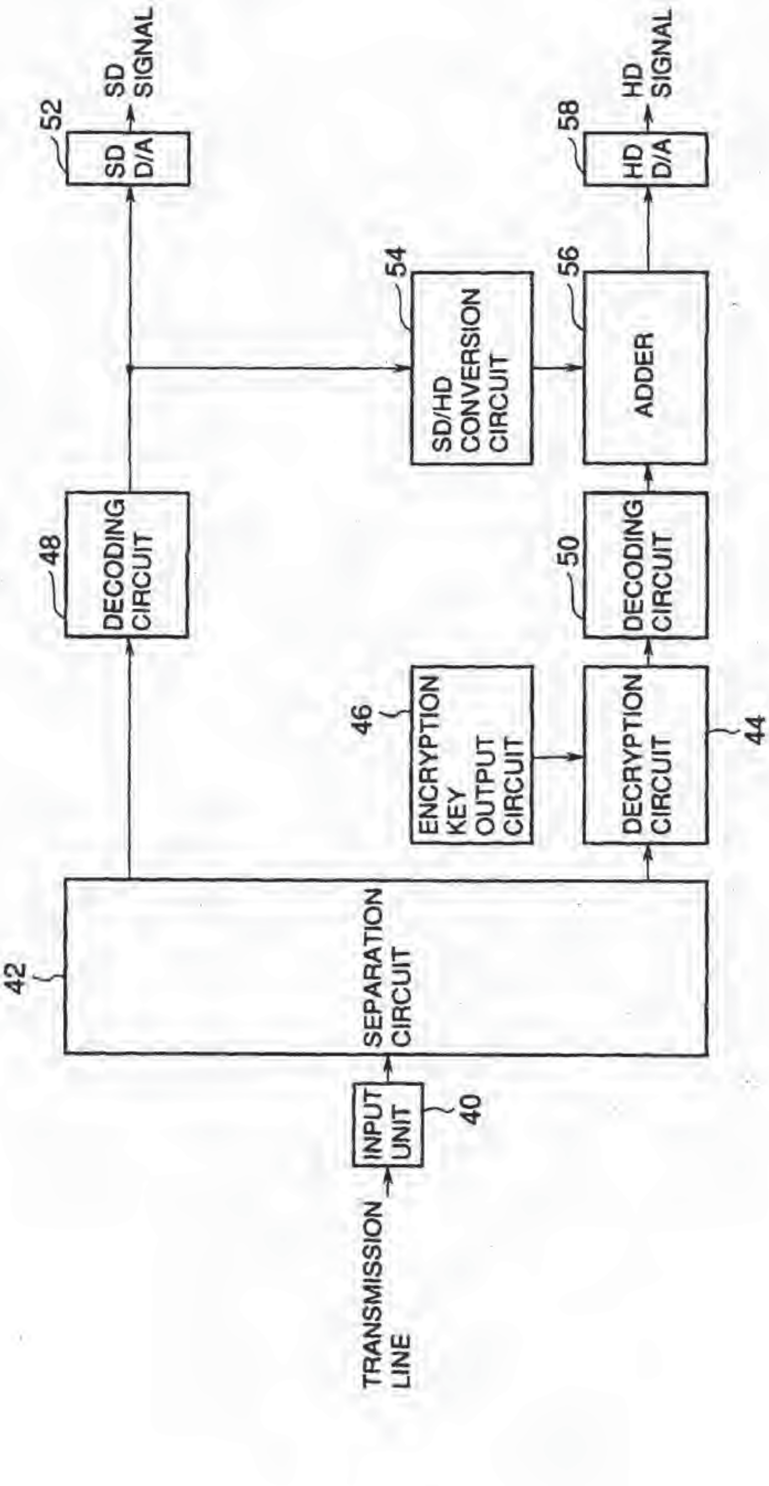

TRANSMISSION LINE
INPUT UNIT
40
SEPARATION CIRCUIT
42
DECODING CIRCUIT
48
SD D/A
52
SD SIGNAL
ENCRYPTION KEY OUTPUT CIRCUIT
46
DECRYPTION CIRCUIT
44
DECODING CIRCUIT
50
SD/HD CONVERSION CIRCUIT
54
ADDER
56
HD D/A
58
HD SIGNAL

FIG. 7

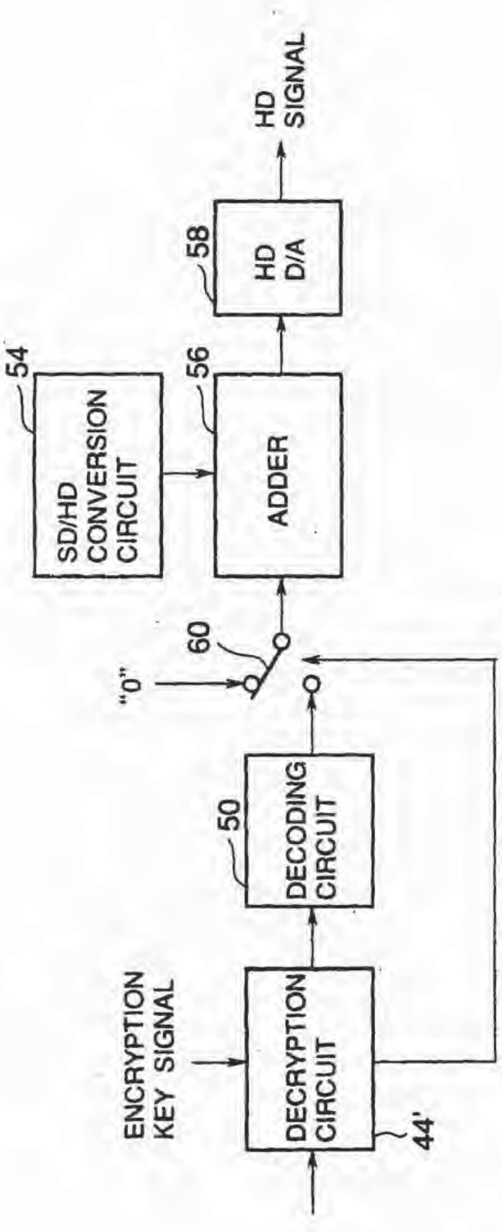

ENCRYPTION KEY SIGNAL
DECRYPTION CIRCUIT
44'
50
DECODING CIRCUIT
"0"
60
54
SD/HD CONVERSION CIRCUIT
56
ADDER
58
HD D/A
HD SIGNAL

FIG. 8

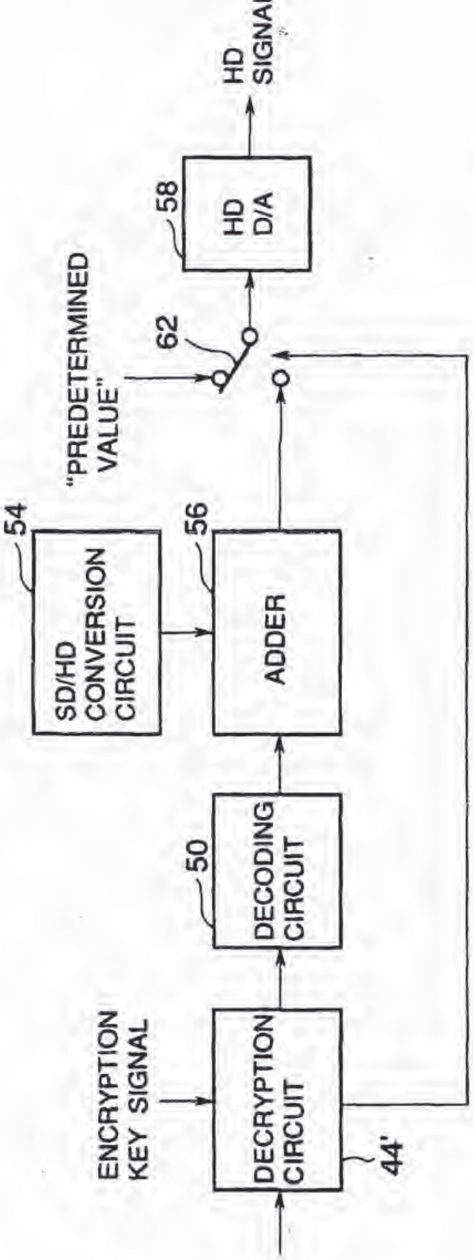

ENCRYPTION KEY SIGNAL
DECRYPTION CIRCUIT
44'
50
DECODING CIRCUIT
54
SD/HD CONVERSION CIRCUIT
56
ADDER
"PREDETERMINED VALUE"
62
58
HD D/A
HD SIGNAL

FIG. 9

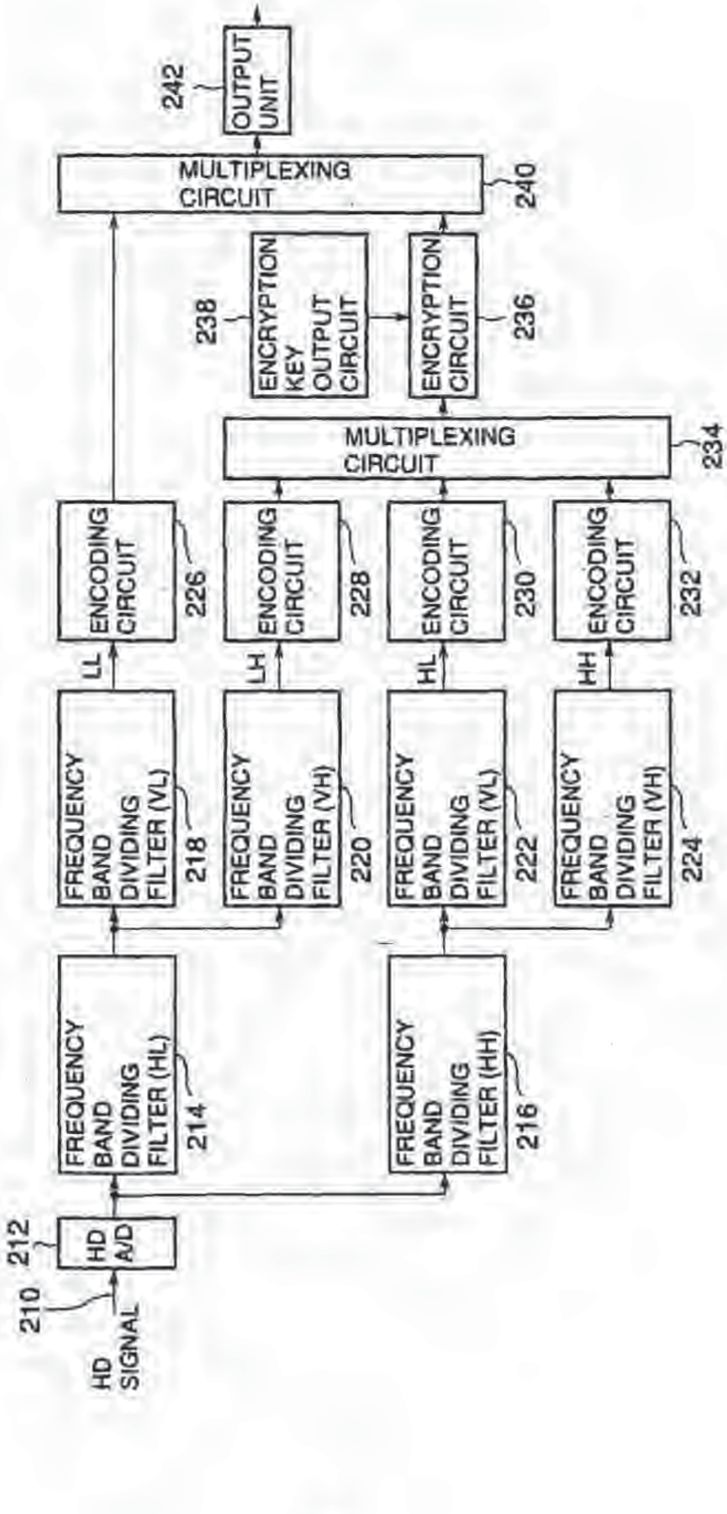

HD SIGNAL
210
212
HD A/D
FREQUENCY BAND DIVIDING FILTER (HL)
214
FREQUENCY BAND DIVIDING FILTER (HH)
216
FREQUENCY BAND DIVIDING FILTER (VL)
218
FREQUENCY BAND DIVIDING FILTER (VH)
220
FREQUENCY BAND DIVIDING FILTER (VL)
222
FREQUENCY BAND DIVIDING FILTER (VH)
224
LL
LH
HL
HH
ENCODING CIRCUIT
226
ENCODING CIRCUIT
228
ENCODING CIRCUIT
230
ENCODING CIRCUIT
232
MULTIPLEXING CIRCUIT
234
ENCRYPTION CIRCUIT
236
ENCRYPTION KEY OUTPUT CIRCUIT
238
MULTIPLEXING CIRCUIT
240
OUTPUT UNIT
242

FIG. 10

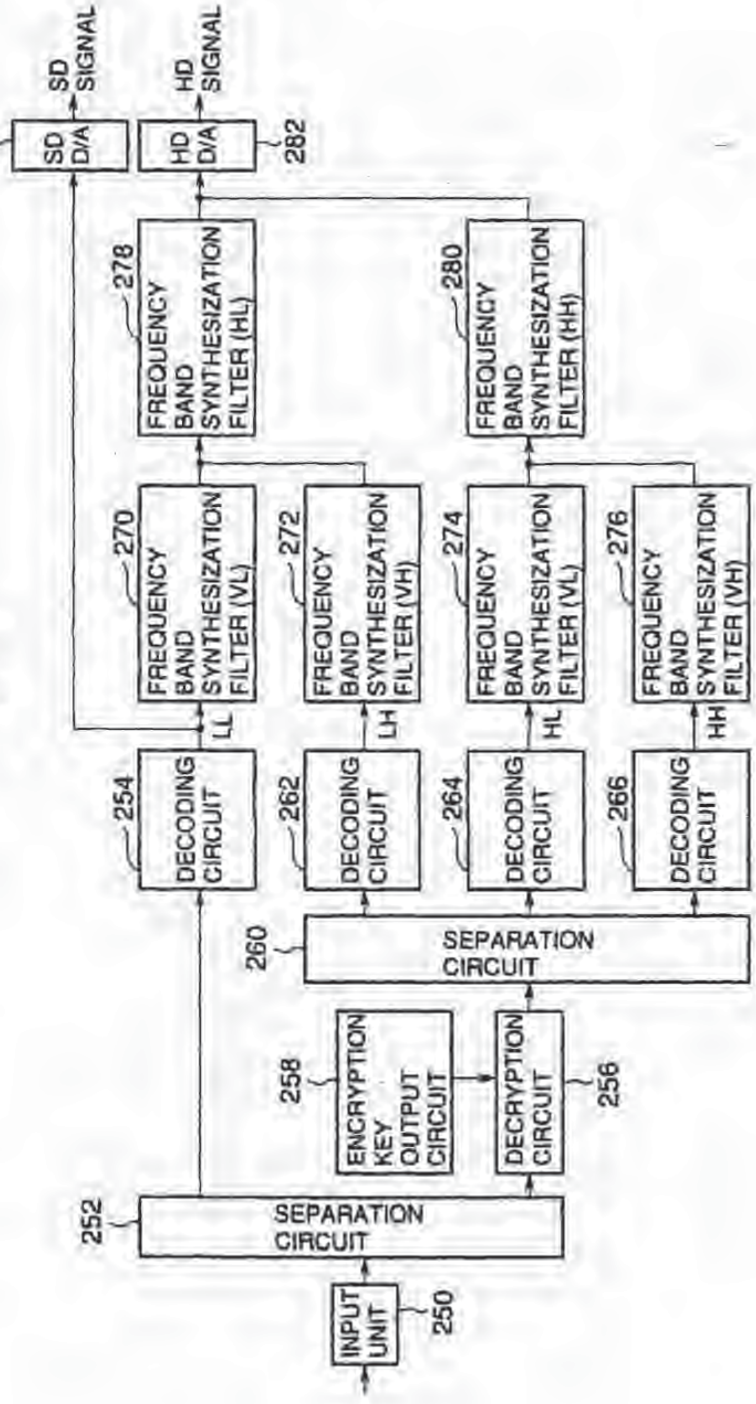

INPUT UNIT
250
SEPARATION CIRCUIT
252
ENCRYPTION KEY OUTPUT CIRCUIT
258
DECRYPTION CIRCUIT
256
SEPARATION CIRCUIT
260
DECODING CIRCUIT
254
DECODING CIRCUIT
262
DECODING CIRCUIT
264
DECODING CIRCUIT
266
LL
LH
HL
HH
FREQUENCY BAND SYNTHESIZATION FILTER (VL)
270
FREQUENCY BAND SYNTHESIZATION FILTER (VH)
272
FREQUENCY BAND SYNTHESIZATION FILTER (VL)
274
FREQUENCY BAND SYNTHESIZATION FILTER (VH)
276
FREQUENCY BAND SYNTHESIZATION FILTER (HL)
278
FREQUENCY BAND SYNTHESIZATION FILTER (HH)
280
SD D/A
268
HD D/A
282
SD SIGNAL
HD SIGNAL

FIG. 11

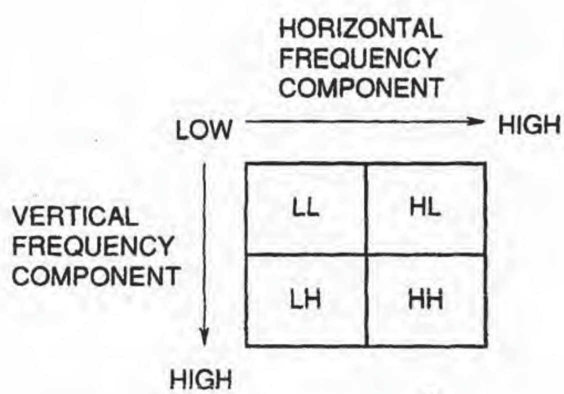

HORIZONTAL
FREQUENCY
COMPONENT
LOW
HIGH
VERTICAL
FREQUENCY
COMPONENT
HIGH
LL
HL
LH
HH

FIG. 12

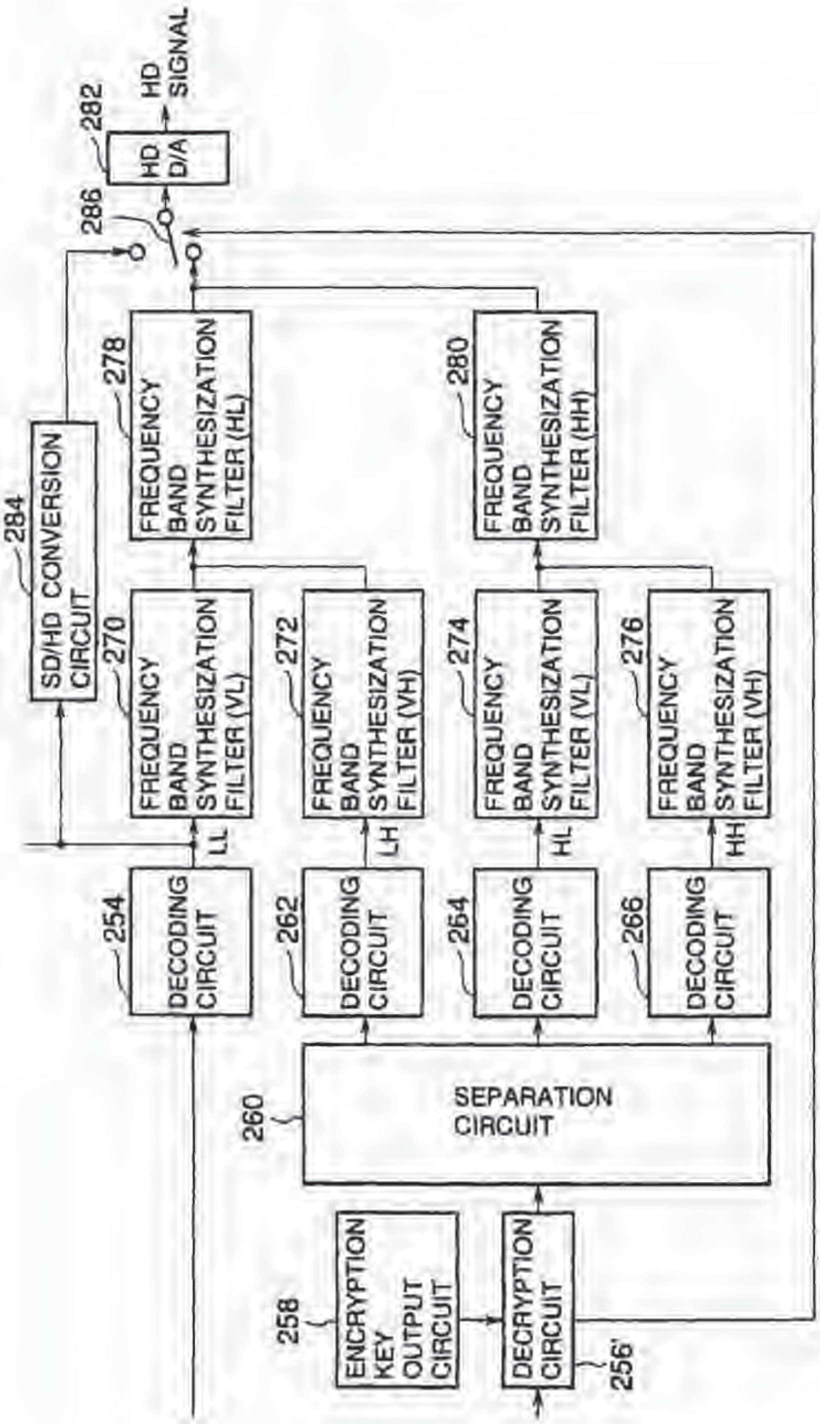

SD/HD CONVERSION CIRCUIT
284
282
HD D/A
HD SIGNAL
286
278
FREQUENCY BAND SYNTHESIZATION FILTER (HL)
280
FREQUENCY BAND SYNTHESIZATION FILTER (HH)
270
FREQUENCY BAND SYNTHESIZATION FILTER (VL)
272
FREQUENCY BAND SYNTHESIZATION FILTER (VH)
274
FREQUENCY BAND SYNTHESIZATION FILTER (VL)
276
FREQUENCY BAND SYNTHESIZATION FILTER (VH)
LL
LH
HL
HH
254
DECODING CIRCUIT
262
DECODING CIRCUIT
264
DECODING CIRCUIT
266
DECODING CIRCUIT
260
SEPARATION CIRCUIT
258
ENCRYPTION KEY OUTPUT CIRCUIT
DECRYPTION CIRCUIT
256'

FIG. 13

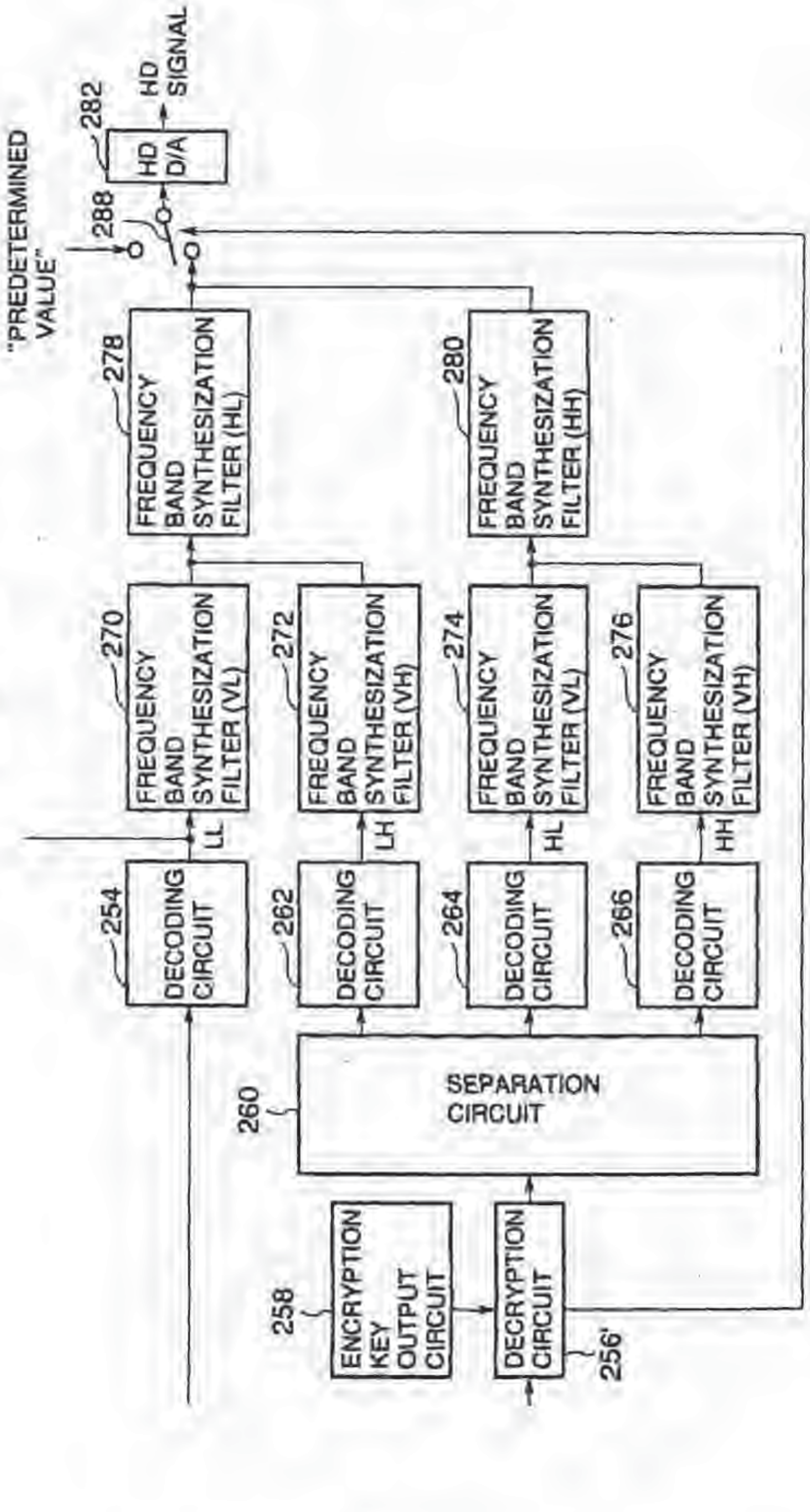

"PREDETERMINED VALUE"
288
HD D/A
282
HD SIGNAL
FREQUENCY BAND SYNTHESIZATION FILTER (HL)
278
FREQUENCY BAND SYNTHESIZATION FILTER (HH)
280
FREQUENCY BAND SYNTHESIZATION FILTER (VL)
270
FREQUENCY BAND SYNTHESIZATION FILTER (VH)
272
FREQUENCY BAND SYNTHESIZATION FILTER (VL)
274
FREQUENCY BAND SYNTHESIZATION FILTER (VH)
276
LL
LH
HL
HH
DECODING CIRCUIT
254
DECODING CIRCUIT
262
DECODING CIRCUIT
264
DECODING CIRCUIT
266
SEPARATION CIRCUIT
260
ENCRYPTION KEY OUTPUT CIRCUIT
258
DECRYPTION CIRCUIT
256'

FIG. 14

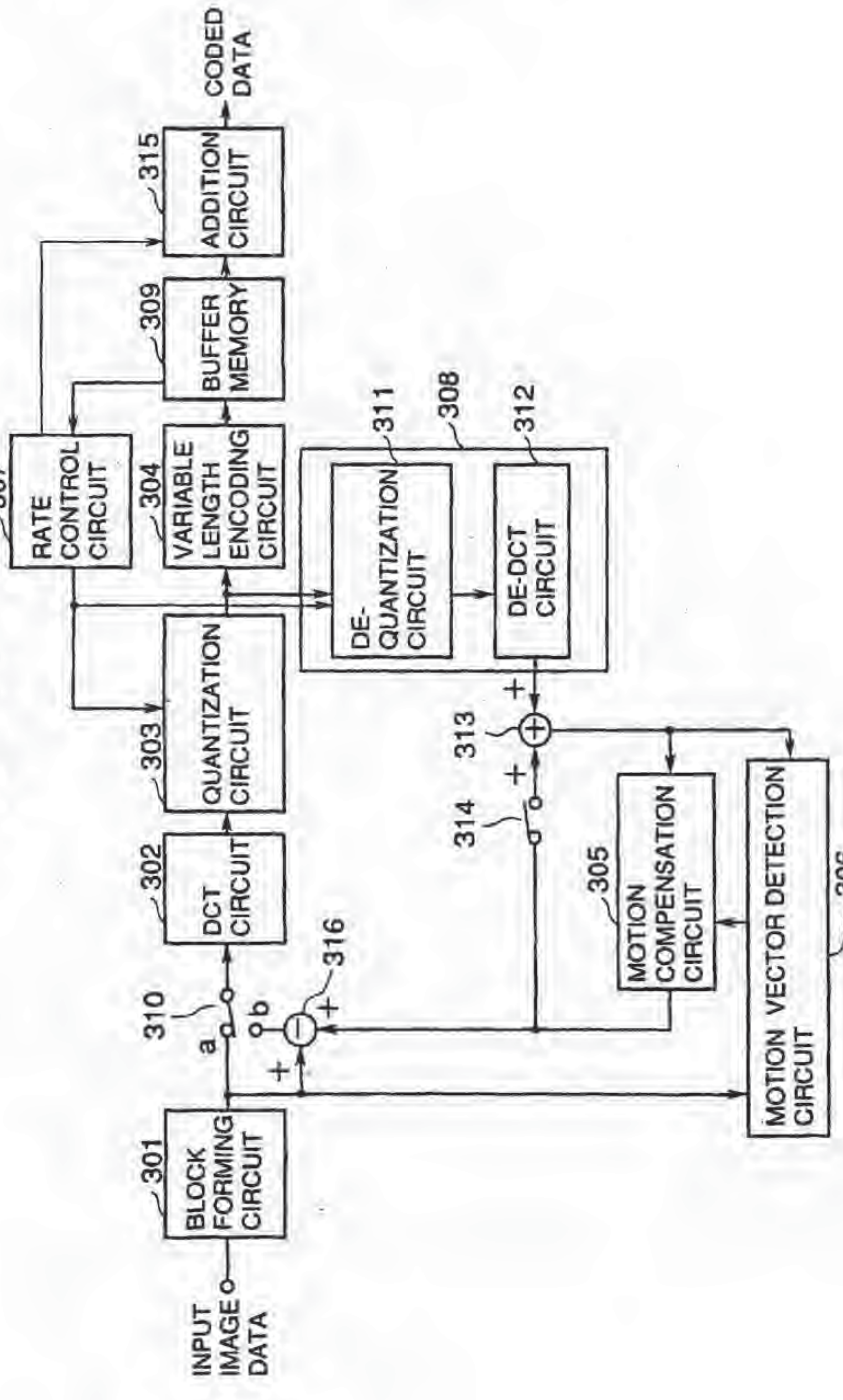
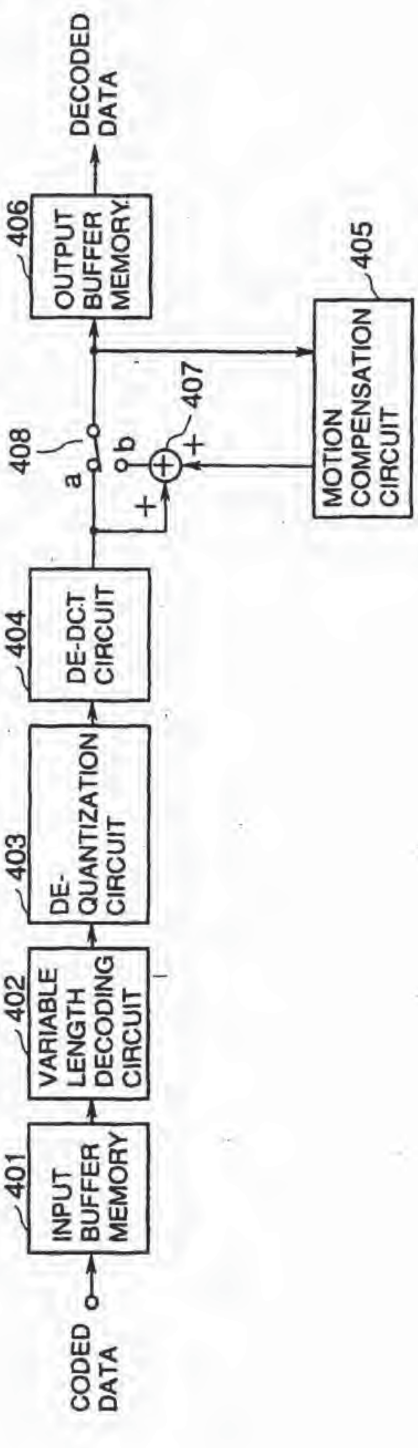

INPUT IMAGE DATA
BLOCK FORMING CIRCUIT
301
310
a
b
+
+
316
DCT CIRCUIT
302
QUANTIZATION CIRCUIT
303
RATE CONTROL CIRCUIT
307
VARIABLE LENGTH ENCODING CIRCUIT
304
BUFFER MEMORY
309
ADDITION CIRCUIT
315
CODED DATA
DE-QUANTIZATION CIRCUIT
311
308
DE-DCT CIRCUIT
312
313
314
MOTION COMPENSATION CIRCUIT
305
MOTION VECTOR DETECTION CIRCUIT
306

FIG. 15


CODED DATA
401
INPUT BUFFER MEMORY
402
VARIABLE LENGTH DECODING CIRCUIT
403
DE-QUANTIZATION CIRCUIT
404
DE-DCT CIRCUIT
408
a
b
+
+
407
405
MOTION COMPENSATION CIRCUIT
406
OUTPUT BUFFER MEMORY
DECODED DATA

(19) Bureau voor de Industriële Eigendom Nederland

(11) 1005523

(12) C OCTROOI[20]

(21) Aanvrage om octrooi: 1005523

(22) Ingediend: 13.03.97

(51) Int.Cl.[6]
H04K1/00, H04L9/00, H04B1/69, H04N7/167

(41) Ingeschreven:
15.09.98

(47) Dagtekening:
15.09.98

(45) Uitgegeven:
02.11.98 I.E. 98/11

(73) Octrooihouder(s):
Technische Universiteit Eindhoven te Eindhoven.

(72) Uitvinder(s):
Giok-Djan Khoe te Eindhoven
Robert Peter Christina Wolters te Montfort
Alfons Willy Leo Janssen te Utrecht

(74) Gemachtigde:
Ir. J.J.H. Van kan c.s. te 5600 AP Eindhoven.

(54) **Werkwijze en communicatiesysteem voor het in gedeeltelijk gecodeerde vorm overdragen van informatiesignalen.**

(57) Werkwijze en middelen voor het in een communicatiesysteem overdragen van informatiesignalen onder toepassing van veilige coderingstechnieken, waarbij een informatiesignaal wordt gesplitst in een voor verwerking van het signaal relevant deel en een restdeel. Het relevante deel wordt in een veilig gecodeerde vorm en het restdeel wordt in ongecodeerde vorm via het communicatiesysteem overgedragen. Na het decoderen daarvan wordt een overgedragen relevant deel van een informatiesignaal met een bijbehorend overgedragen restdeel tot het oorspronkelijke informatiesignaal gereconstrueerd. Het te coderen relevante deel van het informatiesignaal wordt bij voorkeur onder toepassing van 'Code Division Multiple Access' (CDMA)-techniek gecodeerd overgedragen. Het communicatiesysteem kan een 'point-to-multipoint' signaaldistributienet omvatten, waarbij verschillende gebruikers gelijktijdig informatiesignalen kunnen ontvangen en/of verzenden, waaronder begrepen een 'Community Antenna TeleVision' (CATV)-net en distributienetten voor elektrische energie.

NL C 1005523

Korte aanduiding: Werkwijze en communicatiesysteem voor het in gedeeltelijk gecodeerde vorm overdragen van informatiesignalen.

De uitvinding heeft betrekking op een werkwijze voor het in een communicatiesysteem overdragen van informatiesignalen onder toepassing van veilige coderingstechnieken.

Veilige overdracht van data is een belangrijk aspect bij communicatie via een "point-to-multipoint"-signaaldistributienet, waarbij verschillende gebruikers gelijktijdig informatiesignalen kunnen ontvangen en/of verzenden, zoals een "Community Antenna TeleVision" (CATV)-net of distributienetten voor elektrische energie, waaronder begrepen distributienetten voor elektrische tractie.

Een netwerkbeheerder dient in staat te zijn de toegang tot het net te controleren en dient verder te kunnen verzekeren dat overgedragen informatiesignalen alleen kunnen worden ontvangen door de geadresseerde. Met ontvangen wordt in dit verband bedoeld dat de geadresseerde de inhoud van de betreffende informatiesignalen tot zich kan nemen.

Voor het in een signaaldistributienet veilig overdragen van informatiesignalen zijn een groot aantal coderingstechnieken bekend zoals bijvoorbeeld de "Rivest, Shamir, Aldehman" (RSA) en "Data encryption Standard" (DES) encryptie-algoritmes waarbij met codeersleutels wordt gewerkt. Het over te dragen informatiesignaal wordt dan in zijn geheel gecodeerd en via het signaaldistributienet overgedragen, waarbij alleen de ontvanger welke de voor het decoderen van het bericht benodigde sleutel kent, in staat is om de inhoud van het informatiesignaal tot zich te nemen.

De mate van beveiliging hangt naast het gekozen codeeralgoritme ook af van de lengte van de codeersleutel. In het bijzonder geldt dat bij relatief breedbandige informatiesignalen en bij relatief lange codeer- en decodeersleutels, er een aanzienlijke hoeveelheid tijd gemoeid kan zijn met het overdragen van informatiesignalen. In veel praktische toepassingen is een extra vertraging bij de overdracht van signalen echter niet gewenst.

Aan de uitvinding ligt daarom in eerste instantie de opgave ten grondslag een werkwijze aan te geven voor het in een communicatiesysteem overdragen van informatiesignalen onder toepassing van veilige coderingstechnieken met een gereduceerde invloed op de overdrachtssnelheid van informatiesignalen.

Volgens de uitvinding wordt dit daardoor bereikt dat een informatiesignaal wordt gesplitst in een voor verwerking van het signaal relevant deel en een restdeel, waarbij het relevante deel in een veilig gecodeerde vorm en het restdeel in ongecodeerde vorm via het communicatiesysteem worden overgedragen en dat een overgedragen relevant deel van een informatiesignaal wordt gedecodeerd en met een bijbehorend overgedragen restdeel tot het oorspronkelijke informatiesignaal wordt gereconstrueerd.

Aan de uitvinding ligt het inzicht ten grondslag dat, door het van een over te dragen informatiesignaal afsplitsen van een voor de verwerking van het signaal relevant deel, het resterende gedeelte onbruikbaar is geworden. Onder een 'voor verwerking relevant deel' van het signaal worden in dit verband één of meer delen van een signaal begrepen waarmee, bij het ontbreken hiervan, de informatie in het restdeel niet meer kan worden herkend dan wel dat door het ontbreken van het betreffende relevante deel of de relevante delen het signaal niet meer kan worden gereconstrueerd. Overeenkomstig de oplossing volgens de uitvinding kan voor het veilig gecodeerd overdragen van informatiesignalen worden volstaan met het coderen van het betreffende relevante deel van het informatiesignaal, waarbij het resterende gedeelte ongecodeerd kan worden overgedragen.

Door het volgens een verdere uitvoeringsvorm van de uitvinding zodanig selecteren van het te coderen relevante deel van een informatiesignaal dat dit deel een relatief gering, bij voorkeur een zo gering mogelijk deel van de bandbreedte van het informatiesignaal in beslag neemt, kan er voor worden gezorgd dat de door het codeer- en decodeerproces veroorzaakte vertragingen in de signaaloverdracht minimaal zijn.

In bijvoorbeeld een gecodeerd digitaal videosignaal kunnen verschillende velden worden onderscheiden, bijvoorbeeld specifiek op de signaaloverdracht betrekkende hebbende velden waarmee, wanneer zij niet in het signaal aanwezig zijn, het onmogelijk is om de informatie-inhoud van het digitale videosignaal tot zich te nemen. Voorbeelden van dergelijke velden zijn bijvoorbeeld synchronisatievelden of het FEC-veld in een "Digital Video Broadcasting" (DVB)-videosignaal. Deze velden beslaan slechts een relatief gering aantal bits van het totale videosignaal. De werkwijze volgens de uitvinding is in wezen bij alle digitale data-overdracht toepasbaar, omdat vrijwel elk data-overdrachtsprotocol bepaalde stuur-, controle- of andere gegevensvelden bezit welke noodzakelijk zijn om het betreffende signaal te kunnen reconstrueren. De werkwijze volgens de uitvinding is ook toepasbaar bij de overdracht van analoge signalen, waarbij in het algemeen ook door het afsplitsen van een relevant deel van het signaal het resterende deel onbruikbaar wordt.

In een communicatiesysteem dat verschillende transmissiekanalen omvat worden in een voorkeursuitvoeringsvorm van de uitvinding de gecodeerde relevante delen van informatiesignalen via een ander transmissiekanaal overgedragen dan de ongecodeerde restdelen. Hierdoor is het mogelijk om, in plaats van het afzonderlijk veilig coderen van de relevante delen, deze ook via een betreffend beveiligd transmissie-kanaal over te dragen, zoals een transmissiekanaal waarop data middels de zogeheten "Code Division Multiple Access" (CDMA)-techniek gecodeerd worden overgedragen.

Het gebruik van CDMA-technieken garandeert een lage kans op onderschepping, zonder dat de betreffende relevante delen van informatiesignalen afzonderlijk moeten worden gecodeerd.

Een derde welke een betreffend informatiesignaal wil onderscheppen, dient derhalve in staat te zijn om het gecodeerde relevante deel te onderscheppen en het bijbehorende restdeel. Zelfs wanneer dit tot een resultaat zou lijden, dient er ook nog kennis te bestaan omtrent de wijze waarop de betreffende delen tot het oorspronkelijke informatiesignaal moeten worden gecombineerd. Derhalve geniet het de voorkeur om niet steeds eenzelfde relevant deel van een informatiesignaal af te splitsen en gecodeerd over te dragen maar, voor zover mogelijk, verschillende relevante signaaldelen te onderscheiden en van de over te dragen informatiesignalen afwisselend verschillende relevante delen te selecteren.

De uitvinding heeft tevens betrekking op een communicatiesysteem, omvattende codeermiddelen voor het in gecodeerde vorm veilig overdragen van informatiesignalen en decodeermiddelen voor het decoderen van overgedragen informatiesignalen, verder gekenmerkt door middelen voor het splitsen van een over te dragen informatiesignaal in een voor verwerking van het signaal relevant deel en een restdeel, welke middelen werkzaam zijn gekoppeld met de codeermiddelen voor het in veilig gecodeerde vorm overdragen van het relevante deel van een informatiesignaal en met middelen voor het in ongecodeerde vorm overdragen van het restdeel van een informatiesignaal, waarbij de decodeermiddelen zijn ingericht voor het decoderen van een overgedragen relevant deel van een informatiesignaal en werkzaam zijn gekoppeld met middelen voor het tot een oorspronkelijk informatiesignaal reconstrueren van een gedecodeerd relevant deel en een overgedragen bijbehorend restdeel.

In de voorkeursuitvoeringsvorm van het communicatiesysteem volgens de uitvinding zijn de codeermiddelen ingericht voor het CDMA-gecodeerd overdragen van de relevante delen van een informatiesignalen.

De uitvinding heeft tevens betrekking op signaalsplitsmiddelen en signaalcombinatiemiddelen voor het respectievelijk splitsen en combineren van relevante delen en restdelen van een informatiesignaal, zoals boven beschreven.

De uitvinding wordt in het navolgende meer gedetailleerd beschreven en getoond in de bijgevoegde tekeningen, waarin:

fig. 1 schematisch de werkwijze volgens de uitvinding illustreert;

fig. 2 een vereenvoudigd blokschema van een "Direct Sequence" CDMA (DS-CDMA)-systeem toont;

fig. 3 een voorbeeldschema van een CATV-net toont, waarin de werkwijze volgens de uitvinding kan worden toegepast;

fig. 4 een vereenvoudigd blokschema van een eerste uitvoeringsvorm van een communicatiesysteem volgens de uitvinding toont, en

fig. 5 een vereenvoudigd blokschema van een voorkeursuitvoeringsvorm van een communicatiesysteem volgens de uitvinding toont.

Fig. 1 illustreert, in de vorm van een stroomdiagram, de werkwijze volgens de uitvinding, waarbij door middel van pijlen de bewerkingsvolgorde is geïllustreerd. Een informatiesignaal 1 wordt als eerste aan een splitsingsoperatie 2 onderworpen. Het informatiesignaal wordt hier gesplitst in een voor de signaalverwerking relevant deel 3 en een restdeel 4.

Het relevante deel kan uit één of meer delen van het informatiesignaal zijn opgebouwd, welke afzonderlijk of in combinatie noodzakelijk zijn voor de verdere verwerking van het informatiesignaal, dat wil zeggen zodanig dat samen met het restdeel een bruikbaar informatiesignaal wordt verkregen. Het relevante deel 3 kan dus zowel bestaan uit een gedeelte van de informatie-inhoud van het signaal en/of informatie voor het reconstrueren van het signaal, zoals synchronisatie en andere stuurinformatie. Het informatiesignaal kan daarbij bestaan uit zowel een digitaal als een analoog signaal.

In het geval dat een informatiesignaal verschillende voor de verwerking van het signaal relevante delen bezit, kan de splitsingsoperatie 2 zodanig worden uitgevoerd, dat van de arriverende informatiesignalen 1 telkens een selectie uit de relevante delen 3 kan worden gemaakt, zodanig dat van opeenvolgende informatiesignalen de relevante delen 3 en de restdelen 4 qua opbouw verschillend zijn. De wijze waarop de betreffende relevante delen 3 worden geselecteerd kan van te voren vastgelegd zijn of middels een kenmerk worden overgedragen.

Het geselecteerde relevante deel 3 wordt vervolgens aan een codeeroperatie 5 onderworpen. Deze codeeroperatie 5 heeft tot het doel het relevante deel te coderen voor veilige overdracht 6 over een transmissienet, zoals bijvoorbeeld een "point-to-multipoint" signaaldistributienet. Voorbeelden van dergelijke signaaldistributienetten zijn "Community Antenna TeleVision" (CATV)-netten en distributienetten voor elektrische energie zoals het elektriciteitsdistributienet in huizen, kantoren etc. en ook distributienetten voor elektrische tractie zoals in gebruik bij spoorweg-, tram- en trolleybusmaatschappijen.

Voor het coderen van het relevante deel zijn op zichzelf bekende coderingstechnieken bekend, welke met beveiligde codeer- en decodeersleutels werken zoals de "Rivest, Shamir, Aldehman (RSA) en "Data Encryption Standard" (DES) encryptie-algoritmes welke geen deel uitmaken van de onderhavige uitvinding. Voor een meer uitgebreide beschrijving van encryptie-algoritmes wordt verwezen naar het boek "Applied Cryptography", door Bruce Shneier, 2nd edition, John Wiley & Sons 1995.

Aan de ontvangende zijde wordt het overgedragen gecodeerde relevante deel 3 in een decodeeroperatie 7 gedecodeerd. Het restdeel 4 wordt na overdracht 8 aan de ontvangende zijde met het gedecodeerde relevante deel gecombineerd 9, zodanig dat het aldus verkregen informatiesignaal 10 overeenkomt met het oorspronkelijk overgedragen informatiesignaal 1.

Overeenkomstig de uitvinding kan het restdeel 4 in ongecodeerde vorm worden overgedragen omdat het informatiesignaal 1 zodanig is gesplitst, dat het restdeel 4 op zichzelf onbruikbaar is. Onder ongecodeerde overdracht 8 wordt bedoeld dat het restdeel 4 niet wordt begrepen aan een vorm van encryptie of codering van de informatie waarbij het betreffende restdeel zonder kennis omtrent codeer- en/of decodeersleutels niet kan worden verwerkt. Uiteraard kan het restdeel 4 wel volgens een bekend protocol of bekende modulatietechniek worden overgedragen.

In plaats van het afzonderlijk coderen van relevante delen 3, kunnen de codeer-, overdracht- en decodeeroperaties 5, 6 en 7 worden uitgevoerd door het transmissiemedium waarover het relevante deel 3 wordt overgedragen. Dit is in het bijzonder van voordeel in een communicatiesysteem met verschillende transmissiekanalen, waarbij het relevante deel 3 van een informatiesignaal via een veilig gecodeerd transmissiekanaal wordt overgedragen en het restdeel 4 via een niet-beveiligd kanaal kan worden verzonden. In een voorkeursuitvoeringsvorm van de uitvinding wordt het relevante deel 3 overgedragen onder toepassing van de zogeheten "Code Division Multiple Access" (CDMA)-techniek.

CDMA of "Spread Spectrum" (SS) is een transmissietechniek waarbij de databits van een over te dragen digitaal signaal in een aantal elementen of chips worden gecodeerd, zodanig dat elk databit als een reeks van symbolen wordt overgedragen. Deze symbolen kunnen op zichzelf de logische waarde "1" of "0" aannemen of in het ritme van de betreffende reeks overgedragen frequentievariaties. In het eerste geval spreekt van "Direct Sequence CDMA" (DS-CDMA) en in het tweede geval van "Frequency Hopping CDMA" (FH-CDMA). In beide gevallen kan het overgedragen signaal weer worden gereconstrueerd indien de volgorde van de overgedragen chips of de frequenties bij de ontvanger bekend zijn. Afhankelijk van de omvang van de reeks, dat wil zeggen het aantal symbolen waarin het overgedragen bit wordt gecodeerd, zijn een veelvoud van onafhankelijke codes beschikbaar waardoor gelijktijdig verschillende gebruikers van eenzelfde transmissiekanaal gebruik kunnen maken. Alleen de gebruiker met de juiste code is in staat om de met deze code overgedragen databits te ontvangen.

Figuur 2 toont een vereenvoudigd blokschema van een DS-CDMA systeem met een transmissiekanaal 11, een zender 12 en een ontvanger 13. Het kanaal 11 kan een draadgebonden, optisch of draadloos communicatiekanaal zijn waaronder begrepen een radiokanaal, een infrarood-kanaal en een ultrasoon-transmissiekanaal. In een CDMA-transmissiesysteem wordt door verschillende gebruikers j tegelijkertijd informatie over het transmissiekanaal 11 overgedragen, zoals gerepresenteerd middels een sommatieblok 16 waarbij een aantal van j = 1 tot en met N gebruikers 15 is verondersteld. Het totale signaal op het transmissiekanaal 11 wordt dan theoretisch gevormd door de som van een ruisbron 14 en de signalen van de gebruikers 15, zoals schematisch aangeduid door een sommator 17.

De zender 12 bestaat in wezen uit een modulator 18 met een ingang 19 waaraan over te dragen databits worden toegevoerd. De modulator 18 verwerkt de databits 19 tot geschikte signalen voor overdracht via het transmissiekanaal 11. De ontvanger 13 bezit een demodulator 20 met een uitgang 21 voor het afgeven van de overgedragen gedemoduleerde databits.

Voor transmissie volgens het DS-CDMA principe worden de van een zender 12 naar een ontvanger 13 door een gebruiker j over te dragen databits elk met een, door een codegenerator 22 opgewekte code $C_j^w(t)$ en een mengschakeling 23 in een aantal symbolen (chips) gecodeerd. Een logische "1" wordt bijvoorbeeld door de betreffende code zelf en een logische "0" wordt bijvoorbeeld door de inverse van de code gerepresenteerd. Naarmate de code langer is zal het over te dragen signaal meer en meer een ruissignaal benaderen, waardoor detectie zonder kennis van de betreffende code nagenoeg onmogelijk is.

Het op deze wijze in de frequentie gespreide DS-CDMA signaal van de gebruiker j kan na een transmissievertragingstijd τ_j bij de ontvanger 13 via eenzelfde codegenerator 22 echter met de code $C_j^w(t)$ en mengschakeling 24 worden gereconstrueerd, mits de code bekend is waarmee de databits voor de j-de gebruiker zijn gecodeerd.

Voor een meer gedetailleerde uitleg van CDMA- en Spread Spectrum-technieken wordt verwezen naar op dit vakgebied bekende literatuur, waaronder de boeken "Spread Spectrum Systems with Applications", door R.C. Dixon, John Wiley & Sons, Inc., 1994 en "CDMA, Principles of Spread Spectrum Communications", door A.J. Viterbi, Addison-Wesley Publishing Company. In de werkwijze volgens de voorkeursuitvoeringsvorm van de uitvinding wordt derhalve de vereiste veilige codering van het relevante deel van een informatiesignaal door het betreffende transmissiekanaal verzorgt waarover de overdracht plaatsvindt. Het gebruik van CDMA-technieken garandeert een lage kans op onderschepping.

Omdat ook het restdeel via een gemeenschappelijk of een veelheid van gemeenschappelijke transmissiekanalen van een communicatiesysteem wordt overgedragen, zal het zelfs bij onderscheppen van een gecodeerd relevant deel 3 nog bijzonder moeilijk zijn om het bijbehorende restdeel 4 te selecteren en wanneer het relevante deel 3 afwisselend uit een veelvoud van relevante signaaldelen wordt geselecteerd, zal het eveneens problematisch zijn om de beide delen tot het oorspronkelijke informatiesignaal te combineren.

Het relevante deel 3 wordt, in het geval van een relatief breedbandig signaal, zoals een videosignaal, zodanig gekozen, dat het slechts een relatief gering gedeelte van de totale signaalbandbreedte in beslag neemt. In een praktische situatie wordt het relevante deel 3 bij voorkeur zodanig gekozen, dat het via een 64 kb/s transmissiekanaal kan worden overgedragen, terwijl het restdeel 4, bijvoorbeeld in het geval van een videosignaal, via een breedbandig transmissiekanaal in de ordegrootte van 2 Mb/s of hoger wordt overgedragen. Het zal duidelijk zijn dat bij een overdrachtstechniek waarbij meerdere gebruikers tegelijkertijd op eenzelfde kanaal actief kunnen zijn, zoals CDMA, maar ook volgens de zogeheten "Time Division Multiple Access" (TDMA)-techniek werkende transmissiekanalen, met de werkwijze volgens de uitvinding op veilige wijze informatie in een distributienet kan worden overgedragen.

Een voorbeeld van een point-to-multipoint datadistributienet is het reeds eerder genoemde CATV-net, waarvan fig. 3 een voorbeeldsuitvoeringsvorm toont. In de getoonde netstructuur 25 wordt informatie vanaf een hoofdstation 26 naar eindaansluitpunten 27 overgedragen. Tussen het hoofdstation 26 en de eindaansluitpunten 27 zijn diverse bi-directionele versterkers 28, 29, 30 geschakeld, voor het opheffen van transmissieverliezen in het net 25, dat gebruikelijk uit coaxiale kabel 32 is opgebouwd.

In de getoonde uitvoeringsvorm zijn de versterkers 28 in de vorm van een zogeheten ringnet op het hoofdstation 26 aangesloten, waarbij de van een versterker 28 ontvangen signalen in een districtstation 31 verder via een groepsversterker 29 worden gedistribueerd. De gebruikers of eindaansluitpunten 27 zijn stervormig op een eindversterker 30 aangesloten die signalen van een groepsversterker 29 ontvangt.

In Nederlands CATV-netten zijn de versterkers 28, 29 en 30 in het algemeen zodanig ingericht, dat zij signalen vanaf het hoofdstation 26 naar de eindaansluitpunten 27 in een brede frequentieband van circa 50 MHz tot boven 750 MHz doorlaten. De transmissierichting vanaf het hoofdstation 26 naar de eindaansluitpunten 27 wordt ook wel met "stroomafwaarts" aangeduid. In de andere richting, dat wil zeggen vanaf de eindaansluitpunten 27 naar het hoofdstation 26, ook wel "stroomopwaarts" genoemd, is een transmissiefrequentieband van 5 MHz tot circa 50 MHz beschikbaar. Gestreefd wordt naar een volledig passieve transmissiefrequentieband in het frequentiegebied tot ca. 70 MHz, dat wil zeggen zonder versterkers.

Onder meer afhankelijk van de lengte van de code waarmee databits in CDMA worden gecodeerd, kunnen meer dan 100 gebruikers gelijktijdig op eenzelfde transmissiekanaal informatie overdragen.

Fig. 4 toont een vereenvoudigd blokschema van een eerste uitvoeringsvorm van een communicatiesysteem voor het gedeeltelijk gecodeerd overdragen van informatiesignalen volgens de uitvinding. Een over te dragen informatiesignaal wordt aan een ingang 33 van signaalsplitsmiddelen 34 toegevoerd, welke aan een eerste uitgang 35 de relevante signaaldelen en aan een uitgang 36 het restdeel van het over te dragen informatiesignaal afgeven.

Het relevante deel 35 wordt in codeermiddelen 37 veilig gecodeerd volgens een op zichzelf bekende coderingstechniek en aan een uitgang 38 afgegeven. De signalen aan de uitgangen 36 en 38 worden in een multiplexer 39 tot een voor overdracht via een zender 48 en transmissiekanaal 40 geschikt signaal gecombineerd. Het door een ontvanger 49 ontvangen overgedragen signaal wordt in een demultiplexer 41 weer gescheiden in een restdeel en het gecodeerde relevante deel, respectievelijk afgegeven aan uitgangen 42 en 43. Het gecodeerde signaal op de uitgang 43 wordt aan decodeermiddelen 44 toegevoerd en het aan een uitgang 45 van de decodeermiddelen 44 afgegeven gedecodeerde signaal wordt samen met het op de uitgang 42 van de demultiplexer 41 beschikbare restdeel in signaalcombinatiemiddelen 46 tot een informatiesignaal gecombineerd, dat vervolgens op een uitgang 47 van de signaalcombinatiemiddelen 46 beschikbaar is.

Fig. 5 toont een voorkeursuitvoeringsvorm van een communicatiesysteem volgens de uitvinding, waarbij de signalen op de uitgangen 35 en 36 van de signaalsplitsmiddelen 34 via afzonderlijke transmissiekanalen 50, 51 worden overgedragen.

Het kanaal 51, waarover het restdeel van een informatiesignaal 33 wordt overgedragen, kan van het type zijn waarover informatie op ongecodeerde, dat wil zeggen niet versleutelde of anderszins beveiligde wijze, wordt overgedragen via zend- en ontvangmiddelen 52, 53. Uiteraard kan het restdeel wel volgens een geschikt of voorgeschreven transmissieprotocol tot een voor overdracht via het transmissiekanaal 51 geschikt formaat zijn verwerkt.

Overeenkomstig de in fig. 3 geïllustreerde uitvoeringsvorm, kan het relevante deel van het informatiesignaal 33 aan de uitgang 35 van de signaalsplitsmiddelen 34 op geschikte wijze gecodeerd 54, verzonden 55, ontvangen 56 en gedecodeerd 57 worden, onder toepassing van een daartoe geschikt transmissieprotocol en codeeralgoritme.

In de voorkeursuitvoeringsvorm van de uitvinding wordt het relevante deel van een informatiesignaal 33 via een veilig transmissiekanaal overgedragen, in het bijzonder een CDMA-gecodeerd transmissiekanaal, zoals aangegeven met de onderbroken lijnen 58 in fig. 5. De codeer- en zendmiddelen 54, 55 en de ontvang- en decodeermiddelen 56, 57 zijn ingericht voor CDMA-overdracht zoals besproken aan de hand van fig. 2.

De transmissiekanalen 50 en 51 kunnen deel uitmaken van een meer omvangrijke communicatiesysteem zoals een CATV-net waarbij meerdere gebruikers gelijktijdig over een informatiekanaal informatie overdragen. In het bijzonder bij CDMA-data-overdracht kunnen de relevante delen van verschillende gebruikers gelijktijdig over het transmissiekanaal 50 op een veilige wijze worden overgedragen zodanig, dat alleen de eindgebruiker welke beschikt over de juiste sleutel waarmee een betreffend relevant deel is gecodeerd de informatie uit de veelheid van relevante delen van verschillende gebruikers kan terugwinnen.

Voor het combineren van een bijbehorend relevant deel en een restdeel kan aan elk van de delen een specifieker kenmerk worden toegevoegd, zoals een bestemmingsnummer of gebruikersnummer en een volgnummer, zodanig dat de signaalcommunicatiemiddelen 46 de betreffende signaaldelen tot een uiteindelijk compleet informatiesignaal aan de uitgang 47 kunnen combineren.

In plaats van CDMA-transmissie kan ook elke andere vorm van veilige transmissie voor het doel van de uitvinding worden toegepast, zoals bijvoorbeeld transmissie in versleutelde vorm middels een "Time Division Multiple Access" (TDMA)-transmissieprotocol overeenkomstig het "Global Systems voor Mobile Communications" (GSM) of de "Digital Enhanced Cordless Telecommunications" (DECT)-standaard waarbij de informatie standaard in gecodeerde of versleutelde vorm wordt overgedragen.

Hoewel in de figuren 4 en 5 een communicatiesysteem voor simplex-overdracht (d.w.z. éénrichtingsverkeer) is getoond, zal het voor een deskundige geen toelichting behoeven dat de de uitvinding ook voor duplex-overdracht (d.w.z. voor tweerichtingsverkeer) geschikt is.

Conclusies

1. Werkwijze voor het in een communicatiesysteem overdragen van informatiesignalen onder toepassing van veilige coderingstechnieken, met het kenmerk, dat een informatiesignaal wordt gesplitst in een voor verwerking van het signaal relevant deel en een restdeel, waarbij het relevante deel in een veilig gecodeerde vorm en het restdeel in ongecodeerde vorm via het communicatiesysteem worden overgedragen en dat een overgedragen relevant deel van een informatiesignaal wordt gedecodeerd en met een bijbehorend overgedragen restdeel tot het oorspronkelijke informatiesignaal wordt gereconstrueerd.

2. Werkwijze volgens conclusie 1, met het kenmerk, dat het te coderen relevante deel van het informatiesignaal zodanig wordt geselecteerd dat dit een relatief gering deel van de bandbreedte van het informatiesignaal in beslag neemt.

3. Werkwijze volgens conclusie 1 of 2, met het kenmerk, dat het communicatiesysteem verschillende transmissiekanalen omvat, waarbij het gecodeerde relevante deel en het ongecodeerde restdeel van het informatiesignaal elk via verschillende transmissiekanalen worden overgedragen.

4. Werkwijze volgens conclusie 1, 2 of 3, met het kenmerk, dat het te coderen relevante deel van het informatiesignaal onder toepassing van "Code Division Multiple Access" (CDMA)-techniek gecodeerd wordt overgedragen.

5. Werkwijze volgens conclusie 1, 2, 3 of 4, met het kenmerk, dat het communicatiesysteem een "point-to-multipoint" signaaldistributienet omvat, waarbij verschillende gebruikers gelijktijdig informatiesignalen kunnen ontvangen en/of verzenden, waaronder begrepen "Community Antenna TeleVision" (CATV)-netten en distributienetten voor elektrische energie.

6. Communicatiesysteem, omvattende codeermiddelen voor het in gecodeerde vorm veilig overdragen van informatiesignalen en decodeermiddelen voor het decoderen van overgedragen informatiesignalen, verder gekenmerkt door middelen voor het splitsen van een over te dragen informatiesignaal in een voor verwerking van het signaal relevant deel en een restdeel, welke middelen werkzaam zijn gekoppeld met de codeermid-

delen voor het in veilig gecodeerde vorm overdragen van het relevante deel van een informatiesignaal en met middelen voor het in ongecodeerde vorm overdragen van het restdeel van een informatiesignaal, waarbij de decodeermiddelen zijn ingericht voor het decoderen van een overgedragen relevant deel van een informatiesignaal en werkzaam zijn gekoppeld met middelen voor het tot een oorspronkelijk informatiesignaal reconstrueren van een gedecodeerd relevant deel en een overgedragen bijbehorend restdeel.

7. Communicatiesysteem volgens conclusie 6, met het kenmerk, dat de middelen voor het splitsen van het informatiesignaal zijn ingericht voor het selecteren van een relevant deel van het informatiesignaal met een relatief geringe bandbreedte ten opzichte van de bandbreedte van het totale informatiesignaal.

8. Communicatiesysteem volgens conclusie 6 of 7, met het kenmerk, dat het communicatiesysteem verschillende transmissiekanalen omvat voor het via een verschillend transmissiekanaal overdragen van het relevante deel en het restdeel van een informatiesignaal.

9. Communicatiesysteem volgens conclusie 6, 7 of 8, met het kenmerk, dat de codeermiddelen zijn ingericht voor het in "Code Division Multiple Access" (CDMA)-gecodeerd overdragen van het relevante deel van een informatiesignaal.

10. Signaalsplitsmiddelen voor gebruik in een communicatiesysteem volgens conclusie 6, 7, 8 of 9, voor het splitsen van een over te dragen informatiesignaal, met het kenmerk, dat de signaalsplitsmiddelen zijn ingericht voor het, van het informatiesignaal afsplitsen van een voor de verwerking van het signaal relevant deel.

11. Signaalcombinatiemiddelen voor gebruik in een communicatiesysteem volgens conclusie 6, 7, 8 of 9, met het kenmerk, dat de signaalcombinatiemiddelen zijn ingericht voor het tot een totaal informatiesignaal combineren van een gedecodeerd overgedragen relevant deel en een overgedragen bijbehorend restdeel van een informatiesignaal.

1005523

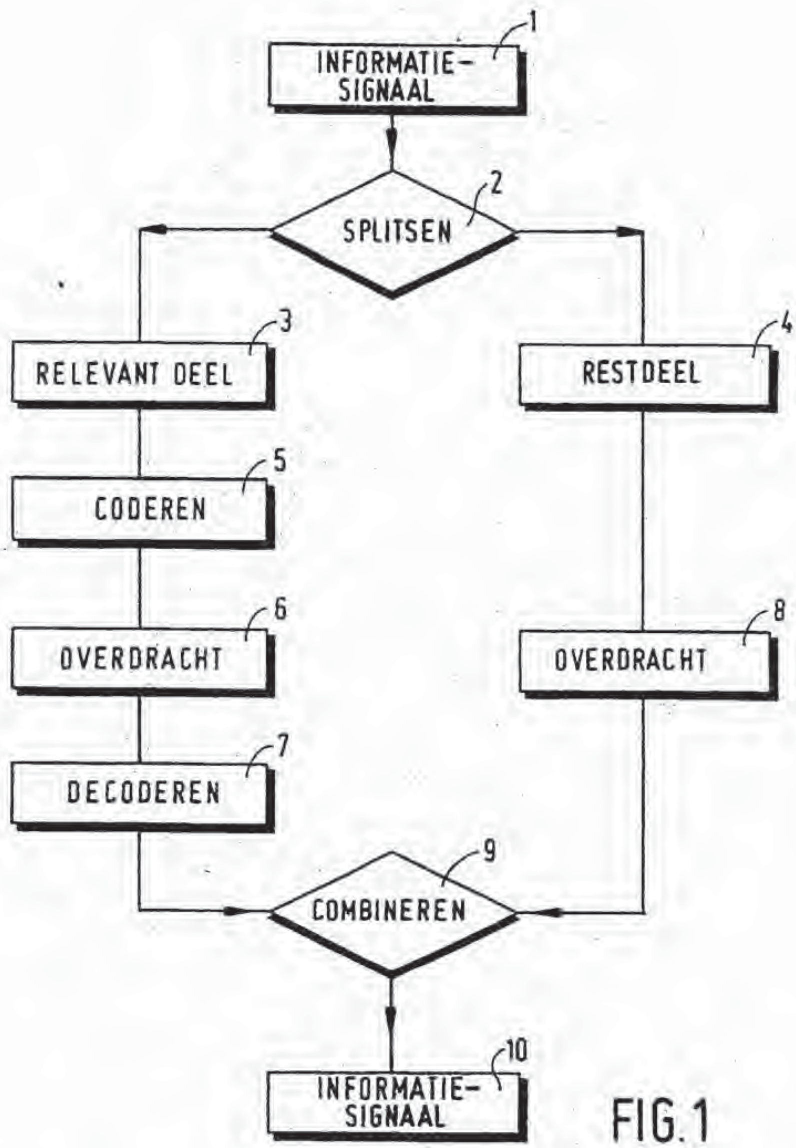


FIG.1

1005523

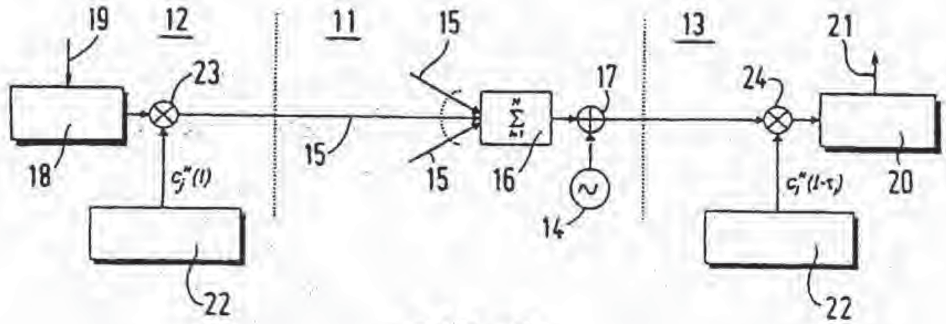


FIG. 2

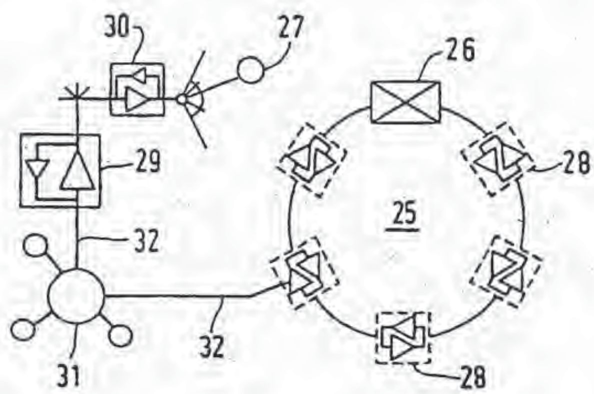


FIG. 3

1005523

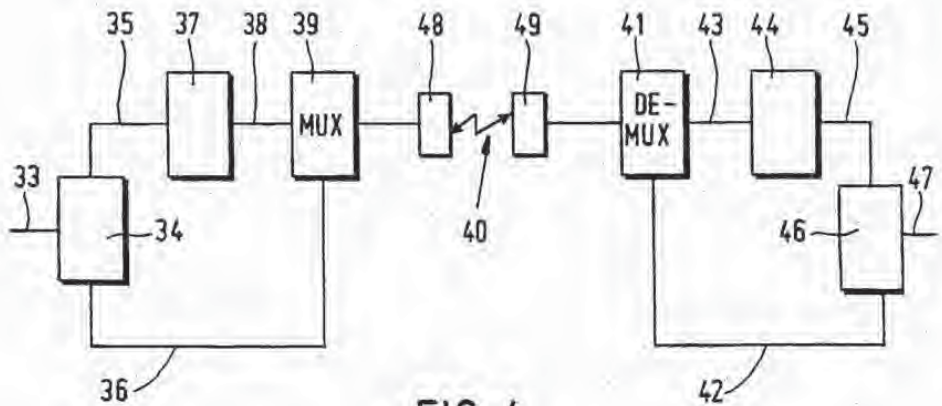


FIG. 4

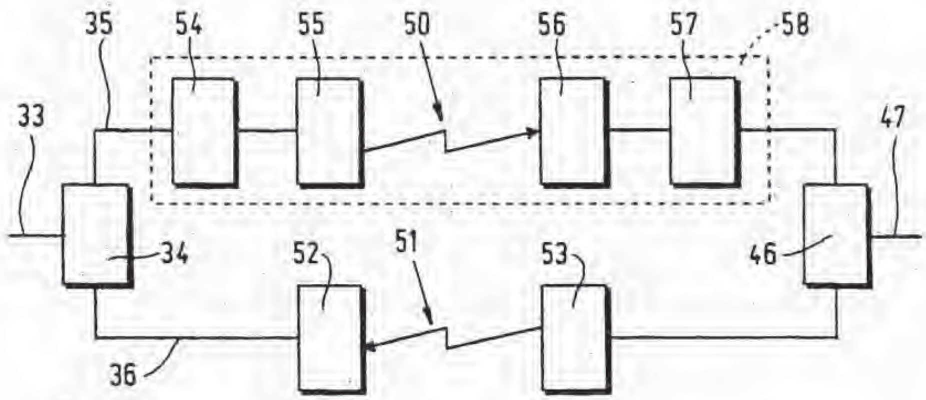


FIG. 5

1005523

SAMENWERKINGSVERDRAG (PCT)
RAPPORT BETREFFENDE
NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

IDENTIFIKATIE VAN DE NATIONALE AANVRAGE	Kenmerk van de aanvrager of van de gemachtigde 37739/JD/jr
Nederlandse aanvrage nr. 1005523	Indieningsdatum 13 maart 1997
	Ingeroepen voorrangsdatum
Aanvrager (Naam) TECHNISCHE UNIVERSITEIT EINDHOVEN	
Datum van het verzoek voor een onderzoek van internationaal type --	Door de Instantie voor Internationaal Onderzoek (ISA) aan het verzoek voor een onderzoek van internationaal type toegekend nr. SN 28858 NL

I. CLASSIFICATIE VAN HET ONDERWERP (bij toepassing van verschillende classificaties, alle classificatiesymbolen opgeven)

Volgens de Internationale classificatie (IPC)

Int. Cl.^{6}: H 04 N 7/167, H 04 N 7/26

II. ONDERZOCHTE GEBIEDEN VAN DE TECHNIEK

Onderzochte minimum documentatie	
Classificatiesysteem	Classificatiesymbolen
Int. Cl.^{6}	H 04 N

Onderzochte andere documentatie dan de minimum documentatie voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

III. ☐ GEEN ONDERZOEK MOGELIJK VOOR BEPAALDE CONCLUSIES (opmerkingen op aanvullingsblad)

IV. ☐ GEBREK AAN EENHEID VAN UITVINDING (opmerkingen op aanvullingsblad)

20

Form PCT/ISA/201(a) 07.1979

BNSDOCID: <NL___1005523C1_I_>

VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

Nummer van het verzoek om een nieuwheidsonderzoek

NL 1005523

A. CLASSIFICATIE VAN HET ONDERWERP

IPC 6 H04N7/167 H04N7/26

Volgens de Internationale Classificatie van octrooien (IPC) of zowel volgens de nationale classificatie als volgens de IPC.

B. ONDERZOCHTE GEBIEDEN VAN DE TECHNIEK

Onderzochte minimum documentatie (classificatie gevolgd door classificatiesymbolen)

IPC 6 H04N

Onderzochte andere documentatie dan de minimum documentatie, voor dergelijke documenten, voor zover dergelijke documenten in de onderzochte gebieden zijn opgenomen

Tijdens het internationaal nieuwheidsonderzoek geraadpleegde elektronische gegevensbestanden (naam van de gegevensbestanden en, waar uitvoerbaar, gebruikte trefwoorden)

C. VAN BELANG GEACHTE DOCUMENTEN

Categorie *	Geciteerde documenten, eventueel met aanduiding van speciaal van belang zijnde passages	Van belang voor conclusie nr.
A	TIHAO CHIANG ET AL: "HIERARCHICAL CODING OF DIGITAL TELEVISION" IEEE COMMUNICATIONS MAGAZINE, deel 32, nr. 5, 1 Mei 1994, bladzijden 38-45, XP000451094 zie bladzijde 41, rechter kolom, regel 40 - bladzijde 43, linker kolom, regel 23 zie figuur 3 ---	1,2,5-7, 10,11
A	DE 44 25 197 A (DEUTSCHE BUNDESPOST TELEKOM) 25 Januari 1996 zie kolom 1, regel 7 - kolom 4, regel 42 zie figuren 1,2 -----	1-11

[ ] Verdere documenten worden vermeld in het vervolg van vak C.

[X] Leden van dezelfde octrooifamilie zijn vermeld in een bijlage

* Speciale categorieën van aangehaalde documenten

"A" document dat de algemene stand van de techniek weergeeft, maar niet beschouwd wordt als zijnde van bijzonder belang

"E" eerder document, maar gepubliceerd op de datum van indiening of daarna

"L" document dat het beroep op een recht van voorrang aan twijfel onderhevig maakt of dat aangehaald wordt om de publicatiedatum van een andere aanhaling vast te stellen of om een andere reden zoals aangegeven

"O" document dat betrekking heeft op een mondelinge uiteenzetting, een gebruik, een tentoonstelling of een ander middel

"P" document gepubliceerd voor de datum van indiening maar na de ingeroepen datum van voorrang

"T" later document, gepubliceerd na de datum van indiening of datum van voorrang en niet in strijd met de aanvrage, maar aangehaald ter verduidelijking van het principe of de theorie die aan de uitvinding ten grondslag ligt

"X" document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet als nieuw worden beschouwd of kan niet worden beschouwd op inventiviteit te berusten

"Y" document van bijzonder belang; de uitvinding waarvoor uitsluitende rechten worden aangevraagd kan niet worden beschouwd als inventief wanneer het document beschouwd wordt in combinatie met één of meerdere soortgelijke documenten, en deze combinatie voor een deskundige voor de hand ligt

"&" document dat deel uitmaakt van dezelfde octrooifamilie

1

Datum waarop het nieuwheidsonderzoek van internationaal type werd voltooid	Verzenddatum van het rapport van het nieuwheidsonderzoek van internationaal type
2 December 1997	

Naam en adres van de instantie	De bevoegde ambtenaar
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Van der Zaal, R

Formulier PCT/ISA/201 (tweede blad) (juli 1992)

BNSDOCID: <NL___1005523C2_I_>

VERSLAG VAN HET NIEUWHEIDSONDERZOEK VAN INTERNATIONAAL TYPE

Informatie over leden van dezelfde octrooifamilie

Nummer van het verzoek om een nieuwheidsonderzoek
NL 1005523

In het rapport genoemd octrooigeschrift	Datum van publicatie	Overeenkomend(e) geschrift(en)	Datum van publicatie
DE 4425197 A	25-01-96	GEEN	

Formulier PCT/ISA/201 (vervolgblad octrooifamilie) (juli 1992)

P ENT COOPERATION TREATY

RECEIVED

MAR 2 8 2001

BROBECK

From the INTERNATIONAL SEARCHING AUTHORITY

To:
BAKER BOTTS L.L.P.
Attn. CHAPMAN, Floyd B.
THE WARNER
1299 PENNSYLVANIA AVENUE, N.W.
WASSHINGTON, D.C. 20004
UNITED STATES OF AMERICA

PCT

INVITATION TO PAY ADDITIONAL FEES

(PCT Article 17(3)(a) and Rule 40.1)

DOCKETED
Add'l Fees Due
16 Apr / 29 Apr 2001

	Date of mailing (day/month/year) 15/03/2001
Applicant's or agent's file reference 066358.0106 031890.0007	PAYMENT DUE within 45 days from the above date of mailing
International application No. PCT/US 00/18411	International filing date (day/month/year) 05/07/2000
Applicant MOSKOWITZ, Scott A.	

1. The International Searching Authority

(i) considers that there are 2 *(number of)* inventions claimed in the international application covered by the claims indicated on the extra sheet:

and it considers that the international application does not comply with the requirements of unity of invention (Rules 13.1, 13.2 and 13.3) for the reasons indicated on the extra sheet:

(ii) [X] has carried out a partial international search (see Annex) [ ] will establish the international search report on those parts of the international application which relate to the invention first mentioned in claims Nos.:
1-5, 26-29

(iii) will establish the international search report on the other parts of the international application only if, and to the extent to which, additional fees are paid

2. The applicant is hereby **invited**, within the time limit indicated above, to pay the amount indicated below:

EUR 945,00 x 1 = EUR 945,00
Fee per additional invention / number of additional inventions / total amount of additional fees

Or, ______ x ______ = ______

The applicant is informed that, according to Rule 40.2(c), **the payment of any additional fee may be made under protest**, i.e., a reasoned statement to the effect that the international application complies with the requirement of unity of invention or that the amount of the required additional fee is excessive.

3. [ ] Claim(s) Nos. ______ have been found to be unsearchable under Article 17(2)(b) because of defects under Article 17(2)(a) and therefore have not been included with any invention.

Name and mailing address of the International Searching Authority	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL-2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Marja Brouwers

Form PCT/ISA/206 (July 1992)

'ent Family Annex

Information on patent family members

Inte... ional Application No
PCT/US 00/18411

Patent document cited in search report		Publication date	Patent family member(s)		Publication date
NL 1005523	C	15-09-1998	NONE		
WO 9744736	A	27-11-1997	AU	3206397 A	09-12-1997
EP 0649261	A	19-04-1995	JP	7115638 A	02-05-1995
			US	5933499 A	03-08-1999
US 5974141	A	26-10-1999	US	6076077 A	13-06-2000
			US	6002772 A	14-12-1999
			US	6097818 A	01-08-2000

Form PCT/ISA/208 (patent family annex) (July 1992)

Annex 'orm PCT/ISA/206
COMMUNICATIC. ELATING TO THE RESULTS
OF THE PARTIAL INTERNATIONAL SEARCH

In ational Application No
PCT/US 00/18411

1. The present communication is an Annex to the invitation to pay additional fees (Form PCT/ISA/206). It shows the results of the international search established on the parts of the international application which relate to the invention first mentioned in claims Nos.:
1-5, 26-29

2. This communication is not the international search report which will be established according to Article 18 and Rule 43.

3. If the applicant does not pay any additional search fees, the information appearing in this communication will be considered as the result of the international search and will be included as such in the international search report.

4. If the applicant pays additional fees, the international search report will contain both the information appearing in this communication and the results of the international search on other parts of the international application for which such fees will have been paid.

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication where appropriate, of the relevant passages	Relevant to claim No.
X	NL 1 005 523 C (EINDHOVEN TECH HOCHSCHULE) 15 September 1998 (1998-09-15) abstract; figure 4 page 1, line 35 -page 3, line 9 page 9, line 21 -page 10, line 5	1,2, 26-29
X	WO 97 44736 A (APPLE COMPUTER) 27 November 1997 (1997-11-27) abstract; figures 2A,2B,2C,3 page 2, line 35 -page 3, line 27 page 9, line 10 -page 11, line 25	1,2
Y		3,4
Y	EP 0 649 261 A (CANON KK) 19 April 1995 (1995-04-19) page 3, line 53 -page 4, line 5 page 7, line 18 - line 23	3,4
A	US 5 974 141 A (SAITO MAKOTO) 26 October 1999 (1999-10-26) abstract; figures 4A-4G column 8, line 24 - line 67	5,26

☐ Further documents are listed in the continuation of box C.

☒ Patent family members are listed in annex.

° Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"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)

"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

"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

"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

"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.

"&" document member of the same patent family

3

Form PCT/ISA/206 (Annex, first sheet) (July 1992)

This International Searching Authority found multiple (groups of) inventions in this international application, as follows:

1. Claims: 1-5, 26-29

   Protecting the distribution of digital data to be used with a digital player charachterized by encrypting format information and allowing low quality play back in case of lack of decrypting key.

2. Claims: 6-25

   Digital signal encrypting technique combining transfer functions with predetermined key creation.

This finding is based on the following reasons.

The prior art has been identified as NL1005523 (D1). This document shows a method for protecting the distribution of digital information, the digital information including two subparts, a digital sample and format information, comprising the steps of: identifying and separating the two subparts; encoding the format information subpart using a key; recombining the encoded first subpart with the un-encoded second subpart, generating in this way an encoded version of the digital information. A predetermined key corresponding to the encoding key is then required for the decryption of the format information. All the features which form the subject matter of claims 1 and 2 are then disclosed by D1 (see following passages: abstract; page 1, line 35 - page 3, line 9; page 9, line 21 - page 10, line 5; fig. 4)

From the comparison between D1 and the 1st invention (see claim 3) the following technical featuree can be seen to make a contribution over this prior art (in the sense of PCT rule 13.2):
- the digital information is configured to be used with a digital player and the information output from said digital player has a degraded quality unless it is provided with a predetermined key (Special Technical Features 1, STF1).
From these STF1 the objective problem to be solved can be summarized as:
- permitting preview of distributed digital information

From the comparison between D1 and the 2nd invention (see claim 6) the following feature can be seen to make a contribution over the same prior art:
- using a transfer function-based mask set for creating a key to manipulate data at the inherent granularity of the file format of a digital sample (STF2).
From this STF2 the objective problem to be solved can be summarized as:
- improving the security of techniques for data protection

The above analysis shows that inventions 1 and 2 do not have same or similar Special Technical Features. Furthermore, a comparison of the objective problem 1 with the objective problem 2, both seen in the light of the description and the drawings of the present application, indicates that there is no technical correspondence between these problems nor do they show any corresponding technical effect.

As a result, inventions 1 and 2 fail to demonstrate a single general inventive concept as required by PCT rule 13.1.

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 12/14 | A1

(11) International Publication Number: WO 97/44736

(43) International Publication Date: 27 November 1997 (27.11.97)

(21) International Application Number: PCT/US97/08264

(22) International Filing Date: 15 May 1997 (15.05.97)

(30) Priority Data: 08/652,862 23 May 1996 (23.05.96) US

(71) Applicant: APPLE COMPUTER, INC. [US/US]; 1 Infinite Loop - MS: 38-PAT, Cupertino, CA 95014 (US).

(72) Inventor: WEHRENBERG, Paul, J.; 3516 Ross Road, Palo Alto, CA 94303 (US).

(74) Agents: CARMICHAEL, Paul, D. et al.; Apple Computer, Inc., 1 Infinite Loop - MS: 38-PAT, Cupertino, CA 95014 (US).

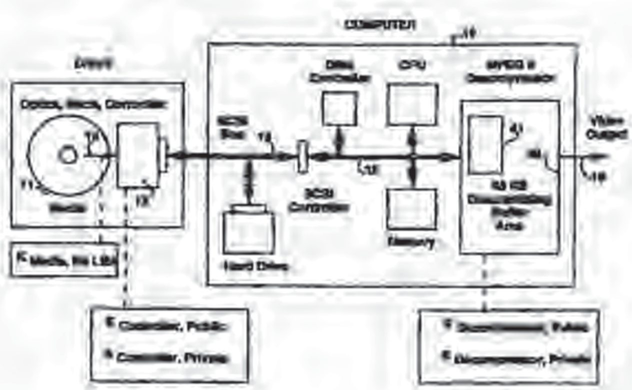
(81) Designated States: AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CU, CZ, DE, DK, EE, ES, FI, GB, GE, GH, HU, IL, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, TJ, TM, TR, TT, UA, UG, UZ, VN, YU, ARIPO patent (GH, KE, LS, MW, SD, SZ, UG), Eurasian patent (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European patent (AT, BE, CH, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI patent (BF, BJ, CF, CG, CI, CM, GA, GN, ML, MR, NE, SN, TD, TG).

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: METHOD AND APPARATUS FOR TWO-LEVEL COPY PROTECTION



(57) Abstract

An apparatus and method for providing two levels of copy protection, including a first method for copy protection, including a key, and a second method for copy protection. One level of copy protection is a moderately secure level to allow decrypting a medium- to high-bandwidth data stream without significant delay of the data stream. The second level of copy protection can be highly secure but can be utilized less often and so can be decrypted more slowly. One useful combination is to use a key encryption scheme for the first level of copy protection of a primary data stream, then to use the second protection scheme to securely transfer the first level key from a protected storage location to a decoding location. Encoded primary data can be stored on a removable media, together with the decryption key stored in a special location. The media drive unit can access the special location and, using the second level copy protection scheme, transfer the key securely to a descrambling unit. The first level copy protection can involve selective reordering of data subunits within a data unit according to a scrambling vector, then encoding the scrambling vector using the first key, and storing the encoded scrambling vector with the corresponding data unit.

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		

METHOD AND APPARATUS FOR TWO-LEVEL COPY PROTECTION

Field of the Invention

This invention relates to data encryption and decryption, and more particularly to an improved method and apparatus for using one level of encryption to establish a secure communication channel, then passing a decryption key over that channel for subsequent decryption. This invention includes a new method of scrambling bulk data. This invention is particularly useful for protecting bulk information intended for widespread distribution such as movies or music in CD or DVD formats.

Background of the Invention

The field of data encryption has been the subject of extensive scholarly investigation and has been the topic of many patents in the United States and other countries. For general reference, the background description in each of United States Patent Nos. 5,497,422 (Tysen et al., 5 March 1996) and 5,438,622 (Normile et al., 1 August 1995) discuss representative encryption schemes known in the art. Each of these patent applications are assigned to Apple Computer, Inc. These patents are incorporated herein by reference in their entirety.

A wide variety of information is sold to consumers in various forms. One major category of information is computer software. Another major category of information is music, often in the form of CDs or tape. Still another major category of information is movies, usually over cable or satellite television links but often in the form of analog tape or LaserDisc. There is a tension in distribution of any form of information because if consumers will buy it from a rightful owner, other consumers are likely to buy illegal copies made from legitimate originals.

Various copy protection schemes have been considered for use with various media. Scrambling of cable or satellite channels is common. A variety of anti-copying schemes are used in analog video tape. CDs or digital tape can be encoded with anti-copying codes.

Distribution of various information in digital form has troubled many content providers because making the information available potentially makes it quite simple for a user to make one or many illegal copies of that content. Forms of such content include movies, music, and data such as encyclopedic compilations. This issue has been widely discussed in relation to audio CDs, LaserDiscs and other formats.

In the personal computer environment, the protection of intellectual property has been of interest since the beginning of the industry. In computer software, a variety of special encoding or encryption schemes have been used. Some software requires a hardware key to be connected in some way to the computer system. Use of such systems frustrates casual copiers but often has some negative impact on legitimate users.

Due to the rapid growth of the industry and the technical difficulties associated with controlling information flow in an intrinsically open architecture, the industry players have more often than not written the problem off as intractable, at least in relevant time and cost frames. However, the problem remains. And as the convergence between entertainment and computing moves forward, driven by the evolution of hardware and software technologies, industry participants with different attitudes and requirements enter the discussion.

The problem is particularly acute with the advent of the DVD technology as a mass storage device in computers. DVD is a new, high density storage medium capable of storing about 4.5 through 18 gigabytes of information on a single 12 centimeter disc. Commercial products have already been announced before May 1996 for availability before December 1996.

The movie industry, with its high degree of sensitivity to intellectual property protection, is concerned that none of the new transmission modalities, including personal computers, enable free copying of their material. Other content providers have similar concerns. Some sort of copy protection scheme would encourage content providers, such as the movie industry, to distribute information such as movies in digital format.

The proposed protection scheme is intended to fall between a "screen door latch" (too weak) and a "Fort Knox" approach (too clumsy and expensive for mass-market products). Although it will be discussed here in the context of DVD, one skilled in the art will appreciate that this copy protection scheme can be used in many other situations or collections of elements.

Summary of the Invention

The invention provides a two-stage copy protection scheme. This is particularly useful where large quantities of data are to be encrypted and decrypted using an encryption key but that encryption key is to be carefully protected until the data is to be decrypted using an authorized retrieval system.

One stage of the retrieval system includes an encryption scheme to assure that the retrieval is made in an authorized system, and another stage of the retrieval system uses a stored encryption key to decode the data of interest. In one preferred implementation, the encryption key is used as a descrambling code.

To minimize the performance impact on the apparatus and not constrain use of system resources by low priority or low value data streams, the information flow can be broken into elements with a distinct hierarchy of bandwidth. For example, an MPEG stream (high bandwidth) may be merely scrambled, the scrambling control bits (much lower bandwidth) may be encoded, and only the MPEG-decode key information necessary to decode the scrambling control bits (very low bandwidth) is key encrypted.

The scrambling can be done in any of many ways, some of which are discussed in detail below. For example, the order of the data within a unit of data can be reordered in a controlled way to give a scrambled signal. Each unit of data, such as a 64 KB block, can be scrambled in a defined way, then a descriptor which characterizes that scrambling can be encrypted using a key and the encoded descriptor can be stored with the relevant block of data. A single key can be used to decrypt any scrambling descriptor and the descriptor can be changed for each unit of data, that is, each unit of data can be independently scrambled. With a key available, it is relatively straightforward to correctly reorder the scrambled data into the original, "clear text" format. With no key, if a sufficiently complex scrambling method has been chosen, it can be challenging to identify the correct key by trial and error, particularly since each data unit is scrambled in a different pattern. With the key, a moderately complex scrambling method will not have a significant effect on data reconstruction rate and thus becomes transparent to the user.

This copy protection becomes much more powerful if the key can be changed for different units of primary information, for example for each movie title.

Storage and access to this key raises an interesting challenge, but this can be managed very conveniently by using a separate encryption mode to secure the key and provide it in a coordinated fashion with the program of interest. One way to do this is to store the key in a secure manner on the same storage medium as the scrambled information. The mechanism of this separate storage mode can be set at a desired level of complexity. One preferred mode is to make this key inaccessible by typical access operations, but readily accessible through special operations. Specifically, in just one preferred embodiment, the key may be stored at a location which is inaccessible to a host computer which can only access a logical block address, but readily accessible to a drive control unit, which may be designed to access a specific physical address, preferably not a logical block address. This access capability can be designed into the drive control unit, and the relevant key can be stored at the corresponding location when the media is prepared.

Subsequent manipulation of the key can be under close security. Since the key need be extracted only once, taking even several seconds to extract and/or transfer the key will not have a significant impact on the user.

In one preferred embodiment, a public/private key pair is stored in a disk drive mechanism and a second public/private key pair is stored in a decryption/decode unit such as an MPEG2 decoder. The key pairs are used to establish a secure channel of communication between the disk drive and the decoder and, once the channel is secure, a message can be read safely from the storage medium into the decoder even if the data path for the channel between these elements is unsecure. This message is the information content or message protected using the high-level security scheme, but is itself the key for the low-level security scheme. Passing this encrypted key over a secure channel makes it extremely difficult to intercept the key and use it for improper purposes.

This inhibits casual copying by setting up the system so that the data flow path between a source, such as a DVD-ROM drive, and a destination, such as an MPEG decoder carries only scrambled information and decryption to clear text occurs only in an isolated portion of the system, preferably within a special descrambler/decoder unit. The scheme cannot be defeated except by system patches, and a new patch is required for each title defeated, that is for each new title encryption key.

Scrambling and encrypting the primary information means that a read of the media by a system that does not implement correct decoding will give unintelligible results. Only the application software, with a little help from the operating system, can allow correct decoding of the primary information, as in correct decoding and display of a movie.

Distributing the copy protection elements balances the economic and processing power burden so that no single part of the overall system bears all the cost and effort of protecting the valuable information. Modifying the media format to carry scrambled data and modifying the drive to take advantage of its closed sub-system status balances these costs.

Moving the implementation burden on the computer system toward the peripheries, i.e. the media, the mass storage device, and the application software minimizes the impact on the operating system software and motherboard hardware. This method and apparatus avoids the need to create new high bandwidth information flow paths and new file systems while providing useful protection for the valuable source information.

One object of this invention is to provide reasonably effective prevention of casual copying by a user.

Another object of this invention is to provide a copy protection scheme with little or no impact on or modification of the traditional, primary computer components.

Still another object of this invention is to minimize the performance impact of the protection scheme by selectively protecting the most unique or most valuable portions of a data stream.

This and other objects and advantages of the invention, as well as the details of an illustrative embodiment, will be more fully understood from the following specification and drawings.

Brief Description of the Drawings

Figure 1 illustrates an apparatus useful in practicing this invention.

Figures 2A, 2B and 2C illustrate a source data structure in its original form (2A), then formatted and addressed after scrambling (2B) and then formatted and addressed after encrypting the scrambling vector (2C).

Figure 3 illustrates encryption of a 32 element scrambling vector.

Figure 4 illustrates descrambling inside an MPEG2 decoder.

Description of the Preferred Embodiments

Representative elements and the process of a preferred implementation of the copy protection scheme are described below. A preferred embodiment will be described by way of example. Figure 1 gives a schematic of the complete system. Note that the MPEG decoder is depicted as a hardware element, but the copy protection method can be used, perhaps with a lesser degree of protection, when the MPEG decoder is a software process. A more generic system includes only a medium, a reader for that medium, a destination for information from that medium, and a channel between the reader and the destination.

The medium does not need to be physically close to the destination. For example, the source information might be stored on a server such as a video-on-demand server, and the destination might be located many miles away, as in a set top box, cable decoder, or other interface. For example, the server might include a reader which securely transfers a decryption key to the destination in a user's home, then communicates a scrambled data stream over some channel to the destination where it is descrambled according to the decryption key.

The channel for communicating the decryption key need not be the same as the channel for communicating the encoded, bulk information, but a single channel might be used for both purposes. A channel might be a data path through a computer but might also be a telephonic, television cable or satellite link or even a combination of two or more such links. The decoding can be done after any number of intervening transfers of the encoded digital information. One useful example would be a decoder coupled directly to a television set for direct and secure transmission of an encoded movie from a source to an end user.

The channel can include several connected data paths and still safely transfer encoded information. For example, the primary information may be stored in encoded form on a server. That server might be connectable through several separate links, perhaps telephone or cable switching boxes, until final delivery to a decoder.

One encoding scheme is used to encode the primary data. A key for this scheme is maintained according to one or more of a variety of methods. A second encoding scheme is used to transfer the key from a secure location to a location for use in decoding the primary data. In a preferred embodiment, the key for the primary data is stored with the data in a generally inaccessible location. This might be in a special track or location on a disk containing the primary information. Alternatively, this might be maintained on a server as in, for example, a video-on-demand system, or in a selected-access system as in, for example, a pay-per-view system.

The specific encoding scheme for the primary information may take any of a variety of forms. Some encoding schemes are known in the art but there are other, new schemes that are particularly useful. One particularly useful scheme is a simple scrambling scheme where the scrambling key is sufficiently complex to make brute-force decoding difficult, but simple enough to allow for rapid decryption when the correct key is available. The encoding scheme for the secondary information, here the scrambling or primary information key itself, also may take any of a variety of forms. In one preferred form, this secondary encoding uses two pairs of private and public keys to establish a secure channel between the reader, for example the device where the primary key is maintained, and the destination, for example the device where the primary key is to be used.

As illustrated in Figure 1, there are five keys involved in one preferred implementation of the copy protection apparatus of this invention, one for the primary information and four for secure transfer of that key.

Secure Transfer of the Primary Information Key

In one preferred embodiment, the primary information key is placed on the media during manufacture. It may be stored in a location or sub channel that is readily accessible to the drive controller but difficult or impossible to access otherwise. In a preferred embodiment, is not in an area that is addressable by logical block address (LBA) and thus is not accessible by devices other than the drive controller itself. This primary information key is transferred as the message for a public key/private key transaction through the open computer system to a descrambler where it is used to descramble the primary information.

The drive controller is possessed of a public key and a private key, and has the capability of receiving another entity's public key. The drive can then encrypt a message using its private key and the received public key. This encrypted message can be requested by the operating system and passed to the owner of the non-drive public key, the destination.

The non-drive entity can then use its own private key and the drive's public key to decrypt the received message. As noted above, the key on the media is the message for the second encoding system. Thus the key for the primary encoding is itself encoded using the second encoding system and transferred through the open computer system to the non-drive entity, where it is decoded according to the second encoding scheme. This key can then be loaded into the primary decoding system and used directly.

The key encoding transaction described above uses very robust encryption which may be computationally intensive. However the size of the message is small and the transaction is a one time thing which is done at startup. The complexity of this encryption allows for a very high level of security. Since this encryption and decryption take place infrequently, preferably only at startup, there is very little penalty to taking some time. A typical user will not mind and may not even notice a delay of up to even a few seconds during the initiation or loading of a media title. One preferred sequence of events in just one preferred embodiment is as follows.

The primary information is MPEG encoded data. The main channel (not shown - part of information stream 12) from the DVD media 11 contains MPEG encoded data. The DVD version of MPEG contains multiple opportunities for scrambling. Scrambling bits are defined and/or reserved bits exist in Video, Audio, Sub-picture, Data Search Information, and Video Blanking Information packs.

The copy protection method described here scrambles the video and/or audio and/or sub pictures. An encoded version of the scrambling control bits are then inserted into the MPEG stream. Direct de-scrambling based on the inserted scrambling control bits will not give the correct results. To obtain correct de-scrambling, the scrambling control bit stream must be processed through a decoder, such as a tapped shift register.

The primary information key includes information on the correct setup of the decoder, such as position of the taps for correct scrambling control bit decoding. This primary information key is put on the media in a sub channel or an area that is addressable by physical address, but not by logical block address.

This last requirement means the drive controller can access the information needed for decoding scrambling control, but the host system 16 cannot obtain it by a read command to a logical block address. The drive controller 13 is designed to pass this information over to the host system 16 only in encrypted form using the controller's private key and the public key of the intended recipient. In Figure 1 the intended recipient is the MPEG decoder 40, particularly the descrambling unit illustrated by its buffer area 41.

The recipient, MPEG decoder 40, uses its private key and the controller's public key to decrypt the information that originated in the media sub channel or logically unaddressable regions.

If the scrambled MPEG data stream 12 is directed to a recording device, the copy protection scheme is not defeated because the information to properly decode the scrambling control bits is not present in any form. The required information passes through the host in encrypted form only and is therefore useless even if trapped and recorded.

The operating system brokers the exchange of public keys between the controller and the MPEG decoder at startup.

At startup, the DVD-ROM device driver (not shown, part of system software) requests the operating system to provide the public keys of any installed MPEG2 decoders. The operating system obtains public keys from drive 10 and MPEG2 decoder 40 (if present). The operating system provides the public key of the decoder 40 to the drive 10 and public key of the drive 10 to the decoder 40. The DVD-ROM device driver refuses to accept any MPEG decoder public key except during the startup sequence. This give some extra security against impersonation.

Use of the Primary Information Key

During primary data transfer operation, the primary information key is used by the recipient, e.g. the MPEG decoder, to correctly reorder the scrambled logical blocks received by streaming off of the storage device, e.g. a DVD disk. The specific function of the primary information key depends on the specific scrambling scheme. One preferred scrambling scheme is described below. Once transferred to the recipient, the primary information key is inserted into an appropriate decoder, then used to unscramble the primary data stream. In a preferred embodiment, the primary data stream is scrambled MPEG data which is descrambled to give a traditional MPEG data stream which then is decoded to give a video image, for example, an NTSC standard image or an RGB image, which can be displayed on an appropriate monitor.

Scrambling Scheme

The preferred scrambling scheme is designed to be computationally intensive to break if attacked as a jig saw puzzle, but easy to reorder if the key is available. A data unit is divided into smaller units, which are then rearranged according to a selected scheme. Information for reordering that data unit is stored for retrieval in conjunction with that data unit. This might take the form of a scrambling vector, which might be stored in a subheader or perhaps embedded in the scrambled data unit. The information can be further protected by encoding the scrambling vector according to an encryption scheme, using a selected primary information key. The same process can be repeated for subsequent data units, but each data unit can be rearranged in a different order. In each instance, the scrambling vector is retrievable and can be reassociated with its corresponding data unit. The same primary information key can be used to encode a series of scrambling vectors. The primary information key, along with each particular instance of the encoded scrambling vector, is used to decode the scrambling vector which in turn is used to correctly reorder the data unit.

In one particularly preferred embodiment, a selected program, such as a movie title, is divided into data units, each of which is scrambled individually, and each scrambling vector is encoded using a single key. That primary information key can be stored with the primary program, and each program can use a different primary information key. The specific scrambling and descrambling schemes can be implemented in specialized hardware for rapid and convenient playback of the primary program.

Figures 2A, 2B, 2C, 3 and 4 describe one scrambling embodiment that uses a scrambling vector subheader on 2 KB data blocks. If the user data stream (information or primary data stream) has places to put this scrambling vector data, it could be placed inside the user data and no subheader would be necessary.

Referring to Figures 2A, 2B and 2C, Figure 2A illustrates representative, primary data as formatted and addressed before scrambling. The data to scramble is segmented into groups of 32 sequential blocks, also referred to as sectors, each having a logical block address (LBA), each containing 2 KB for a total of 64 KB. Data in this form is considered clear text. For example, if it were MPEG2 movie data, it would be directly decodable by an MPEG2 decoder conforming to the published standards.

Changing the order of the sequential blocks scrambles the primary information. Figure 2B illustrates data as formatted and addressed after scrambling of LBAs and user data blocks in the 64 KB sequence. There are 32! distinct ways to randomly assign the data blocks to the 32 LBAs in each 64 KB sequence. The illustrated order, 5, 31, 17, ..., 22, is merely illustrative. Each group of 32 sectors can be scrambled independently and the correct position within the group given by the value of the Scrambling Vector Element (SVE) placed in a subheader.

Figure 2C illustrates data as formatted and addressed after scrambling of LBAs and user data blocks in the 64 KB segment. The scrambled form, SV*, of the scrambling vector, SV, is now placed in the subheaders of the group of 32 sectors. The SV*E user data are mastered onto the media, such as a DVD disc, in the sequence shown in Figure 2C. If the data stream is a scrambled MPEG2 movie, a standard MPEG2 decoder will not be able to make any sense out of it in the scrambled form.

Referring to Figure 3, this figure shows encryption of a 32 element scrambling vector. The elements of the scrambling vector are encrypted using a reversible algorithm whose parameters are defined by the media key, K_{Media}. Recall this is the key that is only readable by the drive 10, and this key is never passed as clear text through the open system. There are a number of simple approaches available for encrypting the scrambling vector, such as tapped shift registers, pseudo random sequence generators, etc.

Referring to Figure 4, descrambling is done inside MPEG2 decoder 40. The descrambling buffer area 41 is equal to or greater than the 64 KB of user data plus the 32 byte overhead of the SV*. Typical memory allocation might be done on 1 KB boundaries, so handling the SV* and converting it back to SV might necessitate 65 KB for the descrambling buffer area. The internal output is a clear text MPEG data stream which is then decoded to give final output 19 as uncompressed video.

Other data streams can be processed in an analogous manner.

Another preferred scrambling scheme reorders only part of the user data block. An MPEG data stream includes high order bits that define information about the sequence of the user data blocks. If data blocks including this information were simply reordered, it would be possible to use those specific bits to reassemble the data in the correct order. However, if only part of the user block is reordered and the expected sequence information is left untouched, the user blocks will be corrupted because the first part of the user block will be matched with the second part of a different user block. In a preferred implementation, the first half of each block is untouched while the second half of each block is reordered as described above in connection with Figures 2A, 2B and 2C. The scrambling vector is prepared, encoded and stored as described above. This scheme still has 32! possible combinations. Since each data unit can be reordered using a different scrambling vector, descrambling will be difficult without the key, but simple with the correct primary information key.

The size of the data unit affects the complexity of encoding and decoding. The example above describes a data unit subdivided into 32 blocks. This allows reordering in 32! possible combinations which gives a fairly complex, and thus secure, encoding scheme. In the DVD specification, a standard data unit is 32 KB of 2 KB subunits. This provides 16 blocks which can be reordered as decribed above, to give 16! possible combinations of scrambled data.

A media drive controller can be designed to support this scheme at minimal cost impact. As far as the transferring a scrambled primary data stream, a traditional drive controller need not be modified at all. To support the secondary encoding, the drive controller needs to maintain a public and a private key had be able to support the selected encryption scheme. To support the preferred embodiment of storing the primary information key in a special location on the media, the drive controller needs to be designed to achieve the needed access and transfer the key appropriately.

The recipient similarly may need only minor modification. If the data stream decoder is a separate unit, there may be no need to modify the decoder. In a preferred embodiment, the recipient is or is coupled to a descrambler unit which in turn is tightly coupled to a decoder such as an MPEG decoder. The descrambler unit should support the selected scrambling scheme and should manage the primary information key as needed. In a preferred embodiment, the descrambler manages a public and a private key, interfacing with the secure data channel, receiving and decrypting the primary information key, and using the primary information key to descramble the primary information.

A general description of the device and method of using the present invention as well as a preferred embodiment of the present invention has been set forth above. One skilled in the art will recognize and be able to practice many changes in many aspects of the device and method described above, including variations which fall within the teachings of this invention. The spirit and scope of the invention should be limited only as set forth in the claims which follow.

Claims

What is claimed is:

1. An apparatus for providing two levels of copy protection, said apparatus comprising
   first means for copy protecting information, said first means including a key, and
   second means for copy protecting information, said second means applied to said key for said first means.

2. The apparatus of claim 1 wherein said first means for copy protecting information is a selective disordering of an information data stream and said key can be used to correctly reorder the disordered information data stream.

3. The apparatus of claim 1 further comprising two devices connected by a communication channel and wherein said second means for copy protecting information is a means to provide a secure communication channel between two devices.

4. The apparatus of claim 3 wherein said second means for copy protecting information includes use of a public and private key by at least one of said two devices.

5. The apparatus of claim 3 wherein said key for said first means for copy protecting information is encoded for transmission over said communication channel between said two devices.

6. The apparatus of claim 1 further comprising
   a source of information encoded according to a first means for copy protection,
   a decoder for said information according to said first means for copy protection, using said key,
   a storage location for said key,
   a means for communicating between said storage location and said decoder,
   wherein said second means for copy protecting information comprises means for encoding said key for secure communication between said storage location and said decoder.

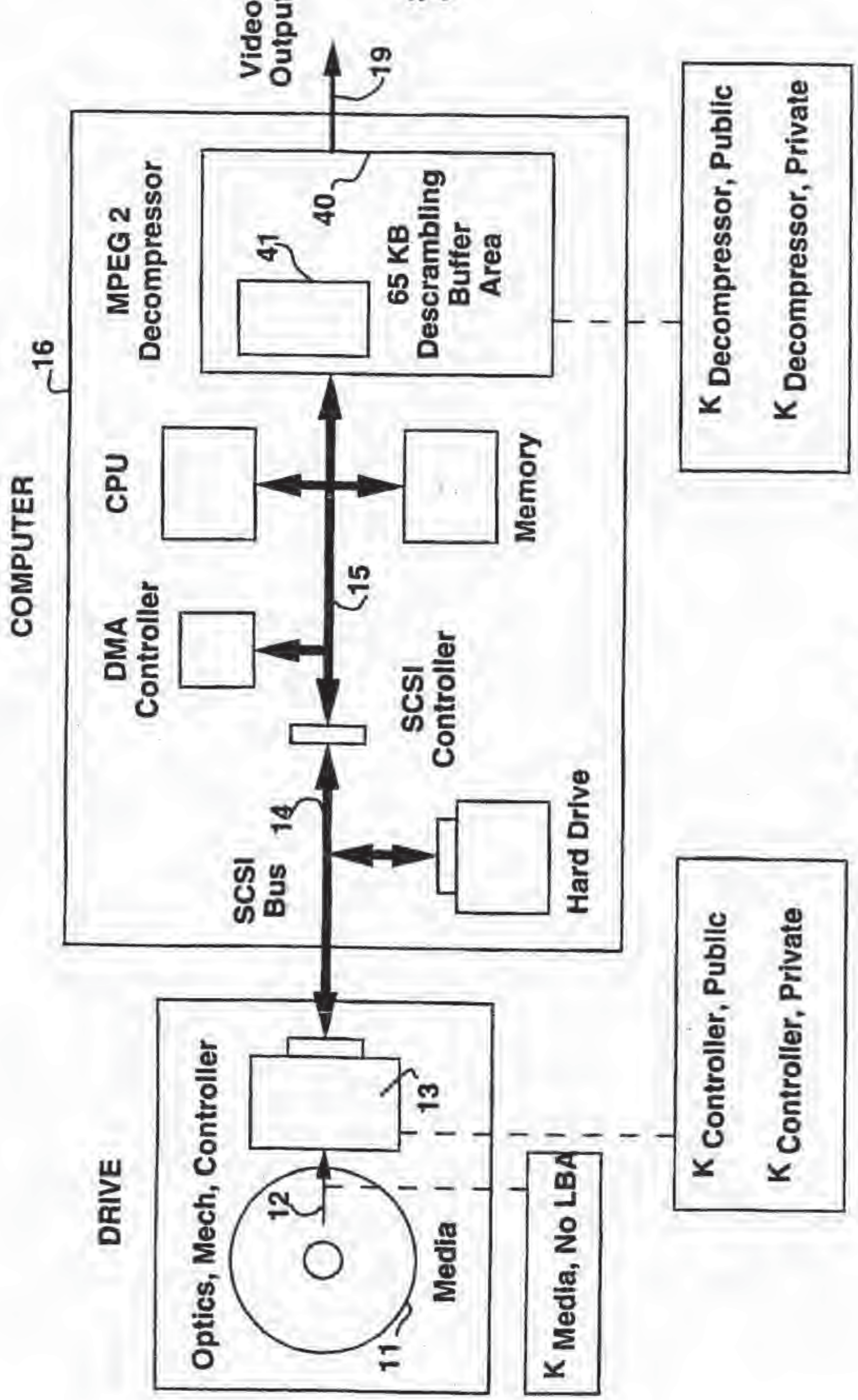

COMPUTER
16
DMA Controller
CPU
MPEG 2 Decompressor
41
40
65 KB Descrambling Buffer Area
Memory
15
SCSI Controller
SCSI Bus
14
Hard Drive
Video Output
19
K Decompressor, Public
K Decompressor, Private
DRIVE
Optics, Mech, Controller
12
13
11
Media
K Media, No LBA
K Controller, Public
K Controller, Private

Figure 1

64 KB

LBA n	2 KB User Data (block n)
LBA n + 1	2 KB User Data (block n + 1)
LBA n + 2	2 KB User Data (block n + 2)
LBA n + 3	2 KB User Data (block n + 3)
LBA n + 4	2 KB User Data (block n + 4)
LBA n + 5	2 KB User Data (block n + 5)
LBA n + 31	2 KB User Data (block n + 31)

FIGURE 2A

LBA n	SVE 0 (5)	2 KB User Data (block n + 5)
LBA n + 1	SVE 1 (31)	2 KB User Data (block n + 31)
LBA n + 2	SVE 2 (17)	2 KB User Data (block n + 17)
LBA n + 3	SVE 3 (4)	2 KB User Data (block n + 4)
LBA n + 4	SVE 4 (24)	2 KB User Data (block n + 24)
LBA n + 5	SVE 5 (0)	2 KB User Data (block n)
....	....	....
....	....	....
LBA n + 31	SVE 31 (22)	2 KB User Data (block n + 22)

FIGURE 2B

LBA n	SV* E 0	2 KB User Data (block n + 5)
LBA n + 1	SV* E 1	2 KB User Data (block n + 31)
LBA n + 2	SV* E 2	2 KB User Data (block n + 17)
LBA n + 3	SV* E 3	2 KB User Data (block n + 4)
LBA n + 4	SV* E 4	2 KB User Data (block n + 24)
LBA n + 5	SV* E 5	2 KB User Data (block n)
....	....	....
....	....	....
LBA n + 31	SV* E 31	2 KB User Data (block n + 22)

FIGURE 2C

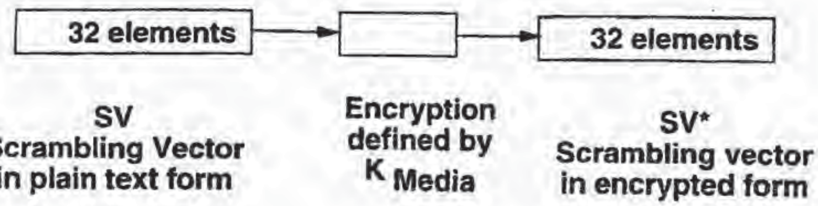


FIGURE 3

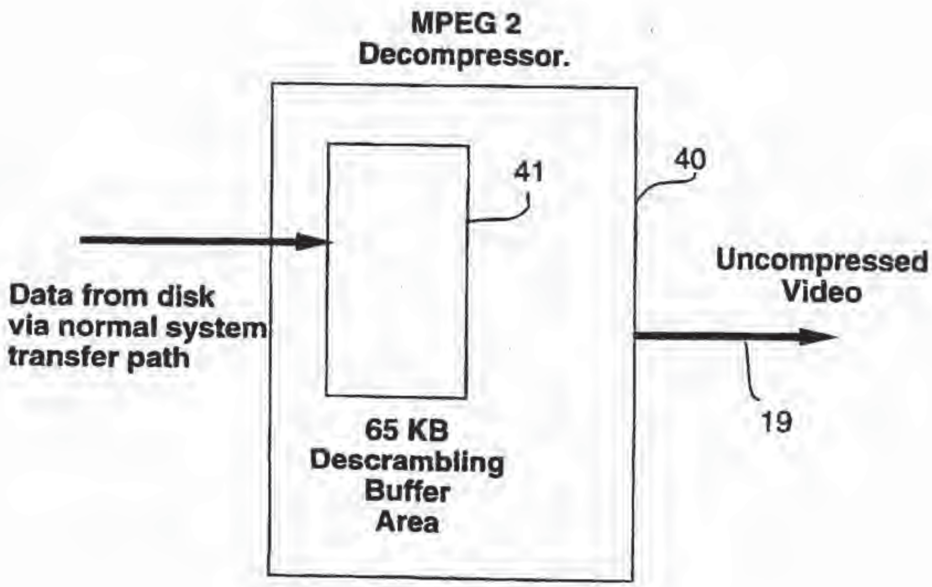


FIGURE 4

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 97/08264

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 G06F12/14

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)
IPC 6 G06F G11B

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
X	US 5 058 162 A (SANTON JOHN C ET AL) 15 October 1991 see abstract; figures 2,6,7 see column 2, line 24 - line 31 see column 3, line 4 - line 19 see column 7, line 20 - line 49 ---	1,3,5,6
X	US 4 903 296 A (CHANDRA AKHILESHWARI N ET AL) 20 February 1990 see abstract; figures 1,7.1 see column 3, line 2 - column 4, line 31 see column 7, line 22 - line 61 see column 8, line 37 - column 9, line 2 ---	1,3-6
A	US 5 438 622 A (NORMILE JAMES O ET AL) 1 August 1995 cited in the application see the whole document ---	1,3-6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"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)

"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

"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

"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

"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.

"&" document member of the same patent family

1

Date of the actual completion of the international search	Date of mailing of the international search report
9 October 1997	13.10.97

Name and mailing address of the ISA	Authorized officer
European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Powell, D

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 97/08264

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 319 705 A (HALTER BERNARD J ET AL) 7 June 1994 see column 3, line 17 - line 29 ---	2
A	US 4 168 396 A (BEST ROBERT M) 18 September 1979 see abstract; figures 1,2 see column 3, line 60 - column 4, line 48 ---	2
A	US 5 224 166 A (HARTMAN JR ROBERT C) 29 June 1993 -----	

1

Form PCT/ISA/210 (continuation of second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

Information on patent family members

Internal Application No
PCT/US 97/08264

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5058162 A	15-10-91	JP 5173891 A	13-07-93
US 4903296 A	20-02-90	US 4644493 A	17-02-87
		DE 3587658 D	23-12-93
		DE 3587658 T	11-05-94
		EP 0174472 A	19-03-86
		JP 1650990 C	30-03-92
		JP 3012744 B	20-02-91
		JP 61072345 A	14-04-86
US 5438622 A	01-08-95	NONE	
US 5319705 A	07-06-94	JP 7093148 A	07-04-95
US 4168396 A	18-09-79	US 4278837 A	14-07-81
US 5224166 A	29-06-93	EP 0583140 A	16-02-94
		JP 2085066 C	23-08-96
		JP 6112937 A	22-04-94
		JP 7107989 B	15-11-95

Form PCT/ISA/210 (patent family annex) (July 1992)

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : H04N 1/32

A1

(11) International Publication Number: WO 99/52271

(43) International Publication Date: 14 October 1999 (14.10.99)

(21) International Application Number: PCT/US99/07262

(22) International Filing Date: 2 April 1999 (02.04.99)

(30) Priority Data:
09/053,628 2 April 1998 (02.04.98) US

(71)(72) Applicant and Inventor: MOSKOWITZ, Scott, A. [US/US]; 16711 Collins Avenue #2505, Miami, FL 33160 (US).

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

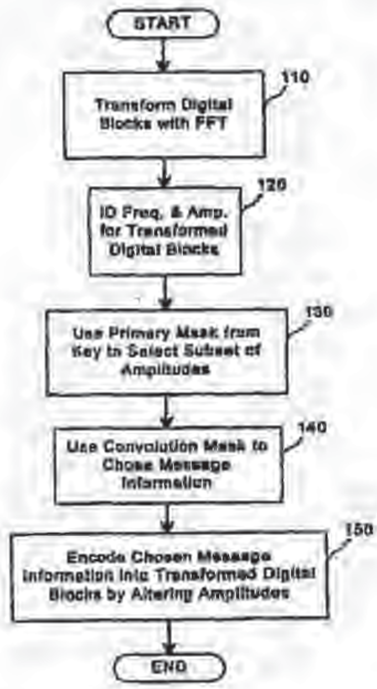
(81) Designated States: JP, European patent (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE).

Published
With international search report.

(54) Title: MULTIPLE TRANSFORM UTILIZATION AND APPLICATIONS FOR SECURE DIGITAL WATERMARKING

(57) Abstract

Multiple transform utilization and applications for secure digital watermarking. In one embodiment of the present invention, digital blocks in digital information to be protected are transformed into the frequency domain using a fast Fourier transform. A plurality of frequencies and associated amplitudes are identified for each of the transformed digital blocks and a subset of the identified amplitudes is selected for each of the digital blocks using a primary mask from a key. Message information is selected from a message using a transformation table generated with a convolution mask. The chosen message information is encoded into each of the transformed digital blocks by altering the selected amplitudes based on the selected message information.



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		

MULTIPLE TRANSFORM UTILIZATION AND APPLICATIONS FOR SECURE DIGITAL WATERMARKING

BACKGROUND

Field of the Invention

The invention relates to the protection of digital information. More particularly, the invention relates to multiple transform utilization and applications for secure digital watermarking.

Cross-Reference To Related Applications

This application claims the benefit of U.S. patent application Serial No. 08/587,943, filed January 17, 1996, entitled "Method for Stega-Cipher Protection of Computer Code," the entire disclosure of which is hereby incorporated by reference.

Description of the Background

Increasingly, commercially valuable information is being created and stored in "digital" form. For example, music, photographs and video can all be stored and transmitted as a series of numbers, such as 1's and 0's. Digital techniques let the original information be recreated in a very accurate manner. Unfortunately, digital techniques also let the information be easily copied without the owner's permission.

Digital watermarks exist at a convergence point where creators and publishers of digitized multimedia content demand local, secure identification and authentication of content. Because piracy discourages the distribution of valuable digital information, establishing responsibility for copies and derivative copies of such works is important. 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 artifacts, with one standard being perceptibility, in the underlying content signal, while maximizing its encoding level and "location sensitivity" in the signal to force damage to the content signal when removal is attempted. In considering the various forms of multimedia content, whether "master," stereo, National Television Standards Committee (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 undergoes damage, and therefore reduction of its value, with subsequent unauthorized distribution, commercial or otherwise. Digital watermarks address many of these concerns and research in the field has provided a rich basis for extremely robust and secure implementations.

Of particular concern is the balance between the value of a digitized "piece" of content and the cost of providing worthwhile "protection" of that content. In a parallel to real world economic behavior, the perceived security of a commercial bank does not cause people to immediately deposit cash because of the expense and time required to perform a bank deposit. For most individuals, possession of a US$100 bill does not require any protection beyond putting it into a wallet. The existence of the World Wide Web, or "Web," does not implicitly indicate that value has been created for media which can be digitized, such as audio, still images and other media. The Web is simply a medium for information exchange, not a determinant for the commercial value of content. The Web's use to exchange media does, however, provide information that helps determine this value, which is why responsibility over digitized content is desirable. Note that digital watermarks are a tool in this process, but they no not replace other mechanisms for establishing more public issues of ownership, such as copyrights. Digital watermarks, for example, do not replace the "historical average" approach to value content. That is, a market of individuals willing to make a purchase based solely on the perceived value of the content. By way of example, a picture distributed over the Internet, or any other electronic exchange, does not necessarily increase the underlying value of the picture, but the opportunity to reach a greater audience by this form of "broadcast" may be a desirable mechanism to create "potentially" greater market-based valuations. That decision rests solely with the rights holder in question.

Indeed, in many cases, depending on the time value of the content, value may actually be reduced if access is not properly controlled. With a magazine sold on a monthly basis, it is difficult to assess the value of pictures in the magazine beyond the time the magazine is sold. Compact disc valuations similarly have time-based variables, as well as tangible variables such as packaging versus the package-less electronic exchange of the digitized audio signals. The Internet only provides a means to more quickly reach consumers and does not replace the otherwise "market-based" value. Digital watermarks, properly implemented, add a necessary layer of ownership determination which will greatly assist in determining and assessing value when they are "provably secure." The present invention improves digital watermarking technology while offering a means to properly "tamper proof" digitized content in a manner analogous to methods for establishing authenticity of real world goods.

A general weakness in digital watermark technology relates directly to the way watermarks are implemented. Too many approaches leave detection and decode control with the implementing party of the digital watermark, not the creator of the work to be protected. This fundamental aspect of various watermark technologies removes proper economic incentives for improvement of the technology when third parties successfully exploit the implementation. One specific form of exploitation obscures subsequent watermark detection. Others regard successful over encoding using the same watermarking process at a subsequent time.

A set of secure digital watermark implementations address this fundamental control issue, forming the basis of "key-based" approaches. These are covered by the following patents and pending applications, the entire disclosures of which are hereby incorporated by reference: US Patent No. 5,613, 004 entitled "Steganographic Method and Device" and its derivative US patent application Serial No. 08/775,216, US patent application Serial No. 08/587,944 entitled "Human Assisted Random Key Generation and Application for Digital Watermark System," US Patent Application Serial No. 08/587,943 entitled "Method for Stega-Cipher Protection of Computer Code," US patent application Serial No. 08/677,435 entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data," and US Patent Application Serial No. 08/772,222 entitled "Z-Transform Implementation of Digital Watermarks." Public key crypto-systems are described in US Patents No. 4,200,770, 4,218,582, 4,405,829 and 4,424,414, the entire disclosures of which are also hereby incorporated by reference.

By way of improving these digital watermark security methods, utilization of multiple transforms, manipulation of signal characteristics and the requisite relationship to the mask set or "key" used for encoding and decoding operations are envisioned, as are optimized combinations of these methods. While encoding a watermark may ultimately differ only slightly in terms of the transforms used in the encoding algorithm, the greater issues of an open, distributed architecture requires more robust approaches to survive attempts at erasure, or even means for making detection of the watermark impossible. These "attacks," when computationally compared, may be diametrically related. For instance, cropping and scaling differ in signal processing orientation, and can result in the weakening of a particular watermarking approach but not all watermarking approaches.

Currently available approaches that encode using either a block-based or entire data set transform necessarily encode data in either the spatial or frequency domains, but never both domains. A simultaneous crop and scale affects the spatial and frequency domains enough to obscure most available watermark systems. The ability to survive multiple manipulations is an obvious benefit to those seeking to ensure the security of their watermarked media. The present invention seeks to improve on key-based approaches to watermarking previously disclosed, while offering greater control of the subsequently watermarked content to rights owners and content creators.

Many currently available still image watermarking applications are fundamentally different from the key-based implementations. Such products include products offered by Digimarc and Signum, which seek to provide a robust watermark by encoding watermark messages that rely entirely on comparisons with the original image for decode operations. The subsequent result of the transform, a discrete cosine transform performed in blocks, is digital signed. The embedded watermarks lack any relationship to the perceptual qualities of the image, making inverse application of the publicly available decoders a very good first line of attack. Similarly, the encoding process may be applied by third parties, as demonstrated by some robustness tests, using one process to encode over the result of an image watermarked with another process. Nonrepudiation of the watermark is not possible, because Digimarc and Signum act as the repository of all registrations of the image's ownership.

Another line of attack is a low pass filter that removes some of the high frequency noise that has been added, making error-free detection difficult or impossible.

Finally, many tests of a simple JPEG transform indicate the watermarks may not survive as JPEG is based on the same transforms as the encoding transforms used by the watermarking process. Other notable implementations, such as that offered by Signafy (developed by NEC researchers), appear to encode watermark messages by performing a transform of the entire image. The goal of this process is to more consistently identify "candidate" watermark bits or regions of the image to encode in perceptually significant regions of the signal. Even so, Signafy relies on the original unwatermarked image to accomplish decoding.

All of these methods still rely on the original unwatermarked image to ensure relatively error-free detection of the watermarks. The steganographic method seeks to provide watermark security without an original unwatermarked copy of the media for decode operations, as well as providing users cryptographic security with ciphered symmetric keys. That is, the same key is used for encode and decode operations. Public key pairs, where each user has a public/private key pair to perform asymmetric encode and decode operations, can also be used. Discussions of public key encryption and the benefits related to encryption are well documented. The growing availability of a public key infrastructure also indicates recognition of provable security. With such key-based implementations of watermarking, security can be off-loaded to the key, providing for a layered approach to security and authentication of the watermark message as well as the watermarked content.

It is known that attacks on the survivability of other implementations are readily available. Interesting network-based attacks on the watermark message are also known which fool the central registration server into assuming an image is owned by someone other than the registered owner. This also substantiates the concern that centralized watermarking technologies are not robust enough to provide proper assurances as to the ownership of a given digitized copy of an multimedia work.

Because the computational requirements of performing multiple transforms may not be prohibitive for certain media types, such as still images and audio, the present invention seeks to provide a means to securely watermark media without the need for an original unwatermarked copy to perform decoding. These transforms may be performed in a manner not plainly evident to observers or the owner of the content, who may assume the watermark is still detectable. Additionally, where a particular media type is commonly compressed (JPEG, MPEG, etc.), multiple transforms may be used to properly set the mask sets, prior to the watermarking process, to alert a user to survivability prior to the release of a watermarked, and thus perceived, "safe" copy to unknown parties. The result of the present invention is a more realistic approach to watermarking taking the media type, as well as the provable security of the keys into consideration. A more trusted model for electronic commerce is therefore possible.

The creation of an optimized "envelope" for insertion of watermarks to establish secured responsibility for digitally-sampled content provides the basis of much watermark security but is also a complementary goal of the present invention. The predetermined or random key that is generated is not only an essential map to access the hidden information signal, but is also the a subset of the original signal making direct comparisons with the original signal unnecessary. This increases the overall security of the digital watermark.

Survival of simultaneous cropping and scaling is a difficult task with image and audio watermarking, where such transformations are common with the inadvertent use of images and audio, and with intentional attacks on the watermark. The corresponding effects in audio are far more obvious, although watermarks which are strictly "frequency-based," such as variations of spread spectrum, suffer from alignment issues in audio samples which have been "cropped," or clipped from the original length of the piece. Scaling is far more noticeable to the human auditory system, though slight changes may affect frequency-only-type watermarks while not being apparent to a consumer. The far greater threat to available audio watermark applications, most of which are variations of frequency-based embedded signaling, are generally time-based transformations, including time-based compression and expansion of the audio signal. Signafy is an example of spread spectrum-based watermarking, as are applications by Solana Technology, CRL, BBN, MIT, etc. "Spatial domain" approaches are more appropriate designations for the technologies deployed by Digimarc, Signum, ARIS, Arbitron, etc. Interestingly, a time-based approached when considered for images is basically a "spatial-based" approach. The pixels are "convolutional." The difference being that the "spread spectrum-ed" area of the frequencies is "too" well-defined and thus susceptible to over-encoding of random noise at the same sub-bands as that of the embedded signal.

Giovanni uses a block-based approach for the actual watermark. However, it is accompanied by image-recognition capable of restoring a scaled image to its original scale. This "de-scaling" is applied before the image is decoded. Other systems used a "differencing" of the original image with the watermarked image to "de-scale." It is clear that de-scaling is inherently important to the survival of any image, audio or video watermark. What is not clear is that the differencing operation is acceptable from a security standpoint. Moreover, differencing that must be carried out by the watermarking "authority," instead of the user or creator of the image, causes the rights owner to lose control over the original unwatermarked content. Aside from utilizing the mask set within the encoding/decoding key/key pair, the original signal must be used. The original is necessary to perform detection and decoding, although with the attacks described above it is not possible to clearly establish ownership over the watermarked content.

In view of the foregoing, it can be appreciated that a substantial need exists for multiple transform utilization and applications for secure digital watermarking that solve the problems discussed above.

Summary of the Invention

The disadvantages of the art are alleviated to a great extent by multiple transform utilization and applications for secure digital watermarking. In one embodiment of the present invention, digital blocks in digital information to be protected are transformed into the frequency domain using a fast Fourier transform. A plurality of frequencies and associated amplitudes are identified for each of the transformed digital blocks and a subset of the identified amplitudes is selected for each of the digital blocks using a primary mask from a key. Message information is selected from a message using a transformation table generated with a convolution mask. The

chosen message information is encoded into each of the transformed digital blocks by altering the selected amplitudes based on the selected message information.

With these and other advantages and features of the invention that will become hereinafter apparent, the nature of the invention may be more clearly understood by reference to the following detailed description of the invention, the appended claims and to the several drawings attached herein.

Brief Description of the Drawings

FIG. 1 is a block flow diagram of a method for encoding digital information according to an embodiment of the present invention.

FIG. 2 is a block flow diagram of a method for descaling digital information according to an embodiment of the present invention.

FIG. 3 is a block flow diagram of a method for decoding digital information according to an embodiment of the present invention.

Detailed Description

In accordance with an embodiment of the present invention, multiple transforms are used with respect to secure digital watermarking. There are two approaches to watermarking using frequency-domain or spatial domain transformations: using small blocks or using the entire data-set. For time-based media, such as audio or video, it is only practical to work in small pieces, since the entire file can be many megabytes in size. For still images, however, the files are usually much smaller and can be transformed in a single operation. The two approaches each have their own strengths. Block-based methods are resistant to cropping. Cropping is the cutting out or removal of portions of the signal. Since the data is stored in small pieces, a crop merely means the loss of a few pieces. As long as enough blocks remain to decode a single, complete watermark, the crop does not remove the mark. Block-based systems, however, are susceptible to scaling. Scaling, such as affine scaling or "shrinking," leads to a loss of the high frequencies of the signal. If the block size is 32 samples and the data is scaled by 200%, the relevant data now covers 64 samples. However, the decoder still thinks that the data is in 32 samples, and therefore only uses half the space necessary to properly read the watermark. Whole-set approaches have the opposite behavior. They are very good at surviving scaling, since they approach the data as a whole, and generally scale the data to a particular size before encoding. Even a small crop, however, can throw off the alignment of the transform and obscure the watermark.

With the present invention, and by incorporation of previously disclosed material, it is now possible to authenticate an image or song or video with the encoding key/key pair, eliminating false positive matches with cryptography and providing for the communication of a copyright through registration with third party authorities, instead of the original unwatermarked copy.

The present invention provides an obvious improvement over the prior art while improving on previous disclosures by offsetting coordinate values of the original signal onto the key, which are then subsequently used to perform decode or detection operations by the user or authorized "key-holder." This offsetting is necessary with content which may have a watermark "payload," the amount of data that may successfully be encoded, based on Shannon's noisy channel coding theorem, that prevents enough invisible "saturation" of the signal with watermark messages to afford the owner the ability to detect a single message. An example, it is entirely possible that some images may only have enough of a payload to carry a single 100 bit message, or 12 ASCII characters. In audio implementations tested by the present inventor, 1000 bits per second are inaudibly encoded in a 16 bit 44.1 kHz audio signal. Most electronically available images do not have enough data to afford similar "payload" rates. Thus the premise that simultaneous cropping and scaling survival is more difficult for images than a comparable commercially available audio or video track. The added security benefit is that the more limited randomizer of a watermarking system based on spread spectrum or frequency-only applications, the random value of the watermark data "hopping "over a limited signaling band, is that the key is also an independent source of ciphered or random data used to more effectively encode in a random manner. The key may actually have random values larger than the watermark message itself, measured in bits. The watermark decoder is assured that the image is in its original scale, and can decide whether it has been cropped based on its "de-scaled" dimensions.

The benefits of a system requiring keys for watermarking content and validating the distribution of said content is obvious. Different keys may be used to encode different information while secure one way hash functions, digital signatures, or even one-time pads may be incorporated in the key to secure the embedded signal and afford nonrepudiation and validation of the watermarked image and "its" key/key pair. Subsequently, these same keys may be used to later validate the embedded digital signature only, or fully decode the digital watermark message. Publishers can easily stipulate that content not only be digitally watermarked, but that distributors must check the validity of the watermarks by performing digital signature checks with keys that lack any other functionality.

Some discussion of secure digital watermarking has begun to appear. Leighton describes a means to prevent collusion attacks in digital watermarks in US Patent No. 5,664,018. Leighton, however, may not actually provide the security described. For example, in particularly instances where the watermarking technique is linear, the "insertion envelope" or "watermarking space" is well-defined and thus susceptible to attacks less sophisticated than collusion by unauthorized parties. Over encoding at the watermarking encoding level is but one simple attack in such linear implementations. Another consideration ignored by Leighton is that commercially-valuable content in many cases may already exist in a unwatermarked form somewhere, easily accessible to potential pirates, gutting the need for any type of collusive activity. Such examples as compact disc or digitally broadcast video abound. Digitally signing the embedded signal with preprocessing of watermark data is more likely to prevent successful collusion. Depending on the media to be watermarked, highly granular watermarking algorithms are far more likely to successfully encode at a level below anything observable given quantization artifacts, common in all digitally-sampled media, than expectations that a baseline watermark has any functionality.

Furthermore, a "baseline" watermark as disclosed is quite subjective. It is simply described elsewhere in the art as the "perceptually significant" regions of a signal: so making a watermarking function less linear or inverting the insertion of watermarks would seem to provide the same benefit without the additional work required to create a "baseline" watermark. Indeed, watermarking algorithms should already be capable of defining a target insertion envelope or region without additional steps. Further, earlier disclosed applications by the present invention's inventor describe watermarking techniques that can be set to encode fewer bits than the available watermarking region's "bit-space" or encoding unrelated random noise in addition to watermark data to confuse possible collusive or other attempts at erasure. The region of "candidate bits" can be defined by any number of compression schemes or transformations, and the need to encode all of the bits is simply unnecessary. What is evident is that Leighton does not allow for initial prevention of attacks on an embedded watermark as the content is visibly or audibly unchanged. Moreover, encoding all of the bits may actually act as a security weakness to those who can replicate the regions with a knowledge of the encoding scheme. Again, security must also be offset outside of the actual watermark message to provide a truly robust and secure watermark implementation.

In contrast, 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. These masks may include primary, convolution and message delimiters but may extend into additional domains such as digital signatures of the message. 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. Prior to encoding, the masks described above are generated by a cryptographically secure random generation process. A block cipher, such as DES, in combination with a sufficiently random seed value emulates a cryptographically secure random bit generator. These keys will be saved along with information matching them to the sample stream in question in a database for use in descrambling and subsequent detection or decode operation.

These same cryptographic protocols can be combined with 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.

The following describes a sample embodiment of a system that protects digital information according to the present invention. Referring now in detail to the drawings wherein like parts are designated by like reference numerals throughout, there is illustrated in FIG. 1 a block flow diagram of a method for encoding digital information according to an embodiment of the present invention. An image is processed by "blocks," each block being, for example, a 32 x 32 pixel region in a single color channel. At step 110, each block is transformed into the frequency domain using a spectral transform or a Fast Fourier Transform (FFT). The largest 32 amplitudes are identified and a subset of these 32 are selected using the primary mask from the key at steps 120 and 130. One message bit is then encoded into each block at steps 140 and 150. The bit is chosen from the message using a transformation table generated using the convolution mask. If the bit is true, the selected amplitudes are reduced by a user defined strength fraction. If the bit is false, the amplitudes are unchanged.

Each of the selected amplitudes and frequencies are stored in the key. After all of the image has been processed, a diagonal stripe of pixels is saved in the key. This stripe can, for example, start in the upper left corner and proceed at a 45 degree angle through the image. The original dimensions of the image are also stored in the key.

FIG. 2 is a block flow diagram of a method for descaling digital information according to an embodiment of the present invention. When an image is chosen to be decoded, it first is checked to determine if it has been cropped and/or scaled. If so, the image is scaled to the original dimensions at step 210. The resulting "stripe," or diagonal line of pixels, is fit against the stripe stored in the key at step 220. If the fit is better than the previous best fit, the scale is saved at steps 230 and 240. If desired, the image can be padded with, for example, a single row or column of zero pixels at step 260 and the process can be repeated to see if the fit improves.

If a perfect fit is found at step 250, the process concludes. If no perfect fit is found, the process continues up to a crop "radius" set by the user. For example, if the crop radius is 4 the image can be padded up to 4 rows and/or 4 columns. The best fit is chosen and the image is restored to its original dimension, with any cropped area replaced by zeroes.

Once the in formation has been descaled, it can be decoded according to an embodiment of the present invention shown in FIG. 3. Decoding is the inverse process of encoding. The decoded amplitudes are compared with the ones stored in the key in order to determine the position of the encoded bit at steps 310 and 320. The message is assembled using the reverse transformation table at step 330. At step 340, the message is then hashed and the hash is compared with the hash of the original message. The original hash had been stored in the key during encoding. If the hashes match, the message is declared valid and presented to the user at step 350.

Although various embodiments are specifically illustrated and described herein, it will be appreciated that modifications and variations of the present invention are covered by the above teachings and within the purview of the appended claims without departing from the spirit and intended scope of the invention. Moreover, similar operations have been applied to audio and video content for time-based manipulations of the signal as well as amplitude and pitch operations. The ability to descale or otherwise quickly determine differencing without use of the unwatermarked original is inherently important for secure digital watermarking. It is also necessary to ensure nonrepudiation and third part authentication as digitized content is exchanged over networks.

What is claimed is:

1. A method for encoding a message into digital information, the digital information including a plurality of digital blocks, comprising the steps of:

transforming each of the digital blocks into the frequency domain using a spectral transform;

identifying a plurality of frequencies and associated amplitudes for each of the transformed digital blocks;

selecting a subset of the identified amplitudes for each of the digital blocks using a primary mask from a key;

choosing message information from the message using a transformation table generated with a convolution mask; and

encoding the chosen message information into each of said transformed digital blocks by altering the selected amplitudes based on the chosen message information.

2. The method of claim 1 wherein the transforming step comprises:

transforming each of the digital blocks into the frequency domain using a fast Fourier transform.

3. The method of claim 2, wherein the digital information contains pixels in a plurality of color channels forming an image, and each of the digital blocks represents a pixel region in one of the color channels.

4. The method of claim 1, wherein the digital information contains audio information.

5. The method of claim 2, wherein said step of identifying comprises:

identifying a predetermined number of amplitudes having the largest values for each of the transformed digital blocks.

6. The method of claim 2, wherein the chosen message information is a message bit and wherein said step of encoding comprises the step of:

encoding the chosen message bit into each of said transformed digital blocks by reducing the selected amplitudes using a strength fraction if the message bit is true, and not reducing the selected amplitudes if the message bit is false.

7. The method of claim 6, wherein the strength fraction is user defined.

8. The method of claim 2, further comprising the step of storing each of the selected amplitudes and associated frequencies in the key.

9. The method of claim 2, further comprising the step of storing a reference subset of the digital information into the key.

10. The method of claim 2, wherein the digital information contains pixels forming an image, further comprising the steps of:

saving a reference subset of the pixels in the key; and

storing original dimensions of the image in the key.

11. The method of claim 1, wherein the digital information contains audio information, further comprising the steps of:

saving a reference subset of audio information in the key; and

storing original dimensions of the audio signal in the key.

12. The method of claim 10, wherein the reference subset of pixels form a line of pixels in the image.

13. The method of claim 11, wherein the reference subset of audio information includes an amplitude setting.

14. The method of claim 8, wherein the image is a rectangle and the reference subset of pixels form a diagonal of the rectangle.

15. The method of claim 2, further comprising the step of:

requiring a predetermined key to decode the encoded message information.

16. The method of claim 2, further comprising the step of:

requiring a public key pair to decode the encoded message information.

17. The method of claim 2, further comprising the steps of:

calculating an original hash value for the message; and

storing the original hash value in the key.

18. A method for descaling digital information using a key, comprising the steps of:

determining original dimensions of the digital information from the key;

scaling the digital information to the original dimensions;

obtaining a reference subset of information from the key; and

comparing the reference subset with corresponding information in the scaled digital information.

19. The method of claim 18 wherein the digital information being descaled is a digital image and the step of obtaining a reference subset of information from the key comprises obtaining a reference subset of pixels from the key.

20. The method of claim 18 wherein the digital information being descaled is audio digital information and the step of obtaining a reference subset of information from the key comprises obtaining a reference subset of audio information from the key.

21. The method of claim 19, wherein said step of comparing determines a first fit value based on the comparison, and wherein the method further comprises the steps of:

padding the scaled digital image with an area of pad pixels; and

re-comparing the reference subset of pixels with corresponding pixels in the padded image to determine a second fit value.

22. The method of claim 20, wherein the area of pad pixels is a row of single pixels.

23. The method of claim 20, wherein the area of pad pixels is a column of single pixels.

24. The method of claim 20, wherein said steps of padding and re-comparing are performed a plurality of times.

25. The method of claim 20, further comprising the step of choosing a best fit value among the determined fit values and restoring the digital image to the original size, including any pad pixels associated with the best fit value.

26. A method of extracting a message from encoded digital information using a predetermined key, comprising the steps of:

decoding the encoded digital information into digital information, including a plurality of digital blocks, using the predetermined key;

transforming each of the digital blocks into the frequency domain using a spectral transform;

identifying a plurality of frequencies and associated amplitudes for each of the transformed digital blocks;

selecting a subset of the identified amplitudes for each of the transformed digital blocks using a primary mask from the key;

comparing the selected amplitudes with original amplitudes stored in the predetermined key to determine the position of encoded message information; and

assembling the message using the encoded message information and a reverse transformation table.

27. The method of claim 26 wherein the step of transforming comprises:

transforming each of the digital blocks into the frequency domain using a fast Fourier transform.

28. The method of claim 27, further comprising the steps of:

calculating a hash value for the assembled message; and

comparing the calculated hash value with an original hash value in the predetermined key.

29. A method for descaling a digital signal using a key, comprising the steps of:

determining original dimensions of the digital signal from the key;

scaling the digital signal to the original dimensions;

obtaining a reference signal portion from the key; and

comparing the reference signal portion with a corresponding signal portion in the scaled signal.

30. A method for protecting a digital signal comprising the step of:

creating a predetermined key comprised of a transfer function-based mask set and offset coordinate values of the original digital signal; and

encoding the digital signal using the predetermined key.

31. The method of claim 30, wherein the digital signal represents a continuous analog waveform.

32. The method of claim 30, wherein the predetermined key comprises a plurality of mask sets.

33. The method of claim 30, wherein the mask set is ciphered by a key pair comprising a public key and a private key.

34. The method of claim 30, further comprising the step of:

using a digital watermarking technique to encode information that identifies ownership, use, or other information about the digital signal, into the digital signal.

35. The method of claim 30, wherein the digital signal represents a still image, audio or video.

36. The method of claim 30, further comprising the steps of:

selecting the mask set, including one or more masks having random or pseudo-random series of bits; and

validating the mask set at the start of the transfer function-based mask set.

37. The method of claim 36, wherein said step of validating comprises the step of:

comparing a hash value computed at the start of the transfer function-based mask set with a determined transfer function of the hash value.

38. The method of claim 36, wherein said step of validating comprises the step of:

comparing a digital signature at the start of the transfer function-based mask set with a determined transfer function of the digital signature.

39. The method of claim 36, further comprising the step of:

using a digital watermarking technique to embed information that identifies ownership, use, or other information about the digital signal, into the digital signal; and

wherein said step of validating is dependent on validation of the embedded information.

40. The method of claim 30, further comprising the step of:

computing a secure one way hash function of carrier signal data in the digital signal, wherein the hash function is insensitive to changes introduced into the carrier signal for the purpose of carrying the transfer function-based mask set.

41. A method for protecting a digital signal, comprising the steps of:

creating a predetermined key comprised of a transfer function-based mask set and offset coordinate values of the original digital signal;

authenticating the predetermined key containing the correct transfer function-based mask set during playback of the data; and

metering the playback of the data to monitor content to determine if the digital signal has been altered.

42. The method of claim 30, wherein the digital signal is a bit stream and further comprising the steps of:

generating a plurality of masks to be used for encoding, including a random primary mask, a random convolution mask and a random start of message delimiter;

generating a message bit stream to be encoded;

loading the message bit stream, a stega-cipher map truth table, the primary mask, the convolution mask and the start of message delimiter into memory;

initializing the state of a primary mask index, a convolution mask index, and a message bit index; and

setting a message size equal to the total number of bits in the message bit stream.

43. The method of claim 42 wherein the digital information has a plurality of windows, further comprising the steps of:

calculating over which windows in the sample stream the message will be encoded;

computing a secure one way hash function of the information in the calculated windows, the hash function generating hash values insensitive to changes in the samples induced by a stega-cipher; and

encoding the computed hash values in an encoded stream of data.

44. The method of claim 40, wherein said step of selecting comprises the steps of:

collecting a series of random bits derived from keyboard latency intervals in random typing;

processing the initial series of random bits through an MD5 algorithm;

using the results of the MD5 processing to seed a triple-DES encryption loop;

cycling through the triple-DES encryption loop, extracting the least significant bit of each result after each cycle; and

concatenating the triple-DES output bits into the random series of bits.

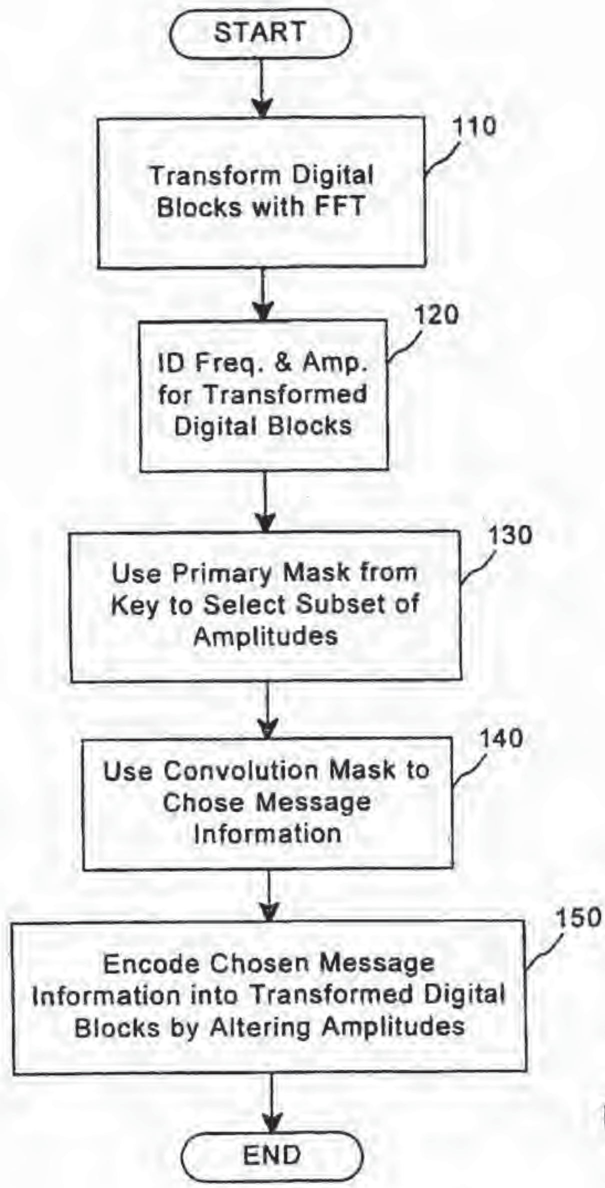

START
Transform Digital Blocks with FFT
110
ID Freq. & Amp. for Transformed Digital Blocks
120
Use Primary Mask from Key to Select Subset of Amplitudes
130
Use Convolution Mask to Chose Message Information
140
Encode Chosen Message Information into Transformed Digital Blocks by Altering Amplitudes
150
END

FIG. 1

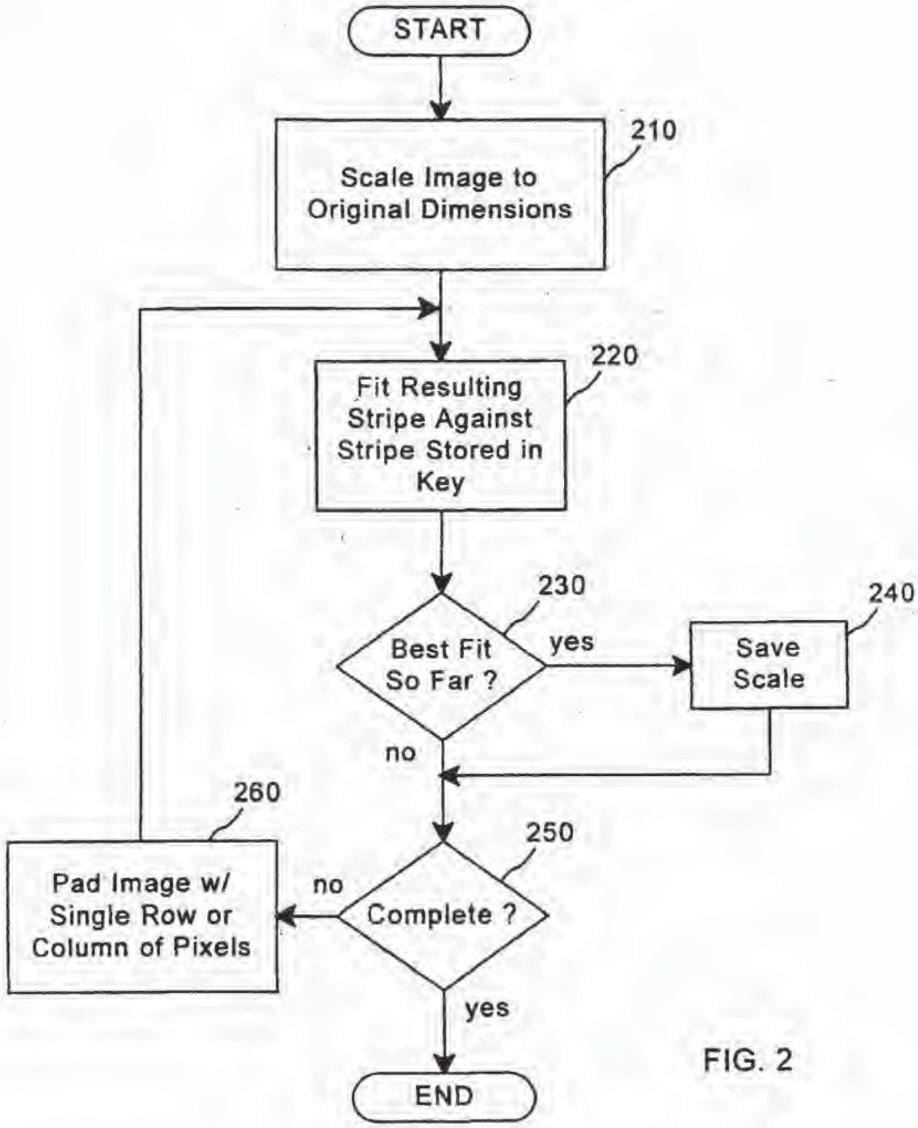

START
210
Scale Image to Original Dimensions
220
Fit Resulting Stripe Against Stripe Stored in Key
230
Best Fit So Far ?
yes
240
Save Scale
no
260
250
Pad Image w/ Single Row or Column of Pixels
no
Complete ?
yes
END

FIG. 2

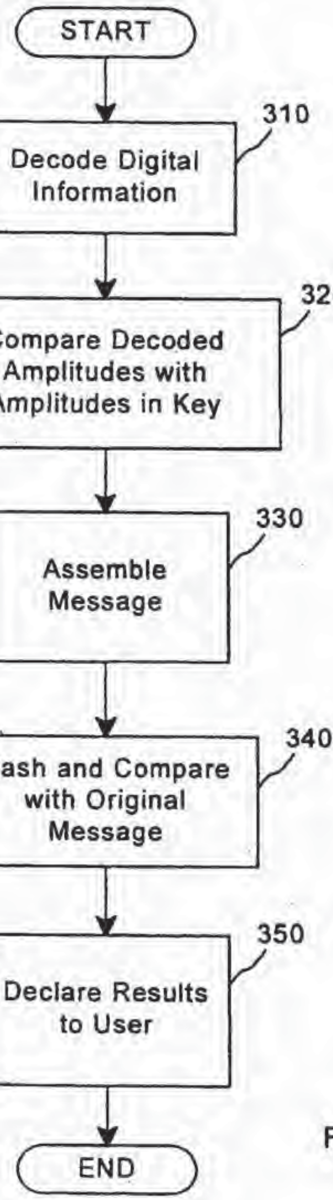

START
310
Decode Digital Information
320
Compare Decoded Amplitudes with Amplitudes in Key
330
Assemble Message
340
Hash and Compare with Original Message
350
Declare Results to User
END

FIG. 3

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/07262

A. CLASSIFICATION OF SUBJECT MATTER
IPC 6 H04N1/32

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)
IPC 6 H04N H04L

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

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

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	US 5 613 004 A (MOSKOWITZ SCOTT A ET AL) 18 March 1997 (1997-03-18) abstract column 6, line 30 - column 9, line 49 column 16, line 8 - line 64	1,2, 15-17, 26-28, 30-38,42
A	DELAIGLE J -F ET AL: "DIGITAL WATERMARKING" PROCEEDINGS OF THE SPIE, vol. 2659, 1 February 1996 (1996-02-01), pages 99-110, XP000604065 the whole document	1,5,6

-/--

[X] Further documents are listed in the continuation of box C.

[X] Patent family members are listed in annex.

* Special categories of cited documents :

"A" document defining the general state of the art which is not considered to be of particular relevance

"E" earlier document but published on or after the international filing date

"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)

"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

"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

"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

"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.

"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
12 July 1999	21/07/1999
Name and mailing address of the ISA European Patent Office, P.B. 5818 Patentlaan 2 NL - 2280 HV Rijswijk Tel. (+31-70) 340-2040, Tx. 31 651 epo nl, Fax: (+31-70) 340-3016	Authorized officer Hubeau, R

2

Form PCT/ISA/210 (second sheet) (July 1992)

INTERNATIONAL SEARCH REPORT

International Application No
PCT/US 99/07262

C.(Continuation) DOCUMENTS CONSIDERED TO BE RELEVANT

Category *	Citation of document, with indication,where appropriate, of the relevant passages	Relevant to claim No.
A	SCHNEIDER M ET AL: "ROBUST CONTENT BASED DIGITAL SIGNATURE FOR IMAGE AUTHENTICATION" PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON IMAGE PROCESSING (IC, LAUSANNE, SEPT. 16 - 19, 1996, vol. 3, 16 September 1996 (1996-09-16), pages 227-230, XP002090178 INSTITUTE OF ELECTRICAL AND ELECTRONICS ENGINEERSISBN: 0-7803-3259-8 the whole document ---	1,17,18, 26-28
A	COX I J ET AL: "SECURE SPREAD SPECTRUM WATERMARKING FOR MULTIMEDIA" IEEE TRANSACTIONS ON IMAGE PROCESSING, vol. 6, no. 12, 1 December 1997 (1997-12-01), pages 1673-1686, XP000724633 ISSN: 1057-7149 the whole document ---	1-3,5,6, 26,27
A,P	PING WAH WONG: "A Public Key Watermark for Image Verification and Authentication" IEEE INTERNATIONAL CONFERENCE ON IMAGE PROCESSING, vol. 1, 4 - 7 October 1998, pages 455-459, XP002108799 Los Alamitos, CA, USA the whole document -----	1-4

2

INTERNATIONAL SEARCH REPORT

.nformation on patent family members

Inte onal Application No
PCT/US 99/07262

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
US 5613004 A	18-03-1997	EP 0872073 A	21-10-1998
		WO 9642151 A	27-12-1996
		US 5687236 A	11-11-1997

Form PCT/ISA/210 (patent family annex) (July 1992)

PCT

WORLD INTELLECTUAL PROPERTY ORGANIZATION
International Bureau

INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

(51) International Patent Classification 6 : G06F 12/14 | A1

(11) International Publication Number: WO 99/63443

(43) International Publication Date: 9 December 1999 (09.12.99)

(21) International Application Number: PCT/SG98/00039

(22) International Filing Date: 1 June 1998 (01.06.98)

(81) Designated States: AU, CA, CN, ID, JP, KR, SG, 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.

(71) Applicant *(for all designated States except US)*: DATAMARK TECHNOLOGIES PTE LTD. [SG/SG]; Innovation Centre, Block 1, Suite 106, 16 Nanyang Drive, Singapore 637722 (SG).

(72) Inventors; and

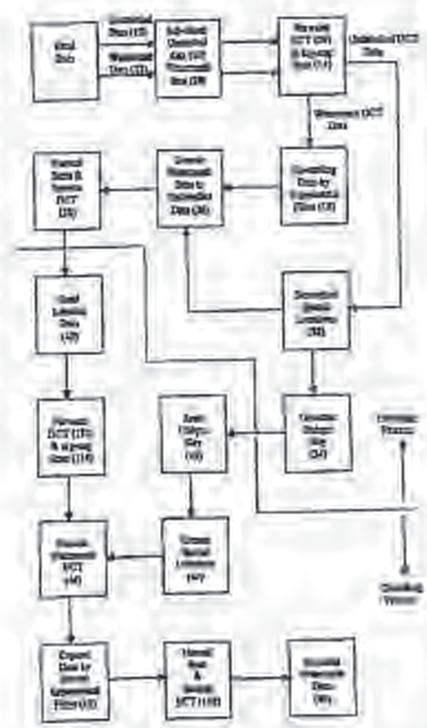
(75) Inventors/Applicants *(for US only)*: HO, Anthony, Tung, Shuen [GB/SG]; Nanyang Technological University, School of Electrical & Electronic Engineering, Block S2, Nanyang Avenue, Singapore 639798 (SG). TAM, Siu, Chung [SG/SG]; Nanyang Technological University, School of Electrical & Electronic Engineering, Block S2, Nanyang Avenue, Singapore 639798 (SG).

(74) Agents: HAQ, Murgiana et al.; Haq & Nanazie Partnership, Robinson Road, P.O. Box 765, Singapore 901515 (SG).

(54) Title: METHODS FOR EMBEDDING IMAGE, AUDIO AND VIDEO WATERMARKS IN DIGITAL DATA

(57) Abstract

A method for embedding an entire image, audio or video watermark sequence within another image, audio or video data sequence with minimum loss of data quality is presented. The method exploits the de-correlation property of data coefficients in the orthogonal transform domain, similar to the application in data compression through transform coding. The present invention describes the usage of a Discrete Cosine Transform as the embedding domain. However, other orthogonal transforms such as Fourier, Walsh-Hadamard, Haar, Sine and Wavelet can also be used for this operation. A unique key derived adaptively from spatial locations registering the thresholds of the ac transform energies is used to unlock or de-watermark the embedded image or audio sequence. Moreover, an exponential filter has been developed to compress and expand the watermark coefficients prior to the embedding and retrieval process. The method can be used in resolving multimedia copyright protection issues arising on the Internet and in the music industry, such as the inclusion of a company's logo or an artist's recorded voice. The method can also be incorporated as a built-in feature for digital recording devices, such as still and video cameras, as well as more recent devices such as VCD and DVD players. Moreover, the method can be applied to the commercial and service sectors, where security in transmission and reception of private information in terms of speech or image is of the utmost importance.



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		

Methods for Embedding Image, Audio and Video Watermarks in Digital Data

FIELD OF THE INVENTION

This invention relates generally to the digital communications and multimedia fields and in particular the invention provides a method for the embedding and retrieval of digital image, audio or video watermarks in the transform domain for digital multimedia data, with applications in copyright protection and security data transmission and reception.

BACKGROUND OF THE INVENTION

The tremendous growth in multimedia products and services through the Internet has led to the need for copyright protection, authentication and integrity of data. In the past few years, a number of digital watermarking techniques have been developed and patents granted, for the purpose of resolving the legal use or misuse of copyright information on the Internet. Unlike data encryption that transforms the original data to another form for security transmission, digital watermarking embeds an invisible or inaudible watermark directly into the original data.

Typical examples of recent work in the field of digital watermarking or data embedding are described in U.S. Patent 5636292 to Rhoads (1997) and U.S. Patent 5659726 to Sandford and Handel (1997). Rhoads discloses methods for embedding an identification code on a carrier signal, such as an electronic data signal or a physical medium. Sandford and Handel disclose a method of embedding auxiliary information into a set of host data, such as a photograph, or a television signal.

Prior art publications in the field of digital watermarking technology, including the two aforementioned granted U.S. Patents, generally envisage only the embedding of a very limited number of bits of information (in the form of binary digits '1' and '0') or a few characters (such as 'A12') into the carrier signal. More detailed ownership information requires a higher level of embedded watermark information either in the form of longer alphanumeric character strings or, if possible, trademarks/logo images, or speech of the original owner, which is embedded into and retrieved from the carrier signal. However, this has previously been considered to be very difficult to achieve, without significant corruption of the data being labelled as the amount of data to be inserted is increased. The present invention describes such a method for embedding digital audio or image watermarks directly into targeted audio or image data, substantially inaudibly or invisibly, respectively.

There are many other potential consumer, commercial and service applications that can benefit from the use of digital watermarking technology in copyright protection and security transmission. These applications include the embedding of owner identification, such as the trademarks or logos of an owner into digital still and video cameras, or copyright protection and royalty tracking monitoring of sound recordings in the music industry with digital audio watermarks of the artists' voice embedded into the sound tracks.

Furthermore, commercial and service sectors are also interested in the secure transmission and reception of sensitive messages, data, and even images that could be camouflaged into normal data streams transmitted over an open channel.

SUMMARY OF THE INVENTION

In this specification and claims the term "unlabelled data" is to be given the meaning of target data to which a new label is to be added by the method of the present invention, whether or not that target data is carrying a previously applied label. Similarly the term "labelled data" is to be given the meaning of target data to which the new label has been added by the method of the present invention.

According to a first aspect, the present invention provides a method for applying digital watermarking image data or digital watermarking audio data to an unlabelled digital image, audio, or video data sample, said method including the steps of :

a) inputting a set of unlabelled digital data and a set of digital watermark data;

b) formatting the unlabelled digital data into a format suitable for orthogonal transformation;

c) performing an orthogonal transformation on the formatted unlabelled data to produce a set of unlabelled data transform coefficients;

d) formatting the digital watermark data into a format suitable for orthogonal transformation;

e) performing an orthogonal transformation on the formatted watermark data to produce a set of watermark data transform coefficients;

f) for each watermark data transform coefficient, allocating an unlabelled data transform coefficient to be replaced and replacing the respective unlabelled data transform coefficients to produce a labelled set of data transform coefficients;

g) storing the locations into which watermark data transform coefficients were encoded in the set of labelled data transform coefficients to generate a unique key for future decoding of the watermark data;

h) performing an inverse orthogonal transformation on the labelled data transform coefficients to convert them into a set of labelled digital data having a form resembling the original unlabelled digital data.

Preferably, the steps of formatting the unlabelled and watermarked data include the steps of mapping the set of unlabelled data and the set of watermark data into two-dimensional matrices prior to performing the orthogonal transformations.

Preferably also the matrices of unlabelled and watermark data are divided into smaller sub-blocks prior to orthogonal transformation.

The preferred method further includes the step of ordering the orthogonal transformation coefficients in each sub-block of the watermark data into one-dimensional arrays in approximately increasing frequency order (throughout the specification and claims, the term "approximately increasing frequency order" is used in respect of one-dimensional arrays of orthogonal transform coefficients to indicate that the coefficients of the array are ordered in generally increasing frequency order, from the first to the last position in the array, with only occasional localised deviations from the generally increasing trend) by performing a zig-zag scan of each sub-block of orthogonally transformed watermark data. The reordered orthogonal transformation coefficients are then divided into segments for subsequent replacement into the set of transformation coefficients of the unlabelled data.

The preferred method further includes the step of ordering the orthogonal transformation coefficients of the unlabelled data into one-dimensional arrays in approximately increasing frequency order by performing a zig-zag scan of each sub-block of orthogonally transformed unlabelled data prior to replacement of the watermark data coefficients and performing an inverse zig-zag scan on the labelled data coefficients prior to the inverse orthogonal transformation. In the step of allocating a segment of the orthogonally-transformed watermark data that will be encoded in each sub-block of the unlabelled data, the allocation may be performed in a structured or random manner.

Alternatively, the zig-zag and inverse zig-zag scans of each data type can be replaced with a radial and inverse radial scans respectively.

It is also preferable to calculate the mean and variance of the ac energies from the orthogonal transformation coefficients for each sub-block of the unlabelled data in order to allocate the locations of the transform coefficients of the unlabelled data which will be replaced by the transform coefficients of the segment of watermark data. Preferably the transform coefficients to be replaced in the transformed unlabelled data will be those in which the ac energies fall below a predetermined threshold value.

The transform coefficients of the watermark data embedded in the labelled digital data are also preferably compressed prior to embedding, using a scaling function. Preferably the compression function has an exponential characteristic, however in other embodiments scaling functions having another characteristic similar to an exponential function may be used to similar effect.

According to a second aspect, the present invention provides a method for extracting digital watermarking image data or digital watermarking audio data from a digital image, audio, or video data sample, said method including the steps of:

a) inputting a set of labelled digital data and unique key data containing information of locations of watermark data imposed as a label on the labelled digital data;

b) mapping the set of labelled digital data into a format suitable for orthogonal transformation;

c) performing an orthogonal transformation on the formatted labelled data to produce a set of labelled data transform coefficients;

d) using the unique key to extract a segment of transform coefficients of orthogonally transformed watermark data from the locations in the set of labelled data transform coefficients specified in the key;

e) using an inverse orthogonal transformation on the transformed watermark data to retrieve the embedded watermark data.

Preferably, the formatting step of the watermark extraction method includes the step of mapping the set of labelled data into a two-dimensional matrix prior to performing the orthogonal transform.

Preferably also, prior to orthogonal transformation, the matrix of labelled data is divided into the same number of smaller sub-blocks as that used in the encoding process.

It is also preferable to order the orthogonal transformation coefficients of the labelled data in each sub-block into a one-dimensional array in approximately increasing frequency order by performing a zig-zag scan of each sub-block of orthogonally transformed labelled data prior to extraction of the watermark data coefficients and performing an inverse zig-zag scan on the extracted watermark data coefficients to build a matrix of sub-blocks of watermark data prior to the inverse orthogonal transformation. In some embodiments of the invention a radial scan is used in the encoding process of the unlabelled data to order the unlabelled data prior to replacement with watermark data in which case a radial scan and inverse radial scan should also be used in the decoding process instead of respectively a zig-zag scan and inverse zig-zag scan.

The transform coefficients of the watermark data embedded in the labelled digital data are also preferably compressed prior to embedding and the extraction method includes the step of expanding the compressed watermark data prior to the inverse orthogonal transformation, the compression and expansion steps using scaling functions each having a characteristic which is the inverse of the other. Preferably the compression function has an exponential characteristic and the expansion function has an inverse exponential characteristic. In other embodiments scaling functions having characteristics similar to an exponential and inverse exponential function respectively may be used to similar effect.

In embodiments of the invention, the retrieved watermark data samples may either be displayed as a visual or audio output of the encoding process for immediate examination or authentication, or may be stored as a digital file for future visual or aural examination or authentication or for digital comparison with a master reference file.

Preferably, the orthogonal transform is a Discrete Cosine Transform (DCT) and the inverse transform is an inverse DCT, however, other orthogonal transforms such as Fourier, Walsh-Hadamard, Haar, Sine, and Wavelet transforms can also be used.

The unlabelled digital data samples may be obtained from a sample stream representing a digitised grayscale or colour image, for example, as provided by a digital still camera. Alternatively, the unlabelled digital data may be obtained from a sample stream representing digitised video in which case the source may be a video camera or a master tape of video program material.

In the second aspect of the invention, the labelled data prior to decoding, will in most cases be obtained from some form of recording such as a recording on a Video CD (VCD), a Laser Disc (LD) or a Digital Versatile Disc (DVD) carrying a recording of the labelled data as the digitised video in a digitised movie or still image contained within a video game or other software. The labelled data may also be obtained from a broadcast transmission.

The unlabelled and labelled digital data may also be a part of an audio signal in which case it may be a digitised sample stream representing digitised sound or music and may include two sample streams representing channel A and channel B of digitised stereo sound, each of which or either will be encoded with watermark data.

In the case of audio data, the transmission step might involve recording the labelled data on a Compact Disc (CD), Digital Audio Tape (DAT), a Laser Disc (LD), a Video CD (VCD), live digital broadcast, or live digital music or conversation down a communication channel such as a telephone line or phone through internet.

The labelled digital data may also be a part of an image or a video signal that contains a digitised audio segment as watermark data. In this case, the transmission step might involve recording the labelled data on a video CD, a digital versatile disc (DVD), a laser disk or live transmission of images or video signals down a communication channel such as a telephone line or through the internet.

Preferably, the watermark digital data will include one or more of: an owner's logo, an owner's trademark, a personal identification, an artist's recorded voice or, general terms for publisher distribution.

Embodiments of the present invention provide a digital watermarking method that embeds and retrieves either digital audio or image watermarks in the temporal (one-dimensional) and spatial (two-dimensional) domain of digital data. Compared with existing methods, which target mainly the embedding of alphanumeric character codes as watermarks, embodiments of the present invention have the distinct advantage of embedding and retrieving an entire audio or image watermark into various digital data formats, inaudibly or invisibly, respectively.

Digital watermarking methods according to the preferred embodiment of the invention are truly generic in the sense that they can be applied to many different formats of digital media. The method operates on orthogonal transform coefficients of the data source. The advantages of using orthogonal transforms in the field of digital image processing such as data compression, restoration, enhancement and pattern recognition have been well documented in the literature. The main advantage of using orthogonal transforms instead of a temporal or spatial domain is the de-correlation processes that result in fewer coefficients with significant energies of interest. Subsequently, a number of data processing techniques such as filtering and thresholding can be directly applied to the transform coefficients.

Using embodiments of the present invention, a digital image of a trademark or logo can be embedded into and retrieved from a grayscale or colour image stored in either BMP, GIF, TIFF, JPEG or MPEG format. In audio watermarking, the same method can be used to embed a signature audio sequence into typical audio formats such as WAV and AIFF or into images or video signals. This method can also be extended to embedding audio watermarks in digital image or video data, such as DVD and VCD formats, or live signals through the internet or down a telephone line.

Correlation studies performed on many experimental tests of the present invention have revealed that the labelled (embedded or watermarked) data and the original unlabelled data can result in high correlation coefficient value in the range of approximately 0.91 to 0.99 (When there are absolutely no differences between two images, the correlation value would equal to 1.). The present method exploits the de-correlation property of coefficients in the transform domain for watermark embedding. In the transform domain, most of transform coefficient energies are associated with only a few low frequency coefficients thus the watermark data can be embedded in the high frequency region.

With the tremendous growth in products and services provided through the Internet, the need for copyright protection, authentication and integrity of digital data is rapidly increasing in importance. With the present method, a company's logo or trademark can be embedded entirely into a digital image invisibly or into a sound track inaudibly. The hidden data or watermark can then be subsequently used in resolving copyright protection issues.

Consumer products, such as digital still and video cameras, can also exploit the benefits of this invention as a built-in feature of their integrated technology, for example in copyright protection and product identification. Digital watermarking can also be very useful in commercial and personal communications. For example, classified or sensitive information can be embedded within an audio, digital still/video data for secure transmission and reception.

Preferably, embodiments of the invention provide the same generic functional capability of a digital watermarking method whether the digital audio, or image watermark is embedded into any one of various data formats, such as grayscale and colour images, or audio or video data.

According to a third aspect, the present invention provides apparatus for applying digital watermarking image data or digital watermarking audio data to an unlabelled digital image, audio, or video data sample, said apparatus including:

a) input means arranged to input a set of unlabelled digital data;

b) processing means arranged to process the unlabelled digital data to encode watermark data into the unlabelled data to form a set of labelled digital data; and

c) output means arranged to output the labelled digital data to a communication or storage medium,

wherein the processing means is arranged to perform the method as herein described.

According to a fourth aspect, the present invention provides an apparatus for extracting digital watermarking image data or digital watermarking audio data from labelled digital image, audio, or video data sample said apparatus including:

a) input means arranged to input a set of labelled digital data;

b) processing means arranged to process the labelled digital data to extract watermark data encoded into the labelled digital data; and

c) output means arranged to output the extracted watermark digital data to a display or storage means,

wherein the processing means is arranged to perform the method as herein described.

According to a fifth aspect, the present invention provides a digital recording, recorded on any recording medium, the recording being encoded with watermark data in accordance with the methods described.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will now be described, by way of example, with reference to the accompanying drawings in which:

Figure 1 illustrates a step of sub-blocking a matrix for orthogonal transformation used in embodiments of the invention;

Figure 2 illustrates a zig-zag scanning technique used in an embodiment of the invention, as compared to conventional line-by-line or raster scanning;

Figure 3 illustrates an image a) before and b) after a step of performing a Discrete Cosine Transform (DCT) on the sub-blocks of the image used in an embodiment of the invention;

Figure 4 illustrates an exponential curve used in a step of re-scaling the transform coefficients used in embodiments of the invention;

Figure 5 illustrates a step of embedding the watermark coefficients in a structured manner in accordance with an embodiment of the invention;

Figure 6 illustrates a step of embedding the watermark coefficients in a random manner in accordance with another embodiment of the invention;

Figure 7 illustrates a schematic block diagram of an embodiment of the present invention for embedding and retrieval of digital watermarks through orthogonal transformation;

Figure 8 illustrates a pseudocode listing of the embodiment of figure 7 providing a digital watermarking system that can apply to audio, image or video data.

Figure 9 illustrates an example of digital image watermarking of a company's logo, of size 128 x 128, into a real image, of size 512 x 512, of a woman's face, created using an embodiment of the present invention;

Figure 10 illustrates another example of digital image watermarking of a company's logo, of size 128 x 128, into a real image, of size 512 x 512, of a satellite image, created using an embodiment of the present invention;

Figure 11 illustrates a block diagram of a communications encoder/decoder for hidden data encoded on a communications channel;

Figure 12 illustrates a block diagram of a multimedia encoder/decoder for watermark data; and

Figure 13 illustrates a block diagram of a personal identification card encoder/decoder.

Detailed description of embodiments of the invention

Embodiments of a digital watermarking method will now be described in which the coefficients of a Discrete Cosine Transform (DCT) are employed. However, implementations of the invention are not limited solely to the use of DCT, and other orthogonal transforms such as discrete Fourier, Walsh-Hadamard, Haar, Sine and Wavelet transforms can also be used to good effect. In the preferred embodiment, both unlabelled data and watermark image data are first converted into two-dimensional matrices and then divided into sub-blocks, prior to orthogonal transformation. The present invention requires that the dimension size of the unlabelled data set must be at least twice the dimension size of the watermark data in each dimension, to fulfil a requirement that is closely related to the concept of the Shannon's sampling theorem. For example, for a 512 x 512 unlabelled image, the watermark image should be typically 256 x 256 or smaller.

Preferably each sub-block of the matrices is 8 x 8 pixels, which is typically considered to be a good size for data compression applications in terms of speed and minimum blocking edge effects, introduced by the sub-blocking process. For example, 8 x 8 and 16 x 16 are commonly used in JPEG and MPEG formats, however other sub-block dimensions may also usefully be employed. After sub-blocking, the individual sub-block data are then mapped into the transform domain through a DCT operation. The respective transform coefficients are then operated on by a number of processing steps necessary for digital watermarking. Figure 1 illustrates the 8 x 8 sub-blocking blocking process in which a matrix 12 is divided into a plurality of 8x8 sub-blocks 10 for orthogonal transformation.

Referring to Figure 2, the first processing step in the transform domain is to re-arrange the transform coefficients of the unlabelled and watermark data by performing a zig-zag scan of each sub-block. The zig-zag scanning technique has been used extensively in data compression. This technique essentially re-orders the transform coefficients from low frequency to high frequency in an approximately ascending manner. For example, for a two-dimensional sub-block of size, M x N, the dc transform coefficient or zero frequency component, is located at (1,1), and the other ac transform coefficients are at the following locations, (1,2), (1,3), ..., (1,N), ..., (2,1), (2,2), (2,3),..., (2,N), ...,(M,1), (M,2), (M,3), ..., (M,N). The zig-zag scanning technique will re-order the coefficient locations as follows: (1,1), (1,2), (2,1), (3,1), (2,2), (1,3), (1,4), ..., (M,N). In this manner, for each sub-block, the elements in the (MxN) matrix will be mapped into a one-dimensional array of size MN. Figure 2 illustrates the zig-zag scanning technique applied to the first 8x8 sub-block 10 of Figure 1.

After zig-zag scanning, the transform coefficients are subjected to statistical analysis. In this operation, the ac transform energies of the unlabelled data are first calculated from the transform coefficients and then compared with a threshold value derived from the mean and standard deviation of the ac transform energies. The use of an adaptive energy threshold allows optimum offset positions in each one-dimensional array to be determined. The offset position in each one-dimensional array corresponds closely with the minimum ac energies within that array. Beyond this position, the transform coefficients do not play a *vital role* even if they are neglected. This is similar to conventional transform coding where data compression is achieved by coding only those transform coefficients with sufficient energies, which generally fall into the low frequency range. Figure 3 illustrates the DCT domain of sub-blocks of an image.

It should be noted that the statistical method described in this embodiment is not the only possible method that can be used to set the location for replacement of the watermark data. Other adaptive filtering techniques include the choice of a fixed location for each watermark block, or alternatively the flexible use of statistical data such as the mean, standard deviation, and higher-order moments.

The embedding process of watermark coefficients must avoid overwriting any relevant transform coefficients of the unlabelled data with significant ac energies, as this would introduce unnecessary errors in the unlabelled data. Locating the optimum locations is therefore not only important in reducing the errors but the locations also generate a unique key that will be used later for decoding. Through the process of embedding the unlabelled data with an invisible or inaudible watermark, the combined data set will now become labelled data. Integrity of the labelled data depends entirely on how the ac transform coefficients of the unlabelled data are overwritten or replaced by the watermark transform coefficients, during the embedding process.

The watermark data is also grouped into a two-dimensional matrix. The data is then divided into sub-blocks. Each sub-block is subjected to DCT or other orthogonal transformation in the same way as the unlabelled data has been treated. Again, zig-zag scanning is applied to arrange the transformation coefficients in an approximately increasing frequency order. The transformation coefficients for the watermark data are then blocked into segments for structured or random embedding in the transformation coefficients of the unlabelled data. Each segment of transformation coefficients to be embedded may be subjected to an optional scaling operation. This will help to minimise the overall effect of the transformation coefficients on the unlabelled data. In one preferred embodiment, the scaling function is an exponential function, although other similar mathematical functions may also be used.

Figure 4 illustrates the adaptive filtering for re-scaling of transform coefficients that follows an exponential curve. An inverse curve to the exponential curve of Figure 4 will be used in the decoding process. Other scaling techniques such as the reciprocal function, normal, log-normal, hyper-exponential, or other appropriate probability density functions can also be used.

As the dimensional size of the unlabelled data 12 is at least twice the dimensional size of the watermark data 13, the embedding or encoding process of watermark coefficients 15 can exploit the additional sub-blocks 10 available in the unlabelled data 12. The encoding process can be performed either in a structured or random manner. For example, in a structured manner, the watermark coefficients 15 can be embedded in every odd or even column or row of the unlabelled transform coefficient locations. While in a random manner, the watermark coefficients can be located in different columns or rows, depending on a specified random sequence. Figures 5 and 6 illustrate the watermark coefficients 15 embedded in a structured 20 and random 22 manner, respectively.

One important feature of the present invention is that the sizes of both unlabelled and labelled data are compatible. For example, a 512 x 512 grayscale image, embedded with a 128 x 128 watermark grayscale image corresponds to exactly the same data size of the unlabelled image, approximately 262 kBytes. A unique key for the labelled image is generated and the size of the key is much less than the watermark grayscale image of size of 16.4 kBytes of data. The size of the key for a 512 x 512 image is only approximately 4 kBytes.

The unique key and the labelled data generated will be transmitted to the decoder for extraction of the digital watermark. For added security, the unique key can be further encrypted through some random sequence. From the unique key, the spatial locations of the embedded watermark transform coefficients are extracted for each sub-block. The extracted transform coefficients are then expanded through the application of an inverse optional exponential or other appropriate compression curve. These expanded coefficients are subsequently converted back to follow a normal scanning pattern in a two-dimensional matrix before being operated on by an inverse DCT.

Figure 7 illustrates a schematic process flow diagram of the present invention for embedding and retrieval of digital watermarks through orthogonal transformation. Referring to figure 7, the unlabelled raw data 12 and the watermark raw data 13 are first divided into sub-blocks 10, 28. Both data sub-blocks are individually transformed through a DCT 30. The transform coefficients of the sub-blocks are then re-ordered to follow a zig-zag pattern 14. Spatial locations for embedding are derived from the ac transform energies 32 of the unlabelled data 12. A unique key 34 for decoding is generated from these spatial locations. Prior to embedding the watermark coefficients onto the unlabelled spatial locations, the watermark coefficients are first compressed by an exponential filter 18. The compressed watermark coefficients are embedded 36 structurally or randomly into the unlabelled sub-block DCT coefficients. The labelled coefficients are then re-ordered from a zig-zag scan pattern back to a normal scan pattern, before an inverse DCT transformation 38 is performed on the coefficients to obtain the labelled data 39.

At the decoding end, the labelled data 38 and the unique key 34 are both read 40. The same process of forward DCT transformation 130 and zig-zag scanning 114 are also performed on the labelled data, as in the case during the embedding stage. From the labelled transform coefficients, the watermark coefficients are decoded 46 from the labelled coefficients based on the spatial locations extracted 44 from the unique key. The watermark coefficients are expanded through an inverse exponential filter 48 and re-arranged to follow a normal scan pattern. This is then followed by an inverse transformation by DCT 138 to obtain the decoded watermark data.

Figure 8a and 8b illustrate pseudocode listings of a digital watermarking coder and decoder system that can be applied to image, audio and video data. Figures 9 and 10 illustrate examples of digital image watermarking in the form of a company logo of size 128 x 128 into two real images of size 512 x 512 of a women's face and a satellite image, respectively. Correlation analysis performed on these examples between the unlabelled and labelled images and original and decoded watermarks have yielded correlation coefficients of 0.9932 and 0.9975 for the face and watermark, respectively While for the satellite image and its logo, the correlation coefficients for unlabelled and labelled images and original and decoded watermarks are 0.9979 and 0.9994, respectively.

The proposed method of digital watermarking of an audio sequence inaudibly or image sequence invisibly into digital data has many potential applications for resolving copyright protection issues in the consumer sector or for security transmission in the commercial and service sectors. This principle applies to personal voice communication through open-channel communication systems. For example, data watermarking of a company's logo/trademark or a person's identification can be incorporated into consumer electronic products, such as digital still/video camera and more recently, VCD and DVD players, to authenticate the true ownership of intellectual property right and consumer identification. Another major consumer area for digital watermarking is in the protection of illegal copying and downloading of music CDs and tapes. For example, the voice of the artist can be inaudibly embedded into a sound track through the use of the present invention.

In the commercial sector, the copyright protection of multimedia data on the Internet needs also to be monitored closely, as there are tremendous amount of original data in the form of music, image and video, illegally downloaded and redistributed without the consent of the true owners. The present invention can be used to address this problem, as well as providing the security transmission of embedded data in some commercial banking operations. Similarly in the service sector, sensitive audio or image data can be embedded into an ordinary speech or image for secure transmission, respectively.

Referring to Figure 11, an application of the method of the present invention is illustrated, in which input digital facsimile or telephone audio data 200, is encoded with hidden digital data 201 in a communication encoder 202 embodying an encoding method according to the invention.

The encoder 202 outputs a set of labelled digital facsimile or telephone data 203 and a unique key 204 as a result of the encoding process and these are transmitted via a communications channel 208 to a communication decoder 205 embodying a decoding method according to the invention. The decoder outputs labelled (i.e. unaltered) digital facsimile or telephone data 206 and extracted hidden data 207 which may represent a hidden message, or may be used to validate the source of the telephone facsimile data.

Turning to the embodiment of Figure 12, a further application of the method of the present invention is illustrated, in which input digital audio, image or video data

210 is encoded with digital watermark data 211 in a multimedia encoder 212 embodying an encoding method according to the invention. The encoder 212 outputs a set of labelled digital audio, video or image data 213 and unique key data 214 as a result of the encoding process and is carried as a recording on any suitable digital recording media or as a transmission over a communications or broadcast channel 218. In turn, the labelled data 213 and key data 214 are fed to a multimedia decoder 215 which extracts the watermark data and outputs the watermark data 217 and the labelled data 216. The extracted label or watermark 217 may be displayed to indicate the origin or ownership of the recording or transmission to the user of the data.

In Figure 13, yet another application of the invention is illustrated in which identification information 220 such as personal identification information from an identification (ID) card is encoded with watermark data 221 in an identification (ID) card encoder 222 such that output labelled ID data 223 may be validated at a later date. The ID card encoder 222 outputs labelled ID data 223 and a unique key 224 produced by the encoding process for transmission 228 as part of a transaction such as a credit card transaction which requires secure transmission of the card holder's identity.

A card decoder 225 which receives the transmission 228 includes a watermark decoder according to the present invention which inputs the transmitted labelled ID data 228 and the unique key 224 and outputs ID data 226 and watermark data 227. The watermark data 227 may then be used to indicate validity or otherwise of the labelled ID data 226 in an authentication process associated with the transaction.

The proposed method of data watermarking can embed audio or image data, inaudibly or invisibly, respectively, into various digital multimedia data formats, such as audio, image and video. Provided the unlabelled data dimension size is at least twice the dimension size of the watermark data, an artist's recorded voice or an entire image of a company's logo or trademark, for example, can be embedded into audio and image and video data, without any serious degradation to the data quality. The proposed method exploits the de-correlation property of orthogonal transforms for embedding and retrieving digital watermarks.

Although the proposed method describes mainly the use of a discrete cosine transform as the domain for watermarking; however, orthogonal transforms such as Fourier, Walsh-Hadamard, Haar, Sine and Wavelet can also be applied. Instead of the current watermarking technology of embedding text strings into digital data, the proposed method would provide additional complementary proof as to the true ownership of the digital data, by the use of a company's logo or a recording of the artist's voice, making a copyright infringement claim easier to substantiate than when just a text string is applied as the watermark.

The ability of the proposed method to embed and retrieve an entire audio or image watermark is a significant advantage over current prior art techniques that could only embed very simple and limited number of bits or characters into the data. Correlation performed on digital data before and after digital watermarking using the proposed method has shown the data to be very close to one, indicating that there is minimum loss in data integrity. A significant advantage of the preferred embodiment is that the labelled and unlabelled data have the same data size. A unique key generated during the embedding process that is necessary for decoding the watermark is only fractional of the watermark data size.

Digital still and video cameras can also benefit from the proposed method as a built-in feature of their integrated technology. Moreover, digital watermarking can be useful in commercial and personal communications. For example, a classified audio or image can be embedded into digital multimedia data for secure transmission.

It will be appreciated by persons skilled in the art that numerous variations and/or modifications may be made to the invention as shown in the specific embodiments without departing from the spirit or scope of the invention as broadly described. The present embodiments are, therefore, to be considered in all respects as illustrative and not restrictive.

CLAIMS:

1. A method for applying digital watermarking image data or digital watermarking audio data to an unlabelled digital image, audio, or video data sample, said method including the steps of:

a) inputting a set of unlabelled digital data and a set of digital watermark data;

b) formatting the unlabelled digital data into a format suitable for orthogonal transformation;

c) performing an orthogonal transformation on the formatted unlabelled data to produce a set of unlabelled data transform coefficients;

d) formatting the digital watermark data into a format suitable for orthogonal transformation;

e) performing an orthogonal transformation on the formatted watermark data to produce a set of watermark data transform coefficients;

f) for each watermark data transform coefficient, allocating an unlabelled data transform coefficient to be replaced and replacing the respective unlabelled data transform coefficients to produce a labelled set of data transform coefficients;

g) storing the locations into which watermark data transform coefficients were encoded in the set of labelled data transform coefficients to generate a unique key for future decoding of the watermark data;

h) performing an inverse orthogonal transformation on the labelled data transform coefficients to convert them into a set of labelled digital data having a form resembling the original unlabelled digital data.

2. The method of claim 1 wherein the step of formatting the watermark data includes the step of mapping the set of watermark data into a two-dimensional matrix.

3. The method of claim 2 wherein the step of formatting the watermark data includes the step of dividing the two-dimensional matrix of watermark data into smaller sub-blocks and the step of performing the orthogonal transformation on the watermark data involves performing the orthogonal transform on each sub-block of the watermark data, such that the watermark data transform coefficients are organised in sub-blocks.

4. The method as claimed in claim 3, including an ordering step in which each sub-block of the watermark data transform coefficients are reordered into a one-dimensional array in approximately increasing frequency order, as hereinbefore

defined, prior to replacement of the allotted unlabelled data transform coefficients with the watermark data transform coefficients.

5. The method of claim 4, in which the step of reordering the watermark data transform coefficients of each sub-block is achieved by performing a zig-zag scan of the watermark data transform coefficients in the respective sub-block.

6. The method of claim 4, in which the step of reordering the watermark data transform coefficients of each sub-block is achieved by performing a radial scan of the watermark data transform coefficients in the respective sub-block .

7. The method as claimed in claim 4, 5 or 6, wherein after the watermark data transform coefficients of each sub-block are reordered into a one-dimensional array and before the replacement of unlabelled data transform coefficients with the watermark data the watermark data transform coefficients of each one-dimensional array are rescaled.

8. The method as claimed in claim 7, wherein the rescaling is performed using a scaling function that reduces the magnitude of lower frequency coefficients of the one-dimensional array by a greater amount than higher frequency coefficients of the respective array.

9. The method of claim 8, wherein the scaling function has an exponential characteristic.

10. The method of any one of claims 4 to 9, including the step of dividing the reordered watermark data transform coefficients of each sub-block into segments for subsequent replacement into the set of transformation coefficients of the unlabelled data.

11. The method as claimed in any one of claims 1 to 10, wherein the step of formatting the unlabelled data includes the step of mapping the set of unlabelled data into a two-dimensional matrix.

12. The method of claim 11 wherein the step of formatting the unlabelled data includes the step of dividing the two-dimensional matrix of unlabelled data into smaller sub-blocks and the step of performing the orthogonal transformation on the unlabelled data involves performing the orthogonal transform on each sub-block of the unlabelled data, such that the unlabelled data transform coefficients are organised in sub-blocks.

13. The method of claim 12, including a first ordering step in which each sub-block of the unlabelled data transform coefficients are reordered into a one-dimensional array in approximately increasing frequency order, as hereinbefore

defined, prior to replacement of allocated unlabelled data transform coefficients with watermark data transform coefficients, and a second ordering step in which each of the one-dimensional arrays of the labelled data transform coefficients are reordered into sub-blocks using an inverse reordering to that of the first ordering step.

14. The method of claim 13, wherein the first ordering step is achieved by performing a zig-zag scan of each sub-block of the unlabelled data transform coefficients and the second ordering step is achieved by performing an inverse zig-zag scan of each one-dimensional array of the labelled data transform coefficients.

15. The method of claim 13, wherein first ordering step is achieved by performing a radial scan of each sub-block of the unlabelled data transform coefficients and the second ordering step is achieved by performing an inverse radial scan of each one-dimensional array of the labelled data transform coefficients.

16. The method of claim 13, 14 or 15, including the step of, for each one-dimensional array of unlabelled data, determining a location beyond which the ac energies will fall below a certain threshold value and selecting transform coefficients beyond that location for replacement by transform coefficients of the watermark data.

17. The method of claim 16, including the step of calculating the mean and variance values of the ac energies from the orthogonal transformation coefficients for each one-dimensional array of unlabelled data and calculating the threshold value as a function of the mean and variance values.

18. The method as claimed in any one of claims 12 to 17, including the step of, for each one-dimensional array of the unlabelled data, allocating a segment of the orthogonally-transformed watermark data that will be encoded in that sub-block, if any.

19. The method as claimed in any one of claims 1 to 18, wherein the orthogonal transform performed on the unlabelled data is one of: a Discrete Cosine Transform (DCT); a Fourier transform; a Walsh-Hadamard transform; a Haar transform; a sine transform; and a Wavelet transform, and the inverse transform is respectively; an inverse DCT; an inverse Fourier transform; an inverse Walsh-Hadamard transform; an inverse Haar transform; an inverse sine transform; and an inverse Wavelet transform.

20. The method as claimed in claim 19, wherein the orthogonal transform performed on the unlabelled data is a Discrete Cosine Transform (DCT) and the inverse transform is an inverse DCT.

21. The method as claimed in any one of claims 1 to 20, wherein the orthogonal transform performed on the watermark data is one of: a Discrete Cosine

Transform (DCT); a Fourier transform; a Walsh-Hadamard transform; a Haar transform; a sine transform; and a Wavelet transform.

22. The method as claimed in claim 21, wherein the orthogonal transform performed on the watermark data is a Discrete Cosine Transform (DCT).

23. The method as claimed in any one of claims 1 to 22, including the further step of allocating in a structured manner a segment of the orthogonally-transformed unlabelled data that will be replaced by each segment of orthogonally transformed watermark data.

24. The method as claimed in any one of claims 1 to 22, including the further step of allocating in a random manner a segment of the orthogonally-transformed unlabelled data that will be replaced by each segment of orthogonally transformed watermark data.

25. The method as claimed in any one of the preceding claims wherein the set of unlabelled digital data is obtained from a sample stream representing a digitised grayscale or colour image.

26. The method as claimed in claim 25, wherein the digitised grayscale or colour image is obtained from a digital still camera or a digital image scanner.

27. The method as claimed in any one of claims 1 to 24, wherein the set of unlabelled digital data is obtained from a sample stream representing digitised video.

28. The method of claim 27, wherein the unlabelled digitised video is obtained from a Data Storage Medium (DSM), or a real time digital data source.

29. The method as claimed in claims 1 to 28, wherein the labelled digitised video is subsequently transmitted over a digital communications channel.

30. The method as claimed in any one of claims 1 to 28, wherein the labelled digitised video is subsequently recorded on a digital recording medium.

31. The method as claimed in claim 30, wherein the digital recording medium is one of: a Video Compact Disc (VCD); a Laser Disc (LD); a Digital Versatile Disc (DVD); a digitised movie and a still image contained within a video game, video-on-demand or other software.

32. The method as claimed in any one of claims 1 to 24, wherein the unlabelled digital data is obtained from a sample stream representing one or more channels of digitised sound or music.

33. The method of claim 32, wherein the unlabelled digitised sound or music is obtained from one of: a master recording on digital audio tape played on a digital tape recorder; and a master recording on an analog audio tape played on an analog tape recorder and digitised via a digitising interface.

34. The method as claimed in any one of claims 32 to 33, wherein the labelled digitised sound or music is subsequently recorded on a digital recording medium.

35. The method as claimed in claim 34, wherein the digital recording medium is one of: a compact Disc (CD); a Digital Audio Tape (DAT); a Laser Disc (LD); a Video Compact Disc (VCD).

36. The method as claimed in any one of the preceding claims wherein the watermark digital data includes one or more of the following data items: an owner's logo; an owner's trademark; a personal identification; an artist's recorded voice; or general terms for publisher distribution.

37. A method for extracting digital watermarking image data or digital watermarking audio data from a digital image, audio, or video data sample, said method including the steps of:

a) inputting a set of labelled digital data and unique key data containing information of locations of watermark data imposed as a label on the labelled digital data;

b) mapping the set of labelled digital data into a format suitable for orthogonal transformation;

c) performing an orthogonal transformation on the formatted labelled data to produce a set of labelled data transform coefficients;

d) using the unique key to extract transform coefficients of orthogonally transformed watermark data from the locations in the set of labelled data transform coefficients specified in the key;

e) using an inverse orthogonal transformation on the transformed watermark data to retrieve the embedded watermark data.

38. The method of claim 37 wherein the step of formatting the labelled data includes the step of mapping the set of labelled data into a two-dimensional matrix.

39. The method of claim 38 wherein the step of formatting the labelled data includes the step of dividing the two-dimensional matrix of labelled data into smaller sub-blocks and the step of performing the orthogonal transformation on the labelled data involves performing the orthogonal transform on each sub-block of the labelled data, such that the labelled data transform coefficients are organised in sub-blocks.

40. The method as claimed in claim 39, including the step of ordering the orthogonal transformation coefficients of the labelled data in each sub-block into a one-dimensional array in approximately increasing frequency order, as hereinbefore defined, prior to extraction of the watermark data coefficients.

41. The method as claimed in claim 40, wherein the ordering step is achieved by performing a zig-zag scan of each sub-block of orthogonally transformed labelled data.

42. The method as claimed in claim 40, wherein the ordering step is achieved by performing a radial scan of each sub-block of orthogonally transformed labelled data.

43. The method of any one of claims 37 to 42, wherein after extraction of the watermark transform coefficients from the orthogonally transformed labelled data, the extracted watermark data transform coefficients are arranged into a number of one-dimensional arrays corresponding to the number of sub-blocks used in the process of encoding the watermark data into the labelled data and each one-dimensional array is then reordered into a two-dimensional sub-block prior to performing the inverse orthogonal transform on the watermark *data transform* coefficients in each sub-block.

44. The method of claim 43, wherein the reordering of each one-dimensional array of watermark data transform coefficients into a respective sub-block is achieved by performing an inverse zig-zag scan.

45. The method of claim 43, wherein the reordering of each one-dimensional array of watermark data transform coefficients into a respective sub-block is achieved by performing an inverse radial scan.

46. The method as claimed in any one of claims 37 to 45, wherein the transform coefficients of the watermark data embedded in the labelled digital data are compressed using a first scaling function and the method includes the step of expanding the compressed watermark data prior to the inverse orthogonal transformation using a second scaling function which is an inverse of the first scaling function.

47. The method of claim 46, wherein the inverse scaling function increases the magnitude of lower frequency coefficients of each one-dimensional array of watermark data to a greater extent than it increases the magnitude of the higher frequency coefficients of the respective one dimensional array.

48. The method of claim 46, wherein the first scaling function has an exponential characteristic and the second scaling function has an inverse exponential characteristic.

49. The method as claimed in any one of claims 37 to 48, wherein the orthogonal transform performed on the labelled data is one of: a Discrete Cosine Transform (DCT); a Fourier transform; a Walsh-Hadamard transform; a Haar transform; a sine transform; and a Wavelet transform.

50. The method as claimed in claim 49, wherein the orthogonal transform performed on the labelled data is a DCT.

51. The method as claimed in any one of claims 37 to 50, wherein the inverse orthogonal transform performed on the watermark data is one of: an inverse Discrete Cosine Transform (DCT); an inverse Fourier transform; an inverse Walsh-Hadamard transform; an inverse Haar transform; an inverse sine transform; and an inverse Wavelet transform.

52. The method as claimed in claim 51, wherein the inverse orthogonal transform performed on the watermark data is an inverse DCT.

53. The method as claimed in any one of claims 37 to 52, including the further step of displaying the watermark data samples for immediate examination or authentication.

54. The method as claimed in any one of claims 37 to 52, including the further step of storing the watermark data samples for future examination or authentication.

55 The method as claimed in any one of claims 37 to 54, wherein the labelled digital data is obtained from a sample stream representing a digitised grayscale or colour image.

56. The method as claimed in claim 55, wherein the labelled digitised grayscale or colour image is obtained from a digital still camera or a digital image scanner.

57. The method as claimed in any one of claims 37 to 54, wherein the labelled digital data is obtained from a sample stream representing digitised video.

58. The method of claim 57, wherein the labelled digitised video is obtained from one of: a Video Compact Disc (VCD) played on a VCD player; a Laser Disc (LD) played on a LD player; a Digital Versatile Disc (DVD) played on a DVD player; a digitised movie or still image contained within a video game or other software or a digital signal transmitted over a communications channel.

59. The method as claimed in any one of claims 37 to 54, wherein the labelled digital data is obtained from a sample stream representing one or more channels of digitised sound or music.

60. The method of claim 59, wherein the labelled digitised sound or music is obtained from one of: a Compact Disc (CD) played on a CD player; a Digital Audio Tape (DAT) played on a DAT player; a Laser Disc (LD) played on a LD player; from a Video Compact Disc (VCD) played on a VCD player.

61. The method as claimed in any one of claims 37 to 60, wherein the watermark digital data includes one or more of the following data items: an owner's logo; an owner's trademark; a personal identification; an artist's recorded voice; and general terms for publisher distribution.

62. An apparatus for applying digital watermarking image data or digital watermarking audio data to an unlabelled digital image, audio, or video data sample, said apparatus including:

a) input means arranged to input a set of unlabelled digital data;

b) processing means arranged to process the unlabelled digital data to encode watermark data into the unlabelled data to form a set of labelled digital data; and

c) output means arranged to output the labelled digital data to a communication or storage medium,

wherein the processing means is arranged to perform the method as claimed in any one of claims 1 to 36.

63. An apparatus for extracting digital watermarking image data or digital watermarking audio data from a labelled digital image, audio, or video data sample said apparatus including:

a) input means arranged to input a set of labelled digital data;

b) processing means arranged to process the labelled digital data to extract watermark data encoded into the labelled digital data; and

c) output means arranged to output the extracted watermark digital data to a display or storage means,

wherein the processing means is arranged to perform the method as claimed in any one of claims 37 to 61.

64. A digital recording stored on any digital recording medium, the recording comprising a set of digital image, audio, or video data labelled with a watermark comprising a set of digital watermark image data or a set of digital watermark audio data, the set of labelled digital data being created by encoding a set of unlabelled digital data with the set of digital watermark data using the method as claimed in any one of claims 1 to 36.

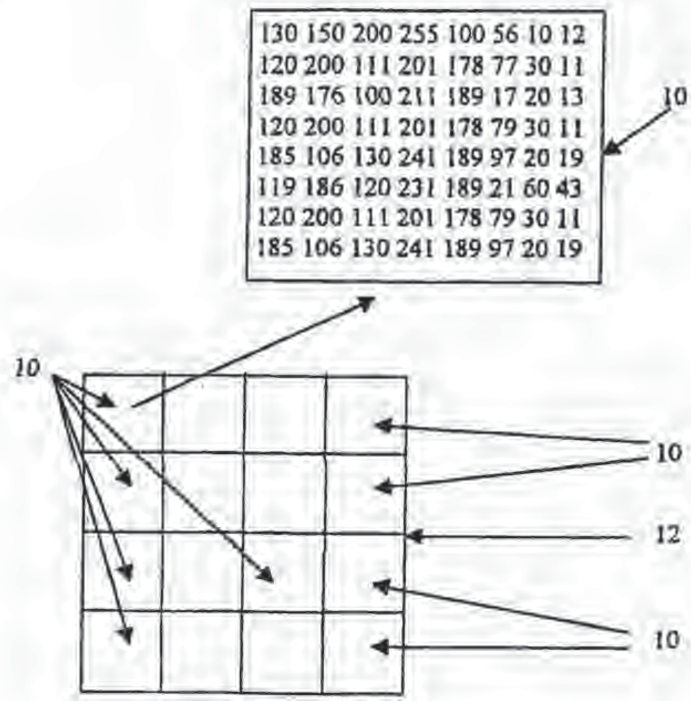


FIGURE 1

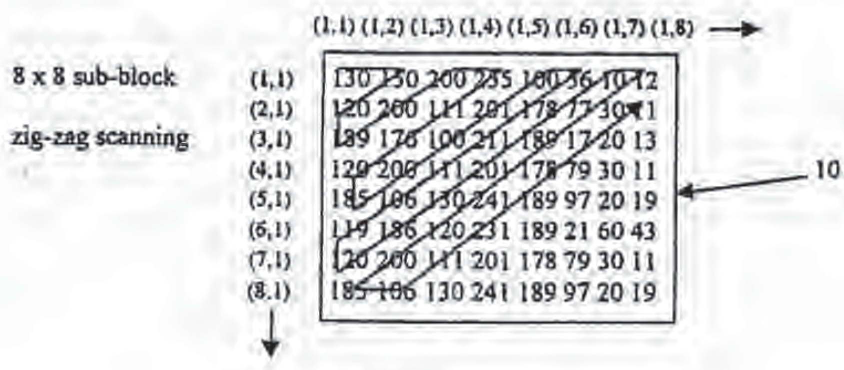


FIGURE 2

(a)

(b)

FIGURE 3

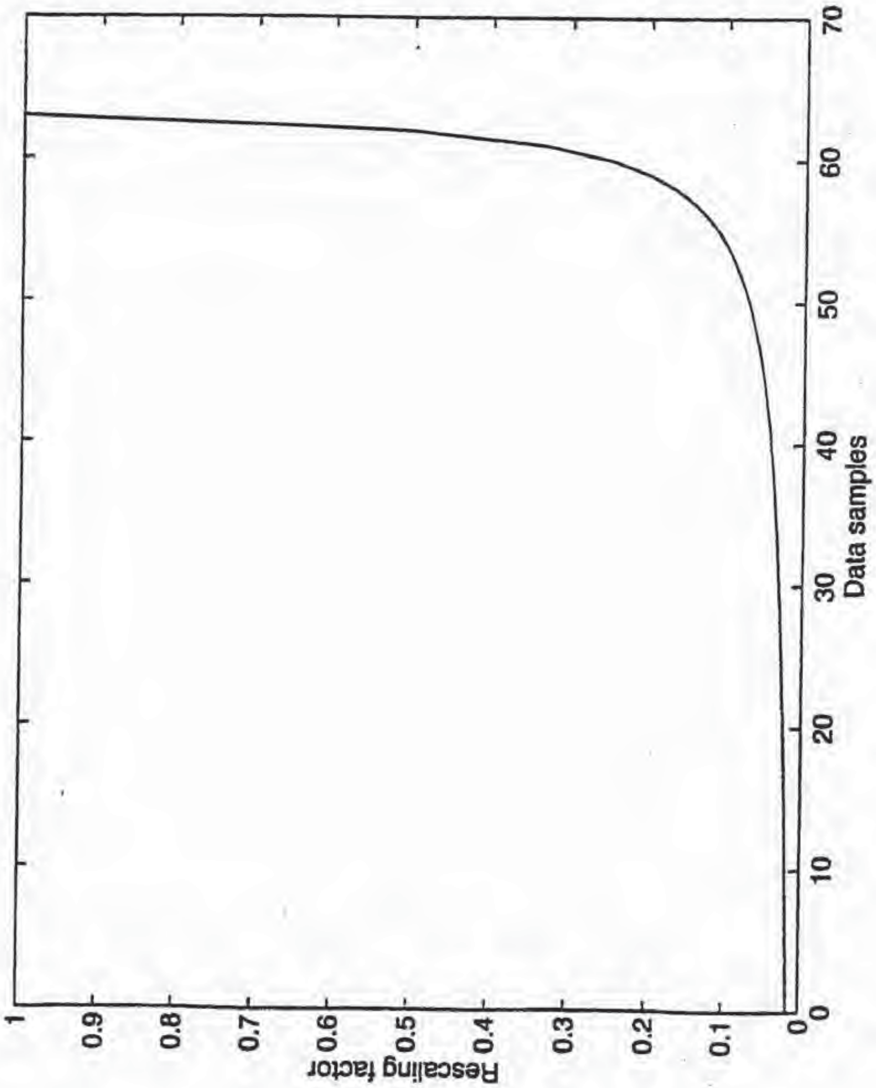

Rescaling factor
Data samples
0
0.1
0.2
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0
10
20
30
40
50
60
70

FIGURE 4

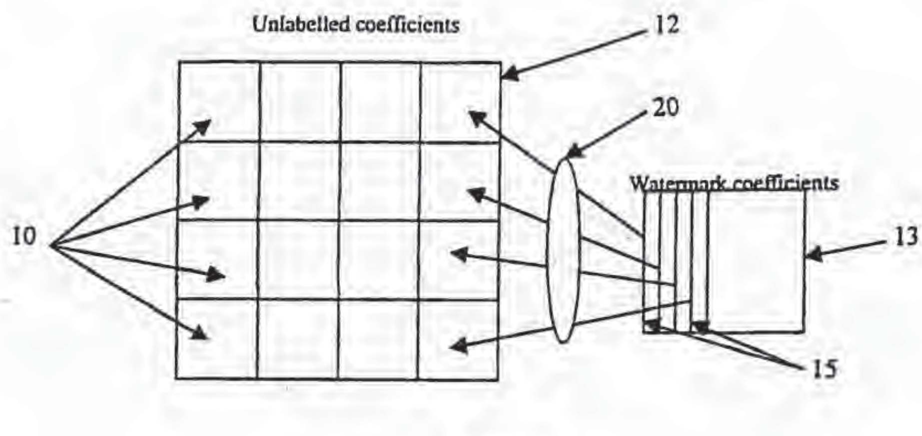


FIGURE 5

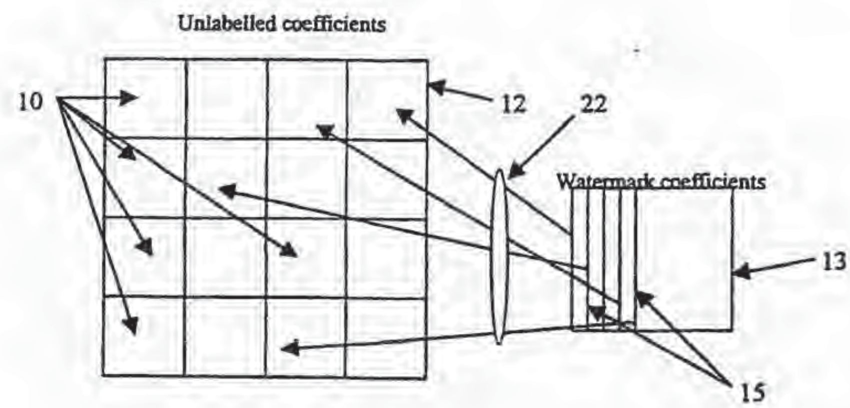


FIGURE 6

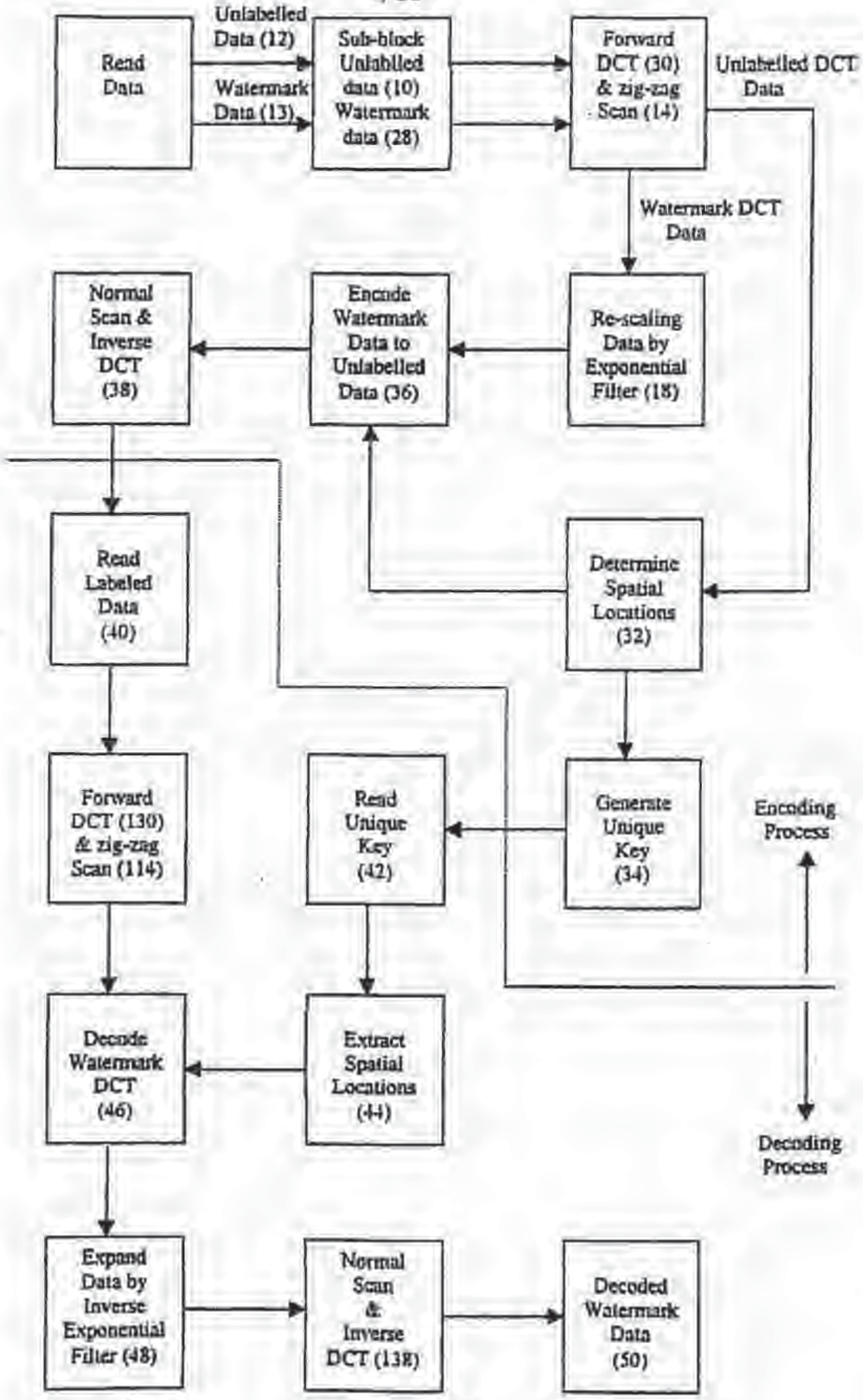

Read Data
Unlabelled Data (12)
Watermark Data (13)
Sub-block Unlabelled data (10) Watermark data (28)
Forward DCT (30) & zig-zag Scan (14)
Unlabelled DCT Data
Watermark DCT Data
Normal Scan & Inverse DCT (38)
Encode Watermark Data to Unlabelled Data (36)
Re-scaling Data by Exponential Filter (18)
Read Labeled Data (40)
Determine Spatial Locations (32)
Forward DCT (130) & zig-zag Scan (114)
Read Unique Key (42)
Generate Unique Key (34)
Encoding Process
Decode Watermark DCT (46)
Extract Spatial Locations (44)
Decoding Process
Expand Data by Inverse Exponential Filter (48)
Normal Scan & Inverse DCT (138)
Decoded Watermark Data (50)

FIGURE 7

```
*PSEUDOCODE*

PROCEDURE WATERMARK CODER

BEGIN
        READ UNLABELLED DATA,
        CONVERT UNLABELLED DATA TO MATRIX (M,N);
        PERFORM SUB-BLOCKING of UNLABELLED DATA;
        PERFORM DCT ON UNLABELLED DATA SUB-BLOCKS;
        RE-ORDER DCT COEFFICIENTS TO FOLLOW ZIG-ZAG PATTERN;
        DETERMINE AC ENERGIES OF DCT COEFFICIENTS;
        SET THRESHOLD BASED ON AC ENERGY MEAN AND STANDARD
        DEVIATION;
        COMPARE SUB-BLOCK AC ENERGIES WITH THRESHOLD;
        IF AC ENERGIES LESS THAN THRESHOLD THEN
              STORE SPATIAL LOCATIONS;
        ELSE
              SET TO OFFSET SPATIAL LOCATIONS;
        END
        GENERATE UNIQUE KEY FROM STRUCTURED/RANDOM SPATIAL
        LOCATIONS;
        STORE UNIQUE KEY FOR DECODING;

        READ WATERMARK DATA;
        CONVERT WATERMARK DATA TO MATRIX (J,K);
        PERFORM SUB-BLOCKING of WATERMARK DATA;
        PERFORM DCT ON UNLABELLED DATA SUB-BLOCKS;
        RE-ORDER DCT COEFFICIENTS TO FOLLOW ZIG-ZAG PATTERN;
        RE-SCALE DCT COEFFICIENTS USING EXPONENTIAL FILTER;

        EMBED RE-SCALED WATERMARK DCT COEFFICIENTS INTO
        UNLABELLED DCT SUB-BLOCKS;
        CONVERT ZIG-ZAG SCAN BACK TO NORMAL SCAN;
        INVERSE DCT SUB-BLOCKS TO OBTAIN LABELED DATA;
END
```

FIGURE 8a

```
*PSEUDOCODE*

PROCEDURE WATERMARK DECODER

BEGIN
      READ LABELED DATA;
      CONVERT LABELED DATA TO MATRIX (M,N);
      PERFORM SUB-BLOCKING of LABELED DATA;
      PERFORM DCT ON LABELED DATA SUB-BLOCKS;
      RE-ORDER DCT COEFFICIENTS TO FOLLOW ZIG-ZAG PATTERN;

      EXTRACT SPATIAL LOCATIONS FROM UNIQUE KEY;
      DECODE WATERMARK DCT COEFFICIENTS FROM SPATIAL
      LOCATIONS;
      SCALE WATERMARK DCT COEFFICIENTS USING INVERSE
      EXPONENTIAL FILTER;
      CONVERT ZIG-ZAG SCAN BACK TO NORMAL SCAN;
      INVERSE DCT SUB-BLOCKS TO OBTAIN WATERMARK DATA;
END
```

FIGURE 8b

(a)

(b)

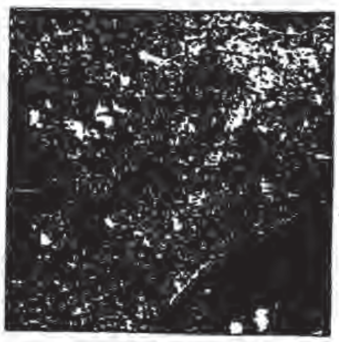
(a)

(b)

FIGURE 9

(a)

(b)



(a)

(b)

FIGURE 10

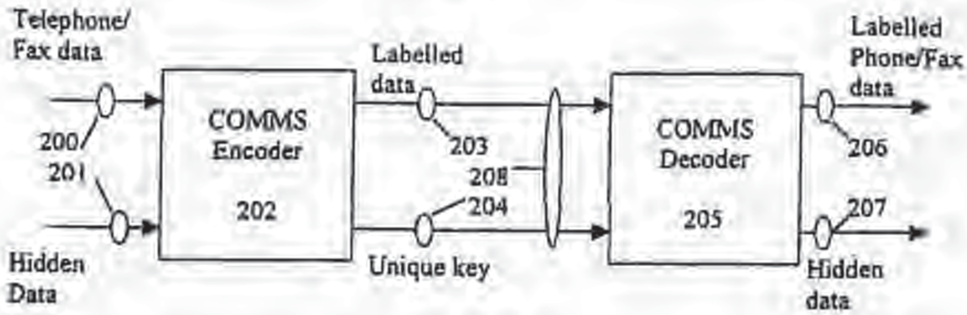


FIGURE 11

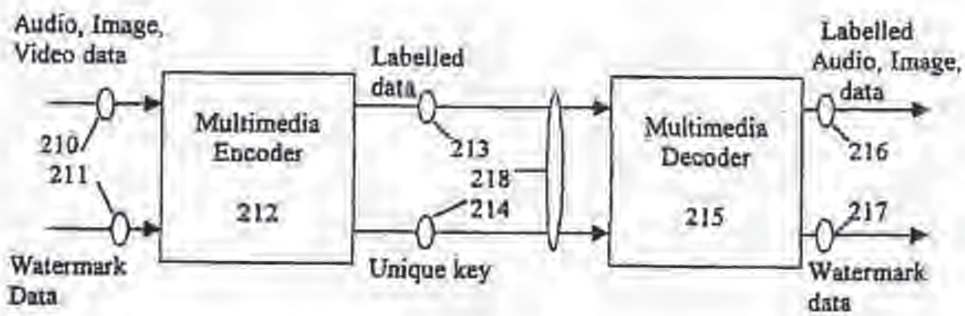


FIGURE 12

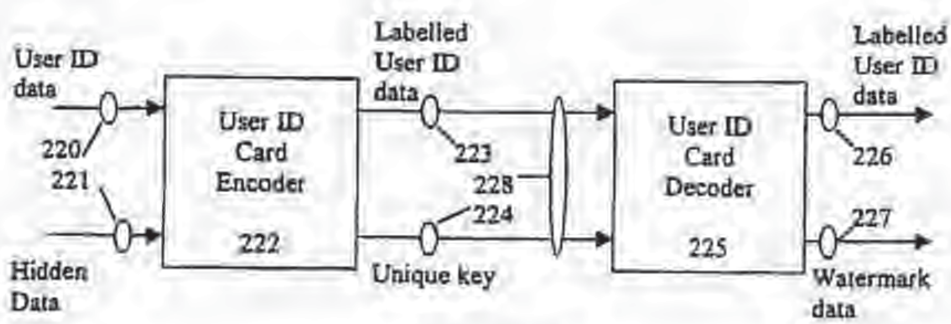


FIGURE 13

INTERNATIONAL SEARCH REPORT

International application No.
PCT/SG 98/00039

A. CLASSIFICATION OF SUBJECT MATTER

IPC[6]: G 06 F 12/14

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)

IPC[6]: G 06 F 12/14

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

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

EPODOC, WPI, PAJ

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
A	EP 0 840 513 A (NIPPON ELECTRIC) 06 Msy 1998 (06.05.98), abstract.	1
T	EP 0 855 681 A (NIPPON TELEGRAPH & TELEPHONE) 29 July 1998 (29.07.98), abstract.	
A	EP 0 766 468 A (NIPPON ELECTRIC) 02 April 1997 (02.04.97), abstract.	1

☐ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents:

„A" document defining the general state of the art which is not considered to be of particular relevance

„E" earlier application or patent but published on or after the international filing date

„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)

„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

„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

„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

„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

„&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
11 May 1999 (11.05.99)	21 May 1999 (21.05.99)

Name and mailing adress of the ISA/AT	Authorized officer
Austrian Patent Office Kohlmarkt 8-10; A-1014 Vienna Facsimile No. 1/53424/535	Fastenbauer Telephone No. 1/53424/447

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

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No.
PCT/SG 98/00039

Im Recherchenbericht angeführtes Patentdokument / Patent document cited in search report / Document de brevet cité dans le rapport de recherche	Datum der Veröffentlichung / Publication date / Date de publication	Mitglied(er) der Patentfamilie / Patent family member(s) / Membre(s) de la famille de brevets	Datum der Veröffentlichung / Publication date / Date de publication
EP 840513		AU A1 44340/97 CA AA 2219205 EP A2 840513 JP A2 10145757	07-05-1998 05-05-1998 06-05-1998 29-05-1998
EP 855681		EP A2 855681 JP A2 10210427 JP A2 10257300 JP A2 10304323 JP A2 11018064 JP A2 11041573	29-07-1998 07-08-1998 25-09-1998 13-11-1998 22-01-1999 12-02-1999
EP 766468		AU A1 65840/96 AU B2 701639 CA AA 2184949 EP A2 766468 JP A2 9191394	10-04-1997 04-02-1999 29-03-1997 02-04-1997 22-07-1997

PTO/SB/06 (07-06)
Approved for use through 1/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

PATENT APPLICATION FEE DETERMINATION RECORD
Substitute for Form PTO-875

Application or Docket Number: 10/049,101 | Filing Date: 07/23/2002 | ☐ To be Mailed

APPLICATION AS FILED – PART I

FOR	NUMBER FILED (Column 1)	NUMBER EXTRA (Column 2)	SMALL ENTITY ☒ RATE ($)	FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	FEE ($)
☐ BASIC FEE (37 CFR 1.16(a), (b), or (c))	N/A	N/A	N/A			N/A	
☐ SEARCH FEE (37 CFR 1.16(k), (i), or (m))	N/A	N/A	N/A			N/A	
☐ EXAMINATION FEE (37 CFR 1.16(o), (p), or (q))	N/A	N/A	N/A			N/A	
TOTAL CLAIMS (37 CFR 1.16(i))	minus 20 =	*	X $ =		OR	X $ =	
INDEPENDENT CLAIMS (37 CFR 1.16(h))	minus 3 =	*	X $ =			X $ =	
☐ APPLICATION SIZE FEE (37 CFR 1.16(s))	If the specification and drawings exceed 100 sheets of paper, the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).						
☐ MULTIPLE DEPENDENT CLAIM PRESENT (37 CFR 1.16(j))							
* If the difference in column 1 is less than zero, enter "0" in column 2.			TOTAL			TOTAL	

APPLICATION AS AMENDED – PART II

		CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)	OR	OTHER THAN SMALL ENTITY RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	02/29/2008									
	Total (37 CFR 1.16(i))	* 31	Minus	** 31	= 0	X $25 =	0	OR	X $ =	
	Independent (37 CFR 1.16(h))	* 7	Minus	***7	= 0	X $105 =	0	OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE	0	OR	TOTAL ADD'L FEE	

		CLAIMS REMAINING AFTER AMENDMENT (Column 1)		HIGHEST NUMBER PREVIOUSLY PAID FOR (Column 2)	PRESENT EXTRA (Column 3)	RATE ($)	ADDITIONAL FEE ($)	OR	RATE ($)	ADDITIONAL FEE ($)
AMENDMENT	Total (37 CFR 1.16(i))	*	Minus	**	=	X $ =		OR	X $ =	
	Independent (37 CFR 1.16(h))	*	Minus	***	=	X $ =		OR	X $ =	
	☐ Application Size Fee (37 CFR 1.16(s))									
	☐ FIRST PRESENTATION OF MULTIPLE DEPENDENT CLAIM (37 CFR 1.16(j))							OR		
						TOTAL ADD'L FEE		OR	TOTAL ADD'L FEE	

* If the entry in column 1 is less than the entry in column 2, write "0" in column 3.
** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 20, enter "20".
*** If the "Highest Number Previously Paid For" IN THIS SPACE is less than 3, enter "3".
The "Highest Number Previously Paid For" (Total or Independent) is the highest number found in the appropriate box in column 1.

Legal Instrument Examiner:
/DALE A. HALL/

This collection of information is required by 37 CFR 1.16. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
[illegible]

NOTICE OF ALLOWANCE AND FEE(S) DUE

[illegible] [illegible]

Scott A. Moskowitz
#2505
16711 Collins Avenue
Miami, FL 33160

EXAMINER	
[illegible]	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/09/2008

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,101	07/23/2002	Scott A. Moskowitz	80408.0011	4025

TITLE OF INVENTION: SECURE PERSONAL CONTENT SERVER

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$720	$0	$0	$720	10/09/2008

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

Scott A. Moskowitz
#2505
16711 Collins Avenue
Miami, FL 33160

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,101	07/23/2002	Scott A. Moskowitz	80408.0031	4025

TITLE OF INVENTION: SECURE PERSONAL CONTENT SERVER

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$720	$0	$0	$720	10/09/2008

EXAMINER	ART UNIT	CLASS-SUBCLASS
AVERY, JEREMIAH L	2131	713/169000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).
   - ☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.
   - ☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list
   (1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 ________
   (2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 ________ 3 ________

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☐ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:
- ☐ Issue Fee
- ☐ Publication Fee (No small entity discount permitted)
- ☐ Advance Order - # of Copies ________

4b. Payment of Fee(s): (**Please first reapply any previously paid issue fee shown above**)
- ☐ A check is enclosed.
- ☐ Payment by credit card. Form PTO-2038 is attached.
- ☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number ________ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)
- ☐ a. Applicant claims SMALL ENTITY status. *See 37 CFR 1.27.*
- ☐ b. Applicant is no longer claiming SMALL ENTITY status. *See 37 CFR 1.27(g)(2).*

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature ________ Date ________

Typed or printed name ________ Registration No. ________

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,101	07/23/2002	Scott A. Moskowitz	80408.0011	8028

7590 07/09/2008

Scott A. Moskowitz
#2505
16711 Collins Avenue
Miami, FL 33160

EXAMINER	
AVERY, JEREMIAH L	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/09/2008

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 683 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 683 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010

Notice of Allowability	Application No.	Applicant(s)
	10/049,101	MOSKOWITZ, SCOTT A.
	Examiner	Art Unit
	JEREMIAH AVERY	2131

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *the Applicant's response received on 02/29/08*.
2. ☒ The allowed claim(s) is/are *1-31*.
3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
   1. ☐ Certified copies of the priority documents have been received.
   2. ☐ Certified copies of the priority documents have been received in Application No. _____.
   3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.
5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
   1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☒ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 02/29/08
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____.
7. ☐ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☒ Other *IDS 02/29/08*.

Examiner's Statement of Reasons for Allowance

1. Claims 1-31 are allowed over the prior art.

2. This action is in reply to the Applicant's correspondence on 02/29/08.

3. The following is an Examiner's statement of reasons for the indication of allowable claimed subject matter.

4. As per claims 1, 3, 16, 17, 20, 24 and 31, generally, the prior art of record, United States Patent No. 5,341,429 to Stringer et al. and United States Patent No. 6,148,333 to Guedalia et al., fails to teach alone, or in combination, other than via hindsight, at the time of the invention, the features as discussed and remarked upon in the response of 02/29/08.

5. Nowhere in the prior art is found, collectively, the *italicized* claim elements (i.e., "*and if the digital content is not authorized for use by the LCS, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content*"), at the time of the invention; serving to patently distinguish the invention from said prior art:

"1. A local content server (LCS) for creating a secure environment for digital content, comprising:

a) a communications port for connecting the system via a network to at least one Secure Electronic Content Distributor (SECD), said SECD storing a plurality of data sets, receiving a request to transfer at least one content data set, and transmitting the at least one content data set in a secured transmission;

b) a rewritable storage medium whereby content received from outside the LCS is stored and retrieved;

c) a domain processor that imposes rules and procedures for content being transferred between the LCS and devices outside the LCS;

d) a programmable address module programmed with an identification code uniquely associated with the LCS;

said domain processor permitting the LCS to receive digital content from outside the LCS provided the LCS first determines that the digital content being delivered to the LCS is authorized for use by the LCS and if the digital content is not authorized for use by the LCS, accepting the digital content at a predetermined quality level, said predetermined quality level having been set for legacy content."

6. Further, the previous 35 U.S.C. 112, 2nd paragraph rejection of claims 1, 3 and 16 has been withdrawn.

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to JEREMIAH AVERY whose telephone number is (571)272-8627. The examiner can normally be reached on Monday thru Friday 8:30am-5pm.

8. If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

9. Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Jeremiah Avery/
Examiner, Art Unit 2131
/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131

Notice of References Cited	Application/Control No. 10/049,101	Applicant(s)/Patent Under Reexamination MOSKOWITZ, SCOTT A.	
	Examiner JEREMIAH AVERY	Art Unit 2131	Page 1 of 1

U.S. PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Name	Classification
*	A	US-6,587,837	07-2003	Spagna et al.	705/26
*	B	US-6,263,313	07-2001	Milsted et al.	705/1
*	C	US-6,931,534	08-2005	Jandel et al.	713/176
*	D	US-7,093,295	08-2006	Saito, Makoto	726/26
*	E	US-6,966,002	11-2005	Torrubia-Saez, Andres	726/29
*	F	US-5,341,429	08-1994	Stringer et al.	705/52
*	G	US-6,389,538	05-2002	Gruse et al.	713/194
*	H	US-5,513,126	04-1996	Harkins et al.	709/228
*	I	US-5,657,461	08-1997	Harkins et al.	715/733
*	J	US-6,148,333	11-2000	Guedalia et al.	709/219
	K	US-			
	L	US-			
	M	US-			

FOREIGN PATENT DOCUMENTS

*		Document Number Country Code-Number-Kind Code	Date MM-YYYY	Country	Name	Classification
	N					
	O					
	P					
	Q					
	R					
	S					
	T					

NON-PATENT DOCUMENTS

*		Include as applicable: Author, Title Date, Publisher, Edition or Volume, Pertinent Pages)
	U	Namgoong, Han. Moon, Ki-Young. Yoo, In-Won. "An Integrated Approach to Legacy Date for Multimedia Applications", Sept. 1997. Proceedings of the 23rd EUROMICRO Conference. Relevant Pages 387-391. Found on the World Wide Web at: http://ieeexplore.ieee.org/iel3/4879/13462/00617321.pdf?tp=&arnumber=617321&isnumber=13462
	V	
	W	
	X	

*A copy of this reference is not being furnished with this Office action. (See MPEP § 707.05(a).)
Dates in MM-YYYY format are publication dates. Classifications may be US or foreign.

Search Notes	Application/Control No. 10049101	Applicant(s)/Patent Under Reexamination MOSKOWITZ, SCOTT A.
	Examiner Avery, Jeremiah	Art Unit 2131

SEARCHED

Class	Subclass	Date	Examiner
none	none	7/2/2008	JLA

SEARCH NOTES

Search Notes	Date	Examiner
Updated EAST Search	7/2/2008	JLA
Updated Inventor Search	7/2/2008	JLA
IEEE Search	7/2/2008	JLA
Discussed with Christian LaForgia regarding search strategy	7/2/2008	JLA
Keyword search within Class 380, subclasses 236, 237 and 238, Class 713, subclass 169, Class 455, subclass 3.06 and Class 726, subclass 26	7/2/2008	JLA

INTERFERENCE SEARCH

Class	Subclass	Date	Examiner
none	(((legacy or early or earlier or earliest or previous$) near (content or data)) and server and (transmi$ or send$) and (data or information or info) and (authori$ or authentic$)).clm.	7/2/2008	JLA

Index of Claims	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10049101	MOSKOWITZ, SCOTT A.
	Examiner	Art Unit
	Avery, Jeremiah	2131

✓	Rejected	-	Cancelled	N	Non-Elected	A	Appeal
=	Allowed	÷	Restricted	I	Interference	O	Objected

☒ Claims renumbered in the same order as presented by applicant ☐ CPA ☐ T.D. ☐ R.1.47

CLAIM		DATE								
Final	Original	07/02/2009								
	1	=								
	2	=								
	3	=								
	4	=								
	5	=								
	6	=								
	7	=								
	8	=								
	9	=								
	10	=								
	11	=								
	12	=								
	13	=								
	14	=								
	15	=								
	16	=								
	17	=								
	18	=								
	19	=								
	20	=								
	21	=								
	22	=								
	23	=								
	24	=								
	25	=								
	26	=								
	27	=								
	28	=								
	29	=								
	30	=								
	31	=								

Issue Classification	Application/Control No.	Applicant(s)/Patent Under Reexamination
	10049101	MOSKOWITZ, SCOTT A.
	Examiner	Art Unit
	JEREMIAH AVERY	2131

ORIGINAL

CLASS	SUBCLASS
713	169

INTERNATIONAL CLASSIFICATION

CLAIMED					NON-CLAIMED				
H	0	4	N	7 / 167 (2006.01.01)	H	0	4	L	9 / 00 (2006.01.01)
H	0	4	H	40 / 00 (2006.01.01)					

CROSS REFERENCE(S)

CLASS	SUBCLASS (ONE SUBCLASS PER BLOCK)				
380	236	237	238		
455	3.06				
726	26				

/JEREMIAH AVERY/ 07/02/08 (Assistant Examiner) (Date)		Total Claims Allowed: 31
/Ayaz Sheikh/ 07/03/08 (Primary Examiner) (Date)	O.G. Print Claim(s) 1	O.G. Print Figure 4

U.S. Patent and Trademark Office

Part of Paper No. 20080702

EAST Search History

Ref #	Hits	Search Query	DBs	Default Operator	Plurals	Time Stamp
L1	1392	((quality near resolution) or (hierarch$ near quality)) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2008/07/02 14:37
L2	703	L1 and filter$	US-PGPUB; USPAT	OR	ON	2008/07/02 14:37
L3	18	L2 and (store or storing or storage or database) and server and authori$	US-PGPUB; USPAT	OR	ON	2008/07/02 14:37
L4	32	(scalable near bitstream) and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2008/07/02 14:38
L5	1	l4 and legacy	US-PGPUB; USPAT	OR	ON	2008/07/02 14:39
L6	601	watermark$ and (second near watermark)	US-PGPUB; USPAT	OR	ON	2008/07/02 14:46
L7	88	L6 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2008/07/02 14:46
L8	29	L7 and server	US-PGPUB; USPAT	OR	ON	2008/07/02 14:46
L9	28	L8 and quality	US-PGPUB; USPAT	OR	ON	2008/07/02 14:46
L10	26	L9 and (low$5 or degrad$)	US-PGPUB; USPAT	OR	ON	2008/07/02 14:46
L11	21	L10 and remote	US-PGPUB; USPAT	OR	ON	2008/07/02 14:46
L12	21	L11 and address$	US-PGPUB; USPAT	OR	ON	2008/07/02 14:46
L13	21	L12 and stor$4	US-PGPUB; USPAT	OR	ON	2008/07/02 14:46
L14	21	L13 and domain	US-PGPUB; USPAT	OR	ON	2008/07/02 14:46
L15	19	L14 and authentic$	US-PGPUB; USPAT	OR	ON	2008/07/02 14:46
L16	860	(380/236.ccls. or 380/237.ccls. or 380/238.ccls. or 713/169.ccls. or 455/3.06.ccls.) and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2008/07/02 14:47
L17	0	l16 and (legacy and (audio or video or digital or multimedia or (multi?media) or data)) and (quality near (degree or level))	US-PGPUB; USPAT	OR	ON	2008/07/02 14:49

L18	3	l16 and (legacy and (audio or video or digital or multimedia or (multi?media) or data))	US-PGPUB; USPAT	OR	ON	2008/07/02 14:49
L19	1	moskowitz-scott-in.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/02 14:59
L20	6	moskowitz.in. and legacy	US-PGPUB; USPAT; EPO	OR	ON	2008/07/02 14:59
L21	567	(380/236.ccls. or 380/237.ccls. or 380/238.ccls. or 713/169.ccls. or 726/26.ccls. or 455/3.06.ccls.) and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2008/07/02 15:02
L22	105	(((legacy or early or earlier or earliest or previous$) near (content or data)) and server and (transmi$ or send$) and (data or information or info) and (authori$ or authentic$)).clm.	US-PGPUB; USPAT; EPO	OR	ON	2008/07/02 15:04
S1	69	watermark$ and ((second near watermark$) and (third near watermark$))	US-PGPUB; USPAT	OR	ON	2006/10/03 09:14
S2	11	S1 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2007/09/28 12:12
S3	0	S2 and server	US-PGPUB; USPAT	OR	ON	2006/10/03 09:15
S4	7	S2 and quality	US-PGPUB; USPAT	OR	ON	2006/10/03 09:17
S5	0	S4 and legacy	US-PGPUB; USPAT	OR	ON	2006/10/03 09:18
S6	470	watermark$ and (second near watermark)	US-PGPUB; USPAT	OR	ON	2006/10/03 09:17
S7	60	S6 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2006/10/03 09:18
S8	25	S7 and server	US-PGPUB; USPAT	OR	ON	2006/10/03 09:18
S9	24	S8 and quality	US-PGPUB; USPAT	OR	ON	2006/10/03 09:18
S10	22	S9 and (low$5 or degrad$)	US-PGPUB; USPAT	OR	ON	2006/10/03 09:19
S11	0	S10 and (add?in)	US-PGPUB; USPAT	OR	ON	2006/10/03 09:19
S12	19	S10 and remote	US-PGPUB; USPAT	OR	ON	2006/10/03 09:19
S13	19	S12 and address	US-PGPUB; USPAT	OR	ON	2006/10/03 09:19

S14	19	S12 and address$	US-PGPUB; USPAT	OR	ON	2006/10/03 09:20
S15	19	S14 and stor$4	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S16	19	S15 and domain	US-PGPUB; USPAT	OR	ON	2006/10/03 09:22
S17	3	S16 and legacy	US-PGPUB; USPAT	OR	ON	2006/10/03 09:28
S18	17	S16 and authenticat$	US-PGPUB; USPAT	OR	ON	2007/04/26 19:21
S19	17	S16 and authentic$	US-PGPUB; USPAT	OR	ON	2006/10/03 09:34
S20	153	baum.xa.	US-PGPUB; USPAT	OR	ON	2006/10/03 09:34
S21	61	S20 and quality	US-PGPUB; USPAT	OR	ON	2006/10/03 09:35
S22	12	S21 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S23	10	("5195135" | "5715316" | "5805700" | "5845088" | "5898779" | "5953506" | "6026164" | "6216228" | "6449718" | "6557102").PN.	US-PGPUB; USPAT; USOCR	OR	OFF	2006/10/03 09:35
S24	74	watermark$ and ((second near watermark$) and (third near watermark$))	US-PGPUB; USPAT	OR	ON	2007/01/03 09:29
S25	0	S24 and (try near buy)	US-PGPUB; USPAT	OR	ON	2007/01/03 09:31
S26	162	(try near buy)	US-PGPUB; USPAT	OR	ON	2007/01/03 09:31
S27	50	S26 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S28	23	S27 and authori$	US-PGPUB; USPAT	OR	ON	2007/01/03 09:33
S29	2	S28 and watermark	US-PGPUB; USPAT	OR	ON	2007/01/03 09:46
S30	710	colvin.in.	US-PGPUB; USPAT	OR	ON	2007/01/03 09:46
S31	13	S30 and revak.xa.	US-PGPUB; USPAT	OR	ON	2007/01/03 09:47
S32	170	(try near buy)	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S33	50	S32 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S34	171	baum.xa.	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S35	64	S34 and quality	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20

S36	12	S35 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S37	524	watermark$ and (second near watermark)	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S38	84	S37 and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S39	27	S38 and server	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S40	26	S39 and quality	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S41	24	S40 and (low$5 or degrad$)	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S42	20	S41 and remote	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S43	20	S42 and address$	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S44	20	S43 and stor$4	US-PGPUB; USPAT	OR	ON	2007/04/26 19:20
S45	20	S43 and stor$4	US-PGPUB; USPAT	OR	ON	2007/04/26 19:21
S46	20	S45 and domain	US-PGPUB; USPAT	OR	ON	2007/04/26 19:21
S47	18	S46 and authenticat$	US-PGPUB; USPAT	OR	ON	2007/04/26 19:22
S48	0	S47 and (try near buy)	US-PGPUB; USPAT	OR	ON	2007/04/26 19:22
S49	0	S47 and ((try near buy) or demo)	US-PGPUB; USPAT	OR	ON	2007/04/26 19:23
S50	16	S47 and temp$5	US-PGPUB; USPAT	OR	ON	2007/04/26 19:23
S52	2983	((legacy or early or earlier or previous$) near (content or data)) and (@ad<"19990804" @prad<"19990804") and server	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 14:57
S53	1513	S52 and (secur$ or safe$2)	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:15
S54	1788	S52 and (secur$ or safe$2 or protect$)	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:16
S55	929	S54 and (authori$ or authenticat$)	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:17
S56	28	S55 and (quality near level)	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:17

S57	31	S55 and ((quality or condition$) near level)	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:22
S58	3	S57 and watermark and identi$	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:18
S59	5	((legacy or early or earlier or previous$) near (content or data)) and moskowitz.in.	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:24
S60	0	scott-moskowitz.in.	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:24
S61	616	moskowitz.in.	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:25
S62	1	moskowitz-scott.in.	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:25
S63	576	S54 and domain	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:26
S64	26	S63 and watermark$	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:26
S65	23	S64 and (author$ or authentic$)	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:26
S66	68	(((legacy or early or earlier or previous$) near (content or data)) and server and (transmi$ or send$) and (data or information or info) and (author$ or authentic$)).clm.	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:33
S67	7	S66 and watermark$	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:33
S68	2972	((legacy or early or earlier or previous$) near (content or data or multimedia)) and (@ad<"19990804" @prad<"19990804") and server	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:40
S69	1251	S68 and (quality or degrad$6)	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:41
S70	31	S69 and watermark$	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 12:41

S71	195640	(quality) and (audio or video or multimedia or media) and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:10
S72	4057	S71 and (qos or (quality near service))	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:01
S73	46	S72 and watermark$	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:01
S74	1181	S71 and watermark$	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:04
S75	17	S74 and legacy	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:04
S76	37328	(quality) and (geograph$ or map or maps or mapping) and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:10
S77	645	S76 and watermark$	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:11
S78	16	S77 and legacy	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:12
S79	15	S78 and server	US-PGPUB; USPAT; EPO	OR	ON	2007/08/28 15:12
S80	48	legacy and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality near level)	US-PGPUB; USPAT	OR	ON	2007/10/23 14:19
S81	37	S80 and (safe$ or secur$ or protect$)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:28
S82	35	S81 and (store or storage or storing or database)	US-PGPUB; USPAT	OR	ON	2007/10/23 14:15
S83	34	S82 and server	US-PGPUB; USPAT	OR	ON	2007/10/23 10:29
S84	26	S83 and author$	US-PGPUB; USPAT	OR	ON	2007/10/23 10:30
S85	2	legacy and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality near (degree or level))	US-PGPUB; USPAT	OR	ON	2007/10/23 10:34

S86	49	legacy and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality near (degree or level))	US-PGPUB; USPAT	OR	ON	2007/10/23 14:16
S87	41	S86 and server	US-PGPUB; USPAT	OR	ON	2007/10/23 10:34
S88	41	S87 and (authori$ or allow$ or permit$)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:51
S89	37	S88 and (store or storing or storage or database)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:35
S90	6	(legacy and (legacy with content)) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality near level)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:39
S91	6	(legacy with content) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality near level)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:39
S92	0	(legacy with content) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality adj level)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:40
S93	7	(legacy with content) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality with level)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:41
S94	33	(legacy with content) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and quality	US-PGPUB; USPAT	OR	ON	2007/10/23 10:42
S95	26	S94 and server	US-PGPUB; USPAT	OR	ON	2007/10/23 10:42
S96	26	S95 and (authori$ or allow$ or permit$)	US-PGPUB; USPAT	OR	ON	2007/10/23 10:51
S97	23	(legacy with content) and (@ad<"19980804" @prad<"19980804")	US-PGPUB; USPAT	OR	ON	2007/10/23 14:11
S98	14	S97 and server	US-PGPUB; USPAT	OR	ON	2007/10/23 14:04

S99	2	(legacy near content) and (@ad<"19980804" @prad<"19980804")	US-PGPUB; USPAT	OR	ON	2007/10/23 14:15
S100	1607	((legacy or old or older) near (version or content)) and (@ad<"19980804" @prad<"19980804")	US-PGPUB; USPAT	OR	ON	2007/10/23 14:15
S101	513	S100 and server	US-PGPUB; USPAT	OR	ON	2007/10/23 14:15
S102	510	S101 and (store or storage or storing or database)	US-PGPUB; USPAT	OR	ON	2007/10/23 14:15
S103	13	S102 and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality near (degree or level))	US-PGPUB; USPAT	OR	ON	2007/10/23 14:17
S104	6	S103 and authori$	US-PGPUB; USPAT	OR	ON	2007/10/23 14:18
S105	1	(legacy adj (content or version)) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and (quality near level)	US-PGPUB; USPAT	OR	ON	2007/10/23 14:21
S106	26	(legacy adj (content or version)) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804") and quality	US-PGPUB; USPAT	OR	ON	2007/10/23 15:01
S107	1367	((quality near resolution) or (hierarch$ near quality)) and (audio or video or digital or multi?media or data) and (@ad<"19990804" @prad<"19990804")	US-PGPUB; USPAT	OR	ON	2007/10/23 15:02
S108	680	S107 and filter$	US-PGPUB; USPAT	OR	ON	2007/10/23 15:02
S109	18	S108 and (store or storing or storage or database) and server and authori$	US-PGPUB; USPAT	OR	ON	2007/10/23 15:03

7/2/2008 2:28:21 PM
C:\ Documents and Settings\ javery\ My Documents\ EAST\ Workspaces\ 10049101.wsp

PTO/SB/08A (10-07)
Approved for use through 10/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 2

Complete if Known	
Application Number	10/049,101
Filing Date	July 23 2002
First Named Inventor	Moskowitz
Art Unit	2131
Examiner Name	AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number (Number-Kind Code[2] (if known))	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US 6,088,455	07/11/2000	Logan et al.	
		US 5,634,040	05/27/1997	Her et al.	
		US 6,381,747	04/30/2002	Wonfor et al.	
		US 4,969,204	11/06/1990	Melnychuck et al.	
		US 6,966,002	11/15/2005	Torrubia-Saez	
		US 6,263,313	07/17/2001	Milsted, et al.	
		US 7,093,295	08/15/2006	Saito	
		US 6,587,837	07/01/2003	Spagna et al.	
		US 6,931,534	08/16/2005	Jandel et al.	
		US 2004/0049695	03/11/2004	Choi et al.	
		US 2004/0083369	07/25/2003	Erlingsson et al.	
		US 5,677,952	10/14/1997	Blakely et al.	
		US 5,768,396	06/16/1998	Sone	
		US 7,266,697	09/04/2007	Kirovski et al.	
		US 5,136,646	08/04/1992	Haber et al.	
		US 5,136,647	08/04/1992	Haber et al.	
		US 7,206,649	04/17/2007	Kirovski et al.	
		US 6,532,284	03/11/2003	Walker et al.	
		US 7,020,285	03/28/2006	Kirovski et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document (Country Code[3] - Number[4] - Kind Code[5] (if known))	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Jeremiah Avery/	Date Considered	07/02/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/08A (01-08)
Approved for use through 01/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 2

Complete If Known	
Application Number	10/049101
Filing Date	July 23, 2002
First Named Inventor	Moskowitz
Art Unit	2131
Examiner Name	AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number (Number-Kind Code[2] (if known))	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-7,046,808	05/12/2006	Metois et al.	
		US-6,430,301	08/06/2002	Petrovic	
		US-2004/0059918	03/25/2004	Xu	
		US-6,345,100	02/05/2002	Levine	
		US-2004/0093521	05/13/2004	Hamadeh et al.	
		US-2007/0083467	04/12/2007	Lindahl et al.	
		US-7,231,524	06/12/2007	Burns	
		US-2005/0246554	11/03/2005	Batson	
		US-6,668,325	02/23/2003	Collberg et al.	
		US-7,050,396	05/23/2006	Cohen et al.	
		US-6,842,862	01/11/2005	Chow et al.	
		US-7,051,208	05/23/2006	Venkatesan et al.	
		US-7,240,210	07/03/2007	Michak et al.	
		US-7,150,003	12/12/2006	Naumovich et al.	
		US-6,389,538	05/14/2002	Gruse et al.	
		US-5,513,126	04/30/1996	Harkins et al.	
		US-5,657,461	08/12/1997	Harkins et al.	
		US-4,390,898	06/28/1983	Bond et al.	
		US-5,471,533	11/28/1995	Wang et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document (Country Code[3] Number[4] Kind Code[5] (if known))	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Jeremiah Avery/	Date Considered	07/02/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A/

OIPE
FEB 2 9 2008

PTO/SB/08B (10-07)
Approved for use through 10/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete If Known	
Application Number	10/049,101
Filing Date	July 25, 2002
First Named Inventor	MOSKOWITZ
Art Unit	2131
Examiner Name	AVERY
Attorney Docket Number	80408.0011

Sheet 1 of 1

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Rivest,et al., PayWord and MicroMint: Two simple micropayment schemes, MIT Laboratory for Computer Science, Cambridge, MA 02139, April 27,2001, pp. 1-18.	
		Horowitz, et al., The Art of Electronics, 2nd Ed., 1989, pp.7.	
		Delaigle, J.-F., et al. "Digital Watermarking," Proceedings of the SPIE, vol. 2659, Feb 1, 1996, pp. 99-110 (Abstract).	
		Schneider, M., et al. "Robust Content Based Digital Signature for Image Authentication," Proceedings of the International Conference on Image Processing (IC. Lausanne), Sept. 16-19, 1996, pp. 227-230, IEEE ISBN:	
		Cox, I. J., et al. "Secure Spread Spectrum Watermarking for Multimedia," IEEE Transactions on Image Processing, Vol. 6 No. 12, Dec. 1, 1997, pp. 1673-1686.	
		Wong, Ping Wah. "A Public Key Watermark for Image Verification and Authentication," IEEE International Conference on Image Processing, Vol. 1, Oct. 4-7, 1998, pp. 455-459.	
		Fabien A.P. Petitcolas, Ross J. Anderson and Markkus G. Kuhn, "Attacks on Copyright Marking Systems," LNCS, Vol. 1525, April 14-17, 1998, pp. 218-238, ISBN: 3-540-65386-4.	
		Ross Anderson, "Stretching the Limits of Steganography," LNCS, Vol. 1174, May/June 1996, 10 pages, ISBN: 3-540-61996-8.	
		Joseph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", pre-publication, Summer 1997, 4 pages.	
		Joseph J.K. O'Ruanaidh and Thierry Pun, "Rotation, Scale and Translation Invariant Digital Image Watermarking", Submitted to Signal Processing, August 21, 1997, 19 pages.	

Examiner Signature	/Jeremiah Avery/	Date Considered	07/02/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

OIPE
FEB 2 8 2008

PTO/SB/08B (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	10/049101
Filing Date	July 23 2002
First Named Inventor	MOSKOWITZ
Art Unit	2131
Examiner Name	AVERY
Attorney Docket Number	80408.0011

Sheet 1 of 2

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		PCT International Search Report, completed Sept. 13, 1995; authorized officer Huy D. Vu (PCT/US95/08159) (2 pages)	
		PCT International Search Report, completed June 11, 1996; authorized officer Salvatore Cangialosi (PCT/US96/10257) (4 pages)	
		Supplementary European Search Report, completed Mar. 5, 2004; authorized officer J. Hazel (EP 96 91 9405) (1 page)	
		PCT International Search Report, completed April 4, 1997; authorized officer Bernarr Earl Gregory (PCT/US97/00651) (1 page)	
		PCT International Search Report, completed May 6, 1997; authorized officer Salvatore Cangialosi (PCT/US97/00652) (3 pages)	
		PCT International Search Report, completed Oct. 23, 1997; authorized officer David Cain (PCT/US97/11455) (1 page)	
		PCT International Search Report, completed July 12, 1999; authorized officer R. Hubeau (PCT/US99/07262) (3 pages)	
		PCT International Search Report, completed June 30, 2000; authorized officer Paul E. Callahan (PCT/US00/06522) (7 pages)	
		Supplementary European Search Report, completed June 27, 2002; authorized officer M. Schoeyer (EP 00 91 9398) (1 page)	
		PCT International Search Report, date of mailing Mar. 15, 2001; authorized officer Marja Brouwers (PCT/US00/18411) (5 pages)	

Examiner Signature	/Jeremiah Avery/	Date Considered	07/02/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	10/049,101
Filing Date	July 23 2002
First Named Inventor	MOSKOWITZ
Art Unit	2131
Examiner Name	AVERY
Attorney Docket Number	80408.001

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		PCT International Search Report, completed July 20, 2001; authorized officer A. Sigolo (PCT/US00/18411) (5 pages)	
		PCT International Search Report, completed March 20, 2001; authorized officer P. Corcoran (PCT/US00/33126) (6 pages)	
		PCT International Search Report, completed January 26, 2001; authorized officer A. Sigolo (PCT/US00/21189) (3 pages)	
		European Search Report, completed October 15, 2007; authorized officer James Hazel (EP 07 11 2420) (9 pages)	

Examiner Signature	/Jeremiah Avery/	Date Considered	07/02/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

OIPE IAP28 FEB 2 8 2008

PTO/SB/08B (01-08)
Approved for use through 01/31/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 1

Complete if Known	
Application Number	10/049101
Filing Date	July 23 2002
First Named Inventor	MOSKOWITZ
Art Unit	2131
Examiner Name	AVERY
Attorney Docket Number	80408.0011

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		STAIND (The Singles 1996-2006), Warner Music - Atlantic, Pre-Release CD image, 2006, 1 page	
		Arctic Monkeys (Whatever People Say I Am, That's What I'm Not), Domino Recording Co. Ltd., Pre-Release CD image, 2005, 1 page	
		Radiohead ("Hail To The Thief"), EMI Music Group - Capitol, Pre-Release CD Image, 2003, 1 page.	

Examiner Signature	/Jeremiah Avery/	Date Considered	07/02/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

An Integrated Approach to Legacy Data for Multimedia Applications

Han Namgoong
Distributed Processing Section
ETRI
Yusong P.O.Box 106
Taejon 305-600, KOREA
nghan@etri.re.kr

Ki-Young Moon
Distributed Processing Section
ETRI
Yusong P.O.Box 106
Taejon 305-600, KOREA
kymoon@etri.re.kr

In-Won Yoo
Distributed Processing Section
ETRI
Yusong P.O.Box 106
Taejon 305-600, KOREA
yooiw@etri.re.kr

Abstract

In this paper we describe our experimental approach to legacy data for multimedia applications in WWW environment. There have been many proposals for the connection to legacy data and got considerable results. Unfortunately those don't cover one of real environmental factors such as guarantee of persistent result to existing data(example, payment of purchase). Our approach shows an easy access to the legacy data via Web and our new WWW interfaces make users do easily Common Gateway Interface(CGI) programming. We also expect mission critical jobs such as banking and financial operation can be served through WWW effectively.

1. Introduction

Users of multimedia applications take three different steps: 1) connection to multimedia applications, 2) doing some business logic, 3) disconnection from multimedia applications. If user wants to buy a book from bookstore in Internet then he connects to the bookstore via Web(*step 1*) and select a book(and fill up necessary information like payment method, shipping address etc., *step 2*). Finally he disconnects(*step 3*) from the bookstore. The final operation of the second step(in the above example, payment) usually needs an access to the legacy data in transaction mode, which provides automatic failure recovery in a fashion of all or nothing. Many legacy data still act as one of important resources in Internet. For example personal bank account is expected to be under current legacy applications quite a long time. Of course user interface may be changed in a short time but its operational state will not be changed. For multimedia applications we have to provide an efficient way of interconnection to legacy data in transaction mode. This paper is organized as follows. Section 2 first describes approach to legacy data and in section 3 we present extended Web structure of our approach. Section 4 shows one of the ways to connect Web and non-Web world through bridge. Finally, section 5 offers conclusion of our approach.

2. Approach

2.1. Current Status

WWW is a Hypertext Information Retrieval System which runs in client/server mode. Web client part is composed of Web browser and server part contains two modules: one for Hypertext information retrieval engine and Hypertext Transfer Protocol Daemon(HTTP Daemon). Currently Web is used mainly as information retrieval services such as an advertisement of products and companies' public relations. But users in business sectors want to get more traditional business services such as banking and reservation operations, which are run under transaction mode, via Web. To provide those traditional business services through Web we need a way to connect legacy application which runs under transaction processing monitor(TP monitor) which provides transaction service, where many distributed transactions can be treated as a single transaction. In current Web environment, shown in figure 1, client/server uses two different protocols: 1) HTTP for Web browser

1089-6503/97 $10.00 © 1997 IEEE

and Web server, 2) environment specific protocol such as SQL/RPC/SNA for the connection to information resources(DB, file system etc.). When client/server is in the same system then CGI is used between client and server.

2.2. Model

To make an access to legacy data in transaction mode first we need a connection between DTP and WWW server. Generally Web and DBMS, which is an application program of Web, is connected via CGI in one system(means WWW server system) but in that case we have an overloading problem because usually DTP needs many resources.

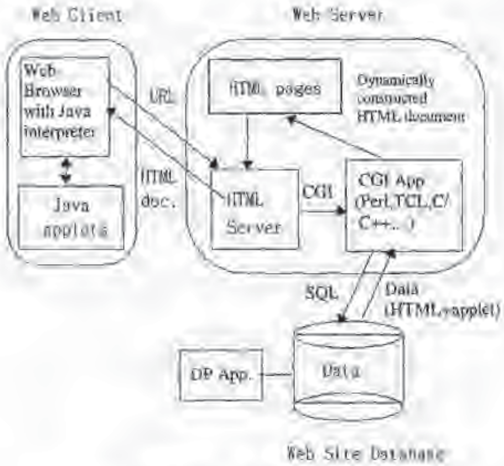
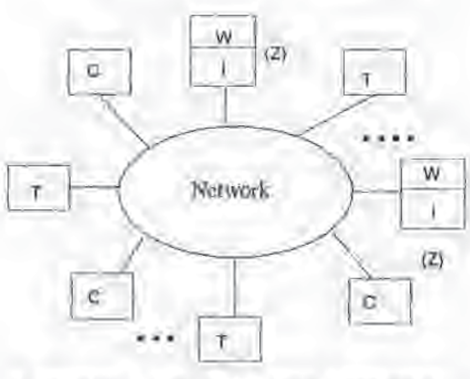


Figure 1. Web Environment[13].



W: Web Server C: Client T: DTP Server I: Web Interface

Figure 2. Connection via Web Interfaces.

We propose a new connection, where DTP and Web server run on different systems. The new connection provides easy CGI programming and convenient DTP service. Web server can connect arbitrary DTP server in network through our new Web interfaces and gives good load balancing. If any Web server wants to provide DTP service and at least one DTP server is in network then only Web interface is needed. We don't need to implement the whole DTP module on every Web server. Figure 2 and 3 show a new connection environment using Web interfaces and environment.

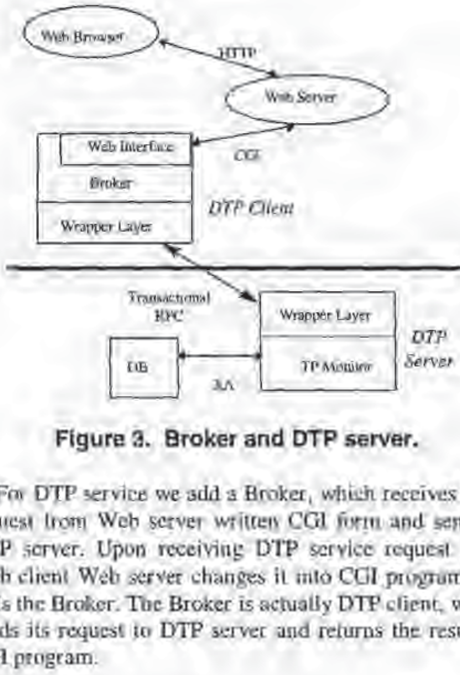


Figure 3. Broker and DTP server.

For DTP service we add a Broker, which receives DTP request from Web server written CGI form and sends it DTP server. Upon receiving DTP service request from Web client Web server changes it into CGI program and calls the Broker. The Broker is actually DTP client, which sends its request to DTP server and returns the result to CGI program.

3. Extended Web Structure

Current HTTP is not suitable for the handling of legacy data in transaction mode and usually DTP uses transactional communication(Transactional RPC etc.) for the guarantee of consistent data. To send users data from Web to DTP server we needs two wrapping layers: 1) client transaction wrapper layer(CTWL) for the conversion from Web data to DTP client program, 2) server transaction wrapper layer(STWL) for DTP server. The extended Web structure for transaction mode is shown in figure 4.

3.1. Transaction Wrapper Layer

CTWL converts client data from Web into transaction data and send them to DTP server. To send user data to DTP server CTWL uses array type and example of array type is shown below.

array[0] : name of application
array[1] : service name 1 = value 1
array[2] : service name 2 = value 2
....
array[n] : service name N = value N

CTWL does the following tasks.

- User authentication and authorization
- Converts data in HTML into predefined STWL's data format
- Keep operation status and user data for recovery
- Preparation of HTML documents as output for the returned result of DTP server

Upon receiving the result from STWL CTWL does conversion into HTML format and display on Web.

STWL converts client data from Web into transaction data and send them to DTP server. STWL does the following tasks.

- Converts client data into predefined DTP server's data format
- Invoke necessary applications
- Return the result of DTP server to CTWL

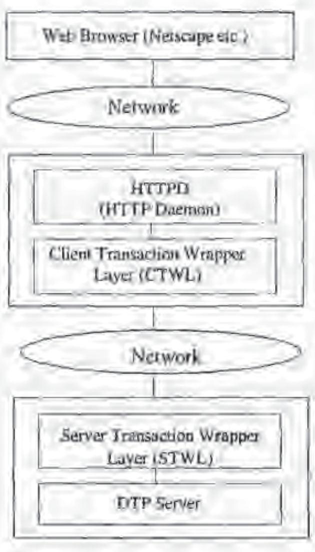


Figure 4. Extended Web Structure.

3.2. Functions for Transaction Data

For send the transaction data to server(ex. Bank account number, amount from web client) we make four functions which are invoked from client stub and server stub.

- rpc_cstub_prologue()
  Transaction RPC client stub calls this function and requests to create transaction branch. Client stub sends transaction data as piggybacked on the normal RPC request. Transaction Monitor returns assigned transaction identifier for the later use like cancel and rollback.
- rpc_cstub_epilogue()
  Upon receiving result from server the client stub calls this function and pass the returned data to local transaction manager.
- rpc_sstub_prologue()
  When user program wants to send a message to remote server transactional RPC calls this function and manager function in the server side invokes actual services operation depending on passed data.
- rpc_sstub_epilogue()
  Manager function calls this function and send result on the RPC reply.

For user programs the following interfaces are provided.

Interface Name	Function
DTP_Connect	Request Connect for Service
DTP_Close	Request Service Termination
DTP_Call	Call Server
DTP_Return	Wait for result /Check timeout
DTP_Rollback	Transaction Rollback Request
DTP_CodeConv	Change data format(RPC)
DTP_AccessControl	Authentication/Authorization
DTP_Set_Transaction_Timeout	Set timeout value

4. Integrating CORBA and DCE

4.1. CORBA and Web

Many benefits of object can be used in Web environment through a gateway between CORBA and Web. We design a gateway, shown in figure 5, which accepted user input and changes into CORBA client program. User in web browser can call CORBA object(service) directly using HTTP protocol. Upon receiving the request and gateway passes the data to CORBA client. The CORBA client calls CORBA server through IIOP protocol and then returns the result to Web client via gateway.

4.2. CORBA and DCE Gateway[1]

There also exists some services which are uniquely to only CORBA or DCE. For example applications on CORBA do not support strong security, while DCE users can get the benefits of object. The Interface Definition Languages(IDLs) used by CORBA and DCE are not compatible, and there is no compatibility in the generated stub or skeleton code each IDL compiler generates. To cover this problem we can think four cases in bridging between DCE and CORBA as follows.

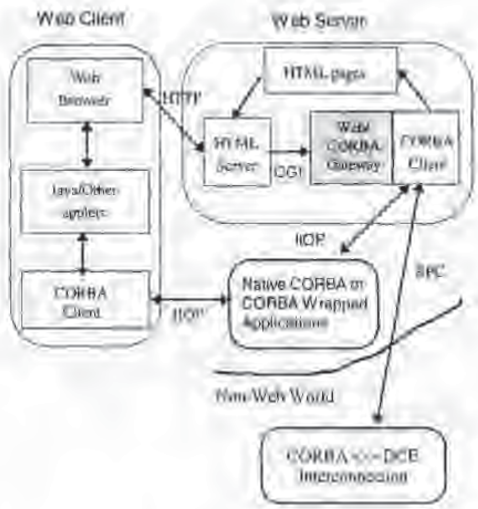


Figure 5. CORBA and Web Environment.

case 1: CORBA-client-to-DCE-server bridge
There are many existing DCE-based servers. New CORBA-based applications need to use the DCE servers but not vice versa. If this is the case, then the bridge-building process is to take the DCE IDL and convert it to CORBA IDL and build a bridge to convert between them.
case 2: DCE-client-to-CORBA-server bridge
If this is the case, then the bridge-building process is to take the CORBA IDL and translate it to DCE IDL and build a bridge to convert between them.
case 3: DCE-based servers and CORBA-based servers
There are both servers in DCE and CORBA(but providing different areas of functionality) and we have to do both of the above(*case 1* and *case 2*).
case 4: DCE-based servers and CORBA-based servers
This is the same case except both servers have same functionality's. Clients might need to use both DCE-based servers and CORBA-based servers to obtain this functionality. If this is the case, then this is very different to the previous cases. In the previous cases(*case 3*), one set of IDL was given, the other IDL can be generated with a view to making it easy to translate between them. Ease of translation means that structurally the generated IDL is similar to the original IDL (e.g. same number of operations with the same parameters). This kind of approach is suitable for automation(or, at least, assisted with tools).
In *case 4*, there are two sets of IDL given. The bridge building process has to understand how the two IDLs relate to one another. E.g. making one operation call at one interface might equate to two operation calls on another interface. This would generally require semantic information beyond that contained in IDL.

We decide to build our bridge, a limited gateway for CORBA client and DCE based server, as follows:
User use specific tool(program) to generates two specific CORBA/DCE interfaces types. This bridge is probably very fast at run-time as all the translation, generation, compilation etc. was done in advance and the result is a bridge ready-to-run. The disadvantage is that you have to know at development time which interfaces require bridges. However, for many standard applications, this information is known. There is no need to use dynamic invocation methods for this kind of bridge. Depending on the approach taken, it might or might not be necessary to use dynamic invocation. Obviously CORBA has dynamic invocation so making dynamic calls to CORBA servers is easy in theory. However, in practice, not all ORBs implement dynamic invocation and some ORBs implement it but the implementation has bugs. DCE does not provide any dynamic invocation capability, although we have done some preliminary work in this area. Implementing dynamic invocations for DCE is an interesting problem in its own right. However, it is not a small problem and decide to do next time. Figure 6 shows overall environment of CORBA/DCE operation.

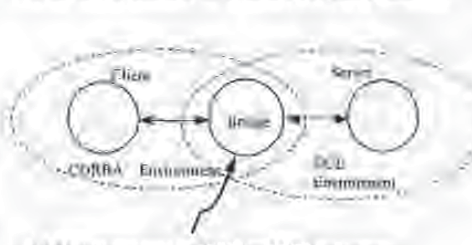


Figure 6. CORBA and DCE Environment.

5. Example

As an example of our approach we build experimental multimedia application, VoD, based on our extension model. User can select movies in Web browser, watch it and makes a payment through the interconnection with remote bank server/credit card server. The current set of WWW protocols are not suitable for real-time delivery of multimedia stream. To overcome this on CORBA/WWW environment we separate control commands and multimedia data by different paths. We use DAVIC[12] style approach, where stream control commands like send/receive use CORBA layer and multimedia streams go different MPEG2 layer. We provides three modules for this: Java/ORB Gateway, Applet class for user interface and QoS negotiation.

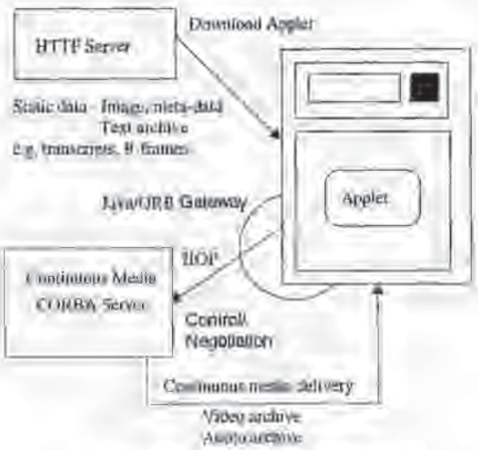


Figure 7. VoD on CORBA[10].

The Internet has an impact on the QoS level in two ways. One is TCP/IP, which protocol shares available resources evenly amongst all competing connections. The characteristics of end-systems give another impact on QoS level. The QoS negotiation protocol aims for the best between capabilities and constraints of multimedia server, the network and client. We currently design QoS management scheme based on CORBA stream standardization.

6. Conclusion

Our approach solves two problems: 1) system overloading which caused by the co-residence of DTP and WWW server in the same system and 2) CORBA/WWW/DCE integration. Furthermore our new WWW interfaces(DTP service via WWW) make users do easily CGI programming. The interfaces is the same format of X/Open DTP interface, so users who is familiar with traditional transaction processing can easily use the same functionality in WWW environment. We also expect mission critical jobs such as banking and financial operations can be served through WWW interfaces effectively.

References

[1] Open Software Foundation, *DCE Administration Guide*, Cambridge, Open Software Foundation, 1992.

[2] X/Open Company Limited, *Distributed Transaction Processing: Reference Model*, Berkshire U.K., X/Open Company Limited, 1993.

[3] Soran Ine et al., "Database Server Client Tool in Client-Server Model," Korea Database Journal, KDBs, Vol.1, No.1, pp. 107-121, August 1994.

[4] Taligent, *Building Object-Oriented Frameworks*, Taligent, CA. 1993.

[5] Object Management Group, *The Common Object Request Broker: Architecture and Specification*, Object Management Group, 1992.

[6] Richard Adler, "Distributed Coordination Models for Client/Server Computing," Computer, Vol.28, No.4, April, 1995, pp.14-22.

[7] Dimitrios Georgakopoulos et al., "An Extended Transaction Environment for Workflows in Distributed Object Computing," IEEE Bulletin of the Technical Committee on Data Engineering, Vol.16, No.2, June, 1993.

[8] Jim Gray and Andreas Reuter, *Transaction Processing: Concept and Techniques*, Morgan Kaufmann, San Mateo, CA, 1993.

[9] Kerry Raymond, *e-mail to Han Namgoong*, April 24, 1996.

[10] Michael Fry et all, *QoS Controlled Continuous Media and the World Wide Web*, IFIP Workshop on QoS, 1996.

[11] Digital Audio-Visual Council, *DAVIC 1.0*, 1995, Geneva, Switzerland.

[12] Han Namgoong, Dukjoo Son, Myung-Joon Kim, *A framework based on Hybrid Broker Model for Multimedia Applications*, Proceeding of The 10th ICOIN, January, 1996.

[13] Vijay Trehan, *CORBA and the World Wide Web*, Proceeding of Object World West, August, 1996.

04-18-07 TFW 2131

PTO/SB/21 (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Total Number of Pages in This Submission

Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott MOSKOWITZ
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

ENCLOSURES (Check all that apply)

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [ ] Amendment/Reply
  - [ ] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [x] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) ______
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please identify below):

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name			
Signature	Scott Moskowitz		
Printed name	Scott MOSKOWITZ		
Date	April 17, 2007	Reg. No.	

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	Scott Moskowitz		
Typed or printed name	Scott MOSKOWITZ	Date	April 17, 2007

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/17 (12-07)
Approved for use through 07/31/2007. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2007

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT ($) $180.00

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott MOSKOWITZ
Examiner Name	Jeremiah AVERY
Art Unit	2131
Attorney Docket No.	80408.0011

METHOD OF PAYMENT (check all that apply)

☐ Check ☑ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): ____

☐ Deposit Account Deposit Account Number: ____ Deposit Account Name: ____

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, **except for the filing fee**

☐ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
Application Type	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fee ($)	Small Entity Fee ($)	Fees Paid ($)
Utility	300	150	500	250	200	100	____
Design	200	100	100	50	130	65	____
Plant	200	100	300	150	160	80	____
Reissue	300	150	500	250	600	300	____
Provisional	200	100	0	0	0	0	____

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	50	25
Each independent claim over 3 (including Reissues)	200	100
Multiple dependent claims	360	180

Total Claims ____ – 20 or HP = Extra Claims ____ x Fee ($) ____ = Fee Paid ($) ____

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims ____ – 3 or HP = Extra Claims ____ x Fee ($) ____ = Fee Paid ($) ____

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims: Fee ($) ____ Fee Paid ($) ____

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $250 ($125 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets ____ – 100 = Extra Sheets ____ / 50 = Number of each additional 50 or fraction thereof ____ (round up to a whole number) x Fee ($) ____ = Fee Paid ($) ____

4. OTHER FEE(S)

Fees Paid ($)

Non-English Specification, $130 fee (no small entity discount)

Other (e.g., late filing surcharge): Information Disclosure Statement $180.00

SUBMITTED BY			
Signature	[signature]	Registration No. (Attorney/Agent)	Telephone 305 950 9041
Name (Print/Type)	Scott MOSKOWITZ		Date April 17, 2007

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	10/049,101	Confirmation No. 8028
Applicant	Scott A. MOSKOWITZ et al.	
Filed	July 23, 2002	
TC/A.U.	2131	
Examiner	Jeremiah AVERY	
Docket No.	80408.0011	

MAIL STOP AMENDMENT
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

INFORMATION DISCLOSURE STATEMENT

Dear Sir:

Applicants submit copies of the references listed on the attached SB08 Form for consideration and request that the U.S. Patent and Trademark Office make them of record in this application.

Applicants state the following.

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the Information Disclosure Statement; or

☐ No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and to the knowledge of Applicant(s) no item of information contained in this Information Disclosure Statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

☐ In accordance with 37 C.F.R. § 1.97(b), this Information Disclosure Statement is believed to be submitted prior to issuance of a first Office Action and/or within three months of the filing date of the application. It is respectfully submitted that no fee is required for consideration of this information.

☒ This Information Disclosure Statement is being submitted after the mailing of a non-final Office Action, but is believed to be prior to a final Office Action or a Notice of Allowance. Pursuant to 37 C.F.R. § 1.97(c), payment in the amount of $180.00 as set forth in 37 C.F.R. § 1.17(p) is enclosed.

While the information and references disclosed in this Information Disclosure Statement are submitted pursuant to 37 C.F.R. § 1.56, this submission is not intended to constitute an admission that any patent, publication or other information referred to is "prior art" to this invention. Applicants reserve the right to contest the "prior art" status of any information submitted or asserted against the application.

Additionally, Applicant wishes to inform the Examiner of the existence of the following co-pending U.S. patents and patent applications that share a common inventor with the present application:

EXAMINER'S INITIALS:

____ U.S. Patent Application No. 08/999,766, filed July 23, 1997, entitled "Steganographic Method and Device";

____ EPO Application No. 96919405.9, entitled "Steganographic Method and Device";

____ U.S. Patent Application No. 11/050,779, filed February 7, 2005, entitled "Steganographic Method and Device";

____ U.S. Patent Application No. 08/674,726, filed July 2, 1996, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management";

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

____ U.S. Patent Application No. 09/545,589, filed April 7, 2000, entitled "Method and System for Digital Watermarking";

____ U.S. Patent Application No. 11/244,213, filed October 5, 2005 entitled "Method and System for Digital Watermarking";

____ U.S. Patent Application No. 11/649,026, filed January 3, 2007, entitled "Method and System for Digital Watermarking";

____ U.S. Patent Application No. 09/046,627, filed March 24, 1998, entitled "Method for Combining Transfer Function with Predetermined Key Creation";

____ U.S. Patent Application 10/602,777, filed June 25, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation";

____ U.S. Patent Application No. 09/053,628, filed April 2, 1998, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

____ U.S. Patent Application No. 09/644,098, filed August 23, 2000, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

____ Jap. App. No 2000-542907, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

____ U.S. Patent Application No. 09/767,733, filed January 24, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

____ U.S. Patent Application No. 11/358,874, filed February 21, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

____ U.S. Patent Application No. 10/417,231, filed April 17, 2003, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth";

____ U.S. Patent Application No. 09/789,711, filed February 22, 2001, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

____ U.S. Patent Application No. 11/497,822, filed August 2, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

____ U.S. Patent Application No. 11/599,964, filed November 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

____ U.S. Patent Application No. 11/599,838, filed November 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

____ U.S. Patent Application No. 10/369,344, filed February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

____ U.S. Patent Application No. 11/482,654, filed July 7, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

____ U.S. Patent Application No. 09/594,719, filed June 16, 2000, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems";

____ U.S. Patent Application No. 11/519,467, filed September 12, 2006, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems";

____ U.S. Patent Application No 09/731,040, filed December 7, 2000, entitled "Systems, Methods And Devices For Trusted Transactions";

____ U.S. Patent Application No 11/512,701, filed August 29, 2006, entitled "Systems, Methods And Devices For Trusted Transactions";

____ U.S. Patent Application No. 10/049,101, filed February 8, 2002, entitled "A Secure Personal Content Server" (which claims priority to International Application No. PCT/US00/21189, filed August 4, 2000, which claims priority to U.S. Patent Application No. 60/147,134, filed August 4, 1999, and to U.S. Patent Application No. 60/213,489, filed June 23, 2000);

____ PCT Application No. PCT/US00/21189, filed August 4, 2000, entitled, "A Secure Personal Content Server";

____ U.S. Patent Application No. 09/657,181, filed September 7, 2000, entitled "Method And Device For Monitoring And Analyzing Signals";

____ U.S. Patent Application No. 10/805,484, filed March 22, 2004, entitled "Method And Device For Monitoring And Analyzing Signals"(which claims priority to U.S. Patent Application No. 09/671,739, filed September 29, 2000, which is a CIP of U.S. Patent Application No. 09/657,181);

____ U.S. Patent Application No. 09/956,262, filed September 20, 2001, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects";

____ U.S. Patent Application No. 11/518,806, filed September 11, 2006, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects";

____ U.S. Patent Application No. 11/026,234, filed December 30, 2004, entitled "Z-Transform Implementation of Digital Watermarks";

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

____ U.S. Patent Application No. 11/592,079, filed November 2, 2006, entitled "Linear Predictive Coding Implementation of Digital Watermarks";

____ U.S. Patent Application No. 09/731,039, filed December 7, 2000, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects";

____ U.S. Patent Application No. 11/647,861, filed December 29, 2006, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects";

____ U.S. Patent No. 5,428,606, issued June 27, 1995, entitled "Digital Commodities Exchange";

____ U.S. Patent No. 5,539,735, issued July 23, 1996, entitled "Digital Information Commodities Exchange";

____ U.S. Patent No. 5,613,004, issued March 18, 1997, entitled "Steganographic Method and Device";

____ U.S. Patent No. 5,687,236, issued November 11, 1997, entitled "Steganographic Method and Device";

____ U.S. Patent No. 5,745,569, issued April 28, 1998, entitled "Method for Stega-Protection of Computer Code";

____ U.S. Patent No. 5,822,432, issued October 13, 1998, entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System";

____ U.S. Patent No. 5,889,868, issued July 2, 1996, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

____ U.S. Patent No. 5,905,800, issued May 18, 1999, entitled "Method & System for Digital Watermarking";

____ U.S. Patent No. 6,078,664, issued June 20, 2000, entitled "Z-Transform Implementation of Digital Watermarks";

____ U.S. Patent No. 6,205,249, issued March 20, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

____ U.S. Patent No. 6,522,767, issued February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

____ U.S. Patent No. 6,598,162, issued July 22, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation";

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

____ U.S. Patent No. 6,853,726, issued February 8, 2005, entitled "Z-Transform Implementation of Digital Watermarks";

____ U.S. Patent No. 7,007,166, issued February 28, 2006, entitled "Method & System for Digital Watermarking";

____ U.S. Patent No. 7,035,049, issued April 25, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

____ U.S. Patent No. 7,095,874, issued August 22, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

____ U.S. Patent No. 7,107,451, issued September 12, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

____ U.S. Patent No. 7,123,718, issued October 17, 2006, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems";

____ U.S. Patent No. 7,127,615, issued October 24, 2006, "Improved Security Based on Subliminal and Supraliminal Channels for Data Objects";

____ U.S. Patent No. 7,152,162, issued December 19, 2006, entitled "Z-Transform Implementation of Digital Watermarks";

____ U.S. Patent No. 7,159,116, issued January 2, 2007, entitled "Systems, Methods and Devices for Trusted Transactions";

____ U.S. Patent No. 7,177,429, issued February 13, 2007, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects"

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. This Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed documents and information.

Respectfully submitted,

Date: April 17, 2007 By:

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

Scott A. Moskowitz
Tel# (305) 956-9041
Fax# (305) 956-9042

For Blue Spike, Inc.

Scott A. Moskowitz
President

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

APR 17 2007

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO	Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT	Application Number	10/049,101
	Filing Date	July 23, 2002
	First Named Inventor	Scott A. MOSKOWITZ et al.
	Art Unit	2131
(Use as many sheets as necessary)	Examiner Name	Jeremiah AVERY
Sheet 1 of 6	Attorney Docket Number	80408.0011

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Schneier, Bruce, Applied Cryptography, 2nd Ed., John Wiley & Sons, pp. 9-10, 1996	
		Menezes, Alfred J., Handbook of Applied Crypography, CRC Press, p. 46, 1997	
		Merriam-Webster's Collegiate Dictionary, 10th Ed., Merriam Webster, Inc., p.207	
		Brealy, et al., Principles of Corporate Finance, "Appendix A-Using Option Valuation Models", 1984, pp. 448-449	
		Copeland, et al., Real Options:A Practioner's Guide, 2001 pp. 106-107, 201-202, 204-208.	
		Sarkar, M. "An Assessment of Pricing Mechanisms for the Internet-A Regulatory Imperative", presented MIT Workshop on Internet Economics, Mar. 1995 http://www.press.vmich.edu/iep/works/SarkAsses.html on	
		Crawford, D.W. "Pricing Network Usage:A Market for Bandwith of Market Communication?" presented MIT Workshop on Internet Economics, Mar 1995 http://www.press.vmich.edu/iep/works/CrawMarket.html on March	
		LOW, S.H., "Equilibrium Allocation and Pricing of Variable Resources Among User-Suppliers", 1988. http://www.citesear.nj.nec.com/366503.html	
		Caronni, Germano, "Assuring Ownership Rights for Digital Images", published proceeds of reliable IT systems, v15 '95, H.H. Bruggemann and W. Gerhardt-Hackel (Ed.), Viewing Publishing Company, Germany, 1995	
		Zhao, Jian. "A WWW Service to Embed and Prove Digital Copyright Watermarks", Proc. of the european conf. on Mulitmedia Applications, Services & Techniques Louvain-La-Nevve, Belgium, May 1996	

Examiner Signature	/Jeremiah Avery/	Date Considered	06/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 6

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Gruhl,Daniel et al.,Echo Hiding. In Proceeding of the Workshop on Information Hiding. No. 1174 in Lecture Notes in Computer Science,Cambridge,England (May/June 1996)	
		Oomen,A.W.J. et al., A Variable Bit Rate Buried Data Channel for Compact Disc, J.Audio Eng.Sc.,Vol.43,No. 1/2,pp. 23-28 (1995).	
		Ten Kate,W. et al., A New Surround-Stereo-Surround Coding Techniques, J. Audio Eng.Soc.,Vol. 40,No. 5,pp. 376-383 (1992)	
		Gerzon, Michael et al., A High Rate Buried Data Channel for Audio CD, presentation notes, Audio Engineering Soc. 94th Convention (1993).	
		Sklar,Bernard, Digital Communications, pp. 601-603 (1988)	
		Jayant, N.S. et al., Digital Coding of Waveforms, Prentice Hall Inc., Englewood Cliffs,NJ, pp. 486-509 (1984)	
		Bender, Walter R. et al., Techniques for Data Hiding, SPIE Int. Soc. Opt. Eng., Vol. 2420, pp. 164-173, 1995	
		Zhao, Jian et al., Embedding Robust Labels into Images for Copyright Protection, (xp 000571976), pp. 242-251, 1995.	
		Menezes, Alfred J., Handbook of Applied Cryptography, CRC Press, p. 175, 1997	
		Schneier, Bruce, Applied Cryptography, 1st Ed., pp. 67-68, 1994.	

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

1 Applicant's unique citation designation number (optional). 2 Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

Sheet 3 of 6

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		ten Kate, W. et al., "Digital Audio Carrying Extra Information", IEEE, CH 2847-2/90/0000-1097, (1990)	
		van Schyndel, et al. A digital Watermark, IEEE Int'l Computer Processing Conference, Austin,TX, Nov 13-16, 1994, pp. 86-90	
		Smith, et al. Modulation and Information Hiding in Images, Springer Verlag, 1st Int'l Workshop, Cambridge, UK, May 30-June 1,1996, pp. 207-227	
		Kutter, Martin et al., Digital Signature of Color Images Using Amplitude Modulation, SPIE-E197, vol. 3022, pp. 518-527	
		Puate, Joan et al., Using Fractal Compression Scheme to Embed a Digital Signature into an Image, SPIE-96 Proceedings, vol. 2915, Mar. 1997, pp 108-118	
		Swanson, Mitchell D.,et al., Transparent Robust Image Watermarking, Proc. of the 1996 IEEE Int'l Conf. on Image Processing, Vol. 111, 1996 , pp. 211-214	
		Swanson, Mitchell D., et al. Robust Data Hiding for Images, 7th IEEE Digital Signal Processing Workshop, Leon, Norway. Sept. 1-4,1996, pp. 37-40	
		Zhao, Jian et al., Embedding Robust Labels into Images for Copyright Protection, Proceeding of the Know Right '95 Conference, pp. 242-251	
		Koch, E., et al., Towards Robust and Hidden Image Copyright Labeling, 1995 IEEE Workshop on Nonlinear Signal and Image Processing, Jun. 1995, Neos Marmaras, pp. 4	
		Van Schyandel, et al., Towards a Robust Digital Watermark, Second Asain Image Processing Conference, Dec. 6-8,1995,Singapore, Vol. 2,pp. 504-508	

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

Sheet 4 of 6

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Tirkel,A.Z., A Two-Dimensional Digital Watermark, DICTA '95, Univ. of Queensland, Brisbane, Dec. 5-8,1995, pp. 7	
		Tirkel,A.Z., Image Watermarking-A Spread Spectrum Application, ISSSTA '96, Sept.96, Mainz, German, pp. 6	
		O'Ruanaidh, et al. Watermarking Digital Images for Copyright Protection, IEEE Proceedings, Vol. 143, No. 4, Aug. 96, pp. 250-256	
		Cox, et al., Secure Spread Spectrum Watermarking for Multimedia, NEC Research Institude, Techinal Report 95-10, pp. 33	
		Kahn, D., The Code Breakers, The MacMillan Company, 1969, pp. xIII, 81-83,513,515,522-526,863	
		Boney, et al., Digital Watermarks for Audio Signals, EVSIPCO, 96, pp. 473-480	
		Dept. of Electrical Engineering, Del Ft University of Technology, Del ft The Netherlands,Cr.C. Langelaar et al.,Copy Protection for Mulitmedia Data based on Labeling Techniques, July 1996 9 pp.	
		F. Hartung, et al., Digital Watermarking of Raw and Compressed Video, SPIE Vol. 2952, pp. 205-213.	
		Craver, et al., Can Invisible Watermarks Resolve Rightful Ownerships? IBM Research Report, RC 20509 (July 25,1996) 21 pp.	
		Press, et al., Numerical Recipes in C, Cambridge Univ. Press, 1988, pp. 398-417	

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

Sheet 5 of 6

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Pohlmann, Ken C., Principles of Digital Audio, 3rd Ed., 1995, pp. 32-37, 40-48,138,147-149,332,333,364, 499-501,508-509,564-571.	
		Pohlmann, Ken C., Principles of Digital Audio, 2nd Ed., 1991, pp. 1-9,19-25,30-33,41-48,54-57,86-107,375-387.	
		Schneier, Bruce, Applied Cryptography, John Wiley & Sons, inc., New York,1994, pp. 68,69,387-392,1-57,273-275,321-324.	
		Boney, et al., Digital Watermarks for Audio Signals, Proceedings of the International Conf. on Multimedia Computing and Systems, June 17-23,1996 Hiroshima, Japan, 0-8186-7436-9196, pp. 473-480.	
		Johnson, et al., Transform Permuted Watermarking for Copyright Protection of Digital Video, IEEE Globecom 1998, Nov 8-12,1998, New York, New York, Vol. 2 1998, pp. 684-689 (ISBN 0-7803-4985-7).	
		Rivest, et al., "Pay Word and Micromint: Two Simple Micropayment Schemes, "MIT Laboratory for Computer Science, Cambridge, MA, May 7,1996, pp. 1-18.	
		Bender, et al., Techniques for Data Hiding, IBM Systems Journal, Vol. 35, Nos 3 & 4,1996,pp. 313-336.	
		Moskowitz, Bandwith as Currency, IEEE Multimedia, Jan-Mar 2003, pp. 14-21.	
		Moskowitz, Multimedia Security Technologies for Digital Rights Management, 2006, Academic Press, "Introduction-Digital Rights Management" pp. 3-22.	
		Rivest, et al., "PayWord and Micromint: Two Simple Micropayment Schemes" MIT Laboratory for Computer Science, Cambridge, MA, April 27, 2001, pp 1-18.	

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/08B (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

Substitute for form 1449/PTO		Complete if Known	
INFORMATION DISCLOSURE STATEMENT BY APPLICANT		Application Number	10/049,101
(Use as many sheets as necessary)		Filing Date	July 23, 2002
		First Named Inventor	Scott A. MOSKOWITZ et al.
		Art Unit	2131
		Examiner Name	Jeremiah AVERY
Sheet 6	of 6	Attorney Docket Number	80408.0011

NON PATENT LITERATURE DOCUMENTS

Examiner Initials*	Cite No.[1]	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T[2]
		Tomsich, et al., "Towards a secure and de-centralized digital watermarking infrastructure for the protection of Intellectual Property", in Electronic Commerce and Web Technologies, Proceedings (ECWEB	
		Moskowitz, "What is Acceptable Quality in the Application of Digital Watermarking: Trade-offs of Security, Robustness and Quality", IEEE Computer Society Proceedings of ITCC 2002 April 10, 2002, pp. 80-84	
		Lemma, et al. "Secure Watermark Embedding through Partial Encryption", International Workshop on Digital Watermarking ("IWDW" 2006). Springer Lecture Notes in Computer Science 2006, (to appear) 13	
		Kocher, et al., "Self Protecting Digital Content", Technical Report from the CRI Content Security Research Initiative, Crytography Research, Inc. 2002-2003, 14 pages	
		Sirbu, M. et al., "Net Bill: An Internet Commerce System Optimized for Network Delivered Services", Digest of Papers of the Computer Society Computer Conference (Spring), 5 March 1995, pp. 20-25, vol. CONF40	
		Schunter, M. et al., "A Status Report on the SEMPER framework for Secure Electronic Commerce", Computer Networks and ISDN Systems, 30 Sept 1998, pp. 1501-1510, Vol. 30, No. 16-18, NL, North Holland	
		Konrad, K. et al., "Trust and Elecronic Commerce-more than a techinal problem," Proceedings of the 18th IEEE Symposium on Reliable Distributed Systems, 19-22 October 1999, pp. 360-365, Lausanne	
		Kini, a. et al., "Trust in Electronic Commerce: Definition and Theoretical Considerations", Proceedings of the 31st Hawaii Int'l Conf on System Sciences (Cat. No. 98TB100216). 6-9 January 1998, pp. 51-61. Los	
		Steinauer D. D., et al., "Trust and Traceability in Electronic Commerce", Standard View, Sept 1997, pp 118-124, vol. 5 No. 3, ACM, USA	
		Hartung, et al. "Multimedia Watermarking Techniques", Proceedings of the IEEE, Special Issue, Identification & Protection of Multimedia Information, pp 1079-1107, July 1999, Vol. 87 No. 7, IEEE	

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

[1] Applicant's unique citation designation number (optional). [2] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: **Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

APR 17 2007

PTO/SB/08A (08-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 1 of 12

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number — Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,939,515	07/03/1990	Adeson	
		US-5,161,210	11/03/1992	Druyvesteyn et.al	
		US-5,450,490	09/12/1995	Jensen et.al.	
		US-5,530,751	06/25/1996	Morris	
		US-5,579,124	11/26/1996	Aijala et al	
		US-5,721,788	02/24/1998	Powell et.al.	
		US-5,828,325	10/27/1998	Wolose Wicz et.al.	
		US-5,912,972	06/15/1999	Barton	
		US-5,930,377	07/27/1999	Powell et al.	
		US-5,583,488	12/10/1996	Sala et.al.	
		US-5,748,783	05/05/1998	Rhoads	
		US-6,330,672	12/11/2001	Shur	
		US-5,243,423	09/07/1993	DeJean et al.	
		US-5,319,735	06/07/1994	Preuss et al.	
		US-5,113,437	05/12/1992	Best et.al.	
		US-4,876,617	10/24/1989	Best et.al.	
		US-5,379,345	01/03/1995	Greenberg	
		US-5,646,997	07/08/1997	Barton	
		US-4,672,605	06/09/1987	Hustig et.al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document — Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		European Patent No. EP0565947A1	10/20/1993	Kuusama, Juha		
		WO 95/14289	05/26/1995	Rhoads, Geoffrey		
		European Patent No. 0581317A2	02/02/1994	Powell, Robert et.al.		
		European Patent No. 0372601A1	06/13/1990	Druyvesteyn, Wm. et al.		
		WO98/37513	08/27/1998	Biggar, Michael et.al.		
		European Patent No. 0651554A	05/03/1995	Eastman Kodak Co.		

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 2 of 12

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,748,668	05/31/1998	Shamir, et.al.	
		US-4,789,928	12/06/1988	Fujisaki	
		US-4,908,873	03/13/1990	Philibert, et.al.	
		US-4,980,782	12/25/1990	Ginkel	
		US-5,073,925	12/17/1991	Nagata, et al.	
		US-5,243,515	09/07/1993	Lee	
		US-5,287,407	02/15/1994	Holmes	
		US-5,428,606	06/27/1995	Moskowitz	
		US-5,365,586	11/15/1994	Indeck, et.al.	
		US-5,394,324	02/28/1995	Clearwater	
		US-5,408,505	04/18/1995	Indeck, et.al.	
		US-5,412,718	05/02/1995	Narasimhalu, et al.	
		US-5,487,168	01/23/1996	Geiner, et al.	
		US-5,493,677	02/20/1996	Balogh, et al.	
		US-5,530,759	06/25/1996	Braudaway, et al.	
		US-5,606,609	02/25/1997	Houser, et.al.	
		US-5,613,004	03/18/1997	Cooperman, et al.	
		US-5,617,119	04/01/1997	Briggs, et.al.	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		WO 99/62044	12/02/1999	Handel, Theodore et.al.		
		WIPO 96/29795	09/26/1996	Micali		
		WIPO 97/24833	07/10/1997	Micali		
		EP 0649261	04/19/1995	Eran		
		NL 100523	09/1998			

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/08A (08-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office, U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 3 of 12

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-4,528,588	07/09/1985	Lofberg	
		US-5,832,119	11/03/1998	Rhoads	
		US-5,859,920	01/12/1999	Daly et al	
		US-4,979,210	12/18/1990	Nagata et al	
		US-5,774,452	06/30/1998	Wolosewicz	
		US-4,405,829	09/20/1983	Rivest et al	
		US-6,330,335	12/11/2001	Rhoads	
		US-3,986,624	10/19/1976	Cates Jr. et al	
		US-5,363,448	11/08/1994	Koopman et al	
		US-5,568,570	10/22/1996	Rabbani	
		US-5,636,292	06/03/1997	Rhoads	
		US-4,972,471	11/20/1990	Gross et al	
		US-5,893,067	04/06/1999	Bender et al.	
		US-5,689,587	11/18/1997	Bender et al.	
		US-3,984,624	10/05/1976	Waggener	
		US-4,038,596	07/26/1977	Lee	
		US-4,200,770	04/29/1980	Hellman, et al	
		US-4,218,582	08/19/1980	Hellman, et al	
		US-4,424,414	01/03/1984	Hellman, et al	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]
		WO 9744736	11/27/1997	Wehrenberg		
		WO 9952271	10/14/1999	Moskowitz		
		WO 9963443	12/09/1999	Ho, Anthony Tung Shuen		

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 4 of 17

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number — Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,640,569	06/17/1997	Miller, et al.	
		US-5,659,726	08/19/1997	Sandford,II, et al	
		US-5,664,018	09/02/1997	Leighton	
		US-5,687,236	11/11/1997	Moskowitz, et al.	
		US-5,734,752	03/31/1998	Knox	
		US-5,745,569	04/28/1998	Moskowitz, et al	
		US-5,506,795	04/09/1996	Yamakawa	
		US-5,680,462	10/21/1997	Miller, et.al.	
		US-5,696,828	12/09/1997	Koopman, Jr.	
		US-5,740,244	04/14/1998	Indeck, et.al.	
		US-5,751,811	05/12/1998	Koopman, Jr.	
		US-5,757,923	05/26/1998	Koopman, Jr.	
		US-5,889,868	03/30/1999	Moskowitz, et al	
		US-6,208,745	03/27/2001	Florenio, et al	
		US-6,285,775	09/04/2001	Wu, et al	
		US-6,385,329	05/07/2002	Sharma, et al	
		US-6,530,021	03/04/2003	Epstein, et al	
		US-6,425,081	07/23/2002	Iwamura	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document — Country Code[3] "Number[4] "Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1]Applicant's unique citation designation number (optional). [2]See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3]Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4]For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5]Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6]Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 5 of 12

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,522,769	02/18/2003	Rhoads, et al.	
		US-2005/0160271	07/21/2005	Brundage, et al.	
		US-6,665,489	12/16/2003	Collart	
		US-2004/0128514	07/01/2004	Rhoads	
		US-2004/0037449	02/26/2004	Davis, et al.	
		US-6,823,455	11/23/2004	Macy, et al.	
		US-2003/0133702	07/17/2003	Collart	
		US-6,668,246	12/23/2003	Young, et al.	
		US-6,405,203	06/11/2002	Collart	
		US-6,141,754	10/31/2000	Choy	
		US-6,493,457	12/10/2002	Quackenbush	
		US-5,629,980	05/13/1997	Stefik, et al.	
		US-5,943,422	08/24/1999	Van Wie, et al.	
		US-5,636,276	06/03/1997	Brugger	
		US-5,341,429	08/23/1994	Stringer, et al.	
		US-6,754,822	06/22/2004	Zhao	
		US-6,131,162	10/10/2000	Yoshiura et al.	
		US-7,058,570	06/06/2006	Yu, et al.	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3]-Number[4]-Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/08A (08-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 6 of 12

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2 (if known)]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,930,369	07/27/1999	Cox, et al.	
		US-6,415,041	07/02/2002	Oami, et al.	
		US-6,141,753	10/31/2000	Zhao, et.al.	
		US-2002/0097873	07/25/2002	Petrovic	
		US-6,785,815	08/31/2004	Serret-Avila, et al.	
		US-6,523,113	02/18/2003	Wehrenberg	
		US-6,233,347	05/15/2001	Chen, et.al.	
		US-6,233,684	05/15/2001	Stefik, et al.	
		US-2006/0013395	01/19/2006	Brundage, et al.	
		US-7,043,050	05/09/2006	Yuval	
		US-5,809,160	09/15/1998	Powell, et al.	
		US-6,272,634	08/07/2001	Tewfik, et al.	
		US-6,282,650	08/28/2001	Davis	
		US-6,557,103	04/29/2003	Boncelet, Jr., et al.	
		US-2003/0126445	07/03/2003	Wehrenberg	
		US-6,978,370	12/20/2005	Kocher	
		US-2006/0005029	01/05/2006	Petrovic, et al.	
		US-6,278,791	08/21/2001	Honsinger, et al.	
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/08A (03-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 7 of 12

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number (Number-Kind Code[2] (if known))	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,061,793	05/09/2000	Tewfik, et al	
		US-5,809,139	09/15/1998	Girod, et al.	
		US-5,848,155	12/08/1998	Cox	
		US-5,915,027	06/22/1999	Cox, et al	
		US-5,940,134	08/17/1999	Wirtz	
		US-5,991,426	11/23/1999	Cox, et al.	
		US-6,069,914	05/30/2000	Cox	
		US-5,943,422	08/24/1999	Van Wie, et al.	
		US-6,539,475	03/25/2003	Cox, et al.	
		US-6,310,962	10/30/2001	Chung, et al.	
		US-6,154,571	11/28/2000	Cox, et al.	
		US-4,969,204	11/06/1990	Jones, et al.	
		US-6,687,683	02/03/2004	Harada, et al.	
		US-6,373,892	04/16/2002	Ichien, et al.	
		US-5,870,474	02/09/1999	Wasilewski, et al.	
		US-5,418,713	05/23/1995	Allen	
		US-6,078,664	06/20/2000	Moskowitz, et al.	
		US-6,009,176	12/28/1999	Gennaro, et al.	
		US-6,081,587	06/27/2000	Hoffstein, et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document (Country Code[3] Number[4] Kind Code[5] (if known))	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 8 of 12

Complete If Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number (Number-Kind Code[2] (if known))	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,598,162	07/22/2003	Moskowitz	
		US-6,275,988	08/14/2001	Nagashima, et al.	
		US-6,051,029	04/18/2000	Paterson, et al.	
		US-5,917,915	06/29/1999	Hirose	
		US-6,775,772	08/10/2004	Binding, et al.	
		US-6,668,246	12/23/2003	Yeung, et al.	
		US-6,351,765	02/26/2002	Pietropaolo, et al.	
		US-6,049,838	04/11/2000	Miller, et al.	
		US-5,398,285	03/14/1995	Borgelt, et al.	
		US-5,737,733	04/07/1998	Eller	
		US-2002/0103883	08/01/2002	Haverstock, et al.	
		US-5,673,316	09/30/1997	Auerbach, et al.	
		US-6,647,424	11/11/2003	Pearson, et al.	
		US-6,977,894	12/20/2005	Achilles, et al.	
		US-6,453,252	09/17/2002	Laroche	
		US-5,077,665	12/31/1991	Silverman, et al.	
		US-5,136,581	08/04/1992	Muehrcke	
		US-5,341,477	08/23/1994	Pitkin, et al.	
		US-5,581,703	12/03/1996	Baugher, et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document (Country Code[3] Number[4] Kind Code[5] (if known))	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 7 of 12

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number: Number-Kind Code[2 (if known)]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,548,579	08/20/1996	Lebrun, et al.	
		US-5,905,975	05/18/1999	Ausubel	
		US-6,457,058	09/24/2002	Ullum et al	
		US-6,381,618	04/30/2002	Jones et al	
		US-2002/0026343	02/28/2002	Duenke	
		US-6,230,268	05/08/2001	Miwa et al	
		US-6,199,058	03/06/2001	Wong et al.	
		US-5,920,900	07/06/1999	Poole et al	
		US-5,884,033	03/16/1999	Duvall et al.	
		US-5,478,990	12/26/1995	Montanari et al.	
		US-6,430,302	08/06/2002	Rhoads	
		US-6,725,372	04/20/2004	Lewis et al	
		US-6,606,393	08/12/2003	Xie et al	
		US-6,584,125	06/24/2003	Katto	
		US-6,442,283	08/27/2002	Tewfik et al	
		US-6,377,625	04/23/2002	Kim	
		US-6,282,300	08/28/2001	Bloom et al.	
		US-6,205,249	03/20/2001	Moskowitz	
		US-6,029,126	02/22/2000	Malvar	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document: Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/08A (09-06)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 10 of 12

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2 (if known)]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,754,697	05/19/1998	Fu et al.	
		US-5,479,210	12/26/1995	Cawley et al.	
		US-3,947,825	03/30/1976	Cassada	
		US-5,903,721	05/11/1999	Sixtus	
		US-5,790,677	08/04/1998	Fox et al.	
		US-5,243,515	09/07/1993	Clearwater	
		US-4,339,134	07/13/1982	Macheel	
		US-4,827,508	05/02/1989	Shear	
		US-4,896,275	01/23/1990	Jackson	
		US-4,977,594	12/11/1990	Shear	
		US-5,050,213	09/17/1991	Shear	
		US-5,369,707	11/29/1994	Follendore, III	
		US-5,406,627	04/11/1995	Thompson et al	
		US-5,410,598	04/25/1995	Shear	
		US-5,469,536	11/21/1995	Blank	
		US-5,497,419	03/05/1996	Hill	
		US-5,513,261	04/30/1996	Maher	
		US-5,530,739	06/25/1996	Okada	
		US-5,598,470	01/28/1997	Cooper et al.	

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature		Date Considered	

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/08A (08-03)
Approved for use through 03/31/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet | 11 | of | 12

Complete if Known

Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2 (if known)]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-5,625,690	04/29/1997	Michel et al.	
		US-5,633,932	05/27/1997	Davis et al.	
		US-5,719,937	02/17/1998	Warren et al.	
		US-5,737,416	04/07/1998	Cooper et al.	
		US-5,765,152	06/09/1998	Erickson	
		US-5,799,083	08/25/1998	Brothers et al.	
		US-5,973,731	10/26/1999	Schwab	
		US-5,894,521	04/13/1999	Conley	
		US-5,905,800	05/18/1999	Moskowitz et al.	
		US-5,963,909	10/05/1999	Warren et al.	
		US-5,974,141	10/26/1999	Saito	
		US-5,999,217	12/07/1999	Berners-Lee	
		US-6,041,316	03/21/2000	Allen	
		US-6,081,251	06/27/2000	Baker et al.	
		US-6,278,780	08/21/2001	Shimada	
		US-6,301,663	10/09/2001	Kato et al.	
		US-6,240,121	05/29/2001	Senoh	
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

PTO/SB/08A (09-06)
Approved for use through 09/21/2007. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449/PTO

INFORMATION DISCLOSURE STATEMENT BY APPLICANT

(Use as many sheets as necessary)

Sheet 12 of 12

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ et al.
Art Unit	2131
Examiner Name	Jeremiah AVERY
Attorney Docket Number	80408.0011

U. S. PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Document Number Number-Kind Code[2 (if known)]	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear
		US-6,088,455	07/11/2000	Logan et al.	
		US-5,634,040	05/27/1997	Her et al.	
		US-6,381,747	04/30/2002	Wonfor et al.	
		US-4,969,204	11/06/1990	Melnychuck et al.	
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			
		US-			

FOREIGN PATENT DOCUMENTS

Examiner Initials*	Cite No.[1]	Foreign Patent Document Country Code[3] Number[4] Kind Code[5] (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages Or Relevant Figures Appear	T[6]

Examiner Signature	/Jeremiah Avery/	Date Considered	08/27/2008

*EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant. [1] Applicant's unique citation designation number (optional). [2] See Kinds Codes of USPTO Patent Documents at www.uspto.gov or MPEP 901.04. [3] Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). [4] For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. [5] Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST.16 if possible. [6] Applicant is to place a check mark here if English language Translation is attached.

This collection of information is required by 37 CFR 1.97 and 1.98. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 2 hours to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

If you need assistance in completing the form, call 1-800-PTO-9199 (1-800-786-9199) and select option 2.

ALL REFERENCES CONSIDERED EXCEPT WHERE LINED THROUGH. /J.A./

FEB 2 9 2008

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Appl. No.	:	10/049,101	Confirmation No. 8028
Applicant	:	Scott MOSKOWITZ	
Filed	:	July 23, 2002	
TC/A.U.	:	2131	
Examiner	:	Jeremiah L. AVERY	
Docket No.	:	80408.0011	

MAIL STOP: AMENDMENT - IDS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

03/04/2008 TNGUYEN2 00000012 10049101
01 FC:1806 180.00 OP

INFORMATION DISCLOSURE STATEMENT

Dear Sir:

Applicant(s) submit copies of the references listed on the attached SB08 Form(s) for consideration and request that the U.S. Patent and Trademark Office make them of record in this application.

Applicant(s) state the following:

☐ Each item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application not more than three months prior to the filing of the Information Disclosure Statement; or

☐ No item of information contained in this Information Disclosure Statement was cited in a communication from a foreign patent office in a counterpart foreign application, and to the knowledge of Applicant(s) no item of information contained in this

Information Disclosure Statement was known to any individual designated in § 1.56(c) more than three months prior to the filing of this Information Disclosure Statement.

☐ In accordance with 37 C.F.R. § 1.97(b), this Information Disclosure Statement is believed to be submitted prior to issuance of a first Office Action and/or within three months of the filing date of the application. It is respectfully submitted that no fee is required for consideration of this information.

☒ This Information Disclosure Statement is being submitted after the mailing of a non-final Office Action, but is believed to be prior to a final Office Action or a Notice of Allowance. Pursuant to 37 C.F.R. § 1.97(c), payment in the amount of $180.00 as set forth in 37 C.F.R. § 1.17(p) is enclosed.

While the information and references disclosed in this Information Disclosure Statement are submitted pursuant to 37 C.F.R. § 1.56, this submission is not intended to constitute an admission that any patent, publication or other information referred to is "prior art" to this invention. Applicant(s) reserve the right to contest the "prior art" status of any information submitted or asserted against the application.

Additionally, pursuant to C.F.R. § 1.78, Applicant(s) wish to inform the Examiner of the existence of the following co-pending U.S. patents and patent applications that share a common inventor with the present application. Under 37 C.F.R. § 1.98(a)(1), Applicant(s) also wish to inform the Examiner of the existence of the following co-pending foreign patents and patent applications that share a common inventor with the present application in the "section separate from the citations of other documents" entitled "Foreign Patent Documents", below:

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

U.S. PATENT DOCUMENTS

EXAMINER'S
INITIALS

_____ U.S. Patent Application No. 08/999,766, filed July 23, 1997, entitled "Steganographic Method and Device";

_____ U.S. Patent Application No. 11/894,443, filed August 21, 2007, entitled "Steganographic Method and Device" – Projected Publication Date – March 27, 2008;

_____ U.S. Patent Application No. 11/894,476, filed August 21, 2007, entitled "Steganographic Method and Device" – Publication No. 20070294536 – December 20, 2007;

_____ U.S. Patent Application No. 11/050,779, filed February 7, 2005, entitled "Steganographic Method and Device" – Publication No. 20050177727 – August 11, 2005;

_____ U.S. Patent Application No. 08/674,726, filed July 2, 1996, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management" (unpublished – issue fee paid – January 23, 2008);

_____ U.S. Patent Application No. 12/009,914, filed January 23, 2008, entitled "Exchange Mechanisms for Digital Information Packages with Bandwidth Securitization, Multichannel Digital Watermarks, and Key Management";

_____ U.S. Patent Application No. 09/545,589, filed April 7, 2000, entitled "Method and System for Digital Watermarking" (issued as U.S. Patent No 7,007,166);

_____ U.S. Patent Application No. 11/244,213, filed October 5, 2005, entitled "Method and System for Digital Watermarking" – Publication No 20060101269 – May 11, 2006 (issue fee paid – December 26, 2007);

_____ U.S. Patent Application No. 11/649,026, filed January 3, 2007, entitled "Method and System for Digital Watermarking" – Publication No 20070113094 – May 17, 2007;

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

All References Are Considered, Except Where Lined Through. /J.A./

_____ U.S. Patent Application No. 12/005,230, filed December 26, 2007, entitled "Method and System for Digital Watermarking";

_____ U.S. Patent Application No. 09/046,627, filed March 24, 1998, entitled "Method for Combining Transfer Function with Predetermined Key Creation" (issued as U.S. Patent No. 6,598,162);

_____ U.S. Patent Application 10/602,777, filed June 25, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation" – Publication No. 20040086119 – May 6, 2004;

_____ U.S. Patent Application 11/895,388, filed August 24, 2007, entitled "Data Protection Method and Device" – Publication No. 20080016365 – January 17, 2008;

_____ U.S. Patent Application No. 09/053,628, filed April 2, 1998, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" (issued as U.S. Patent No. 6,205,249);

_____ U.S. Patent Application No. 09/644,098, filed August 23, 2000, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" (issued as U.S. Patent No. 7,035,409);

_____ U.S. Patent Application No. 09/767,733, filed January 24, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" – Publication No. 20010010078 - July 26, 2001;

_____ U.S. Patent Application No. 11/358,874, filed February 21, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking" – Publication No. 20060140403 – June 29, 2006;

_____ U.S. Patent Application No. 10/417,231, filed April 17, 2003, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth" – Publication No. 20030200439 – October 23, 2003 (issued as U.S. Patent No. 7,287,275);

_____ U.S. Patent Application No. 11/900,065, filed September 10, 2007, entitled "Methods, Systems And Devices For Packet Watermarking And

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

All References Are Considered, Except Where Lined Through. /J.A./

Efficient Provisioning Of Bandwidth" – Publication No. 20080005571 – January 3, 2008;

_____ U.S. Patent Application No. 11/900,066, filed September 10, 2007, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth" – Publication No. 20080005572 – January 3, 2008;

_____ U.S. Patent Application No. 09/789,711, filed February 22, 2001, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20010010078 – October 11, 2001 (issued as U.S. Patent No. 7,107,451);

_____ U.S. Patent Application No. 11/497,822, filed August 2, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070011458 – January 11, 2007;

_____ U.S. Patent Application No. 11/599,964, filed November 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20080046742 – February 21, 2008;

_____ U.S. Patent Application No. 11/599,838, filed November 15, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070226506 – September 27, 2007;

_____ U.S. Patent Application No. 11/897,790, filed August 31, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070300072 – December 27, 2007;

_____ U.S. Patent Application No. 11/897,791, filed August 31, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20080022113 – January 24, 2008;

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

All References Are Considered, Except Where Lined Through. /J.A./

_____ U.S. Patent Application No. 11/899,661, filed September 7, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20070300073 – December 27, 2007;

_____ U.S. Patent Application No. 11/899,662, filed September 7, 2007, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data" – Publication No. 20080022114 – January 24, 2008;

_____ U.S. Patent Application No. 10/369,344, filed February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data" – Publication No. 20030219143 – November 27, 2003 (issued as U.S. Patent No. 7,095,874);

_____ U.S. Patent Application No. 11/482,654, filed July 7, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data" – Publication No. 20060285722 – December 21, 2006;

_____ U.S. Patent Application No. 09/594,719, filed June 16, 2000, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems" (issued as U.S. Patent 7,123,718);

_____ U.S. Patent Application No. 11/519,467, filed September 12, 2006, entitled "Utilizing Data Reduction in Steganographic and Cryptographic Systems" – Publication No. 20070064940 – March 22, 2007;

_____ U.S. Patent Application No 09/731,040, filed December 7, 2000, entitled "Systems, Methods And Devices For Trusted Transactions" – Publication No. 20020010684 – January 24, 2002 (issued as U.S. Patent 7,159,116);

_____ U.S. Patent Application No 11/512,701, filed August 29, 2006, entitled "Systems, Methods And Devices For Trusted Transactions" – Publication No. 20070028113 – February 1, 2007;

_____ U.S. Patent Application No. 10/049,101, filed February 8, 2002, entitled "A Secure Personal Content Server" (which claims priority to International

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

All References Are Considered, Except Where Lined Through. /J.A./

Application No. PCT/US00/21189, filed August 4, 2000, which claims priority to U.S. Patent Application No. 60/147,134, filed August 4, 1999, and to U.S. Patent Application No. 60/213,489, filed June 23, 2000);

_____ U.S. Patent Application No. 09/657,181, filed September 7, 2000, entitled "Method And Device For Monitoring And Analyzing Signals" (paid issue fee January 23, 2008);

_____ U.S. Patent Application No. 12/005,229, filed December 26, 2007, entitled "Method And Device For Monitoring And Analyzing Signals" – Publication No. NA –;

_____ U.S. Patent Application No. 10/805,484, filed March 22, 2004, entitled "Method And Device For Monitoring And Analyzing Signals"(which claims priority to U.S. Patent Application No. 09/671,739, filed September 29, 2000, which is a CIP of U.S. Patent Application No. 09/657,181) – Publication No. 20040243540 – December 2, 2004 – abandoned;

_____ U.S. Patent Application No. 09/956,262, filed September 20, 2001, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects" – Publication No. 20020056041 – May 9, 2002 (issued as U.S. Patent No. 7,127,615);

_____ U.S. Patent Application No. 11/518,806, filed September 11, 2006, entitled "Improved Security Based on Subliminal and Supraliminal Channels For Data Objects" – Publication No. 20080028222 – January 31, 2008;

_____ U.S. Patent Application No. 11/026,234, filed December 30, 2004, entitled "Z-Transform Implementation of Digital Watermarks" – Publication No. 20050135615 – June 23, 2005 (issued as U.S. Patent No. 7,152,162);

_____ U.S. Patent Application No. 11/592,079, filed November 2, 2006, entitled "Linear Predictive Coding Implementation of Digital Watermarks" – Publication No. 20070079131 – April 5, 2007;

_____ U.S. Patent Application No. 09/731,039, filed December 7, 2000, entitled "System and Methods for Permitting Open Access to Data Objects and

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

All References Are Considered, Except Where Lined Through. /J.A./

for Securing Data within the Data Objects" – Publication No. 20020071556 – June 13, 2002 (issued as U.S. Patent No. 7,177,429);

_____ U.S. Patent Application No. 11/647,861, filed December 29, 2006, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects" – Publication No. 20070110240 – April 5, 2007;

_____ U.S. Patent No. 5,428,606, issued June 27, 1995, entitled "Digital Commodities Exchange";

_____ U.S. Patent No. 5,539,735, issued July 23, 1996, entitled "Digital Information Commodities Exchange";

_____ U.S. Patent No. 5,613,004, issued March 18, 1997, entitled "Steganographic Method and Device";

_____ U.S. Patent No. 5,687,236, issued November 11, 1997, entitled "Steganographic Method and Device";

_____ U.S. Patent No. 5,745,569, issued April 28, 1998, entitled "Method for Stega-Protection of Computer Code";

_____ U.S. Patent No. 5,822,432, issued October 13, 1998, entitled "Method for Human Assisted Random Key Generation and Application for Digital Watermark System";

_____ U.S. Patent No. 5,889,868, issued July 2, 1996, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 5,905,800, issued May 18, 1999, entitled "Method & System for Digital Watermarking";

_____ U.S. Patent No. 6,078,664, issued June 20, 2000, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 6,205,249, issued March 20, 2001, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

_____ U.S. Patent No. 6,522,767, issued February 18, 2003, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 6,598,162, issued July 22, 2003, entitled "Method for Combining Transfer Function with Predetermined Key Creation";

_____ U.S. Patent No. 6,853,726, issued February 8, 2005, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 7,007,166, issued February 28, 2006, entitled "Method & System for Digital Watermarking";

_____ U.S. Patent No. 7,035,049, issued April 25, 2006, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

_____ U.S. Patent No. 7,095,874, issued August 22, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digitized Data";

_____ U.S. Patent No. 7,107,451, issued September 12, 2006, entitled "Optimization Methods for the Insertion, Protection, and Detection of Digital Watermarks in Digital Data";

_____ U.S. Patent No. 7,123,718, issued October 17, 2006, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems";

_____ U.S. Patent No. 7,127,615, issued October 24, 2006, "Improved Security Based on Subliminal and Supraliminal Channels for Data Objects";

_____ U.S. Patent No. 7,152,162, issued December 19, 2006, entitled "Z-Transform Implementation of Digital Watermarks";

_____ U.S. Patent No. 7,159,116, issued January 2, 2007, entitled "Systems, Methods and Devices for Trusted Transactions";

_____ U.S. Patent No. 7,177,429, issued February 13, 2007, entitled "System and Methods for Permitting Open Access to Data Objects and for Securing Data within the Data Objects";

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

All References Are Considered, Except Where Lined Through. /J.A./

_____ U.S. Patent No. 7,287,275, issued October 23, 2007, entitled "Methods, Systems And Devices For Packet Watermarking And Efficient Provisioning Of Bandwidth"

All References Are Considered, Except Where Lined Through. /J.A./

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

FOREIGN PATENT DOCUMENTS

EXAMINER'S
INITIALS:

_____ PCT Application No. PCT/US95/08159, filed June 26, 1995, entitled, "Digital Information Commodities Exchange with Virtual Menuing";

_____ PCT Application No. PCT/US96/10257, filed June 7, 1996, entitled, "Steganographic Method and Device" – corresponding to – EPO Application No. 96919405.9, entitled "Steganographic Method and Device";

_____ PCT Application No. PCT/US97/00651, filed January 16, 1997, entitled, "Method for Stega-Cipher Protection of Computer Code" – corresponding to AU199718294A (not available);

_____ PCT Application No. PCT/US97/00652, filed January 17, 1997, entitled, "Method for an Encrypted Digital Watermark" – corresponding to AU199718295A (not available);

_____ PCT Application No. PCT/US97/11455, filed July 2, 1997, entitled, "Optimization Methods for the Insertion, Protection and Detection of Digital Watermarks in Digitized Data" – corresponding to AU199735881A (not available);

_____ PCT Application No. PCT/US99/07262, filed April 2, 1999, entitled, "Multiple Transform Utilization and Applications for Secure Digital Watermarking" – corresponding to – Japan App. No. 2000-542907, entitled "Multiple Transform Utilization and Application for Secure Digital Watermarking";

_____ PCT Application No. PCT/US00/06522, filed March 14, 2000, entitled, "Utilizing Data Reduction in Steganographic and Cryptographic Systems";

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

All References Are Considered, Except Where Lined Through. /J.A./

_____ PCT Application No. PCT/US00/18411, filed July 5, 2000, entitled, "Copy Protection of Digital Data Combining Steganographic and Cryptographic Techniques" – corresponding to AU200060709A5 (not available);

_____ PCT Application No. PCT/US00/21189, filed August 4, 2000, entitled, "A Secure Personal Content Server";

_____ PCT Application No. PCT/US00/33126, filed December 7, 2000, entitled, "Systems, Methods and Devices for Trusted Transactions" – corresponding to AU200120659A5 (not available);

_____ EPO Divisional Patent Application No. 07112420.0, entitled "Steganographic Method and Device" (corresponding to PCT Application No. PCT/US96/10257, filed June 7, 1996, entitled, "Steganographic Method and Device" – cited above – previously provided)

All References Are Considered, Except Where Lined Through. /J.A./

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

In accordance with 37 C.F.R. § 1.97(g), the filing of this Information Disclosure Statement shall not be construed to mean that a search has been made or that no other material information as defined in 37 C.F.R. § 1.56(a) exists. This Information Disclosure Statement is in compliance with 37 C.F.R. § 1.98 and the Examiner is respectfully requested to consider the listed documents and information.

Respectfully submitted,

Date: February 29, 2008

By:

Scott A. Moskowitz
Tel# (305) 956-9041
Fax# (305) 956-9042

For Blue Spike, Inc.

Scott A. Moskowitz
President

EXAMINER: Please initial if reference is considered, whether or not the citation is in conformance with MPEP § 609. Draw line through citation if not in conformance and not considered. Please include copy of this form with next communication to the applicant.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,101	07/23/2002	Scott A. Moskowitz	80408.0011	8028

7590 09/03/2008

Scott A. Moskowitz
#2505
16711 Collins Avenue
Miami, FL 33160

EXAMINER	
AVERY, JEREMIAH L	
ART UNIT	**PAPER NUMBER**
2131	
MAIL DATE	**DELIVERY MODE**
09/03/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

UNITED STATES DEPARTMENT OF COMMERCE
U.S. Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450

APPLICATION NO./ CONTROL NO.	FILING DATE	FIRST NAMED INVENTOR / PATENT IN REEXAMINATION	ATTORNEY DOCKET NO.
10049101	7/23/2002	MOSKOWITZ, SCOTT A.	80408.0011

Scott A. Moskowitz
#2505
16711 Collins Avenue
Miami, FL 33160

EXAMINER	
JEREMIAH AVERY	
ART UNIT	**PAPER**
2131	20080827

DATE MAILED:

Please find below and/or attached an Office communication concerning this application or proceeding.

Commissioner for Patents

The IDS received on 4/17/07 and the IDS Letter received on 2/29/08 have been considered.

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131

PTO-90C (Rev.04-03)

10 - 10 - 08

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

1550 07/02/2008

Scott A. Moskowitz
#2505
16711 Collins Avenue
Miami, FL 33160

OIPE OCT 0 9 2008 PATENT & TRADEMARK OFFICE

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

SCOTT MOSKOWITZ	(Depositor's name)
[signature]	(Signature)
OCTOBER 9, 2008	(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,101	07/23/2002	Scott A. Moskowitz	80408.0011	8022

TITLE OF INVENTION: SECURE PERSONAL CONTENT SERVER

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$720	$0	$0	$720	10/09/2008

EXAMINER	ART UNIT	CLASS-SUBCLASS
AVERY, JEREMIAH L	2131	713-169000

10/10/2008 MGEBREM2 00000056 10049101
01 FC:8001 9.00 OP
02 FC:1501 720.00 OP

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

☐ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

☐ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. Use of a Customer Number is required.

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively, 1 ______

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed. 2 ______ 3 ______

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE: BLUE SPIKE, INC.

(B) RESIDENCE: (CITY and STATE OR COUNTRY): SUNNY ISLES BEACH, FL, USA

Please check the appropriate assignee category or categories (will not be printed on the patent): ☐ Individual ☑ Corporation or other private group entity ☐ Government

4a. The following fee(s) are submitted:

☑ Issue Fee
☑ Publication Fee (No small entity discount permitted)
☑ Advance Order - # of Copies 3

4b. Payment of Fee(s): (Please first reapply any previously paid issue fee shown above)

☐ A check is enclosed.
☑ Payment by credit card. Form PTO-2038 is attached.
☐ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number ______ (enclose an extra copy of this form).

5. Change in Entity Status (from status indicated above)

☑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27. ☐ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature [signature] Date OCTOBER 9, 2008

Typed or printed name SCOTT MOSKOWITZ Registration No. ______

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,101	07/23/2002	Scott A. Moskowitz	80408.0011	8028

7590 07/09/2008

Scott A. Moskowitz
#2505
16711 Collins Avenue
Miami, FL 33160

OIPE IAP57 OCT 09 2008 PATENT & TRADEMARK OFFICE

EXAMINER	
AVERY, JEREMIAH L	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/09/2008

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 683 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 683 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

7590 07/09/2008

Scott A. Moskowitz
#2505
16711 Collins Avenue
Miami, FL 33160

OIPE
OCT 0 9 2008
PATENT & TRADEMARK OFFICE

EXAMINER	
AVERY, JEREMIAH L	
ART UNIT	PAPER NUMBER
2131	

DATE MAILED: 07/09/2008

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,101	07/23/2002	Scott A. Moskowitz	80408.0011	8028

TITLE OF INVENTION: SECURE PERSONAL CONTENT SERVER

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	YES	$720	$0	$0	$720	10/09/2008

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

Document Code: IMIS

Notice of Fee Due

Date: 10-10-08

Application Number: 10 049101

A fee is due for the attached document for the reason indicated below. Please check the application for the appropriate authorization to charge a deposit account. If an authorization is present, please charge the appropriate fee*. If an authorization is not present, notify the application of the fee deficiency.

***If the fee due is for any of the filing fees, check for authorization to charge the surcharge. If authorization is present, charge the surcharge for late payment of the filing fees as well.**

- ☐ Insufficient payment by check or money order.
- ☐ Insufficient funds in deposit account __________ at __________ (time).
- ☒ Insufficient payment by credit card.
- ☐ Declined credit card.
- ☐ No authorization to charge a deposit account.

Fee code(s) to be applied: 2501 $755; 9506 $720

Amount in holding fee code: 1506; 1622/2622; 1999

Total remaining due from applicant: $35

RAM Operator [signature]

Rev. 12/27/07

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,101	07/23/2002	Scott A. Moskowitz	80408.0011	8028

7590 10/31/2008

Scott A. Moskowitz
#2505
16711 Collins Avenue
Miami, FL 33160

EXAMINER	
AVERY, JEREMIAH L	

ART UNIT	PAPER NUMBER
2131	

MAIL DATE	DELIVERY MODE
10/31/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Scott A. Moskowitz
#2505
16711 Collins Avenue

Mail Date: 10/31/08

Application Number: 10/049101

NOTICE TO PAY BALANCE OF ISSUE FEE

The issue fee payment filed on 10/09/08 has been received. Although the fee paid in the Notice of Allowance was paid, new patent fees went into effect on October 2, 2008 after the mailing date of the Notice. In accordance with Sections 801 and 803 of the Consolidated Appropriations Act, 2005 (H.R. 4818) "the provisions of this title shall take effect on the date of enactment of this Act. . . the provisions of section 801 shall apply to all patents, whenever granted, and to all patent applications pending on or filed after the effective date." See also, Revision of Patent Fees for Fiscal Year 2009-Final Rule, 73 Fed. Reg. 47534 (Aug. 14, 2008) and Consolidated Security, Disaster Assistance and Continuing Appropriations Act, 2009 (H.R. 2638). Because the issue fee was paid on or after October 2, 2008, the new issue fee was due instead of the amount specified in the Notice of Allowance.[1]

In accordance with 37 CFR 1.18, applicant is given a time period of **THREE (3) MONTHS** from the mailing date of this notice during which to pay the **BALANCE DUE** indicated below. The balance due is the difference between the issue fee required on the date that the correct issue fee is paid and the amount that was previously paid. This three-month time period may not be extended. If the balance due is not paid before the expiration of the three-month period, the application will become abandoned (if not issued) or the patent will lapse (if issued) at the termination of the three-month period.

App. Type	Column A Issue Fee Req. large entity / small entity	Column B Issue Fee PAID	Balance Due Col. A minus Col. B
UTILITY or REISSUE	$1,510.00/ $755.00	$ 720.00	$ 35.00
DESIGN	$860.00 / $430.00	$	$
PLANT	$1,190.00 / $595.00	$	$

/ Betty Powell /
Office of Data Management
Office: 703-308-9250x160
Fax: 571-270-9937

A copy of this notice MUST be returned with payment.
CERTIFICATE OF MAILING

[1] Applicants should check the current fee schedule posted on the USPTO Internet web site at http://www.uspto.gov/main/howtofees.htm before paying the balance due in order to ensure that the correct issue fee is paid. If applicable, fees may also be paid by EFS Web, Credit Card or Deposit Account.

I hereby certify that this notice and the required additional fee are being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to Mail Stop Issue Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date indicated below.

Printed Name: ______________________ Signature: ______________________

11/14/08

UNITED STATES PATENT AND TRADEMARK OFFICE

NOV 13 2008

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

Scott A. Moskowitz
#2505
16711 Collins Avenue

Mail Date: 10/31/08

Application Number: 10/049101

NOTICE TO PAY BALANCE OF ISSUE FEE

The issue fee payment filed on 10/09/08 has been received. Although the fee paid in the Notice of Allowance was paid, new patent fees went into effect on October 2, 2008 after the mailing date of the Notice. In accordance with Sections 801 and 803 of the Consolidated Appropriations Act, 2005 (H.R. 4818) "the provisions of this title shall take effect on the date of enactment of this Act. . . the provisions of section 801 shall apply to all patents, whenever granted, and to all patent applications pending on or filed after the effective date." See also, Revision of Patent Fees for Fiscal Year 2009-Final Rule, 73 Fed. Reg. 47534 (Aug. 14, 2008) and Consolidated Security, Disaster Assistance and Continuing Appropriations Act, 2009 (H.R. 2638). Because the issue fee was paid on or after October 2, 2008, the new issue fee was due instead of the amount specified in the Notice of Allowance.[1]

In accordance with 37 CFR 1.18, applicant is given a time period of **THREE (3) MONTHS** from the mailing date of this notice during which to pay the **BALANCE DUE** indicated below. The balance due is the difference between the issue fee required on the date that the correct issue fee is paid and the amount that was previously paid. This three-month time period may not be extended. If the balance due is not paid before the expiration of the three-month period, the application will become abandoned (if not issued) or the patent will lapse (if issued) at the termination of the three-month period.

App. Type	Column A Issue Fee Req. large entity / small entity	Column B Issue Fee PAID	Balance Due. Col. A minus Col. B
UTILITY or REISSUE	$1,510.00/ $755.00	$ 720.00	$ 35.00
DESIGN	$860.00 / $430.00	$	$
PLANT	$1,190.00 / $595.00	$	$

/ Betty Powell /
Office of Data Management
Office: 703-308-9250x160
Fax: 571-270-9937

A copy of this notice MUST be returned with payment.
CERTIFICATE OF MAILING

Adjustment date: 11/14/2008 CNGUYEN3
10/10/2008 MGEBREM2 00000056 10049101
01 FC:1501
-720.00 OP

[1] Applicants should check the current fee schedule posted on the USPTO Internet Web site at: http://www.uspto.gov/main/howtofees.htm before paying the balance due in order to ensure that the correct issue fee is paid. If applicable, fees may also be paid by EFS Web, Credit Card or Deposit Account.

11/14/2008 CNGUYEN3 00000065 10049101
01 FC:2501
755.00 OP

I hereby certify that this notice and the required additional fee are being deposited with the United States Postal Service with sufficient postage for first class ~~mail in an~~ envelope addressed to Mail Stop Issue Fee, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date indicated below.

Printed Name: SCOTT MOSKOWITZ Signature: [signature]

November 13, 2008

NOV 13 2008

PTO/SB/21 (10-08)
Approved for use through 11/30/2008. OMB 0651-0031
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ
Art Unit	2131
Examiner Name	Jeremiah L. AVERY
Attorney Docket Number	80408.0011
Total Number of Pages in This Submission	

ENCLOSURES *(Check all that apply)*

- [x] Fee Transmittal Form
  - [x] Fee Attached
- [x] Amendment/Reply
  - [x] After Final
  - [ ] Affidavits/declaration(s)
- [ ] Extension of Time Request
- [ ] Express Abandonment Request
- [ ] Information Disclosure Statement
- [ ] Certified Copy of Priority Document(s)
- [ ] Reply to Missing Parts/ Incomplete Application
  - [ ] Reply to Missing Parts under 37 CFR 1.52 or 1.53
- [ ] Drawing(s)
- [ ] Licensing-related Papers
- [ ] Petition
- [ ] Petition to Convert to a Provisional Application
- [ ] Power of Attorney, Revocation Change of Correspondence Address
- [ ] Terminal Disclaimer
- [ ] Request for Refund
- [ ] CD, Number of CD(s) ________
  - [ ] Landscape Table on CD
- [ ] After Allowance Communication to TC
- [ ] Appeal Communication to Board of Appeals and Interferences
- [ ] Appeal Communication to TC (Appeal Notice, Brief, Reply Brief)
- [ ] Proprietary Information
- [ ] Status Letter
- [ ] Other Enclosure(s) (please identify below):

Remarks

Please see attached "Notice to Pay Balance of Issue Fee"

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm Name			
Signature	[signature]		
Printed name	Scott A. MOSKOWITZ		
Date	November 13, 2008	Reg. No.	

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below:

Signature	[signature]		
Typed or printed name	Scott A. MOSKOWITZ	Date	November 13, 2008

NOV 13 2009 (stamp)

PTO/SB/17 (10-08)
Approved for use through 06/30/2010. OMB 0651-0032
U.S. Patent and Trademark Office; U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number

Effective on 12/08/2004.
Fees pursuant to the Consolidated Appropriations Act, 2005 (H.R. 4818).

FEE TRANSMITTAL
For FY 2009

☑ Applicant claims small entity status. See 37 CFR 1.27

TOTAL AMOUNT OF PAYMENT	($) 35.00

Complete if Known	
Application Number	10/049,101
Filing Date	July 23, 2002
First Named Inventor	Scott A. MOSKOWITZ
Examiner Name	Jeremiah L. AVERY
Art Unit	2131
Attorney Docket No.	80408.0011

METHOD OF PAYMENT (check all that apply)

☐ Check ☑ Credit Card ☐ Money Order ☐ None ☐ Other (please identify): ______

☐ Deposit Account Deposit Account Number: ______ Deposit Account Name: ______

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below ☐ Charge fee(s) indicated below, except for the filing fee

☐ Charge any additional fee(s) or underpayments of fee(s) under 37 CFR 1.16 and 1.17 ☐ Credit any overpayments

WARNING: Information on this form may become public. Credit card information should not be included on this form. Provide credit card information and authorization on PTO-2038.

FEE CALCULATION

1. BASIC FILING, SEARCH, AND EXAMINATION FEES

	FILING FEES		SEARCH FEES		EXAMINATION FEES		
		Small Entity		Small Entity		Small Entity	
Application Type	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fee ($)	Fees Paid ($)
Utility	330	165	540	270	220	110	______
Design	220	110	100	50	140	70	______
Plant	220	110	330	165	170	85	______
Reissue	330	165	540	270	650	325	______
Provisional	220	110	0	0	0	0	______

2. EXCESS CLAIM FEES

Fee Description	Fee ($)	Small Entity Fee ($)
Each claim over 20 (including Reissues)	52	26
Each independent claim over 3 (including Reissues)	220	110
Multiple dependent claims	390	195

Total Claims ______ – 20 or HP = ______ Extra Claims × ______ Fee ($) = ______ Fee Paid ($)

HP = highest number of total claims paid for, if greater than 20.

Indep. Claims ______ – 3 or HP = ______ Extra Claims × ______ Fee ($) = ______ Fee Paid ($)

HP = highest number of independent claims paid for, if greater than 3.

Multiple Dependent Claims: Fee ($) ______ Fee Paid ($) ______

3. APPLICATION SIZE FEE

If the specification and drawings exceed 100 sheets of paper (excluding electronically filed sequence or computer listings under 37 CFR 1.52(e)), the application size fee due is $270 ($135 for small entity) for each additional 50 sheets or fraction thereof. See 35 U.S.C. 41(a)(1)(G) and 37 CFR 1.16(s).

Total Sheets ______ – 100 = ______ Extra Sheets / 50 = ______ Number of each additional 50 or fraction thereof (round up to a whole number) × ______ Fee ($) = ______ Fee Paid ($)

4. OTHER FEE(S) Fees Paid ($)

Non-English Specification, $130 fee (no small entity discount) ______

Other (e.g., late filing surcharge): Fiscal Year Fee Change - See Attached Letter - Balance of Issue Fee $35.00

SUBMITTED BY

Signature	[signature]	Registration No. (Attorney/Agent)		Telephone 305 956 9041
Name (Print/Type)	Scott A. MOSKOWITZ			Date November 13, 2009

This collection of information is required by 37 CFR 1.136. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 30 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, VA 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. **SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.**

If you need assistance in completing the form, call 1-800-PTO-9199 and select option 2.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	ISSUE DATE	PATENT NO.	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/049,101	01/06/2009	7475246	80408.0011	8028

7590 12/17/2008

Scott A. Moskowitz
#2505
16711 Collins Avenue
Miami, FL 33160

ISSUE NOTIFICATION

The projected patent number and issue date are specified above.

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)
(application filed on or after May 29, 2000)

The Patent Term Adjustment is 683 day(s). Any patent to issue from the above-identified application will include an indication of the adjustment on the front page.

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at (571)-272-4200.

APPLICANT(s) (Please see PAIR WEB site http://pair.uspto.gov for additional applicants):

Scott A. Moskowitz, Miami, FL;
Michael Berry, Albuquerque, NM;

IR103 (Rev. 11/05)

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-00063	1/31/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, PLLC	LeMall Corp. & LeEco Group

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5,745,569	4/28/1998	Blue Spike, LLC
2 8,930,719	1/6/2015	Blue Spike, LLC
3 7,475,246	1/6/2009	Blue Spike, LLC
4 8,171,561	5/1/2012	Blue Spike, LLC
5 8,739,295	5/27/2014	Blue Spike, LLC
8,538,011	09/17/2013	Blue Spike, LLC
7,159,116	01/02/2007	Blue Spike, LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-00060	1/30/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, PLLC	VIZIO, INC

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5,745,569	4/28/1998	Blue Spike, LLC
2 8,930,719	1/6/2015	Blue Spike, LLC
3 7,475,246	1/6/2009	Blue Spike, LLC
4 8,171,561	5/1/2012	Blue Spike, LLC
5 8,739,295	5/27/2014	Blue Spike, LLC
8,538,011	09/17/2013	Blue Spike, LLC
7,159,116	01/02/2007	Blue Spike, LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	**DATE OF PATENT OR TRADEMARK**	**HOLDER OF PATENT OR TRADEMARK**
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-96	2/15/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, LLC	NVIDIA CORPORATION

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5745569	4/28/1998	Blue Spike, LLC
2 8930719	1/6/2015	Blue Spike, LLC
3 7475246	1/6/2009	Blue Spike, LLC
4 8171561	5/1/2012	Blue Spike, LLC
5 8739195	5/27/2014	Blue Spike, LLC
7159116	1/2/2007	Blue Spike LLC
8538011	9/17/2013	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	**DATE OF PATENT OR TRADEMARK**	**HOLDER OF PATENT OR TRADEMARK**
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-97	2/15/2017	Eastern District of Texas
PLAINTIFF		DEFENDANT
Blue Spike, LLC		ELEMENT TECHNOLOGIES CORPORATION

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5745569	4/28/1998	Blue Spike, LLC
2 8930719	1/6/2015	Blue Spike, LLC
3 7475246	1/6/2009	Blue Spike, LLC
4 8171561	5/1/2012	Blue Spike, LLC
5 8739195	5/27/2014	Blue Spike, LLC
7159116	1/2/2007	Blue Spike LLC
8538011	9/17/2013	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK
Mail Stop 8 **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-175	3/23/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, PLLC	BARNES & NOBLE, INC., BARNES & NOBLE BOOKSELLERS, INC., NOOK DIGITAL LLC

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7779261	1/3/2007	Blue Spike LLC
2 8161286	6/21/2010	Blue Spike LLC
3 8307213	6/21/2010	Blue Spike LLC
4 7475246	8/4/2000	Blue Spike LLC
5 8171561	10/9/2008	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print Save As... Reset

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-175	3/23/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, PLLC	BARNES & NOBLE, INC., BARNES & NOBLE BOOKSELLERS, INC., NOOK DIGITAL LLC

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8739295	3/7/2012	Blue Spike LLC
2 7813506	3/30/2009	Blue Spike LLC
3 8798268	3/11/2013	Blue Spike LLC
4 7953981	8/10/2009	Blue Spike LLC
5 8121343	10/10/2010	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print Save As... Reset

AO 120 (Rev. 08/10)

TO:	
Mail Stop 8 **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-175	3/23/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, PLLC	BARNES & NOBLE, INC., BARNES & NOBLE BOOKSELLERS, INC., NOOK DIGITAL LLC

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7159116	12/7/2000	Blue Spike LLC
2		
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY	
	☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print Save As... Reset

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-099	2/15/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, LLC	RAZER USA LTD.,

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5745569	4/28/1998	Blue Spike, LLC
2 8930719	1/6/2015	Blue Spike, LLC
3 7475246	1/6/2009	Blue Spike, LLC
4 8171561	5/1/2012	Blue Spike, LLC
5 8739195	5/27/2014	Blue Spike, LLC
7159116	1/2/2007	Blue Spike LLC
8538011	9/17/2013	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY	
	☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	**DATE OF PATENT OR TRADEMARK**	**HOLDER OF PATENT OR TRADEMARK**
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: **Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 6:17-cv-100	DATE FILED 2/15/2017	U.S. DISTRICT COURT Eastern District of Texas
PLAINTIFF Blue Spike, LLC		DEFENDANT ROKU, INC.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5745569	4/28/1998	Blue Spike, LLC
2 8930719	1/6/2015	Blue Spike, LLC
3 7475246	1/6/2009	Blue Spike, LLC
4 8171561	5/1/2012	Blue Spike, LLC
5 8739195	5/27/2014	Blue Spike, LLC
7159116	1/2/2007	Blue Spike LLC
8538011	9/17/2013	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-0098	2/15/2017	Eastern District of Texas
PLAINTIFF: Blue Spike, LLC		DEFENDANT: GIADA TECHNOLOGY, INC.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5745569	4/28/1998	Blue Spike, LLC
2 8930719	1/6/2015	Blue Spike, LLC
3 7475246	1/6/2009	Blue Spike, LLC
4 8171561	5/1/2012	Blue Spike, LLC
5 8739195	5/27/2014	Blue Spike, LLC
7159116	1/2/2007	Blue Spike LLC
8538011	9/17/2013	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-101	2/15/2017	Eastern District of Texas
PLAINTIFF		DEFENDANT
Blue Spike, LLC		Skystream Technologies, LLC

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5745569	4/28/1998	Blue Spike, LLC
2 8930719	1/6/2015	Blue Spike, LLC
3 7475246	1/6/2009	Blue Spike, LLC
4 8171561	5/1/2012	Blue Spike, LLC
5 8739195	5/27/2014	Blue Spike, LLC
7159116	1/2/2007	Blue Spike LLC
8538011	9/17/2013	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
2:16-cv-00329-RWS	4/1/2016	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, PLLC	Verimatrix, Inc., et al.,

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5,889,868	3/30/1999	Blue Spike LLC
2 7,475,246	1/6/2009	Blue Spike LLC
3 7,770,017	8/3/2010	Blue Spike LLC
4 7,813,506	10/12/2010	Blue Spike LLC
5 7,877,609	1/25/2011	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

DOCKET REFERENCE: SCOT0016-1
PATENT NO: 7475246 issued January 6, 2009 from application 10/049,101 filed August 4, 2000 as PCT/US00/21189, published in the international stage as WO01/18628 on March 15, 2001.
Benefit claim to US provisional applications: 60147134, filed Aug 4, 1999 and 60213489, filed Jun 23, 2000
ASSIGNEE: WISTARIA TRADING LTD

Power of Attorney and Correspondence Address Change

The undersigned is empowered to act on behalf of the assignee, WISTARIA TRADING LTD.

The undersigned appoints the practitioners associated with:

Customer Number 31518

as attorneys of record in this patent.

Please change the correspondence address for this patent to the address associated with the foregoing 31518 Customer number.

Signed:
Scott Moskowitz,
~~Manager~~ President, BLUE SPIKE, INC.

DOCKET REFERENCE: SCOT0016-1
PATENT NO: 7475246 issued January 6, 2009 from application 10/049,101 filed August 4, 2000 as PCT/US00/21189, published in the international stage as WO01/18628 on March 15, 2001.
Benefit claim to US provisional applications: 60147134, filed Aug 4, 1999 and 60213489, filed Jun 23, 2000.
ASSIGNEE: WISTARIA TRADING LTD

APPLICATION DATA SHEET

37 CFR 1.76(c)(2):

> c) Correcting and updating an application data sheet.
> ... (2) An application data sheet providing corrected or updated information may include all of the sections listed in paragraph (b) of this section or only those sections containing changed or updated information. The application data sheet must include the section headings listed in paragraph (b) of this section for each section included in the application data sheet, and must identify the information that is being changed, with underlining for insertions, and strike-through or brackets for text removed, except that identification of information being changed is not required for an application data sheet included with an initial submission under 35 U.S.C. 371.

37 CFR 1.76(b)(2) CORRESPONDENCE ADDRESS

~~Scott A. Moskowitz~~
~~#2505~~
~~16711 Collins Avenue~~
~~Miami, FL 33160~~

Customer Number: 31518

37 CFR 1.76(b)(4) REPRESENTATIVE INFORMATION

Customer Number: 31518

37 CFR 1.76(b)(7) APPLICANT INFORMATION

~~Scott A. Moskowitz; Michael Berry~~

WISTARIA TRADING LTD

/RichardNeifeld/
RICHARD NEIFELD, REG. NO. 35,299
ATTORNEY FOR APPLICANT

Electronic Acknowledgement Receipt

EFS ID:	29818329
Application Number:	10049101
International Application Number:	
Confirmation Number:	8028
Title of Invention:	SECURE PERSONAL CONTENT SERVER
First Named Inventor/Applicant Name:	Scott A. Moskowitz
Correspondence Address:	Scott A. Moskowitz - #2505 16711 Collins Avenue Miami FL 33160 US 305-956-9041 -
Filer:	Richard A. Neifeld
Filer Authorized By:	
Attorney Docket Number:	80408.0011
Receipt Date:	18-JUL-2017
Filing Date:	23-JUL-2002
Time Stamp:	16:35:50
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1		POA_CorrAddress_ADS_SCOT0016-1_Executed.pdf	952305	yes	3

	Multipart Description/PDF files in .zip description		
	Document Description	**Start**	**End**
	Power of Attorney	1	1
	Application Data Sheet	2	3

Warnings:

Information:

Total Files Size (in bytes): 952305

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

STATEMENT UNDER 37 CFR 3.73(c)

Applicant/Patent Owner: WISTARIA TRADING LTD

Application No./Patent No.: 7475246 Filed/Issue Date: Issued January 6, 2009

Titled: SECURE PERSONAL CONTENT SERVER

BLUE SPIKE, INC. , a CORPORATION

(Name of Assignee) (Type of Assignee, e.g., corporation, partnership, university, government agency, etc.)

states that, for the patent application/patent identified above, it is (choose **one** of options 1, 2, 3 or 4 below):

1. [✓] The assignee of the entire right, title, and interest.

2. [ ] An assignee of less than the entire right, title, and interest (check applicable box):

[ ] The extent (by percentage) of its ownership interest is ________%. Additional Statement(s) by the owners holding the balance of the interest must be submitted to account for 100% of the ownership interest.

[ ] There are unspecified percentages of ownership. The other parties, including inventors, who together own the entire right, title and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

3. [ ] The assignee of an undivided interest in the entirety (a complete assignment from one of the joint inventors was made). The other parties, including inventors, who together own the entire right, title, and interest are:

Additional Statement(s) by the owner(s) holding the balance of the interest must be submitted to account for the entire right, title, and interest.

4. [ ] The recipient, via a court proceeding or the like (e.g., bankruptcy, probate), of an undivided interest in the entirety (a complete transfer of ownership interest was made). The certified document(s) showing the transfer is attached.

The interest identified in option 1, 2 or 3 above (not option 4) is evidenced by either (choose **one** of options A or B below):

A. [ ] An assignment from the inventor(s) of the patent application/patent identified above. The assignment was recorded in the United States Patent and Trademark Office at Reel ________, Frame ________, or for which a copy thereof is attached.

B. [✓] A chain of title from the inventor(s), of the patent application/patent identified above, to the current assignee as follows:

1. From: MOSKOWITZ, SCOTT A., BERRY, MICHAEL To: BLUE SPIKE, INC.

The document was recorded in the United States Patent and Trademark Office at

Reel 028482, Frame 0720, or for which a copy thereof is attached.

2. From: BLUE SPIKE, INC. To: WISTARIA TRADING LTD

The document was recorded in the United States Patent and Trademark Office at

Reel 036388, Frame 0248, or for which a copy thereof is attached.

STATEMENT UNDER 37 CFR 3.73(c)

3. From: ______________________ To: ______________________

The document was recorded in the United States Patent and Trademark Office at

Reel __________, Frame __________, or for which a copy thereof is attached.

4. From: ______________________ To: ______________________

The document was recorded in the United States Patent and Trademark Office at

Reel __________, Frame __________, or for which a copy thereof is attached.

5. From: ______________________ To: ______________________

The document was recorded in the United States Patent and Trademark Office at

Reel __________, Frame __________, or for which a copy thereof is attached.

6. From: ______________________ To: ______________________

The document was recorded in the United States Patent and Trademark Office at

Reel __________, Frame __________, or for which a copy thereof is attached.

☐ Additional documents in the chain of title are listed on a supplemental sheet(s).

☐ As required by 37 CFR 3.73(c)(1)(i), the documentary evidence of the chain of title from the original owner to the assignee was, or concurrently is being, submitted for recordation pursuant to 37 CFR 3.11.

[NOTE: A separate copy (i.e., a true copy of the original assignment document(s)) must be submitted to Assignment Division in accordance with 37 CFR Part 3, to record the assignment in the records of the USPTO. See MPEP 302.08]

The undersigned (whose title is supplied below) is authorized to act on behalf of the assignee.

/Scott Moskowitz/	July 18, 2017
Signature	Date
SCOTT MOSKOWITZ	DIRECTOR
Printed or Typed Name	Title or Registration Number

Privacy Act Statement

The **Privacy Act of 1974 (P.L. 93-579)** requires that you be given certain information in connection with your submission of the attached form related to a patent application or patent. Accordingly, pursuant to the requirements of the Act, please be advised that: (1) the general authority for the collection of this information is 35 U.S.C. 2(b)(2); (2) furnishing of the information solicited is voluntary; and (3) the principal purpose for which the information is used by the U.S. Patent and Trademark Office is to process and/or examine your submission related to a patent application or patent. If you do not furnish the requested information, the U.S. Patent and Trademark Office may not be able to process and/or examine your submission, which may result in termination of proceedings or abandonment of the application or expiration of the patent.

The information provided by you in this form will be subject to the following routine uses:

1. The information on this form will be treated confidentially to the extent allowed under the Freedom of Information Act (5 U.S.C. 552) and the Privacy Act (5 U.S.C 552a). Records from this system of records may be disclosed to the Department of Justice to determine whether disclosure of these records is required by the Freedom of Information Act.
2. A record from this system of records may be disclosed, as a routine use, in the course of presenting evidence to a court, magistrate, or administrative tribunal, including disclosures to opposing counsel in the course of settlement negotiations.
3. A record in this system of records may be disclosed, as a routine use, to a Member of Congress submitting a request involving an individual, to whom the record pertains, when the individual has requested assistance from the Member with respect to the subject matter of the record.
4. A record in this system of records may be disclosed, as a routine use, to a contractor of the Agency having need for the information in order to perform a contract. Recipients of information shall be required to comply with the requirements of the Privacy Act of 1974, as amended, pursuant to 5 U.S.C. 552a(m).
5. A record related to an International Application filed under the Patent Cooperation Treaty in this system of records may be disclosed, as a routine use, to the International Bureau of the World Intellectual Property Organization, pursuant to the Patent Cooperation Treaty.
6. A record in this system of records may be disclosed, as a routine use, to another federal agency for purposes of National Security review (35 U.S.C. 181) and for review pursuant to the Atomic Energy Act (42 U.S.C. 218(c)).
7. A record from this system of records may be disclosed, as a routine use, to the Administrator, General Services, or his/her designee, during an inspection of records conducted by GSA as part of that agency's responsibility to recommend improvements in records management practices and programs, under authority of 44 U.S.C. 2904 and 2906. Such disclosure shall be made in accordance with the GSA regulations governing inspection of records for this purpose, and any other relevant (*i.e.*, GSA or Commerce) directive. Such disclosure shall not be used to make determinations about individuals.
8. A record from this system of records may be disclosed, as a routine use, to the public after either publication of the application pursuant to 35 U.S.C. 122(b) or issuance of a patent pursuant to 35 U.S.C. 151. Further, a record may be disclosed, subject to the limitations of 37 CFR 1.14, as a routine use, to the public if the record was filed in an application which became abandoned or in which the proceedings were terminated and which application is referenced by either a published application, an application open to public inspection or an issued patent.
9. A record from this system of records may be disclosed, as a routine use, to a Federal, State, or local law enforcement agency, if the USPTO becomes aware of a violation or potential violation of law or regulation.

Electronic Acknowledgement Receipt

EFS ID:	29820095
Application Number:	10049101
International Application Number:	
Confirmation Number:	8028
Title of Invention:	SECURE PERSONAL CONTENT SERVER
First Named Inventor/Applicant Name:	Scott A. Moskowitz
Correspondence Address:	Scott A. Moskowitz - #2505 16711 Collins Avenue Miami FL 33160 US 305-956-9041 -
Filer:	Richard A. Neifeld
Filer Authorized By:	
Attorney Docket Number:	80408.0011
Receipt Date:	18-JUL-2017
Filing Date:	23-JUL-2002
Time Stamp:	17:58:46
Application Type:	U.S. National Stage under 35 USC 371

Payment information:

Submitted with Payment	no

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Assignee showing of ownership per 37 CFR 3.73	373_aia0096_SCOT0016-1.pdf	120067 [illegible]	no	3

Warnings:	
Information:	
Total Files Size (in bytes):	120067

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111
If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.
National Stage of an International Application under 35 U.S.C. 371
If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.
New International Application Filed with the USPTO as a Receiving Office
If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

PETITION TO ACCEPT UNINTENTIONALLY DELAYED PAYMENT OF MAINTENANCE FEE IN AN EXPIRED PATENT (37 CFR 1.378(b))

Patent Number	Issue Date	Application Number	Filing Date	Docket Number (if applicable)
7475246	06-Jan-2009	10049101	23-Jul-2002	

CAUTION: Maintenance fee (and surcharge, if any) payment must correctly identify: (1) the patent number and (2) the application number of the actual U.S. application leading to issuance of that patent to ensure the fee(s) is/are associated with the correct patent. 37 CFR 1.366(c) and (d).

Applicants claims the following fee status:

○ Small Entity

○ Micro Entity

◉ Regular Undiscounted

Applicants selects the following :

○ 3 1/2 ◉ 7 1/2 ○ 11 1/2

PETITION FEE
The petition fee required by 37 CFR 1.17(m) (Fee Code 1558/2558) must be paid as a condition of accepting unintentionally delayed payment of the maintenance fee.

MAINTENANCE FEE (37 CFR 1.20(e)-(g))
The appropriate maintenance fee must be submitted with this petition.

STATEMENT
THE UNDERSIGNED CERTIFIES THAT THE DELAY IN PAYMENT OF THE MAINTENANCE FEE TO THIS PATENT WAS UNINTENTIONAL

PETITIONER(S) REQUEST THAT THE DELAYED PAYMENT OF THE MAINTENANCE FEE BE ACCEPTED AND THE PATENT REINSTATED

THIS PORTION MUST BE COMPLETED BY THE SIGNATORY OR SIGNATORIES

37 CFR 1.378(c) states: "Any petition under this section must be signed in compliance with 37 CFR 1.33(b) ;"

I certify, in accordance with 37 CFR 1.4(d)(4) that I am

○ An attorney or agent registered to practice before the Patent and Trademark Office who has been given power of attorney in this application.

○ An attorney or agent registered to practice before the Patent and Trademark Office

○ A sole patentee

○ A joint patentee; I certify that I am authorized to sign this submission on behalf of all the other patentees as evidenced by the power of attorney in the application

○ A joint patentee; all of whom are signing this e-petition

◉ The assignee of record of the entire interest that qualifies as an authorized party under 37 CFR 1.33(b)

The Assignee of record of the entire interest			
Under 37 CFR 3.71 an assignee becomes of record by filing a statement in compliance with 37 CFR 3.73(b). Signature requirements are set forth in 37 CFR 1.4(d), and the undersigned certifies that he / she is empowered to act on behalf of the assignee of the entire interest			
Signature	/Scott Moskowitz/		
Name	SCOTT MOSKOWITZ		
Enter Reel and Frame Number			Remove
Reel Number	013126	Frame Number	0959
Enter Reel and Frame Number			Remove
Reel Number	036388	Frame Number	0248
Click ADD for additional Reel Number and Frame Number			Add

Electronic Patent Application Fee Transmittal

Application Number:	10049101
Filing Date:	23-Jul-2002
Title of Invention:	SECURE PERSONAL CONTENT SERVER
First Named Inventor/Applicant Name:	Scott A. Moskowitz
Filer:	Richard A. Neifeld
Attorney Docket Number:	80408.0011

Filed as Large Entity

Filing Fees for Utility under 35 USC 111(a)

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Basic Filing:				
MAINTENANCE FEE DUE AT 7.5 YEARS	1552	1	3600	3600
PET. DELAY PYMT MAINTAIN PATENT IN FORCE	1558	1	1700	1700
Pages:				
Claims:				
Miscellaneous-Filing:				
Petition:				
Patent-Appeals-and-Interference:				

Description	Fee Code	Quantity	Amount	Sub-Total in USD($)
Post-Allowance-and-Post-Issuance:				
Extension-of-Time:				
Miscellaneous:				
		Total in USD ($)		**5300**

UNITED STATES PATENT AND TRADEMARK OFFICE

Commissioner for Patents
United States Patent and Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450
www.uspto.gov

In re Patent No. 7475246
Issue Date: January 6,2009
Application No. 10049101
Filed: July 23,2002
Attorney Docket No. 80408.0011

:DECISION GRANTING PETITION
:UNDER 37 CFR 1.378(b)

This is a decision on the electronic petition, filed July 18,2017 ,under 37 CFR 1.378(b) to accept the unintentionally delayed payment of the 7.5 year maintenance fee for the above-identified patent.

The petition is **GRANTED**.

The maintenance fee is accepted, and the above-identified patent reinstated as of July 18,2017 This decision also constitutes notice that the fee has been accepted. An electronic copy of the petition and this decision has been created as an entry in the Image File Wrapper. Nevertheless, petitioner should print and retain an independent copy.

Telephone inquiries related to this electronic decision should be directed to the Electronic Business Center at 1-866-217-9197.

Electronic Acknowledgement Receipt

EFS ID:	29820217
Application Number:	10049101
Patent Number:	7475246
Confirmation Number:	
Petition Issued Date:	July 18,2017
Title of Invention:	SECURE PERSONAL CONTENT SERVER
First Named Inventor/Applicant Name:	Scott A. Moskowitz
Correspondence Address:	
Filer:	Richard A. Neifeld
Filer Authorized By:	
Attorney Docket Number:	80408.0011
Receipt Date:	18-JUL-2017
Filing Date:	23-JUL-2002
Time Stamp:	18:07:35
Application Type:	Utility under 35 USC 111(a)

Payment information:

Submitted with Payment	yes

Payment Type	CARD
Payment was successfully received in RAM	$5300
RAM confirmation Number	071917INTEFSW18091900
Deposit Account	
Authorized User	

The Director of the USPTO is hereby authorized to charge indicated fees and credit any overpayment as follows:

File Listing:

Document Number	Document Description	File Name	File Size(Bytes)/ Message Digest	Multi Part /.zip	Pages (if appl.)
1	Petition automatically granted by EFS	petition-request.pdf	35284 [illegible]	no	2
Warnings:					
Information:					
2	Fee Worksheet (SB06)	fee-info.pdf	31872 [illegible]	no	2
Warnings:					
Information:					
		Total Files Size (in bytes):	67156		

This Acknowledgement Receipt evidences receipt on the noted date by the USPTO of the indicated documents, characterized by the applicant, and including page counts, where applicable. It serves as evidence of receipt similar to a Post Card, as described in MPEP 503.

New Applications Under 35 U.S.C. 111

If a new application is being filed and the application includes the necessary components for a filing date (see 37 CFR 1.53(b)-(d) and MPEP 506), a Filing Receipt (37 CFR 1.54) will be issued in due course and the date shown on this Acknowledgement Receipt will establish the filing date of the application.

National Stage of an International Application under 35 U.S.C. 371

If a timely submission to enter the national stage of an international application is compliant with the conditions of 35 U.S.C. 371 and other applicable requirements a Form PCT/DO/EO/903 indicating acceptance of the application as a national stage submission under 35 U.S.C. 371 will be issued in addition to the Filing Receipt, in due course.

New International Application Filed with the USPTO as a Receiving Office

If a new international application is being filed and the international application includes the necessary components for an international filing date (see PCT Article 11 and MPEP 1810), a Notification of the International Application Number and of the International Filing Date (Form PCT/RO/105) will be issued in due course, subject to prescriptions concerning national security, and the date shown on this Acknowledgement Receipt will establish the international filing date of the application.

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 2:16-cv-00329-RWS	DATE FILED 4/1/2016	U.S. DISTRICT COURT Eastern District of Texas
PLAINTIFF Blue Spike, PLLC		DEFENDANT Verimatrix Inc., et al.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5,889,868	3/30/1999	Blue Spike LLC
2 7,475,246	1/6/2009	Blue Spike LLC
3 7,770,017	8/3/2010	Blue Spike LLC
4 7,813,506	10/12/2010	Blue Spike LLC
5 7,877,609	1/25/2011	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print | Save As... | Reset

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
10/049,101	07/23/2002	Scott A. Moskowitz	

CONFIRMATION NO. 8028

31518
NEIFELD IP LAW, PC
5400 Shawnee Road
Suite 310
ALEXANDRIA, VA 22312-2300

POA ACCEPTANCE LETTER

OC000000092963442

Date Mailed: 07/24/2017

NOTICE OF ACCEPTANCE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 07/18/2017.

The Power of Attorney in this application is accepted. Correspondence in this application will be mailed to the above address as provided by 37 CFR 1.33.

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/jtfitzhugh sr/

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NUMBER	FILING OR 371(C) DATE	FIRST NAMED APPLICANT	ATTY. DOCKET NO./TITLE
10/049,101	07/23/2002	Scott A. Moskowitz	80408.0011

CONFIRMATION NO. 8028

POWER OF ATTORNEY NOTICE

Scott A. Moskowitz
#2505
16711 Collins Avenue
Miami, FL 33160

OC000000092963441

Date Mailed: 07/24/2017

NOTICE REGARDING CHANGE OF POWER OF ATTORNEY

This is in response to the Power of Attorney filed 07/18/2017.

- The Power of Attorney to you in this application has been revoked by the assignee who has intervened as provided by 37 CFR 3.71. Future correspondence will be mailed to the new address of record(37 CFR 1.33).

Questions about the contents of this notice and the requirements it sets forth should be directed to the Office of Data Management, Application Assistance Unit, at **(571) 272-4000** or **(571) 272-4200** or **1-888-786-0101**.

/jtfitzhugh.sr/

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-0098	2/15/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, LLC	GIADA TECHNOLOGY, INC.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5745569	4/28/1998	Blue Spike, LLC
2 8930719	1/6/2015	Blue Spike, LLC
3 7475246	1/6/2009	Blue Spike, LLC
4 8171561	5/1/2012	Blue Spike, LLC
5 8739195	5/27/2014	Blue Spike, LLC
7159116	1/2/2007	Blue Spike LLC
8538011	9/17/2013	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT
ORDER DISMISSING CASE. Plaintiff Blue Spike, LLC's claims against Defendant Giada Technology, Inc. are dismissed without prejudice. Each party will bear all its own attorneys' fees and costs in this case.

CLERK	(BY) DEPUTY CLERK	DATE
David A O'Toole	Michael Lantz	5/30/2017

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-00060	1/30/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, PLLC	VIZIO, INC

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5,745,569	4/28/1998	Blue Spike, LLC
2 8,930,719	1/6/2015	Blue Spike, LLC
3 7,475,246	1/6/2009	Blue Spike, LLC
4 8,171,561	5/1/2012	Blue Spike, LLC
5 8,739,295	5/27/2014	Blue Spike, LLC
8,538,011	09/17/2013	Blue Spike, LLC
7,159,116	01/02/2007	Blue Spike, LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	**DATE OF PATENT OR TRADEMARK**	**HOLDER OF PATENT OR TRADEMARK**
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court California Central District Court on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 17cv01172	DATE FILED 7/10/2017	U.S. DISTRICT COURT California Central District Court
PLAINTIFF Blue Spike, LLC		DEFENDANT VIZIO, Inc.
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5,745,569		
2 8,930,719		
3 7,475,246		
4 8,171,561		
5 8,739,295		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7,159,116		
2 8,538,011		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-101	2/15/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, LLC	Skystream Technologies, LLC

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5745569	4/28/1998	Blue Spike, LLC
2 8930719	1/6/2015	Blue Spike, LLC
3 7475246	1/6/2009	Blue Spike, LLC
4 8171561	5/1/2012	Blue Spike, LLC
5 8739195	5/27/2014	Blue Spike, LLC
7159116	1/2/2007	Blue Spike LLC
8538011	9/17/2013	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-175	3/23/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, PLLC	BARNES & NOBLE, INC., BARNES & NOBLE BOOKSELLERS, INC., NOOK DIGITAL LLC

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7779261	1/3/2007	Blue Spike LLC
2 8161286	6/21/2010	Blue Spike LLC
3 8307213	6/21/2010	Blue Spike LLC
4 7475246	8/4/2000	Blue Spike LLC
5 8171561	10/9/2008	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	**DATE OF PATENT OR TRADEMARK**	**HOLDER OF PATENT OR TRADEMARK**
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print Save As... Reset

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-175	3/23/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, PLLC	BARNES & NOBLE, INC., BARNES & NOBLE BOOKSELLERS, INC., NOOK DIGITAL LLC

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8739295	3/7/2012	Blue Spike LLC
2 7813506	3/30/2009	Blue Spike LLC
3 8798268	3/11/2013	Blue Spike LLC
4 7953981	8/10/2009	Blue Spike LLC
5 8121343	10/10/2010	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print Save As... Reset

AO 120 (Rev. 08/10)

TO: **Mail Stop 8** **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-175	3/23/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, PLLC	BARNES & NOBLE, INC., BARNES & NOBLE BOOKSELLERS, INC., NOOK DIGITAL LLC

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7159116	12/7/2000	Blue Spike LLC
2		
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print Save As... Reset

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO. 6:17-cv-099	DATE FILED 2/15/2017	U.S. DISTRICT COURT Eastern District of Texas
PLAINTIFF Blue Spike, LLC		DEFENDANT RAZER USA LTD.,
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5745569	4/28/1998	Blue Spike, LLC
2 8930719	1/6/2015	Blue Spike, LLC
3 7475246	1/6/2009	Blue Spike, LLC
4 8171561	5/1/2012	Blue Spike, LLC
5 8739195	5/27/2014	Blue Spike, LLC
7159116	1/2/2007	Blue Spike LLC
8538011	9/17/2013	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO:	
Mail Stop 8 **Director of the U.S. Patent and Trademark Office** **P.O. Box 1450** **Alexandria, VA 22313-1450**	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-96	2/15/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, LLC	NVIDIA CORPORATION

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5745569	4/28/1998	Blue Spike, LLC
2 8930719	1/6/2015	Blue Spike, LLC
3 7475246	1/6/2009	Blue Spike, LLC
4 8171561	5/1/2012	Blue Spike, LLC
5 8739195	5/27/2014	Blue Spike, LLC
7158116	1/2/2007	Blue Spike LLC
8538011	9/17/2013	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	**DATE OF PATENT OR TRADEMARK**	**HOLDER OF PATENT OR TRADEMARK**
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

FINAL JUDGMENT that all claims, counterclaims, and third-party claims in the instant suit be DISMISSED WITH PREJUDICE in their entirety, with costs to be borne by the party that incurred them. Signed by District Judge Robert W. Schroeder, III on 1/3/18.

CLERK	(BY) DEPUTY CLERK	DATE
David A. O'Toole	M. Covey	1/3/18

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-00063	1/31/2017	Eastern District of Texas

PLAINTIFF	DEFENDANT
Blue Spike, PLLC	LeMall Corp. & LeEco Group

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 5,745,569	4/28/1998	Blue Spike, LLC
2 8,930,719	1/6/2015	Blue Spike, LLC
3 7,475,246	1/6/2009	Blue Spike, LLC
4 8,171,561	5/1/2012	Blue Spike, LLC
5 8,739,295	5/27/2014	Blue Spike, LLC
8,538,011	09/17/2013	Blue Spike, LLC
7,159,116	01/02/2007	Blue Spike, LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

It is ORDERED that the claims asserted herein by Plaintiff Blue Spike LLC against Defendants be, and hereby are, DISMISSED WITHOUT PREJUDICE; ORDERED that any defenses asserted herein by Defendants against Blue Spike LLC be, and hereby are, DISMISSED WITHOUT PREJUDICE; and ORDERED that the Parties shall bear their own attorneys' fees, expenses and costs; and ORDERED that all motions not previously ruled on are DENIED AS MOOT

CLERK	(BY) DEPUTY CLERK	DATE
		1/22/18

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-0138	03/02/2017	Eastern District of Texas
PLAINTIFF: Blue Spike, PLLC		DEFENDANT: AnyMark, Inc.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7475246	Jan 6, 2009	Blue Spike LLC
2 7770017	Aug 3, 2010	Blue Spike LLC
3 7913087	Mar 22, 2011	Blue Spike LLC
4 7953981	May 31, 2011	Blue Spike LLC
5 8121343	Feb 21, 2012	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print Save As... Reset

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-0138	03/02/2017	Eastern District of Texas
PLAINTIFF		DEFENDANT
Blue Spike, PLLC		AnyMark, Inc.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8161286	Apr 17, 2012	Blue Spike LLC
2 8171561	May 1, 2012	Blue Spike LLC
3 8175330	May 8, 2012	Blue Spike LLC
4 8265278	Sep 11, 2012	Blue Spike LLC
5 8307213	Nov 6, 2012	Blue Spike LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print Save As... Reset

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	**REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK**

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☒ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:17-cv-0138	03/02/2017	Eastern District of Texas
PLAINTIFF: Blue Spike, PLLC		DEFENDANT: AnyMark, Inc.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 8739295	May 27, 2014	Blue Spike LLC
2 9231980	Jan 5, 2016	Blue Spike LLC
3		
4		
5		

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print Save As... Reset

AO 120 (Rev. 08/10)

TO: Mail Stop 8 Director of the U.S. Patent and Trademark Office P.O. Box 1450 Alexandria, VA 22313-1450	REPORT ON THE FILING OR DETERMINATION OF AN ACTION REGARDING A PATENT OR TRADEMARK

In Compliance with 35 U.S.C. § 290 and/or 15 U.S.C. § 1116 you are hereby advised that a court action has been filed in the U.S. District Court Eastern District of Texas on the following

☐ Trademarks or ☑ Patents. (☐ the patent action involves 35 U.S.C. § 292.):

DOCKET NO.	DATE FILED	U.S. DISTRICT COURT
6:18-cv-0242	5/31/2018	Eastern District of Texas
PLAINTIFF		DEFENDANT
Blue Spike, PLLC		Frontier Communications Corp.

PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1 7,475,246	1/6/2009	Blue Spike, LLC
2 8,739,295	5/27/2014	Blue Spike, LLC
3 9,021,602	4/28/2015	Blue Spike, LLC
4 9,104,842	8/11/2015	Blue Spike, LLC
5 9,934,408	4/3/2018	Blue Spike, LLC

In the above—entitled case, the following patent(s)/ trademark(s) have been included:

DATE INCLUDED	INCLUDED BY ☐ Amendment ☐ Answer ☐ Cross Bill ☐ Other Pleading	
PATENT OR TRADEMARK NO.	DATE OF PATENT OR TRADEMARK	HOLDER OF PATENT OR TRADEMARK
1		
2		
3		
4		
5		

In the above—entitled case, the following decision has been rendered or judgement issued:

DECISION/JUDGEMENT

CLERK	(BY) DEPUTY CLERK	DATE

Copy 1—Upon initiation of action, mail this copy to Director Copy 3—Upon termination of action, mail this copy to Director
Copy 2—Upon filing document adding patent(s), mail this copy to Director Copy 4—Case file copy

Print Save As... Reset