

(19) World Intellectual Property
Organization
International Bureau



(43) International Publication Date
25 November 2004 (25.11.2004)

PCT

(10) International Publication Number
WO 2004/102464 A2

(51) International Patent Classification⁷: **G06K**
(21) International Application Number:
PCT/US2004/014161
(22) International Filing Date: 7 May 2004 (07.05.2004)
(25) Filing Language: English
(26) Publication Language: English

(30) Priority Data:
10/435,517 8 May 2003 (08.05.2003) US
10/435,612 8 May 2003 (08.05.2003) US

(71) Applicant (for all designated States except US): **DIGI-MARC CORPORATION** [US/US]; 9405 SW Gemini Drive, Beaverton, OR 97008 (US).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **ALATTAR, Adnan, M.** [US/US]; 14336 SW Chesterfield Lane, Tigard, OR 97224 (US). **STACH, John** [US/US]; 4800 SW Saum Way, Tualatin, OR 97062 (US). **TIAN, Jun** [CN/US]; 6455 SW Nyberg Lane, Apt. B208, Tualatin, OR 97062 (US).

(74) Agent: **MEYER, Joel, R.**; Digimarc Corporation, 9405 SW Gemini Drive, Beaverton, OR 97008 (US).

(81) Designated States (unless otherwise indicated, for every kind of national protection available): AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States (unless otherwise indicated, for every kind of regional protection available): ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

Published:

— without international search report and to be republished upon receipt of that report

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.

(54) Title: REVERSIBLE WATERMARKING AND RELATED APPLICATIONS

(57) Abstract: Reversible watermarking methods enable auxiliary data to be embedded in data sets, such as images, audio, video and software. The reversible nature of the method enables the original data set to be perfectly restored. Control systems with feedback loops are used to optimize embedding based on distortion or auxiliary data capacity constraints. The watermarking may be applied recursively to embed several layers, where subsequent layers are embedded into a previously watermarked data set. To recover the original data, each layer is extracted and the data restored in reverse order of the embedding. Sets of elements that are expanded to carry auxiliary data in each layer overlap or are interleaved to maximize embedding capacity or quality of the host data. A reversible watermarking program transforms a host data file into a logical storage unit for auxiliary data files by embedding the auxiliary files in the data stored in the host data file. The reversible watermark modifies host data such as an image, audio, video, or software code, to carry auxiliary data. For perceptual content such as visual or audio media, the reversible watermark can maintain a desired level of perceptual quality, effectively hiding the auxiliary data in the host data. The reversible watermark enables the original host data prior to modifications due to the embedding to be restored.



WO 2004/102464 A2

Reversible Watermarking and Related Applications

Technical Field

The invention relates to digital watermarking.

Background and Summary

5 Digital watermarking is a process for modifying physical or electronic media to embed a machine-readable code into the media. The media may be modified such that the embedded code is imperceptible or nearly imperceptible to the user, yet may be detected through an automated detection process. Most commonly, digital watermarking is applied to media signals such as images, audio signals, and video signals. However, it may also be applied to other
10 types of media objects, including documents (e.g., through line, word or character shifting, or line/character thickness variations), software, multi-dimensional graphics models, and surface textures of objects.

 Digital watermarking systems typically have two primary components: an encoder that embeds the watermark in a host media signal, and a decoder that detects and reads the
15 embedded watermark from a signal suspected of containing a watermark (a suspect signal). The encoder embeds a watermark by subtly altering the host media signal. The reading component analyzes a suspect signal to detect whether a watermark is present. In applications where the watermark encodes information, the reader extracts this information from the detected watermark.

20 Several particular watermarking techniques have been developed. The reader is presumed to be familiar with the literature in this field. Particular techniques for embedding and detecting imperceptible watermarks in media signals are detailed in the assignee's co-pending application serial numbers 10/319,404, 09/503,881 and US Patent 6,122,403, which are hereby incorporated by reference.

25 A particular class of digital watermarking, called reversible watermarking, enables the original host signal to be reconstructed. One example is disclosed in assignee's application 10/319,404, which describes a variety of methods for reversible watermarking of data, including a technique specifically referred to as difference expansion. Reversible watermarking has a number of applications, as illustrated in the patent documents incorporated
30 above. In one application, a reversible watermark is used to verify that content in which it is embedded has not been altered. In particular, if the reversible watermark can be recovered and/or the content verified (e.g., via comparison of a hash of the perfectly restored content and a hash of original content carried in watermark), then the content is deemed authentic. Many

- 2 -

proposed techniques focus on high data carrying capacity while maintaining fidelity of the content. Others propose making the watermark robust, and conditionally reversible in the event that the content has not been altered. For some applications, the reversible watermark can be used to degrade fidelity intentionally, and then restore high quality content through reversal of the watermark, assuming the content user has paid for, licensed, or otherwise been granted permission to access the high quality version.

The needs of a particular application vary, including the extent to which content quality is preserved, auxiliary data carrying capacity is maximized, and robustness is maintained.

The invention provides various methods for reversible watermarking and related software and systems. One aspect of the invention is a method for performing reversible watermarking to embed auxiliary data in an original data set. The method reversibly embeds the auxiliary data into the original data set by expanding values in the original data set that distorts the values, yet enables the values to be perfectly re-constructed. The method applies rate control to determine how to expand the values to minimize distortion for a desired auxiliary data carrying capacity or to maximize data carrying capacity for a desired distortion.

In another variation, the method applies a perceptual model to determine how to expand the values to minimize distortion for a desired auxiliary data carrying capacity or to maximize data carrying capacity for a desired perceptual distortion. This perceptual model may be used in conjunction with a control system with feedback to optimize the embedding based on quality and/or data capacity constraints.

Another aspect of the invention is a method for performing reversible watermarking to embed auxiliary data in an original data set. The method selects sets of elements in the original data set for expansion. It reversibly embeds the auxiliary data into the original data set by expanding values associated with the selected sets in a manner that distorts the values, yet enables the values to be perfectly re-constructed. The reversible watermarking is performed iteratively in layers, and for the layers, interleaving sets of elements are selected for expansion in successive layers.

The invention provides a software program, and related methods and systems that transform a host data file into a logical storage unit for auxiliary data files by embedding the auxiliary files in the data stored in the host data file. In one particular implementation, the program embeds auxiliary files in a reversible watermark. This reversible watermark modifies host data such as an image, audio, video, or software code, to carry auxiliary data. For perceptual content, the reversible watermark can maintain a desired level of perceptual quality, effectively hiding the auxiliary data in the host data. The reversible watermark enables the original host data prior to modifications due to the embedding to be restored.

- 3 -

One aspect of the invention is software for transforming a host data file carrying host media data into a logical storage unit for storing auxiliary data files in a reversible watermark embedded into the host media data. The software, stored on a storage medium, includes a watermarking module for modifying original values of host media data elements in the host data file to embed a reversible watermark carrying auxiliary data files. The reversible watermark enables the host media data elements to be restored to the original values. It also includes a user interface module for representing the host data files as a container for the auxiliary data files, and enables the adding or removing of auxiliary data files from the reversible watermark.

A variety of modules may be included in the software for providing additional functionality, including modules for determining capacity of the host data, partitioning the host data into randomly accessible storage units, displaying overlay files, executing links, such as hyperlinks to related information, controlling access to the host data or embedded data layers, controlling distribution of the host, tracking the history of the host data, facilitating visual searching, controlling rendering of the host, etc.

Further features will become apparent from the following detailed description and accompanying drawings.

Brief Description of the Drawings

Fig. 1 illustrates an example of how to configure vectors for reversible watermarking. Fig. 2 is a diagram of a rate controller for use in reversible watermarking. Fig. 3 is a diagram illustrating recursive embedding of a reversible watermark. Fig. 4 is a diagram illustrating an example of a permutation used for reversible watermark embedding.

Fig. 5 is a diagram illustrating an example of a program used to transform a host data file into a logical storage unit using a reversible watermark.

Fig. 6 is a diagram illustrating an example of a graphical user interface for the program illustrated in Fig. 5.

Fig. 7 is a diagram illustrating an example of a user interface used to depict overlays that are extracted from a reversible watermark and superimposed over a host image, along with links to related information.

Detailed Description

1. Introduction

In this document, we describe a method for reversible watermarking and related applications. While the method is described for still images, it may be applied to other data sets, including audio, video, graphical models, text, and software (e.g., object code).

A reversible watermarking system includes an embedder and a reader. The embedder modifies the host data set to embed auxiliary data. In some applications, there is a desire to maintain some level of perceptual quality (e.g., embedding auxiliary data, yet making the resulting images or audio with embedded data look or sound substantially the same as the original image or audio). In this case, controls can be applied to ensure that a desired level of quality is maintained while maximizing the auxiliary data capacity, or maximizing the quality for a particular amount of auxiliary data. The reader analyzes a data set suspected of carrying embedded auxiliary data, extracts the auxiliary data, and restores the data set to its original values prior to embedding.

The method described below performs an expansion of values in a data set to embed auxiliary data. In the specific example provided for images, the method performs an invertible transform to convert the input data into a set that includes expandable data values. This transform is not necessary if the input data set is already in a form that includes sufficiently expandable data values to carry the desired amount of auxiliary data. In general, the transform attempts to create a set of values that maintains the perceptual quality of the host (for data sets where perceptual quality is important) and provides expandable values. One way to accomplish this is to exploit redundancy or correlation among values in the host signal by expanding the difference values between redundant or closely correlated values. One particular way to expand the difference values is detailed further below.

2. Generalized Difference Expansion

Vector: For the purpose of this example, the vector $\mathbf{u} = (u_0, u_1, \dots, u_{N-1})$ is formed from N pixel values chosen from N different locations within the same color component for an image according to a predetermined order. This order may serve as a security key. The simplest way to form this vector is to consider every $a \times b$ adjacent pixel values as shown in Fig. 1 as a vector. If w and h are the height and the width of the host image, then $1 \leq a \leq h$, $1 \leq b \leq w$ and $a + b \neq 2$.

- 5 -

For simplicity, we treat each color component independently, and, hence, each component has its own set of vectors. Also, we select vectors that do not overlap each other; i.e., each pixel exists in only one vector. These requirements may be removed at the expense of complicating the watermarking algorithm due to the extra caution required to determine the processing order of the overlapped vectors.

Forward Reversible Integer Transform: The forward reversible integer transform, $f(\cdot)$, for the vector $\mathbf{u} = (u_0, u_1, \Lambda, u_{N-1})$ is defined as:

$$\begin{aligned} v_0 &= \left\lfloor \frac{u_0 + u_1 + \Lambda + u_{N-1}}{N} \right\rfloor \\ v_1 &= u_1 - u_0 \\ &\vdots \\ v_{N-1} &= u_{N-1} - u_0 \end{aligned} \quad (1)$$

where $\lfloor \cdot \rfloor$ is the least nearest integer.

The inverse transform, $f^{-1}(\cdot)$, for the transformed vector, $\mathbf{v} = (v_0, v_1, \Lambda, v_{N-1})$ is defined as:

$$\begin{aligned} u_0 &= v_0 - \left\lfloor \frac{v_1 + v_2 + \Lambda + v_{N-1}}{N} \right\rfloor \\ u_1 &= v_1 + u_0 \\ &\vdots \\ u_{N-1} &= v_{N-1} + u_0 \end{aligned} \quad (2)$$

Proof: To prove that equation (2) is the inverse of equation (1) one can substitute $v_0, v_1, \dots, v_{N-1}$ from equation (1) into u_0 of equation (2). This gives:

- 6 -

$$\begin{aligned}
u_0 &= \left\lfloor \frac{u_0 + u_1 + \Lambda + u_{N-1}}{N} \right\rfloor - \\
&\quad \left\lfloor \frac{(u_1 - u_0) + (u_2 - u_0) + \Lambda + (u_{N-1} - u_0)}{N} \right\rfloor \\
&= \left\lfloor \frac{u_0 + u_1 + \Lambda + u_{N-1}}{N} \right\rfloor - \\
&\quad \left\lfloor \frac{u_0 + u_1 + \Lambda + u_{N-1}}{N} - u_0 \right\rfloor \\
&= \left\lfloor \frac{u_0 + u_1 + \Lambda + u_{N-1}}{N} \right\rfloor - \\
&\quad \left\lfloor \frac{u_0 + u_1 + \Lambda + u_{N-1}}{N} \right\rfloor + u_0 = u_0
\end{aligned} \tag{3}$$

Now, the reversibility concerning $u_1, u_2, \dots, u_{N-1}$ can be proven by simple mathematical manipulation of $v_1, v_2, \dots, v_{N-1}$ in equation (1).

Definition 1: The vector $\mathbf{u} = (u_0, u_1, \Lambda, u_{N-1})$ is said to be expandable if for all values of $b_1, b_2, \dots, b_{N-1} \in \{0,1\}$

$$\begin{aligned}
0 &\leq v_0 - \left\lfloor \frac{\tilde{v}_1 + \tilde{v}_2 + \Lambda + \tilde{v}_{N-1}}{N} \right\rfloor \leq 255 \\
0 &\leq \tilde{v}_1 + v_0 - \left\lfloor \frac{\tilde{v}_1 + \tilde{v}_2 + \Lambda + \tilde{v}_{N-1}}{N} \right\rfloor \leq 255 \\
&\text{M} \\
0 &\leq \tilde{v}_{N-1} + v_0 - \left\lfloor \frac{\tilde{v}_1 + \tilde{v}_2 + \Lambda + \tilde{v}_{N-1}}{N} \right\rfloor \leq 255
\end{aligned} \tag{4}$$

5 where:

$$\begin{aligned}
v_0 &= \left\lfloor \frac{u_0 + u_1 + \Lambda + u_{N-1}}{N} \right\rfloor \\
\tilde{v}_1 &= 2 \times v_1 + b_1 \\
&\text{M} \\
\tilde{v}_{N-1} &= 2 \times v_{N-1} + b_{N-1}
\end{aligned} \tag{5}$$

Notice that each of $\tilde{v}_1, \tilde{v}_2, \dots, \tilde{v}_{N-1}$ is one-bit left shifted version of the original value $v_1, v_2, \dots, v_{N-1}$, respectively, but potentially with a different LSB (least significant bit). The conditions of equation (4), above, ensures that changing the LSBs of $v_1, v_2, \dots, v_{N-1}$ according

- 7 -

to equation (5) does not introduce an overflow or underflow in the values of $\tilde{u}_0$,

$\tilde{u}_1, \dots, \tilde{u}_{N-1}$ when the inverse transform is computed.

Definition 2: The vector $\mathbf{u} = (u_0, u_1, \Lambda, u_{N-1})$ is said to be changeable if, for all values of $b_1, b_2, \dots, b_{N-1} \in \{0,1\}$, $\tilde{v}_1, \tilde{v}_2, \dots, \tilde{v}_{N-1}$ given by equation (6), below, satisfy equation (4).

$$\begin{aligned} v_0 &= \left\lfloor \frac{u_0 + u_1 + \Lambda + u_{N-1}}{N} \right\rfloor \\ \tilde{v}_1 &= 2 \times \left\lfloor \frac{v_1}{2} \right\rfloor + b_1 \\ &\text{M} \\ \tilde{v}_{N-1} &= 2 \times \left\lfloor \frac{v_{N-1}}{2} \right\rfloor + b_{N-1} \end{aligned} \tag{6}$$

- 5 Notice that $\tilde{v}_1, \tilde{v}_2, \dots, \tilde{v}_{N-1}$ in the above equation are the same as the original $v_1, v_2, \dots, v_{N-1}$, but with different LSBs. Also, notice that a changeable vector remains changeable even after changing the LSBs of its $v_1, v_2, \dots, v_{N-1}$. Also, from definitions 1 and 2, it can be observed that an expandable vector is also changeable.

- 10 This approach can be extended to embed an auxiliary data value with multiple states by shifting or multiplying the difference value by more than one bit position or a number greater than 2, respectively, as discussed in the patent documents incorporated above. Further, it can be extended to values other than difference values, and data types other than images.

2.1 Another Integer Transform

- 15 In this section, we describe an integer-to-integer vector transform based on averages and differences that is unique and exactly reversible for any integer vector. The transform is computed through the use of matrix operations including an inverse, and the floor and ceiling functions that round down or up to the nearest integer respectively. We show that even though the floor and ceiling functions introduce a non-linearity, when used in conjunction, they provide uniqueness and reversibility. Although there are many other matrix structures that can form a basis for integer transforms, we will focus here on the matrix structure that implements a difference expansion method.
- 20

- Let D be a matrix that operates on an integer vector with the following 3 properties; (1) the matrix D is full rank, and the matrix-vector product results in (2) an average value of the integer vector, and (3) $N-1$ independent differences between vector elements. A weighted average where the weights sum to 1 is equally valid but will not be addressed in this document.
- 25

- 8 -

For example, if $N = 4$ and we reference all differences to the same (first) integer element, then one possible D is given by

$$D = \begin{bmatrix} \frac{1}{N} & \frac{1}{N} & \frac{1}{N} & \frac{1}{N} \\ -1 & 1 & 0 & 0 \\ -1 & 0 & 1 & 0 \\ -1 & 0 & 0 & 1 \end{bmatrix}.$$

Note that to satisfy the full rank and $N - 1$ difference properties, (1) there are exactly one $(-1, 1)$ pair in each row, and (2) each element of the integer vector is used to compute at least one difference.

The structure of the first column of D^{-1} can now be completely determined by noting that $DD^{-1} = I$, the identity matrix. In this particular case, the first column of the identity matrix, i.e., a 1 followed by $N - 1$ zeros, must be satisfied when D operates on the first column of D^{-1} . The inner product of the first row of D and the first column of D^{-1} must be 1, and the inner product of each of the $N - 1$ difference rows of D and the first column of D^{-1} must generate a zero. Therefore, each element of the first column of D^{-1} must be identical (to satisfy the element differences equal to zero) and the first column of D^{-1} must be a column of 1's (to satisfy the inner product of the first row of D and the first column of D^{-1} equal 1).

Next, let p be a vector of integer pixel values. Then the matrix-vector product, Dp , results in a vector that consists of the average, $\langle p \rangle$, and $N - 1$ integer differences. If we now examine the product, $D^{-1}Dp$, we can establish the identity for any given p_i as

$p_i = \langle p \rangle + (p_i - \langle p \rangle)$, where the first $\langle p \rangle$ comes from the first column of D^{-1} , and the bracketed expression comes from the remaining columns of D^{-1} .

Next, if we now apply the floor function (i.e., round down to nearest integer) to Dp to force integers, we get $D^{-1}\lfloor Dp \rfloor$, where $\lfloor \cdot \rfloor$ indicates the floor function. The identity for p_i now becomes: $p_i = \lfloor \langle p \rangle \rfloor + (p_i - \langle p \rangle) = p_i + (\lfloor \langle p \rangle \rfloor - \langle p \rangle)$, where $-1 < (\lfloor \langle p \rangle \rfloor - \langle p \rangle) \leq 0$. Therefore, for any vector p , we get the identity $p = \lceil D^{-1}\lfloor Dp \rfloor \rceil$, where $\lceil \cdot \rceil$ indicates the ceiling function (i.e. round up to nearest integer). In sum, this difference expansion transform, and its inverse, provide a more general form of equations 1 and 2, and can be used in place of equations 1 and 2 in implementations of a reversible watermarking method.

As discussed in prior patent documents incorporated above, there are other possible reversible integer to integer transforms that may be used to produce a set of expandable values for carrying embedded data. In addition, the embedder may apply a series of reversible integer

- 9 -

to integer transforms to the host data to produce a set of expandable values. The transforms applied in series may be recursive in the sense that a reversible transform is applied to the output of the previous iteration. In this case, the set of values produced by the last iteration of the transform is modified to embed auxiliary data, and then the transforms are reversed on the modified data in the reverse order of which they were applied. The transforms may also be many to one in the sense that the transform takes as input a vector of length N , and produces a set of potentially expandable values of $N-1$ or less.

To illustrate these options, consider the example where the generalized transform described in this section is applied recursively to the difference values, such that with each iteration, the absolute value of the difference values from the previous iteration are input to the next iteration of the reversible integer to integer transform. At the end of this series of transforms, the embedder has a set of potentially expandable values. The expandable values, x , are then modified (e.g., $2x + b$, where b is an auxiliary data bit) to carry bits from an auxiliary bit stream.

This particular approach has a number of potential advantages. First, the changes made to embed data in the output of the series of transforms translates into smaller changes to the original elements of the host data set. As such, in the case of images for example, the perceptual distortion is lower. This approach provides a way to distribute the error associated with embedding auxiliary data over a wider number of host data elements than might be achieved by applying only one iteration of the integer to integer transform. Thus, if an implementer wishes to optimize perceptual quality vs. auxiliary data capacity, the reversible integer to integer transform can be applied repeatedly to generate a smaller set of expandable values. This approach also enables the embedder to produce a set of expandable values through extra iterations of a reversible transform, where one or fewer iterations of the transform yield no or an insufficient number of expandable values.

3. Example Method for REVERSIBLE Watermark

Let $I(i, j, k)$ be an RGB image, and assume that:

1. the pixel values in the red component, $I(i, j, 0)$, are arranged into the set of $1 \times N$ vectors $U_R = \{\mathbf{u}_l^R, l = 1 \wedge L\}$ using the security key K_R
- 30 2. the pixel values in the green component, $I(i, j, 1)$, are arranged into the set of $1 \times N$ vectors $U_G = \{\mathbf{u}_n^G, n = 1 \wedge N\}$ using the security key K_G
3. the pixel values in the blue component, $I(i, j, 2)$, are arranged into the set of $1 \times N$ vectors $U_B = \{\mathbf{u}_p^B, p = 1 \wedge P\}$ using the security key K_B .

- 10 -

Although it is not necessary, usually all color components in the image have the same dimensions and are processed using the same difference transform. This makes the number of vectors in the sets U_R , U_G , and U_B to be the same (i.e., $L = N = P$). Let also the set

- $U = \{\mathbf{u}_r, r = 1 \wedge R\}$ represent any of the above set of vectors U_R , U_G , and U_B , and K represent its associated security key. Also, let $V = \{\mathbf{v}_r, r = 1 \wedge R\}$ be the transformation of V under the difference expansion transform $f(\cdot)$ (i.e. $V = f(U)$ and $U = f^{-1}(V)$). Also, let $\mathbf{u}_r = (u_0, u_1, \Lambda, u_{N-1})$ and its difference expansion transform be $\mathbf{v}_r = (v_0, v_1, \Lambda, v_{N-1})$.

- The vectors in U can now be classified into three groups according to the definitions given in Section (2), above. The first group, S_1 , contains all expandable vectors whose $v_1 \leq T_1$, $v_2 \leq T_2, \dots, v_{N-1} \leq T_{N-1}$, where $T_1, T_2, \dots, T_{N-1}$ are predefined thresholds. The second group, S_2 , contains all changeable vectors that are not in S_1 . The third group, S_3 , contains the rest of the vectors (not changeable). Also, let S_4 denote all changeable vectors (i.e., $S_4 = S_1 \cup S_2$).

- Let's now identify the vectors of S_1 using a binary location map, M , whose entries are 1s and 0s, where the 1 symbol indicates the S_1 vectors, and the 0 symbol indicates S_2 or S_3 vectors. Depending on how the vectors are formed, the location map can be 1- or 2-dimensional. For example, if vectors are formed from 2x2 adjacent pixels, the location map forms a binary image that has one-half the number of rows and one-half the number of columns as the original image. However, if a random key is used to identify the locations of the entries of each vector, then the location map is a binary stream of ones and zeros. The security key and an indexing table are needed in this case to map the zeros and ones in this stream to the actual locations in the image. Such a table is predefined and assumed to be known to both the embedder and the reader.

3.1. Embedding of Reversible Watermark

The embedding algorithm can be summarized using the following steps:

1. For every $U \in \{U_R, U_G, U_B\}$, do the following:
 - a. Form the set of vectors U from the image $I(i, j, k)$ using the security key K .
 - b. Calculate V using the difference expansion transform, $f(\cdot)$ (see equation (1)).
 - c. Use V , equations (5) and (6), and the conditions in equation (4) to divide U into the sets S_1 , S_2 , and S_3 .

- 11 -

- d. Form the location map, M ; then compress it using a lossless compression algorithm, such as JBIG or an arithmetic compression algorithm, to produce sub-bitstream B_1 .
Append a unique identifier, EOS, symbol to B_1 to identify its end.
- e. Extract the LSBs of $v_1, v_2, \dots, v_{N-1}$ of each vector in S_2 . Concatenate these bits to form
5 sub-bitstream B_2 .
- f. Assume the watermark to be embedded forms a sub-bitstream B_3 , and concatenate sub-bitstreams B_1, B_2 , and B_3 to form the bitstream B .
- g. Sequence through the member vectors of S_1 and S_2 as they occur in the image and through the bits of the bit-stream B in their natural order. For S_1 , expand the vectors as
10 described in equation (5). For S_2 , expand the vectors as in equation (6). The values of $b_1, b_2, \dots, b_{N-1}$ are taken sequentially from the bitstream.
- h. Calculate the inverse difference expansion transform of the resulting vectors using $f^{-1}(\cdot)$ (see equation (2)) to produce the watermarked S_1^w and S_2^w .
- i. Replace the pixel values in the image, $I(i, j, k)$, with the corresponding values from
15 the watermarked vectors in S_1^w and S_2^w to produce the watermarked image $I^w(i, j, k)$.

It should be noted here that the size of bitstream B must be less than or equal to $N-1$ times the size of the set S_4 . To meet this condition, the values of the threshold $T_1, T_2, \dots, T_{N-1}$ must be properly set. Also, it should be noted that the algorithm is not limited to RGB images. Using the RGB space in the previous discussion was merely for illustration purpose, and using
20 the algorithm with other type of spectral images is straightforward.

3.2. Reading Watermark and Restoring Original Image

To read the watermark and restore the original image, the following steps must be followed:

1. For every $U \in \{U_R, U_G, U_B\}$, do the following:
 - a. Form the set of vectors U from the image $I^w(i, j, k)$ using the security key K .
 - b. Calculate V using the difference expansion transform, $f(\cdot)$ (see equation (1)).
- 25

- 12 -

- c. Use V , equation (6), and the conditions in equation (4) to divide the vectors in T into the two sets $\hat{S}_4$ and S_3 . $\hat{S}_4$ has the same vectors as S_4 , which was constructed during embedding, but the values of the entities in each vector may be different. Similarly, S_3 is the same set constructed during embedding, since it contains non-changeable vectors.
- 5 d. Extract the LSBs of $\tilde{v}_1, \tilde{v}_2, \dots, \tilde{v}_{N-1}$ of each vector in $\hat{S}_4$, and concatenate them to form the bitstream B , which is identical to that formed during embedding.
- e. Identify the EOS symbol and extract sub-bitstream B_1 . Then, decompress B_1 to restore the location map M , and, hence, identify the member vectors of the set S_1 (expandable vectors). Collect these vectors into set $\hat{S}_1$.
- 10 f. Identify the member vectors of S_2 . They are the members of $\hat{S}_4$ who are not members of $\hat{S}_1$. Form the set $\hat{S}_2 = \hat{S}_4 - \hat{S}_1$.
- g. Sequence through the member vectors of $\hat{S}_1$ and $\hat{S}_2$ as they occur in the image and through the bits of the bit-stream B in their natural order after discarding the bits of B_1 . For $\hat{S}_1$, restore the original values of $v_1, v_2, \dots, v_{N-1}$ as follows:
- $$v_1 = \left\lfloor \frac{\tilde{v}_1}{2} \right\rfloor, \quad v_2 = \left\lfloor \frac{\tilde{v}_2}{2} \right\rfloor, \dots, v_{N-1} = \left\lfloor \frac{\tilde{v}_{N-1}}{2} \right\rfloor \quad (7)$$
- 15 For $\hat{S}_2$, restore the original values of $v_1, v_2, \dots, v_{N-1}$ according to equation (6). The values of $b_1, b_2, \dots, b_{N-1}$ are taken sequentially from the bitstream.
- h. Calculate the inverse difference expansion transform of the resulting vectors using $f^{-1}(\cdot)$ (see equation (2)) to restore the original S_1 and S_2 .
- i. Replace the pixel values in the image $I''(i, j, k)$ with the corresponding values from the restored vectors in S_1 and S_2 to restore the original image $I(i, j, k)$.
- 20 j. Discard all the bits in the bit-stream B , which were used to restore the original image. Form the sub-bitstream B_3 from the remaining bits. Read the payload and authenticate the image using the watermark contained in B_3 . For example, recomputed a hash of the restored image and compare this recomputed hash with a hash stored in the
- 25 embedded bit-stream.

4. Payload Size

To be able to embed data into the host image, the size of the bitstream B is less than or equal to $N-1$ times the size of the set S_4 . This means that

$$\|S_1\| + \|S_2\| = \frac{\|B_1\| + \|B_2\| + \|B_3\|}{N-1} \quad (8)$$

where $\|x\|$ indicates number of elements in x . But $\|B_2\| = (N-1)\|S_2\|$; hence, equation (8) can be reduced to

$$\|B_3\| = (N-1)\|S_1\| - \|B_1\| \quad (9)$$

For the case where $N=2$, the bit-stream size is $\|B_3\| = \|S_1\| - \|B_1\|$.

Equation (9), above, indicates that the size of the payload that can be embedded into a given images depends on the number of expandable vectors that can be selected for embedding and on how well their location map can be compressed.

- 10 With $w \times h$ host image, the algorithm would generate $\frac{w \times h}{N}$ vectors. Only a portion, α ($0 \leq \alpha \leq 1$), of these vectors can be selected for embedding; i.e., $\|S_1\| = \alpha \frac{w \times h}{N}$. Also, the algorithm would generate a binary map, M , containing $\frac{w \times h}{N}$ bits. This map can be losslessly compressed by a factor β ($0 \leq \beta \leq 1$). This means that $\|B_1\| = \beta \frac{w \times h}{N}$. Ignoring the unchangeable vectors (i.e., assuming $\|S_3\| = 0$) and using equation (9), the potential payload size (in bits) becomes,

$$\begin{aligned} \|B_3\| &= (N-1)\alpha \frac{w \times h}{N} - \beta \frac{w \times h}{N} \\ &= \left(\frac{N-1}{N}\alpha - \frac{1}{N}\beta \right) \times w \times h \end{aligned} \quad (10)$$

- 20 Equation (10), above, indicates that the algorithm is effective when N and the number of selected expandable vectors are reasonably large. In this case, it does not matter if the binary map, M , is difficult to compress (this is because its size is very small). But, when each vector is formed from N consecutive pixels (row- or column-wise) in the image, and N is large, the number of expandable vectors may substantially decrease; consequently, the values of the thresholds $T_1, T_2, \dots, T_{N-1}$ must be increased to maintain the same number of selected expandable vectors. This causes a decrease in the quality of the embedded image. Such a

- 14 -

decrease can be ignored by many applications, since the embedding process is reversible and the original image can be obtained at any time. In this case, the algorithm becomes more suitable for low signal-to-noise ratio (SNR) embedding than for high SNR embedding. To maximize $\|B_1\|$ for high SNR embedding, N must either be kept relatively small or each vector must be formed from adjacent pixels in two-dimensional area in the image. The quad ($N = 4$) structure given in the next section satisfies both requirements simultaneously.

- When $\alpha \leq \frac{\beta}{N-1}$, the payload size in equation (10) becomes negative. In this case, nothing can be embedded into the image. This scenario is less likely to happen with natural images. Most loss-less compression algorithms can achieve a 2:1 compression ratio (i.e., $\beta = \frac{1}{2}$). In this case, α must be greater than $\frac{1}{2(N-1)}$ to be able to embed a non-zero payload. This is can be easily satisfied when $N > 2$. For the case where $N = 2$, the payload size becomes

$$\|B_3\| = \left(\frac{\alpha}{2} - \frac{\beta}{2} \right) \times w \times h \quad (11)$$

Equation (11), above, suggests that the ratio of selected expandable pairs, α , has to be much higher than the achievable compression ratio, β , in order for this case to be effective.

- Since pairs of pixels are used as vectors, the correlation of the pixels in each pair is expected to be very high in natural images. This makes the pair easier to satisfy smaller thresholds, and, hence, to produce a large portion of selected expandable pairs. One approach is to apply the algorithm row-wise, then column-wise, in order to almost double the amount of data that can be embedded into the host image.

20 5. Rate Controller

- For a given vector size, N , the payload size that can be embedded into an image and the quality of the resulting image is solely determined by the host image itself and by the value of the thresholds used. However, many practical applications embed a fixed-size payload regardless of the nature of the host image. Hence, an automatic data-rate controller is necessary to adjust the value of the thresholds properly and to compensate for the effect of the host image. The iterative feedback system depicted in Fig. 2 can be used for this purpose.

Fig. 2 illustrates a control system with a feedback loop. This system attempts to minimize the distortion to the host signal for a desired payload size. A similar system may be used to maximize the payload size for a desired amount of perceptual distortion. Finally, a

- 15 -

system that satisfies both a perceptual distortion constraint can a auxiliary data capacity constraint may be made by constructing a control system that is a function of both constraints.

The control system fits the error signal to a function to modify the thresholds. The error signal may be the difference between the desired payload and the actual payload, or the
 5 desired perceptual quality and the actual perceptual quality. The perceptual quality may be measured using a measure of distortion between the original and host signal, including, for example, using human visual system models (e.g., the Watson metric as described in USP 5,629,780, a Just Noticeable Difference Metric such as the JNDMetrix™ Technology from Sarnoff Corp. and as described in USP 6,360,022, 6,285,797, 5,974,159, 5,719,966 and
 10 5,694,491), or human audibility system models (e.g., models used in audio compression such as MPEG coding AAC) in the case of embedding in audio. The perceptual model can be used to generate a mask that controls the amount of or sets a threshold for changes to values of the host data set. This mask can be computed as a function of the host data set alone, or as a function of the host data set and the host data set with auxiliary data embedded. With each iteration of
 15 embedding, the perceptual model can be applied to measure the perceptual quality of the embedded data set relative to a reference data set (such as the previous embedded version or the original host data). At each iteration, the perceptual model can also provide a mask for controlling the amount of changes to the host data set or value representing quality of the embedded data set for use in the control system.

20 If $T(n) = [T_1(n), T_2(n), \Lambda T_{N-1}(n)]$ is the thresholds vector at the n^{th} iteration, and C is the desired payload length, then the following proportional feedback controller can be used:

$$T(n) = T(n-1) - \lambda(C - \|B_3\|)T(n-1) \quad (12)$$

where $0 < \lambda < 1$ is a constant that controls the speed of convergence. $T(0)$ is a pre-set value that reflects the relative weights between the entities of the vector used in the difference expansion transform.

25 An alternative feedback controller is:

$$T'(n) = T'(n-1) - \lambda'(Q - q)T'(n-1) \quad (13)$$

Where Q represents the desired quality and q represents the current quality as measured by a perceptual quality metric. $T'(n) = [T'_1(n), T'_2(n), \Lambda T'_{N-1}(n)]$ is the thresholds vector at the n^{th} iteration.

30 There are at least two approaches for introducing a perceptual quality metric into these control system. One approach, for images, is to use the visual quality model to compute a perceptual model threshold map for the host image, and then use a table to map this perceptual model threshold map to the thresholds vector, using the mapped thresholds as a constraint for

- 16 -

the threshold vector used in the control system. Another approach is to introduce the perceptual model in λ where $\lambda(T, \Delta T, Q_{metric})$.

To combine the payload and perceptual quality constraints, the threshold vectors from equations (12) and (13) can be combined (e.g., through a weighting function that applies a
5 desired preference to capacity or quality) to form a single composite threshold vector.

6. Recursive and Cross-Spectral Embedding

Applying the algorithm recursively as in Fig. 3 can increase its hiding capacity. This is possible because the proposed watermark embedding is reversible, which means that the input image can be exactly recovered after embedding. However, the difference between the original
10 image and the embedded images increases with every application of the algorithm. At one point this difference becomes unacceptable for the intended application. Most applications, however, have a high tolerance to this error, since the original image can always be recovered exactly. To reduce the perceptibility of the error introduced by each layer, the embedder is implemented such that it distributes the error more evenly across the host signal to avoid a concentration of
15 error at particular locations, which might become perceptible.

One potential way to distribute the error when the algorithm is applied recursively is to use permutations of the entities of the input vector, which is depicted in Fig. 4. for quad vectors. The figure suggests four difference quad structures, each of which can be used in a different iteration for a total of four iterations. For $\mathbf{u}_0$, the difference expansion of equation (1)
20 is performed based on u_0 , so the closer u_0 is to u_1 , u_2 , and u_3 , the smaller the difference is, and, hence, the smaller the embedding error is. Similarly, for $\mathbf{u}_1$, $\mathbf{u}_2$, and $\mathbf{u}_3$, the difference expansion will be based on u_1 , u_2 , and u_3 , respectively. This allows the algorithm to completely exploit the correlation within a quad.

To hide even more data, the algorithm can be applied across spectral components after it is
25 applied independently to each color component. In this case, the vector $\mathbf{u}$ contains the color components (R, G, B) of each pixel arranged in a predefined order. This can be done either as cross-spectral triple $\mathbf{u} = (R, G, B)$ or as cross-spectral quad $\mathbf{u} = (R, G, G, B)$, or permutation thereof. For the cross-spectral quad arrangement, the integer difference expansion transform becomes:

- 17 -

$$v_0 = \left\lfloor \frac{R + 2G + B}{4} \right\rfloor$$

$$v_1 = R - G$$

$$v_2 = B - G$$
(14)

$$G = v_0 - \left\lfloor \frac{v_1 + v_2}{4} \right\rfloor$$

$$R = v_1 + G$$

$$B = v_2 + G$$
(15)

which is the reversible component transform proposed in JPEG2000 for color conversion from RGB to YUV.

Although, the spirit of the payload size analysis of section (4) applies to the cross-spectral vectors, the results need some modification. This is because only two bits are embedded per cross-spectral triplet or quad, rather than $N - 1$, and the number of vectors, in this case, equals the area of the location map, which equals the area of the original image. Hence,

$$\|B_3\| = 2\|S_1\| + \|B_1\|$$

$$\|B_3\| = (2\alpha - \beta) \times w \times h$$
(16)

We implemented the algorithm detailed above and tested it with spatial triplets, spatial quads, cross-color triplets, and cross-color quads with $a_0 = a_1 = \Lambda = a_{N-1} = 1$. In all cases, we used a random binary sequence derived from a uniformly distributed noise as a watermark signal. We tested the algorithm with the common 512x512 RGB test images: *Lena*, *Baboon*, and *Fruits*. We set $T_1 = T_2 = T_3$ in all experiments.

A spatial triplet is a 1x3 or 3x1 vector formed from three consecutive pixel values in the same color component row- or column-wise, respectively. We applied the algorithm recursively to each color component: first to the columns and then to the rows. The achievable embedding capacity depends on the nature of the image itself. Some images can bear more bits with lower distortion in the sense of PSNR than others. Images with a lot of low frequency contents and high correlation, like *Lena* and *Fruits*, produce more expandable triplets with lower distortion (in the PSNR sense) than high frequency images, such as *Baboon*, and, hence, can carry more watermark data at higher PSNR.

In general, the embedded images hardly can be distinguished from the original. However, a sharpening effect can be observed when the original and the embedded images are displayed alternatively. This effect is more noticeable at lower PSNR than at higher PSNR.

- 18 -

A spatial quad was assembled from 2x2 adjacent pixels in the same color component as shown in Fig. 4a. We applied the algorithm to each color component independently. Our experiments indicate that the achievable embedding capacity depends on the nature of the image itself. The algorithm performs with *Fruits* and *Lena* much better than *Baboon*, and it
5 performs slightly better with *Fruits* than with *Lena*. With *Fruits*, the algorithm is able to embed 867 kbits with image quality of 33.59 dB. It is also able to embed 321 kbits with high image quality of 43.58 dB. Nevertheless, with *Baboon* the algorithm is able to embed 802 kbits at 24.73 dB and 148 kbits at 36.6 dB.

In our experiments, we estimate that the achievable payload size for the spatial quad-
10 based algorithm is about 300,000 bits higher than for the spatial triplets-based algorithm at the same PSNR, and the PSNR is about 5 dB higher for spatial quad-based algorithm than for spatial triplet-based algorithm at the same payload size. Also, the spatial quad-based algorithm has finer control over the payload size and the PSNR than the spatial triplet-based algorithm. For example, it was possible to produce images at PSNRs in the 38 dB to 46 dB range with
15 spatial quad-based algorithm, but not with spatial triplet-based algorithm. This result is because 2x2 spatial quads have higher correlation than 1x3 spatial triplets and because the single location map used by the spatial quad-based algorithm is smaller than each of the two location maps used by the spatial triplet-based algorithm (one location map for each pass).

In general, the quality of the embedded images is better than that obtained by the
20 algorithm using spatial triplets. Also, the sharpening effect is less noticeable.

The cross-color triplets and quads were formed from the RGB values of each pixel, as described above. Our experiments show that the achievable payload size and the PSNR using cross-color vectors are much lower than those using spatial vectors. Hence, for a given PSNR level, we observed that it is better to use spatial vectors than cross-color vectors.

Our results show that the cross-color triplet-based algorithm has almost the same
25 performance as the cross-color quad-based algorithm with all test images except *Lena* at PSNR greater than 30. While the cross-color triplet-based algorithm was able to embed small payloads at these higher PSNRs, the cross-color quad-based algorithm was not. Upon closer inspection of the *Lena* image, we noticed that the blue channel of *Lena* is very close to the green channel.
30 Also, upon further inspection of the cross-color triplet-based and cross-color quad-based transforms, we noticed that when the red or blue channel is close in value to the green channel, the dynamic range of G after expansion according to equation (5) becomes wider for the cross-color quad-based transform than for the cross-color triplet-based transform. Hence, in this case, the cross-color triplet-based algorithm has the potential of producing more expandable vectors

- 19 -

and a location map of less entropy than the cross-color quad-based transform. And, indeed, this was the case with the *Lena* image.

Interleaving

- Another method for iteratively embedding multiple layers into a data set is called interleaving. This method interleaves selected pairings of data values on which to perform difference expansion. Here's an example for iterative embedding of layers into an image:
- [1] first layer: reversible watermarking on the horizontal pairing pattern with pixel coordinates $(i, 2*j-1)$ and $(i, 2*j)$
 - [2] second layer: reversible watermarking on the horizontal pairing pattern $(i, 2*j)$, $(i, 2*j+1)$
 - 10 [3] third layer: reversible watermarking on the vertical pairing pattern $(2*i-1, j)$, $(2*i, j)$
 - [4] fourth layer: reversible watermarking on the vertical pairing pattern $(2*i, j)$, $(2*i+1, j)$

In a prior approach, we performed multi-layer embedding as follows: layer[1] followed by layer[3], then layer[1], layer[3], and so on.

- 15 We experimented by comparing results of this and the prior approach on the Lena test image using the scalar difference expansion (pair of two pixels). Starting at about 40 dB, the interleaving approach proposed above gives a higher PSNR than the prior approach. Also the embedding capacity is increased from 2.0 bits/pixel to 2.5 bits/pixel.

- 20 This interleaving approach may be used in combination with the other multi-layer approaches discussed above. As detailed above, we have generalized the expansion method to apply to vectors of arbitrary length N . When the reversible watermarking method is applied iteratively to embed two or more layers, the positions of the elements of the vectors selected for each layer can be overlapped and/or interleaved in a variety of ways to obtain a desired embedding capacity and/or quality level.

25 **Program to Transform Data Files into Logical Storage Unit for Auxiliary Data**

- The reversible watermarking method, or other reversible watermarking method, may be implemented as a computer program that transforms a data file (or defined collection of files) into a data structure acting as storage for auxiliary data files. In particular, the program transforms a host data file, or a collection of files, into a logical storage unit, e.g., one that
- 30 appears as a hard disk through the interface of the program. This program may be designed to store a variety of files and data types in a host image, audio, video, text or object code file. In the case of perceptual data, such as audio, video, graphics, or images, the program retains perceptual quality of the audio, video, graphics or images stored in the host file to a desired level, and retains the format of the perceptual data. As such, standard applications used to view

- 20 -

or render output from the file can still be used to view or listen to the host data, notwithstanding the presence of embedded files in the host data.

For applications where the host data file carries codes whose meaning is changed due to the reversible watermark embedding, such as software code or text representations like
5 ASCII, the file can still retain its same format after embedding, yet the altered data is restored to its original, un-modified form before use.

For the sake of this discussion, we illustrate an example of the program particularly adapted for images, which transforms image files in a standard format like GIF or TIF into a file storage unit that retains the perceptual quality and file format of the host image through the
10 interface of the program. Though the use of the difference expansion method is not required, it has the advantage that it segregates an image into an average, which remains fixed, and expanded difference values, enabling the average part to provide thumbnail images that are identical to thumbnails generated from the original image. Users can view files that act as storage disks on their hard drives or some other storage location as if they have been
15 unmodified. In addition, the user gains the convenience that all of the functionality and data associated with files embedded in the host image are all in the same location of the host image. Thus, when the user finds a desired image on a computer system (e.g., using a typical file browser that is part of the operating system) and selects it for opening the file (e.g., double clicks on the file icon in the file browser window) all of the functionality and data associated
20 with the files embedded in that image are available automatically.

From the standpoint of file size, the reversible watermarking method typically makes the host image less compressible. However, the extra space needed to store a host file with embedded files is, at least in part, compensated by the space savings created by carrying other files within the host image. In addition, the host file may be subject to a lossy
25 compression/decompression process to maximize its embedding capacity for the particular reversible watermarking method. Examples of such lossy compression methods include wavelet based methods such as JPEG 2000. In the case of the difference expansion method of reversible watermarking, this pre-processing is designed to increase inter-pixel correlation in the image such that the inter-pixel differences are smaller, and thus, more expandable. The
30 auxiliary files to be embedded in the host image may be compressed as well before being inserted into the host image.

Fig. 5 is a diagram illustrating an example of a program used to transform a host image file into a storage unit. In this example, the program is implemented as an executable application program 500. It also may be implemented as a plug-in module, set of modules, or
35 library that is integrated or linked into another application program or operating system. In a

- 21 -

typical user installation, this application program resides on a computer system, which includes a processor 502, memory 504, persistent storage 506 (e.g., a hard disk), and other peripherals, such as a keyboard, cursor control device, display, printer, audio and video card, etc. The application program is installed in the persistent storage, and is loaded into computer memory
5 for execution by the processor. The application program operates in conjunction with an operating system 508, which provides basic computing services such as file browsing, process scheduling, file system, input/output services, graphical user interface, etc.

The application program preferably operates on image files 510 in a standard format, like TIF or GIF, so that other applications can make use of the files after embedding. These
10 image files are stored in persistent storage 506, and are loaded into memory for processing. The application program includes a number of functional component modules. Some of these components manage particular types of embedded data in the host data file. Below, we describe the component and the corresponding data in the host file that it manages.

Embedding, Reading, Restoring

15 The primary function of the program is to implement the reversible watermark embedding, reading, and original image restoring functions. We have detailed one reversible watermark method above that performs these functions, but others may be substituted.

The watermarking module 512 implements reversible watermarking functions. It operates in conjunction with the other code modules in the program to form an auxiliary bit
20 stream for embedding in the host data set. It also extracts the embedded data stream, and restores the host data to its original unmodified state.

Format "Image as Disk"

A formatting module 514 performs functions to prepare a host data file for embedding. These functions include:

- 25
- checking the auxiliary data carrying capacity (e.g., using rate control analyzer described above),
 - pre-compressing the image to increase data carrying capacity, and
 - partitioning the image into fixed or image dependent regions (e.g., based on image quality constraints, embedding capacity constraints, regions of interest to be
30 purposefully modified or left unmodified, etc.)

The partitioning enables the program to provide a form of randomly accessible storage locations within the host data set corresponding to regions in the host. Also, or alternatively, it enables localized control of embedding capacity and perceptual quality constraints, region by

- 22 -

region. This partitioning enables the different partitions to be formatted as different logical storage units or “folders” for entirely separate, and independently embedded auxiliary bit streams. Each partition can store different file or files and be accessed randomly and independently via different access control, such as different passwords and/or biometric data used to generate a key for decoding a reversible watermark from the particular partition that it pertains to. In the case where multiple reversible watermark layers are embedded, the last level embedded (also the first decoded) can be used to store the information on variable partitioning, enabling the program to extract the location of the partitions from the embedded reversible watermark layer, and then randomly access information from each partition. Of course, if the partitioning is fixed, either by using fixed patterns for partitioning the host data, or by using host data features that are expected to remain fixed, then the partitioning information need not be embedded.

Lossy and lossless compression utilities may also be included or may be provided separately to compress data files before embedding them in the host data file.

The formatting module also provides file system functions for managing the embedded data. The structure of the embedded files, including file names, sizes and location within the embedded bit stream are stored in the file structure 516. To save embedding capacity, the file structure can be implemented using delimiters in the embedded bit stream.

Display/Edit/Overlays

The display/editor module 518 controls display of the host signal (with or without embedded data), and other related images, such as thumbnails, overlays, etc. To display the original, unmodified host image, it invokes the reading and restoring components of the reversible watermarking module to reconstruct the original image. It also includes a graphical user interface for the program that depicts the host data in the host data file as a container for auxiliary data files stored in the reversible watermark.

Figs. 6-7 are diagrams illustrating an example of the graphical user interface 600. In this implementation, the program displays this interface 600 when a user selects (e.g., double clicks) on a graphical representation of a host data file 602 stored on the computer’s file system using the file browser of the operating system, or when the user selects the program using the operating system, and then selects a file open command on a host data file. At the same time, the program displays a view of the host image in a separate window 604 as shown in Fig. 6. Thus, by simply selecting a host file, the program automatically provides the user with an interface 600 for viewing/changing the embedded data files, as well as a host image viewer interface 604 for viewing the host data.

- 23 -

This user interface 600 enables the user to add or remove files from the container by dragging and dropping files to and from the window. When files are added or removed from the container, the program formats them for embedding in a reversible watermark layer, or layers, depending on user's instructions and available auxiliary data capacity per layer. When
5 the user has finished selecting auxiliary data for embedding and wishes to have the host data file, the program invokes the watermarking module to embed the auxiliary data. When the user wishes to extract auxiliary data, the program first prompts the user for applicable passwords, and then proceeds to extract at least a first layer including information about the embedded data files. It then displays them in a user interface window depicting the files stored within the host
10 data file such as the interface 600 shown in Fig. 6. The user can select individual files in this window (e.g., with a mouse), and in response, the watermarking module extracts these files and invokes any associated functionality.

For example, when the user selects an overlay in the interface 600, the program automatically gets the overlay from the embedded data (which may have been previously
15 extracted upon file opening), superimposes it over the host image, and displays the result as shown in Fig. 7. The graphical representations of the overlay files 606, 608 may be shown as simple file icons representing a generic overlay, or as thumbnail images of the specific overlay graphic in the overlay file (e.g., low resolution versions of the overlay graphic). As shown in Fig. 7, the overlay highlights a region of the host image in this example. It also has associated
20 links (e.g., to another website or to related information) that the user may select to activate a browser and fetch the linked web page at the URL stored in the link file embedded in the host image.

It also manages other display functions such as superimposing related overlay images, such as overlay images that are embedded in the host image. The display component automates
25 overlays rather than requiring the user to piece them together from disparate files stored separately. When the user opens the image for viewing, an option window informs the user that the image has overlays. The user can then select the overlays, and in response, the display component superimposes them onto the display of the host image.

Another related feature is visible change detection, where changes made by a particular
30 user are highlighted on the image in the region where the change occurred. These change markings may be implemented as an overlay image (stored either as a compressed bitmap or vector graphic including coordinates where the changes occurred). These change markings can also be cross-referenced with tracking data described below to track who made the changes, when the changes were made, and where the changes were made.

- 24 -

Another related feature is the use of other graphical structures or image overlays to introduce interactivity or animation in the image. Consider the case where the host image represents a business card, company brochure, product diagram, instruction manual, installation manual, or other marketing document. In this case, the display component activates and
5 superimposes the display of embedded graphics files or overlays to create animated effects, provide additional information related to parts of the document, etc.

Another related feature is enabling image editing. This component allows the user to make changes, add text annotations or graphical markings and overlays, rotate, crop, scale or otherwise enhance the image. It works in conjunction with the watermarking module to update
10 the host image and then embed or re-embed related files.

The overlay data and other related graphics and change markings are stored in overlay structures 520 embedded in the host data set.

Tracking

A tracking module 522 creates tracking data 524 representing information tracking the
15 origin, distribution history and change history of the host data, and optionally, the history of changes to embedded data added by users of the host data. This tracking data may be separate from or combined with other embedded data in one or more embedded data files.

The tracking data 524 includes information identifying:

- processes applied to the host image;
- 20 • name or device identifier of user or device that has seen the image;
- history of distribution, including who has received/processed the image, and what has been done to the image.

The tracking module also provides a graphical user interface for displaying the tracking data for authorized users.

Linking

The linking module 526 provides a mechanism for activating links to related data. This may be implemented using browser software to fetch files from the computer, network or Internet. The links may be pointers to files, hyperlinks, URLs, etc. compatible with known object and hyper-linking software. These links are stored in linking data 528 and form part of
30 the embedded bit stream. The targets of these links may be files embedded in the image, or files stored elsewhere on the computer system or network.

The linking module also operates in conjunction with the display module to associate active links with highlighted regions and/or overlays in the image. For example, if the user

- 25 -

clicks on a highlighted building portrayed in the image, the display module communicates the coordinates of the selected location to the linking module, which in turn fetches the linked information, such as a text, image or audio file providing related information for a particular semantic object within the host image. This feature enables users of the image to add links and
5 annotations to objects of interest depicted in the host image.

Distribution and Control

A distribution and control module 530 manages rules associated with distribution and control of the host image. These rules are stored in distribution and control data 532 and
10 embedded in the host image.

The rules define directions for distribution for the host data file. For example, they may include automated instructions for e-mail distribution of the host data file. The distribution and control module reads these instructions and schedules the delivery and any appropriate follow up tasks of the host file. This may be implemented by interfacing the
15 distribution module with available e-mail and scheduling software, such as Microsoft Outlook ® and Microsoft Exchange ®, for example.

The rules may also include a check list of individuals who must review the host data, which gets updated as each person on the list completes his or her review.

The rules may also include an auto-destruct rule that destroys the file after a
20 predetermined event has been detected. This event may be, in part, based on a predetermined time or date as measured relative to a system clock. It may be triggered when review is complete. It also may be location or device dependent, where the image is destroyed if an attempt is made to open the file on an unauthorized system, in an unauthorized location, by an unauthorized person or application program.

25 The control information may also include rendering control information. For images, this rendering control information includes information to control printing and/or display. The printing control may include a variety of instructions and parameters for controlling printing on different types of printers. Examples of the information include Page Description Language (PDL) instructions. For instance, formatting and control information typically stored in a PDF
30 file separate from image data in the file may be embedded in the image data using the reversible watermarking application program.

The control information may also include instructions for embedding a robust watermark, such as described in 09/503,881 or other robust watermark, in the rendered output. Such a robust watermark may be used to identify the source device or user that rendered the

- 26 -

host data (e.g., for forensic tracing of the output to a particular device or user), to identify the rendered output through an object identifier persistently embedded in the rendered output, to persistently link the rendered output to metadata, including an electronic version of the host data, etc.

5 The control information may also include instructions that govern when copies of the host file can be made, as well as circumstances under which the host file can be transferred to another device.

 Similar control information can be reversibly embedded in other media types like audio, video, and text. In the case of text, the reversible watermark can carry instructions for
10 embedding a robust text or image watermark in the rendered text document.

Security

 A security module 534 controls access to the host image as well as the auxiliary data embedded in it. This module operates in conjunction with other modules, such as the display and watermarking modules, to control access to the host image and embedded data. It provides
15 an interface for determining the user's permission status, and enabling certain functions of the program, such as display, embedding and reading, based on that status.

 The program can also be used to provide different levels of quality of the image with access to each level controlled based on the user's permission status. The security module manages this access by determining the permission status, and enabling display of selected
20 parts of the image or selected levels of quality associated with the permission status. Levels of quality can be controlled by providing different levels of spatial resolution, or levels with varying amounts of perceptual distortion (e.g., distortion introduced by the reversible watermark, or some other noise source). Opaque overlays, embedded in the image, may be used to block or redact sensitive portions of a host image or document depending on permission
25 level.

 As described above, an image (or other host data set) can be recursively embedded with layers of reversible watermarks. In this case, each additional reversible watermark layer is embedded in a host data set that has been previously embedded with a reversible watermark by operating on values that have been modified by previous layers. As such, the process of
30 extracting each layer and restoring the host data set operates in reverse order of the order in which the layers were embedded.

 There are a number of ramifications of this approach. An image that serves as a logical storage unit (e.g., image as disk) for files in a first watermark layer can be used as a new disk for storing additional files in a second or subsequent reversible watermark layer. In order to

- 27 -

extract files in the first layer, the files in the second layer are extracted and the image is restored to the state that it was in immediately after embedding the first layer. Each layer can store different auxiliary data, enabling a variety of different features or applications. The embedding of several layers in this manner can act as a method for progressively controlling the quality of the host data, where each layer progressively degrades quality such that with the extraction and restoration of the data set for each layer, the quality is improved.

The layers provide a method of access control for the auxiliary data. Each layer can be embedded with a different key used to extract and/or de-scramble a layer. Thus, in addition to extracting the layers in the correct order, one also needs the layer key to extract each layer. This enables the program to control access to the auxiliary data for each layer, as well as control access to higher quality versions of the host data, in the case where the layers are used to progressively control quality of the host data. To control access, the program may include an access control table that receives user identification, such as a user password or even biometric information (such as a facial image, fingerprint, voice print, iris or retinal scan, etc.) and generates the appropriate key or keys enabling that user to decode one or more reversible watermark layers.

The program may also be used to detect whether the host data has been altered. In the case of reversible watermarking by difference expansion, alteration can be detected based on the inability to perfectly restore the image, or based on comparing an embedded hash of the original image with a hash of the re-constructed image. This alteration detection may be localized to regions if the host image is partitioned into separate regions. In some applications, compressed versions of image blocks in the host image may be embedded in other blocks, enabling tampered portions to be restored by replacing them with the compressed version.

The security module may also be used to manage keys used to encrypt or scramble parts of the embedded bit stream, or scramble the location of the embedded data. These keys as well as other security data, such as access permissions, may be stored in security data 536 embedded in the host data set.

Visual Search

A visual search module 538 is used to facilitate searching for contents of host files based on descriptive material of the host content. This module provides descriptive data, such as text or descriptive graphics (e.g., icons) that describe what is depicted in the host image. This descriptive data is stored in visual search data 540 embedded in the host image. It can be used to facilitate automated searching, or manual "visual" searching.

- 28 -

In content database applications, it is advantageous to provide efficient mechanisms for searching a large collection of host data files. This can be achieved by using the descriptive data to form a searchable index of descriptive text or images that describe contents of corresponding host data files. One particular way to form the index is by creating a hierarchical structure of the descriptive data of the images in the collection based on content descriptors. These content descriptors may include names or graphical icons representing objects in the images, descriptors of regions of interest, geographic location, etc.

When the database finds images whose descriptive data matches with items in a search query, the thumbnails of the images can be displayed, along with the graphical descriptors of the file contents extracted from the embedded bit stream, enabling a user to view the search results graphically and quickly pick images that he or she is looking for.

Robust Watermark Parameters

The program may also be used to store parameters of any robust watermarks embedded in the host data. One application of robust watermarks for images is to include auxiliary embedded data in a robust watermark that survives digital to analog conversion, such as printing of the image. Methods for embedding robust watermarks in images that survive print are described in 09/503,881 and 6,122,403, incorporated above. These robust watermarks survive one or more generations of printing and re-scanning, and are automatically read from digital images scanned from printed images. This type of robust digital watermark is useful for forensic tracking to trace a printed image to a source device or user that printed the image.

It is also useful for persistent identification and linking back to an electronic version of the image in a database. For example, if a printed document is passed to another user, who wishes to see the original version, its history, etc., the user scans the document, extracts the robust watermark providing a pointer to the digital version, and fetches the digital version. This digital version has all of the features provided by the reversible watermark embedding.

It is also useful for device control, such as an embedded control instruction that blocks reproduction on devices enabled with watermark detectors. The message carried in a robust watermark may include identifiers, such as content identifier, source identifiers, device identifiers, etc., metadata or pointers to metadata stored in a database, and instructions.

The robust watermark parameters include information used to remove the robust watermark in the event that the host image has not been altered. For example, these parameters may include a key or a pointer to a key stored elsewhere that is used to generate a set of difference values that may be added to the host image to perfectly remove changes due to the

- 29 -

robust watermark. Alternatively, the parameters may include a compressed version of the actual difference values needed to perfectly restore the original image. For more information on methods to make a robust, reversible watermark, see U.S. Application 10/319,380 incorporated above.

5

Uses for the "Image as Disk" Program

There are a number of uses for the program, including digital asset management, security, content database searching, medical record management, promotional materials and documentation, document management, and photography.

10 Organizations with collections of documents, images and other embeddable files can use the program for tracking files. The program can also be used to enhance productivity of groups that work on documents, images, etc. by providing overlay capability for graphical annotations, links to related information and analyst annotations, and the capability to embed related data into the host data itself.

15 For sensitive files, the program enables multilevel security, controlling access to varying levels of quality of the host data set, as well as varying amounts of information embedded into or associated with the host data set via the reversible watermark.

As noted in the visual search section above, the program facilitates efficient, content-based searching through a database representing a collection of images, documents, etc.

20 In medical applications, the program provides an effective tool for storing and managing patient records by enabling the related records to be encapsulated within a medical image file or set of images. The host medical image (e.g., X-ray, patient photo, CAT scan, etc.) serves as a storage unit for related diagnosis with x-rays, patient photos, etc. In addition, the program provides access control to sensitive records stored within embedded image files. Also,
25 the medical service provider can add annotations to the medical record that travel with the medical imagery that those annotations pertain to. These annotations can include links to information about related diseases, treatments, test data, etc. Embedded overlays may be used to highlight regions of interest in a medical image, such as a tumor, broken bone, or blocked artery. Color coded overlays may be used to highlight different body parts or regions of
30 interest.

Businesses can use the program to provide asset management for documents and images. The above example implementation is adapted to images, and therefore, can be applied to documents rendered as images, such as PDF files or other Page Description Language files that include images. Alternatively, reversible watermarking may be applied to text

- 30 -

representations, such as ASCII text, for example, where the numbers representing ASCII text characters are modified to carry auxiliary data.

As noted above, documents such as brochures, manuals, and electronic business cards can be created and made interactive using the program. For example, a host image representing a document can be reversibly embedded with links, additional information, pictures, graphical overlays, animation, etc. When the user selects the file of the host document, the program opens the file and displays the document, along with selectable options for getting the embedded data or activated embedded links. Searching through collections of such documents can be facilitated using the search tools described above.

10 This feature also enables a single file to represent many different versions of a single document. At the time of rendering for display or printing, the user can select which version he or she wants to view or print. Versions of an image or document with or without changes applied, or with or without overlays can be selected and printed.

The program also has a number of uses in photography. A photograph may serve as a host data set in which other related data is reversibly embedded and conveniently stored along with the host data. For example, the user can reversibly embed a variety of compressed files into the host photograph, including, for example, a compressed picture of photographer, as well as contact information for the photographer and metadata relating to the photograph. The photographer can distribute a degraded quality image with a key to access a higher quality version of that image to authorized users. In addition, the photographer can include audio tracks within the image by embedding compressed audio clips in the image.

25 These uses can also be extended to other media types, including audio and video files. Frames of video can include related information, such as accompanying audio track and audio-video track synchronization information. Different language audio tracks can be distributed with movies using reversible embedding to carry multiple compressed audiotracks. Audio files, similarly, can include song lyrics, links to related information (fan websites) and e-commerce sites to buy related products and services. The reversible watermark can be used to provide progressive levels of quality, which are accessible by removing layers of the reversible watermark.

30 Various versions of a movie, music track or image can be distributed as a single file with embedded data that controls which version to render. For example, a movie with content unsuitable for children can include embedded control flags, and even alternative scenes that are swapped into the movie depending on the age or tastes of the consumer.

Software Features and Integration with other Software

While the above discussion describes an application program, the program and related functions may be implemented as part of another program. One such example is compression utility program, such as PKZip ® from PKWare, Inc. The compression and security features of such a program can be combined with reversible watermarking services to create a program that implements some of the functions described above. In such an application, the host data file, such as TIF or GIF image retains its image format, yet serves as a container for other files embedded in it using the reversible watermarking module. The user interface of the program, in this example, includes a window that represents the host data as a container for other files, which can be added or removed from the container by dragging and dropping the files' icons into the window. Double clicking the file icon of a host file automatically enables all of the features provided by the embedded data including:

- a window, drop down menu, or other graphical user interface (GUI) displaying list of overlays, which, when selected are superimposed on the host image.
- a GUI for multilevel security access control to different levels of detail or parts of the host image and related embedded data; this GUI enables entry of user log-on data (e.g., user name and password), and manages secure log-on table to control access to contents of host image, progressive levels of quality, and embedded data;
- a GUI displaying tracking information, and corresponding software for capturing tracking information each time host data is moved, opened, edited, etc.
- a GUI, e.g., pop up windows for embedded links; and
- software initiation of related programs, e.g., through software object automation, scripts, or Java that is triggered in response to opening the host image or selecting certain features enabled by the embedded data. Examples of automatic program activation include activating a file browser to get linked information, an image editor for editing host or embedded images, word processor for text annotation, media player for playing embedded audio clips, e-mail program for distribution of host file according to embedded distribution rules, etc.

Since the capacity of a host data file will vary, the program can also be designed to expand the host file size to create additional capacity, and format the extra space in the host file to carry compressed auxiliary data. This additional capacity can be provided in a manner that

- 32 -

does not change the basic format of the host image file. For example, in an image file, the compressed data stored in the extra space may appear as a colorful region at the bottom of the image when displayed by a standard image viewer.

As described above, there are a variety of uses of a software program and related system for placing a structure of files within host media in a host file. Information, software code (e.g., application programs, scripts, web pages), encryption keys, etc. can be covertly stored within host media files on the computer system to protect sensitive data or thwart hacking. Often, encryption keys can be discovered by a hacker within an application program file or other file by searching the binary data for key-like characteristics. This type of key discovery is more difficult or impossible if the key were stored inside a digital watermark in an image or other host media signal. Likewise, a hacker or virus may attach malicious code to an executable file or library. This too would be prevented if the executable were hidden inside an image or other host media signal.

The technology for reversibly embedding files in other files can also be very useful when the data is to be passed to remote users, either via network downloads or removable media shipments. In the case where an image is to be sent along with descriptive analysis, it is often the analysis and annotation that is more sensitive than the image itself. Hiding the sensitive files within a host image or other media signal can prevent both interception and interpretation of the sensitive data, as well as preventing separation of the descriptive analysis from the image. Combining this with the described methods for controlled image degradation can allow sensitive images and annotations to be passed to authorized users over an unsecured channel without danger of the sensitive value being discovered by an interceptor. In other cases, the data may not be sensitive, but using this method can ensure that the data is not separated during transmission, while also providing the ease of a single file download or transfer.

In the case of image overlays stored in the reversible watermark, the overlays could, in fact, be small images that replace certain portions of the host image. This technique could be used to highlight areas where a change has occurred; for example, in the case of satellite imagery, displaying before and after images for damage assessment, natural disaster, traffic flow, crop management, urban sprawl, etc.

In medical images, the technology can be used to assist in compliance with HIPAA (and other future related acts). By hiding sensitive user data in the image, the data can be properly protected so that only appropriate data can be accessed by viewers of the data depending on their need and authorization as defined in HIPAA. Data with different levels of

- 33 -

sensitivity can be embedded in the medical image in separate layers of the reversible watermark or randomly accessible reversible watermarks, each having their own decoding keys to restrict access to particular users, devices or systems. In this case, the program performs key management in the security module to control and facilitate restricted access to various parts of the embedded data.

Above, we discussed that the reversible watermark may be used to create animation rendered along with the host data. Embedded images or movies could be automatically initiated either by an event, such as opening the image, detecting the mouse cursor has passed over the image or a particular location in the image, or some other event. For example, when the user clicks on the image's file icon (selects "file open command" or otherwise selects the file), the reversible watermark application program is associated with the file such that the program is automatically launched by the operating system, and the program automatically extracts the reversible watermark, including any animation or graphic files, and displays the animation in conjunction with the display of the host data. As another example, the program displays the image in the host file, and when the user passes the cursor over an item of interest in the displayed image, or selects a feature, the program launches the animation extracted from the reversible watermark (or linked to the host file via a link embedded in the reversible watermark) that is uniquely associated with that location, feature or item in the image. The animation or link to animation stored elsewhere may be extracted previously from the reversible watermark, or automatically extracted upon an event, such as the cursor passing over or selecting an item of interest depicted in the image.

Object Code Applications

In U.S. Application 10/319,404, we discussed how reversible watermarking may be used to reversibly embed auxiliary data in software code. Here, we elaborate on that application further.

The reversible watermark embedder can embed auxiliary information in an object code file using reversible watermarking to alter code data values in the file. One approach is to use the reversible watermarking scheme described above using difference expansion of correlated pairs of bytes, where the bytes of data being altered are not image pixel data, but bytes of code. In this particular case, the correlation may be less than in images, leading to lesser embedding capacity. However, for many applications, the data carrying capacity need not be as great.

One example application for reversible watermarking of object code is forensic tracking. In particular, the embedded bit stream includes user or machine information for forensic tracking purposes. The auxiliary bit stream can be embedded in segments of code

- 34 -

when the program was installed. In addition, some code could be embedded with a global identifier or key while other parts could be embedded with auxiliary data customized by the user.

5 This forensic tracking application applies to multimedia content distribution, where files distributed or copied by a user are tagged with that user's ID. This can be used to combat piracy in electronic file delivery and sharing systems, including peer to peer file sharing systems.

10 The embedder can use the user's public key to encrypt the watermark so that only that user's private key would allow decoding of the embedded information, restoration of the original code, and then execution of the un-modified code. While one might alternatively encrypt the code to prevent access to the original executable code, encryption does not have the benefit of being able to include auxiliary data in the software code itself.

15 The object code to be reversibly watermarked could be treated specially and loaded by an application program or operating system equipped with a detector of watermarked code fragments. In this case, the program or operating system retrieves the watermark key in order to decode the watermark and restore the original un-modified code before executing it. As part of the decoding process, the program or operating system verifies that the payload of the watermark matches other user or machine information before enabling execution of the code.

20 The reversible embedder can also hide additional object code or software documentation within the reversible watermark of the target object code.

Examples of Novel Features

Examples of novel and inventive features described in this document include:

25 A1. A tangible medium on which is stored software for transforming a host data file carrying host media data into a logical storage unit for storing auxiliary data files in a reversible watermark embedded into the host media data, the medium including:

30 a watermarking module for modifying original values of host media data elements in the host data file to embed a reversible watermark carrying auxiliary data files, the reversible watermark enabling the host media data elements to be restored to the original values; and

a user interface module for representing the host data files as a container for the auxiliary data files, and enables the adding or removing of auxiliary data files from the reversible watermark.

- 35 -

A2. The medium of feature A1 wherein the reversible watermark includes a file structure identifying the auxiliary data files stored in the reversible watermark.

5 A3. The medium of feature A1 including:
a formatting module for determining auxiliary data carrying capacity of the host media data.

10 A4. The medium of feature A3 wherein the formatting module includes a rate controller for maximizing embedding capacity for a desired perceptual distortion.

A5. The medium of feature A3 wherein the formatting module includes a compressor for maximizing auxiliary data carrying capacity of the host media data elements after compression.

15 A6. The medium of feature A1 wherein the host media data comprises a host image, and the software transforms the host image into a logical storage device for storing the auxiliary data files in the image.

20 A7. The medium of feature A6 wherein at least one of the auxiliary data files comprises an image overlay file, and the software is operable to extract an image overlay file from the reversible watermark, and display an image overlay stored in the image overlay file superimposed on the host image.

25 A8. The medium of feature A7 wherein the overlay file is associated with one or more links and the software enables the user to activate the one or more links to get additional information related to the overlay.

30 A9. The medium of feature A1 wherein at least one of the auxiliary data files includes one or more links to additional information related to the host media data, and the software enables the user to activate the one or more links to get additional information related to the host media data.

35 A10. The medium of feature A1 further including a tracking module for obtaining and storing tracking data in the reversible watermark indicating identifiers of individuals or devices that have received or opened the host media data file.

- 36 -

A11. The medium of feature A1 further including a distribution control module for managing and storing distribution control information in the reversible watermark, the distribution control information controlling distribution of the host media data file.

5

A12. The medium of feature A1 wherein the host media data comprises an audio file, and the software transforms audio data in the file into a logical storage device for storing the auxiliary data files in the audio data.

10

A13. The medium of feature A1 wherein the reversible watermark is embedded in two or more layers, each of the layers being embedded iteratively in the host media data, wherein the host media data file embedded with a first layer is input to a subsequent reversible embedding process to embed a second layer.

15

A14. The medium of feature A13 including a security module for controlling access to the two or more layers.

20

A15. The medium of feature A13 wherein the layers are extracted in reverse order, and as each layer is extracted, the changes made to the host media data to embed the layer are reversed such that successive extraction and restoration of all of the layers enables perfect reconstruction of the original host media data file.

25

A16. The medium of feature A13 wherein the layers add distortion to the host media data and enable progressive perceptual quality control of the host media data by enabling reversal of changes made to embed each layer through successive reversal of the layers in reverse order of embedding.

30

A17. The medium of feature A13 wherein a separate key is used to embed each layer and enables selective control over access to each embedded layer of the reversible watermark.

A18. The medium of feature A1 including software for partitioning the host media data into partitions that store randomly accessible reversible watermarks embedded in the partitions.

- 37 -

A19. The medium of feature A1 wherein the reversible watermark includes rendering control information for controlling rendering of the host media data.

5 A20. The medium of feature A19 wherein the host media data includes an image and the rendering control information includes information for controlling printing of the image.

A21. The medium of feature A1 wherein the reversible watermark includes visual search information used to facilitate visual searching of the host media data file.

10 A22. The medium of feature A1 wherein the host media data comprises a medical image, and the reversible watermark includes information identifying a region of interest in the medical image.

15 A23. The medium of feature A1 wherein the host media data comprises a medical image, and the reversible watermark includes a medical record corresponding to the medical image.

A24. A method of reversibly embedding forensic tracking information in a host data comprising:
20 obtaining forensic tracking information used to track the host data to a particular device or user;
modifying original values in the data file to embed a reversible watermark that carries auxiliary forensic tracking information in the host data file; wherein the reversible watermark enables the original values to be perfectly restored by extracting the reversible watermark and
25 inverting modifications made to embed the reversible watermark.

A25. The method of feature A24 wherein the host data comprises object code.

30 A26. The method of feature A24 wherein the reversible watermark is embedded using a key associated with a particular device or user.

A27. The method of feature A26 wherein the key comprises is one of a public – private key pair.

- 38 -

A28. The method of feature A24 wherein the host data includes object code and the reversible watermark is embedded into at least one segment of the object code when the object code is installed.

- 5 A29. The method of feature A28 wherein the reversible watermark is used to control execution of the object code.

Concluding Remarks

- 10 Having described and illustrated the principles of the technology with reference to specific implementations, it will be recognized that the technology can be implemented in many other, different, forms. To provide a comprehensive disclosure without unduly lengthening the specification, applicants incorporate by reference the patents and patent applications referenced above.

- 15 The methods, processes, and systems described above may be implemented in hardware, software or a combination of hardware and software. For example, the auxiliary data encoding processes may be implemented in a programmable computer or a special purpose digital circuit. Similarly, auxiliary data decoding may be implemented in software, firmware, hardware, or combinations of software, firmware and hardware. The methods and processes
20 described above may be implemented in programs executed from a system's memory (a computer readable medium, such as an electronic, optical or magnetic storage device).

- The particular combinations of elements and features in the above-detailed embodiments are exemplary only; the interchanging and substitution of these teachings with other teachings in this and the incorporated-by-reference patents/applications are also
25 contemplated.

- 39 -

We claim:

1. A method for performing reversible watermarking to embed auxiliary data in an original data set, the method comprising:
 - 5 reversibly embedding the auxiliary data into the original data set by expanding values in the original data set that distorts the values, yet enables the values to be perfectly re-constructed; and
 - applying rate control to determine how to expand the values to minimize distortion for a desired auxiliary data carrying capacity or to maximize data carrying capacity for a desired
 - 10 distortion.
2. The method of claim 1 wherein the expanding is performed on difference values.
3. The method of claim 1 wherein the expanding includes multiplying a value by a
- 15 number and adding auxiliary data to the multiplied value.
4. The method of claim 3 wherein the multiplying and adding are performed so as to avoid an overflow or underflow of the value.
- 20 5. The method of claim 1 wherein the rate control includes fitting an error function.
6. The method of claim 1 wherein the rate control is applied iteratively using a feedback loop.
- 25 7. A computer readable medium on which is stored software for performing the method of claim 1.
8. The method of claim 1 wherein the auxiliary data is embedded iteratively in layers.
- 30 9. The method of claim 8 wherein each layer expands difference values between pairs of elements, and the pairs of elements for each layer are chosen such that the pairs interleave.
10. A method for performing reversible watermarking to embed auxiliary data in an original data set, the method comprising:
 - 35 selecting sets of elements in the original data set for expansion; and

- 40 -

reversibly embedding the auxiliary data into the original data set by expanding values associated with the selected sets in a manner that distorts the values, yet enables the values to be perfectly re-constructed;

5 wherein the reversible watermarking is performed iteratively in layers, and for the layers, interleaving sets of elements are selected for expansion in successive layers.

11. The method of claim 10 wherein the original data set comprises an image and the interleaving sets of elements includes selecting a pattern of horizontal and vertical pairs across successive layers.

10

12. The method of claim 10 wherein sets selected for expansion in successive layers overlap according to a pattern, the pattern is not in the same position in successive layers, and the pattern is selected so as to increase embedding capacity for a desired quality level.

15 13. A computer readable medium on which is stored software for performing the method of claim 10.

14. A method for performing reversible watermarking to embed auxiliary data in an original data set, the method comprising:

20 reversibly embedding the auxiliary data into the original data set by expanding values in the original data set that distorts the values, yet enables the values to be perfectly re-constructed; and

25 applying a perceptual model to determine how to expand the values to minimize distortion for a desired auxiliary data carrying capacity or to maximize data carrying capacity for a desired perceptual distortion.

15. The method of claim 14 wherein the perceptual model used in a feedback control loop.

30 16. The method of claim 15 wherein the perceptual model is used to control thresholds, which control the expanding of values in the original data set.

17. The method of claim 14 wherein the perceptual model is computed as a function of the host data set and an instance of the host data set embedded with the auxiliary data.

35

- 41 -

18. The method of claim 17 wherein the perceptual model is applied iteratively for different instances of the host data set embedded with the auxiliary data.

19. A computer readable medium on which is stored software for performing the
5 method of claim 14.

20. A method for watermarking a data set comprising:
applying a vector difference transform to vectors in the data set, wherein the vector
difference transform transforms selected sets of values in a corresponding vector into difference
10 values; and
modifying the difference values to embed auxiliary data into the data set; and
applying an inverse vector difference transform to the modified vectors to produce a
watermarked data set.

15 21. The method of claim 20 wherein the vector difference transform comprises a
reversible integer to integer transform that enables perfect reconstruction of the data set after
watermark extraction.

22. The method of claim 20 wherein the vector difference transform enables
20 differences to be generated from an arbitrary selection of elements of the vectors.

23. The method of claim 22 wherein the vector difference transform enables
transformation of vectors of arbitrary length into differences.

25 24. A computer readable medium on which is stored instructions for performing the
method of claim 20.

25. The method of claim 20 wherein the vector difference transform is applied
recursively to a vector in the data set to generate difference values to be modified to carry
30 auxiliary data.

26. A method for reversible watermarking of a host data set, the method comprising:
applying a series of two or more reversible, integer to integer transforms of values in
the data set to produce a set of modifiable values for carrying a reversible watermark;

- 42 -

modifying the modifiable values to embed the reversible watermark in the host data to produce watermarked transformed values; and

computing an inverse of the two more reversible transforms in the series on the watermarked transformed values to produce a watermarked host data set.

5

27. The method of claim 26 wherein at least one of the reversible integer to integer transforms comprises a transform that maps a vector of length N to a vector of length less than N.

10

28. The method of claim 26 wherein at least one of the reversible integer to integer transforms comprises a transform that maps a vector into a set of difference values.

29. The method of claim 26 wherein a reversible integer to integer transform is performed recursively to form the series.

15

30. A computer readable medium on which is stored instructions for performing the method of claim 26.

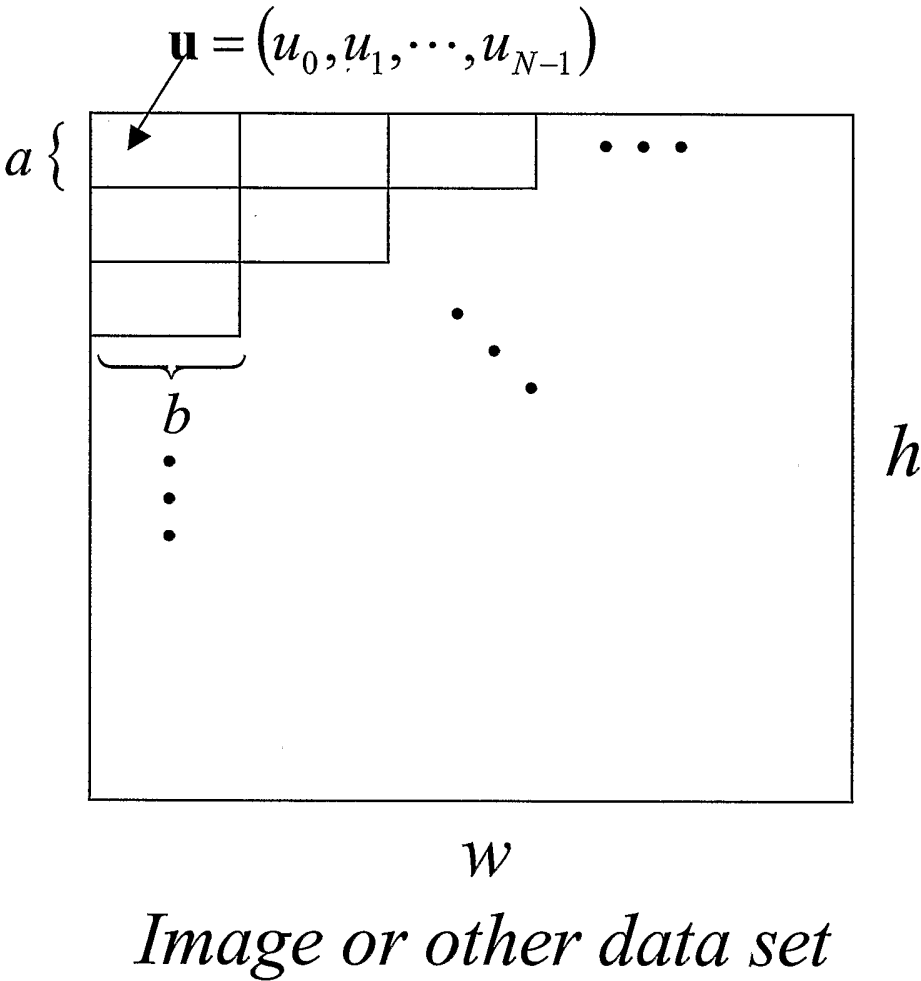


Fig. 1

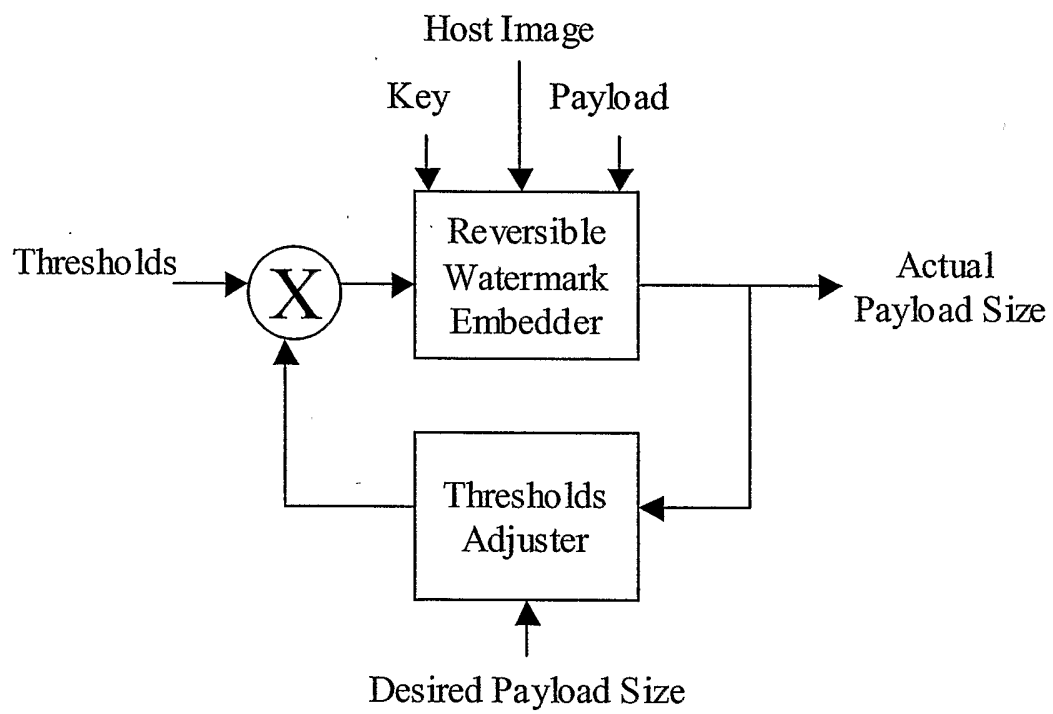


Fig. 2

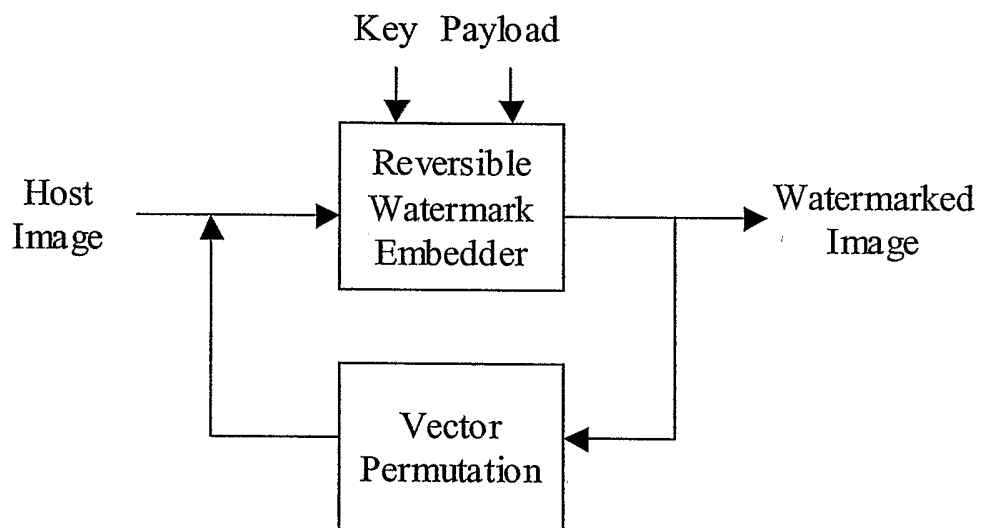


Fig. 3

u_0	u_1
u_2	u_3

$$\mathbf{u}_0 = (u_0, u_1, u_2, u_3) \quad \mathbf{u}_1 = (u_1, u_0, u_2, u_3)$$

(a) (b)

u_0	u_1
u_2	u_3

u_0	u_1
u_2	u_3

$$\mathbf{u}_2 = (u_2, u_0, u_1, u_3) \quad \mathbf{u}_3 = (u_3, u_0, u_1, u_2)$$

(c) (d)

u_0	u_1
u_2	u_3

Fig. 4

5/7

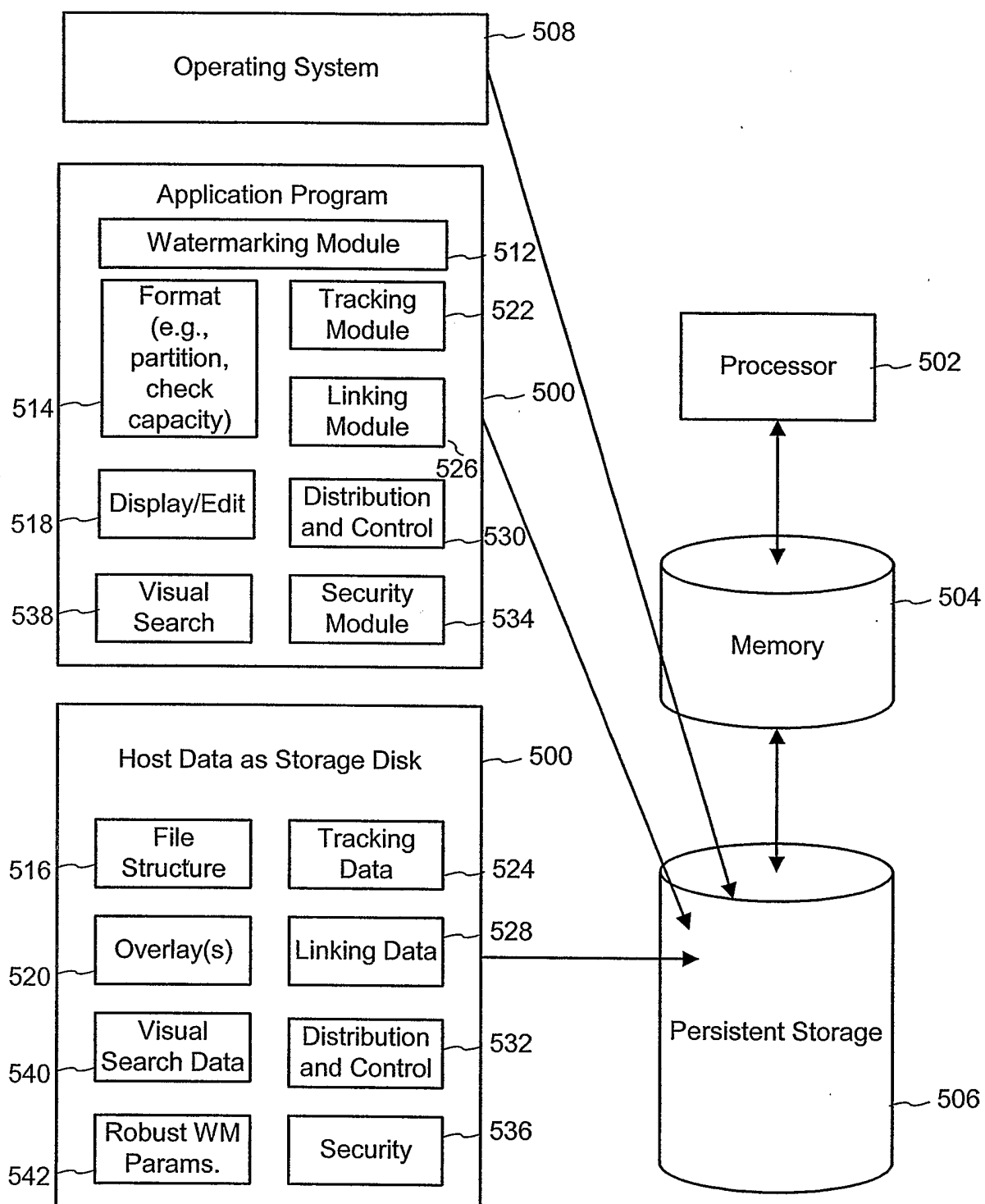


Fig. 5

6/7

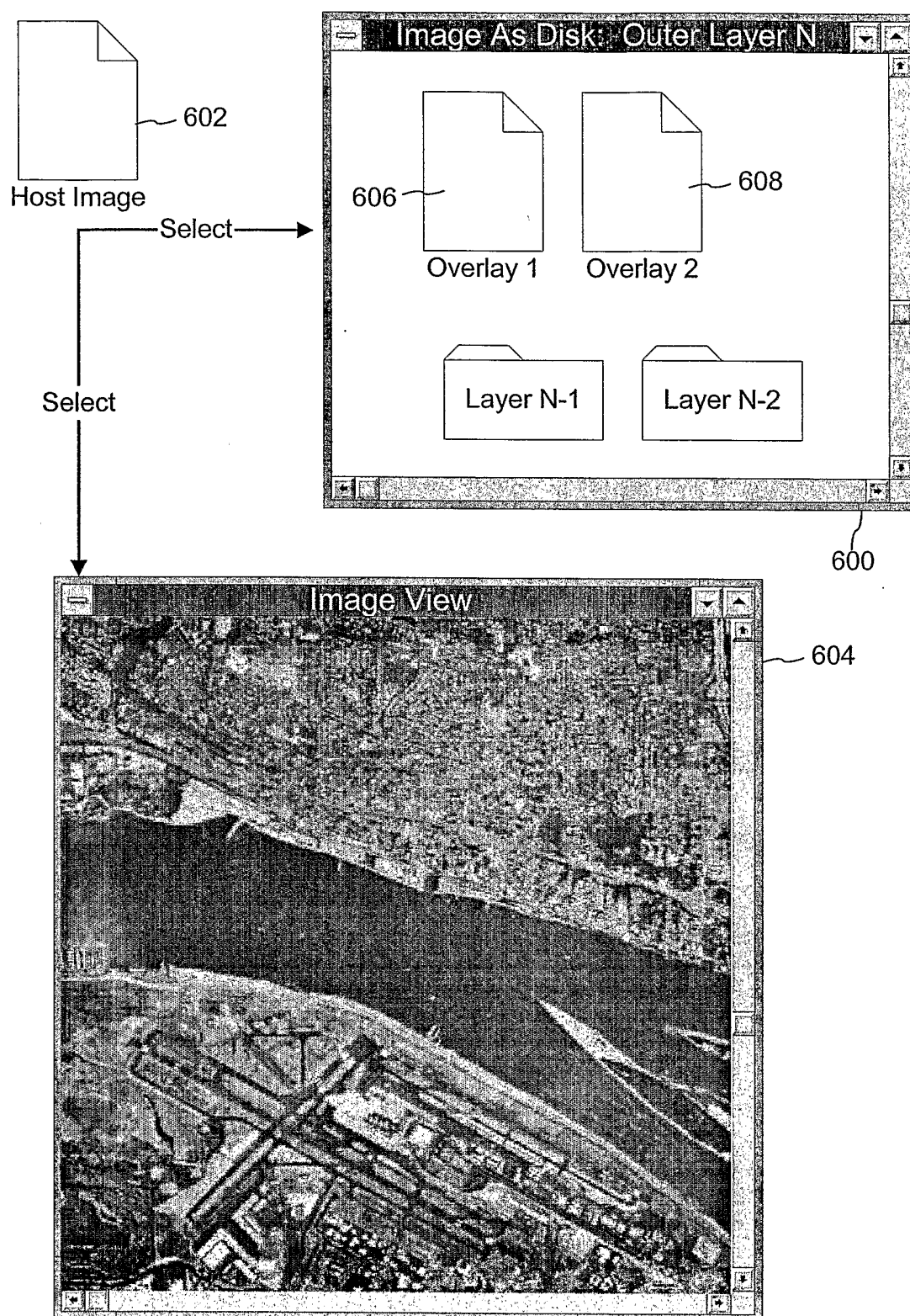


Fig. 6

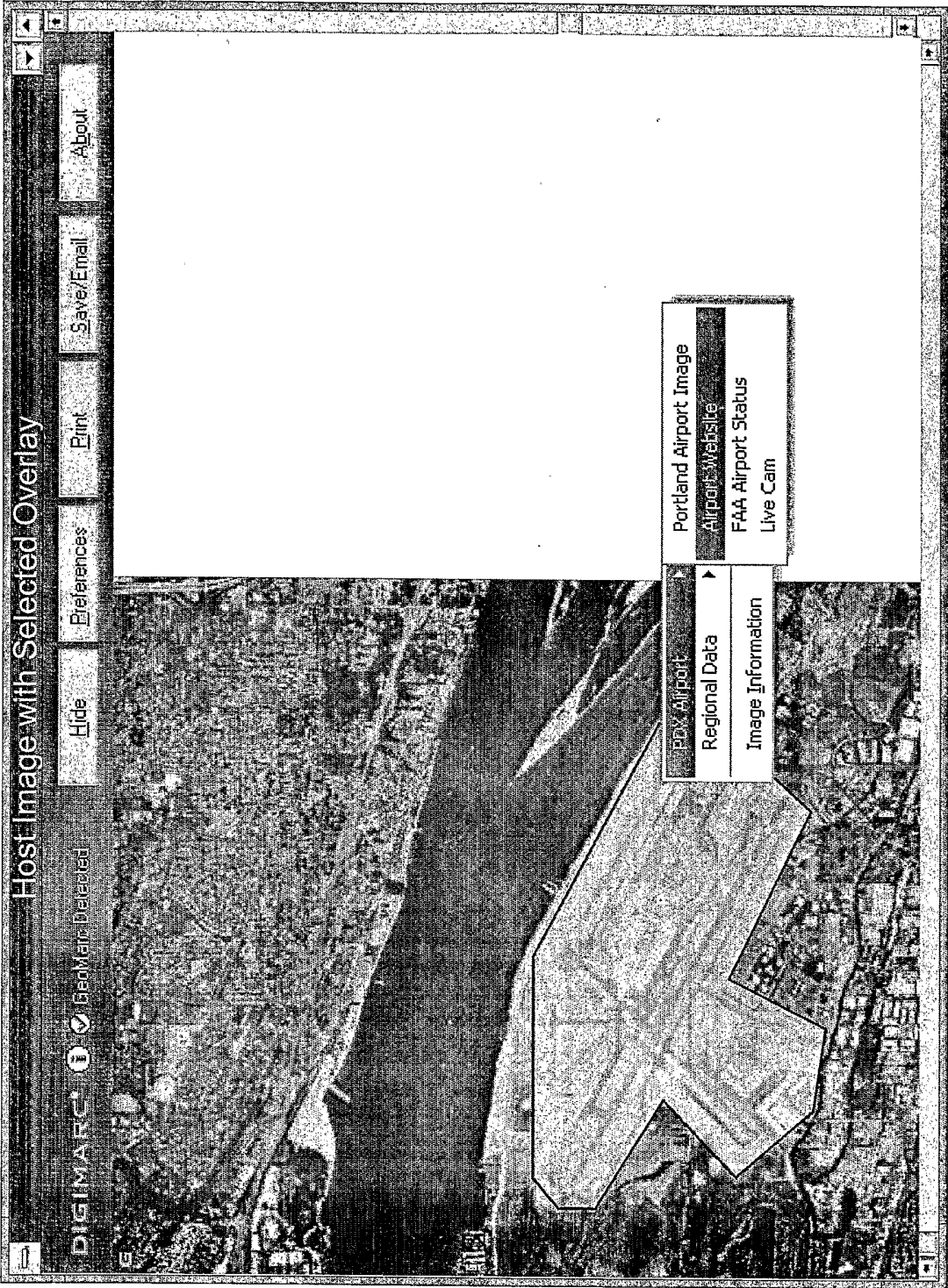


Fig. 7