



## Techniques for embedding and detection of watermarks in images

### Field of the invention

The present invention relates to techniques for embedding and detecting watermarks in digital image data.

### 5 Background of Invention

With the development of the digital technology, there has been an explosion in use of digital multimedia data. Analogue audio and video equipment is gradually in the process of being replaced by its digital successors. With the help of digital storage and Internet connections, the distribution of multimedia data and applications is becoming much easier and faster, so copyright issues are increasingly important to the owners of the digital content data, and for this reason techniques are being developed for modifying digital data ("watermarking" the data), in such a way that the fact that the data has been modified can be detected. Digital watermarking technology makes it easier for copyright to be enforced, because it makes it easier for the copyright owner to prove that the data originates from him. However, digital watermarking is not only used for copyright protection, but also for indexing, captioning, data hiding, etc.

20 A watermarking system usually has two stages: (i) watermark embedding and (ii) watermark detection/extraction. When it is required to protect the ownership of the image, the embedded watermark is detected and extracted from the modified image.

25 A first key issue in technology for embedding watermarks is the choice of the domain ("workspace") in which watermark embedding should be performed. For example, most existing watermarking techniques operate in the spatial domain, discrete cosine transform (DCT) domain, Mellin-Fourier transform

domain, wavelet domain, etc. A further key issue is the selection of the pixels, blocks or transform coefficients where the watermarks should be hidden.

Desirably, a watermark is embedded in a host image by modifying the image  
5 so that the modifications in the image are not visible. Such “imperceptibility” is one of the most important requirements in image watermarking systems. Also, desirably, the watermark should be hard to remove (to “attack”).

We now review some known watermarking techniques in relation to these two  
10 desiderata.

(1) Spatial domain watermarking is the most straightforward watermarking technique. An advantage of the spatial domain techniques is that they can be easily applied to any image, regardless of subsequent processing. One  
15 approach is called the Least-Significant-Bits modification method (LSB). In this technique the watermark may be embedded anywhere in the host image, so there is a high channel capacity and a small watermark object may be embedded multiple times. Even if most of these objects are lost due to attacks, a single surviving watermark would be considered a success. LSB  
20 substitution, however, despite its simplicity brings a host of drawbacks. Although it may survive transformations such as cropping, any addition of noise or lossy compression will totally remove the watermark. An even better attack is simply to reset the LSB bits of each pixel, since this would fully remove the watermark with negligible impact on the original data.  
25 Furthermore, once the embedding algorithm is known, the embedded watermark can be easily discovered. An improvement on basic LSB substitution is to use a pseudo-random number generator to determine the pixels to be used for embedding based on a given “seed” or key. More advanced spatial domain methods exist too, such as correlation based  
30 techniques. Another disadvantage of spatial techniques is that the embedding

technique for producing them cannot be published without making the watermark more easily removable. In addition, adaptive watermarking techniques are difficult in the spatial domain, as it is hard to distinguish between smooth and noisy regions.

5

(2) Discrete Cosine Transform (DCT) domain watermarking has been widely studied in the context of JPEG and MPEG, normally in the mid-frequency AC components. Embedding operations in the DCT domain are often robust to JPEG and MPEG compression, so the watermark can resist JPEG/MPEG attacks more easily. Watermarking in DCT domain offers the possibility of embedding watermarks directly in the compressed format, so as to minimise the computation time. However, previous studies on visibility in DCT domain compression predict the visible impact of the watermark on the watermarked image. Usually, the watermark is embedded in the low-frequency AC coefficients in the DCT domain.

(3) Wavelet domain techniques exploit the Wavelet analysis signal processing method which has been popularly applied in image processing in recent decades. Wavelet analysis is usually based on multi-resolution analysis (MRA) which analyzes an image in detail in the frequency domain. The wavelet transform consists of a multiscale spatial-frequency decomposition of an image, e.g. into four bands such as an approximate image LL and three detail images LH, HL and HH. The MRA is compatible with perception by human eyes, therefore, it is helpful in managing a good selection of watermark embedding locations in the original image in terms of robustness versus visibility. Wavelets are also key in the ongoing compression standard JPEG2000, so wavelet domain watermarking also has the advantage of robustness to JPEG2000 compression.

(4) Most watermarking techniques encounter serious problems in extracting watermarks after an affined geometric distortion, i.e. image rotation, scaling and translation (RST), which is called mis-synchronization. For this reason Mellin-Fourier Transform domain watermarking techniques have been introduced since this transform is invariant under RST transformations and even their combination and permutation in any order. Watermarking in this way may also have the advantage of combining the watermarking embedding process with methods dealing with solving geometric distortion problems. However, one drawback is that this watermarking technique increases the complexity of watermarking very much so practical adoption of such techniques may not be possible. Another disadvantage is that it may not be easy to achieve imperceptibility of the watermarks.

Imperceptibility is one of the most important requirements in an invisible image watermarking system. As no golden measurement parameter for measuring imperceptibility has yet been devised, the final judgment still relies on our human eyes. Therefore, a workspace to be chosen and its WM-embedding elements to be selected should be ideally based on our Human Vision System (HVS). None of the above-mentioned WMing domains is directly based on HVS, but instead they are derived from frequency-based mathematical functions. Although some WMing methods, such as wavelet methods, consider the workspace and use WM-embedding locations closely matched with HVS by selecting certain frequency bands for WM embedding, they do not fully satisfy the requirements of HVS and do not guarantee the invisibility of the WMs.

The two components of a transformed image are the basis function used and the resultant coefficients, but the basis function is the dominant factor to determine a transform in the above classical transforms. In other words, such a transform is fixed if and only if its appropriate basis functions are

determined. The coefficients depend on the audiovisual data that is supplied to the basis function. Therefore, when we refer to a transform, we normally refer to its basis function (or to a coupled pair of basis functions). Usually, the basis functions are fixed, which is not flexible to various types of images, so there is the disadvantage is that a given basis function is only best for certain types of data. However, the advantage of fixed basis transforms such as DCT, FFT and WT, is their simplicity. A watermarking scheme based on them can share the known basis function at both the embedding and detection sides without any communication overhead.

10

In an earlier patent application [9], two of the present inventors proposed a technique for watermarking a single image which made use of ICA transforms. An ICA transform is a new signal processing method that converts a signal to mutually independent components in the complete statistical sense. The ICA transform can in theory convert highly correlated audiovisual data into statistically independent coefficients. The ICA transform originated from the desire to produce signal components, i.e. the coefficients, having statistical independence. The only fixed factor in the ICA transform is the statistical independence of the coefficients, and in order to meet the independence criterion, the basis functions need to be changed for every supplied audiovisual object. Thus, an ICA transform can overcome the limitations of DCT and Wavelet transformations, which have one basis function for all images.

20

25 In an ICA-based image analysis, the amplitudes of the ICA-transformed components usually have a probability density function (pdf) which is a very sparse distribution, also known as a super-Gaussian distribution. The properties of this probability distribution are 1) a very high peak appearing at the mean value of the distribution, 2) a long tail appearing at the two sides.

30 Figure 1(a) shows a typical super-Gaussian distribution. From Figure 1(a), we

can notice two properties of the amplitudes of ICA coefficients: a small number of coefficients have very large values (and which represent very significant components of the image) and a large number of coefficients have small values.

5

Although the ICA transform picks out many kinds of different ICA features from each individual image, they all have in common that the features are spatially oriented, band-passed, and localized both in the spatial and frequency domains [1][2][7]. In other words, they are some edges and bars  
10 with certain angles, widths and lengths. These are the essential elements or significant shapes in 2D images.

Interestingly, these are also matched with the primary neural cell patterns in the human visual cortex. It is now believed that the HVS splits visual stimuli  
15 from the retina of the eye into many different components. These components pass by different tuned channels from the retina to the cortex, each channel being tuned to a different respective component [1][3][4]. The characteristics of a component in the visual field are

- Its location (corresponding to its co-ordinates in the image domain)
- 20 • Its orientation (corresponding to a phase in the Fourier domain)
- A spatial frequency (corresponding to a magnitude in the Fourier domain).

A perceptive channel can only be stimulated by a signal whose characteristics are tuned to its own characteristics. Different channels have different  
25 characteristics. Moreover, according to the perceptive model of human vision [4], signals that have similar characteristics use the same channels from the eye to the cortex. It appears that such signals interact and are subject to non-linear effects. Masking is one of those effects. Masking occurs when a signal cannot be seen because of another signal with close characteristics but at a  
30 higher energy level [5][6].

As the characteristics of a component in the visual field closely match the properties of features in the ICA transform, most of ICA image features obtained by ICA transform represent the edge-like or bar-like details that are the most essential elements in images: perceptually significant components. Fig. 1(b) shows a part of the transform  $W$  for a typical image, and Fig. 1(c) the Fourier transform of it. In both cases amplitude values are represented as grey-scale values. Fig. 1(b) high amplitudes are white, whereas in Fig. 1(c) high amplitudes are dark.

The process described in [9] is as follows.

A first stage is to adaptively learn ICA features from a single digital image which is later watermarked. From the digital image, a large number of  $8 \times 8$  pixel patches are selected at random. These patches are vectorized and used to form a first data matrix  $X$ . The rows and columns of the matrix  $X$  are processed to reduce their means to zero, and then the matrix is pre-whitened by removing row-wise correlation to form a pre-whitened matrix  $V$ . An ICA learning stage is then performed on the pre-whitened matrix  $V$ , to derive a demixing matrix  $dW$ , such that the rows of a matrix  $Y$  which is a product of the demixing matrix  $dW$ , the pre-whitened matrix  $V$  and the first data matrix  $X$  are as independent as possible. Finally, in an ICA feature forming stage, an ICA transform matrix  $W$  is formed as the product of the demixing matrix  $dW$  and the pre-whitened matrix  $V$ . The rows of the ICA transform matrix  $W$  represent 64 ICA filters of the image, which can be applied to the image to extract from it ICA coefficients representing the respective intensities of its statistically independent components. The corresponding columns of its inverse matrix  $A$  represent the corresponding 64 ICA synthesis filters.

A second stage is to embed a watermark into the image by: (i) preprocessing the image in the spatial domain, (ii) using the ICA transform matrix obtained earlier to transform the image from image intensities to ICA coefficients, (iii) watermarking the ICA coefficients, (iv) using the inverse matrix  $\mathbf{A}$  to transform the watermarked ICA coefficients back into the spatial domain, and (v) post-processing in the spatial domain. This results in the watermarked digital image.

Detection of the watermark has the same first two stages resulting in retrieval of the watermarked ICA coefficients. Of these, step (ii) typically uses the ICA transform matrix  $\mathbf{W}$  derived during the embedding process, so that in this case the matrix  $\mathbf{W}$  has to be made available to the detection process also. The retrieval of the watermarked ICA coefficients is followed by a step (iii) detecting the digital watermark in those coefficients. This may be by a "blind detection process" (not making use of the original watermarked image) or a "non-blind detection" process (using the original, unwatermarked image).

The ICA watermarking technique proposed in [9], while in many ways a great advance on earlier techniques, does, however, suffer from some practical issues in certain applications. Specifically, in some applications there is a time-consuming computation for the generation of basis functions for each of the watermarked images. Furthermore, certain applications may have a huge storage requirement to store the matrix  $\mathbf{W}$  for each of the watermarked images (and also, in the case that the watermark detection process is carried out in a different location from the embedding process, a high transmittal burden between the locations).

### Summary of the Invention

The present invention aims to provide a new and useful method for watermarking of digital data, and apparatus for performing the method. The invention further provides methods and apparatus for extracting watermarks  
5 from the watermarked digital data.

In general terms, the invention proposes that a group of similar digital data objects (typically digital images) are used together to obtain a set of ICA basis functions. These basis functions are then used in a watermarking process for watermarking one or more digital data objects which are either one or more  
10 (or all) of the group of images, or other digital data objects which are similar to them.

The condition that two data objects are "similar" may be expressed as meaning that they obey at least one similarity criterion in relation to each other, such as having a mutual correlation which is above a threshold level.

15 The digital data objects may be part of a database of digital data objects, and the process may include a pre-watermarking step of partitioning the data objects into groups according to the similarity condition. For example, if the data objects are images then the pre-watermarking step may be the identification of similar image frames in a similar scene inside a movie, or  
20 alternatively a plurality of images may be clustered into groups by one or more numerical similarity criteria.

Optionally, there may be a process of partitioning a database of digital data objects into objects which obey a similarity criterion, and those which do not. Optionally, only the former objects may be used for watermarking. Or  
25 alternatively, the one of more latter objects may be watermarked individually, e.g. based on a procedure as in [9] in which the ICA basis functions are derived individually for those digital data objects.

Optionally, a clustering algorithm can be performed using the database of digital data objects to derive a plurality of groups of digital data objects, each object of each group obeying a similarity criterion in relation to the other members of the group. Then a set of ICA basis functions can be derived for each respective group, and used to watermark one or more data objects of the group (and/or other data objects obeying sufficiently similar to the objects of the group).

Alternatively, the one or more groups of digital data objects in the database may be pre-defined.

Compared to the prior art ICA-based watermarking scheme described above, the present invention is more practical and efficient in real applications. A single set of ICA basis functions is learnt from the group of digital objects as a common basis set for these digital objects. The ICA learning process is just done once for the whole group of objects, so that the computational complexity of deriving the basis set is lower per digital object than the prior art method. Furthermore, only the common basis set is shared between embedding and detection sides. These two factors mean that the overhead of the watermarking process is low compared to the prior art ICA watermarking technique and very practical in real applications. The exact degree of improvement typically depends upon the number of similar digital objects in the database. This improvement is achieved while still providing to watermarked images with good imperceptibility and a robust detection result.

#### Brief Description of The Figures

Preferred features of the invention will now be described, for the sake of illustration only, with reference to the following figures in which:

Fig. 1, which is composed of Figs. 1(a) to 1(c), illustrates some properties of an ICA image;

Fig. 2 is the flowchart of a ICA-based watermarking system which is an embodiment of the invention;

Fig. 3 is a flowchart of an ICA feature learning process which is part of the system of Fig. 2;

5        Fig. 4 is composed of Fig. 4(a) and Fig. 4(c) which respectively are a flowchart of an ICA-based watermark embedding process which is part of the system of Fig. 2, an illustration of a classification of ICA coefficients performed in a step of the flowchart, and an illustration of the ICA basis functions following the ordering;

10       Fig. 5 is a flowchart of an ICA-based watermark detection process which is a part of the system of Fig. 2;

Fig. 6 is a flowchart illustrating how the embedding process of Figs. 2, 3 and 4 can be applied to compressed Images;

15       Fig. 7 is a flowchart illustrating how the ICA-based WM Detection process of Fig. 5 can be applied to the images obtained in the process of Fig. 6; and

Fig. 8, which is composed of Figs. 8(a) and 8(b), illustrates an encoding and decoding process in a further embodiment of the invention.

## 20    Detailed Description of the embodiments

As described in detail below, many of the process steps of the embodiment of the present invention are in common with embodiments described in reference [9] and according Figs. 2, 4(a) and (b), and 5 to 8 in the present application are taken from [9]. These figures will however be described below  
25    with reference to an embodiment of the present invention for ease of understanding. In certain cases the input to the process steps is different from that in [9], giving the figures a different significance in the context of the present application.

Referring to Fig. 2, the method which is an embodiment of the invention of is illustrated schematically, acting on an image taken from a database 1.

5 In a first stage of the embedding process, "ICA feature learning", a plurality of images (a "group of images") from a database 1 is used by a unit marked as 4 to obtain an ICA transform and an ICA inverse transform (as described below in detail with reference to Fig. 3).

10 In a second stage of the embedding process, "ICA-WM embedding", the ICA transform is used together with an image from the database 1 to generate ICA-based coefficients (by a unit shown as 7). A watermark from a second database 3 and a key from a third database 5 are used by a unit shown as 9 to produce a watermark pattern, which is combined by a unit shown as 11 with the ICA-based coefficients to form watermarked coefficients. The  
15 watermarked coefficients are then transformed by a unit 13 using the inverse ICA transform to produce the watermarked image.

Once this watermarked image has been generated it can be put into the public domain, where it is typically subjected to compression/decompression  
20 operations, attack, and noise.

In the detecting process, "ICA-WM detection", there is a first pre-processing stage, performed by a unit 14, of compensating the image for any distortion it may have received in the public domain (e.g. geometrical distortion, digital-to-  
25 analogue or analogue-to-digital effects, luminance variation effects, etc). Subsequently, a unit 15 uses the ICA transform to convert the watermarked image into warped watermarked data. A unit 17 uses the warped watermarked data and the watermark pattern to produce a result indicative of the presence of the watermark in the watermarked image.

The procedure of adaptive ICA feature learning is illustrated in Fig. 3, as follows, where the left of the figure gives the process steps and elements on the right of the figure illustrate typical results of those steps:

- 1) In step 21, a group of images, such as image 10, is used to generate patches 20. These patches are 8x8 pixel arrays randomly selected from different images of the group.

The image group can be pre-selected within the database 1, according to one or more similarity criteria. For example, one possible similarity criterion is simply that a correlation between the images is above a threshold. Optionally, a clustering algorithm may be carried out, as a pre-step, using the database 1 to identify one or more groups. In the clustering algorithm the images are clustered into one or more groups (possibly omitting one or more images which are not sufficiently similar to other images of any of the groups).

Alternatively the group may be predefined. For example, each group of images may be images carrying a respective pre-allocated label, e.g. indicating they show similar scenes within a move.

Twelve such patches 20 are shown in Fig. 3, but in fact more preferably hundreds of thousands of 8 x 8 image patches are randomly selected from every image of the group in order to cover all kinds of image shapes in the image (note that an alternative to generating the patches randomly is to obtain the patches regularly block-by-block, e.g. by selecting blocks in turn adjacently from left to right and top to bottom). This process yields the most common images features in the group of images.

2) In step 22, the 8x8 patches 20 are each vectorised into respective 64 x 1 column vectors, and the vectors are used as respective columns in a data

matrix  $\mathbf{X}$ . Thus the matrix  $\mathbf{X}$  is 64 elements high and has a number of elements in the lateral direction equal to the number of patches 20.

3) In step 23, the rows and columns of the matrix  $\mathbf{X}$  are processed by:

- 5 subtraction from each of the elements of each row of the respective mean of that row, to form a modified matrix; then subtraction from each of the elements of each column of the modified matrix of the respective mean of that column. This results in a matrix of "preprocessed image patches" in which each of the rows or columns have zero means.

10

4) In step 24, "PCA pre-whitening" is carried out, in which the data matrix  $\mathbf{X}$  is pre-whitened by performing a principal component analysis (PCA) to remove the row-wise correlation. Specifically, we first obtain the covariance matrix  $\text{Cov} = \mathbf{X} * \mathbf{X}^T$ , which is a 64x64 matrix. We then obtain its 64 eigenvectors, and  
 15 form a whitening matrix  $\mathbf{V}$  which has these eigen-vectors as respective rows. In statistics this process is called 2nd-order de-correlation. The data matrix  $\mathbf{X}$  is processed using  $\mathbf{V}$  to form a new matrix  $\mathbf{X}'$  given by  $\mathbf{X}' = \mathbf{V} \times \mathbf{X}$ .

5) In step 25, "ICA learning" is carried out, e.g. the algorithm called fastICA by  
 20 Aapo Hyvarinen [8]. This ICA learning uses the data matrix  $\mathbf{X}'$  to form a demixing matrix,  $\mathbf{dW}$ . The rows of an output matrix  $\mathbf{Y}$  given by  $\mathbf{Y} = \mathbf{dW} \times \mathbf{X}'$  are as independent as possible when the system is convergent. The matrix  $\mathbf{dW}$  is orthogonal because the input is 2nd-order uncorrelated.

- 25 6) In step 26, "ICA feature forming" is carried out to produce a matrix  $\mathbf{W}$  (the "ICA transform" of Fig. 2) which may be considered as a set of ICA basis functions, and is given by  $\mathbf{W} = \mathbf{dW} \times \mathbf{V}$ . The rows of the matrix  $\mathbf{W}$  represent 64 ICA weight filters of the image 10. The "inverse transform" of Fig. 2 is an inverse matrix  $\mathbf{A}$  given by  $\mathbf{A} = \mathbf{W}^{-1}$  (or equivalently  $\mathbf{A} = \mathbf{V}^{-1} \times \mathbf{dW}^T$ ). The columns  
 30 of the matrix  $\mathbf{A}$  represent the corresponding 64 ICA synthesis functions. Each

of the matrices  $A$  and  $W$  is a  $64 \times 64$  matrix. The synthesis matrix (set of synthesis filters)  $A$  and analysis matrix (set of analysis filters)  $W$  will be used later in the ICA watermark embedding and watermark detection processes.

- 5 Turning to Fig. 4(a), the ICA-based watermark embedding procedure is shown. It includes five stages: (31) pre-processing the host image in the spatial domain, (32) ICA transforming the pre-processed host image into the ICA domain to derive ICA coefficients, by making use of the analysis matrix  $W$ , (33) watermark embedding onto the ICA coefficients, (34) an inverse ICA  
10 transform from ICA coefficients back to image intensities by making use of the synthesis matrix  $A$ , (35) post-processing in the spatial domain. We now explain these stages in detail:

Pre-processing in spatial domain (stage 31) is performed by obtaining the  
15 global mean value of the host image, subtracting it from each pixel value of the image, and also recording it for image restoration later (step 36). The host image is then divided into continuous blocks of 8 pixels by 8 pixels (step 37), illustrated as 30. The number of such blocks  $N$  depends upon the size of the host image (as shown in Fig. 4,  $N$  is 64, but the invention is not limited in this  
20 respect).

The local means of these blocks are obtained, subtracted from each pixel of the blocks, and recorded for image restoration later (step 38). The  $8 \times 8$  pixel blocks are vectorized into  $N$  respective column vectors, each having 64  
25 components (step 39), and the  $N$  columns vectors are put together to a  $64 \times N$  matrix,  $Z$ .

The ICA transform (stage 32) is performed by applying the weight (analysis) matrix  $W$  to data matrix  $Z$ , to form a matrix  $C = W \times Z$  (step 40). The portion  
30 of the matrix  $C$  corresponding to each block represents 64 ICA coefficients  $c$ .

The 64 coefficients  $c$  of each block are normalized to zero mean and unit variance with the original mean and variance recorded for later restoration (step 41).

- 5 We turn now to the watermark embedding stage (stage 33). Some important issues here are the selection of ICA coefficients for WM embedding, the formulation of WM patterns and their modulations with ICA coefficients.

10 In a first step (step 42) of the watermark embedding stage (stage 33), we select which of the ICA coefficients in the image obtained in step 41 are suitable to be used for embedding watermarks. In order to fully utilize the masking effects for imperceptibility in this system, two schemes for selection of ICA coefficients for embedding are described here as follows (although the invention is not limited to these schemes and many other schemes may be developed for selecting the ICA coefficients to watermark embedding):

One possible strategy for the selection is based on the energy of the ICA coefficients corresponding to every ICA feature. The ICA analysis and synthesis functions are sorted in the order of their coefficients' energy (variance). The functions corresponding to large energies are put at the beginning of the list. To explain, Fig. 4(b) shows a typical distribution of ICA coefficients. We can classify the ICA coefficients of this distribution according to their magnitudes into three classes: a small number of coefficients with big magnitudes (shown as class 1); coefficients having middle-range magnitudes with enough numbers to represent significant features (shown as class 2); the coefficients with small magnitudes, close to zero (shown as class 3). Fig. 4(c) shows the resultant basis functions ordered by magnitude, showing that they are also ordered from low to high frequency.

The coefficients labelled as class 1 have big magnitudes and are usually associated with particular primary-cortex channels, so they can perform a marking effect to tolerate a high watermark strength while still giving invisible and robust watermarks.

5

There are enough middle-magnitude coefficients, class 2, to hide a large amount of watermark data, and their relatively small magnitudes minimizes any bias effect in the detection stage (which means that it may be preferably to use class 2 coefficients instead of class 1 coefficients in the context of blind  
10 detection). Furthermore, owing to the similar characteristics of image features and the large difference of coefficient magnitudes between class 1 and 2 and among class 2, small modifications to class 2 coefficients caused by watermarking are masked by strong HVS-perceptual features to result in the excellent imperceptibility.

15

The small-magnitude coefficients, class 3, are preferably not used for the watermarking as they are insignificant features.

Based on our experiments, it is found that is suitable to define the class 1  
20 coefficients as those with the 1<sup>st</sup> – 16<sup>th</sup> highest amplitudes (i.e. about the highest quarter of the components), and define the class 2 coefficients as the 17<sup>th</sup>-48<sup>th</sup> functions (i.e. the next 50% of the coefficients) in the energy-ordered list. Then the class 1 and class 2 coefficients, or (particularly in the blind detection case) the class 2 coefficients, are selected for watermark  
25 embedding.

An optional enhancement to this strategy for the selection is to select coefficients within the class 2 which have further desired properties. Specifically, in this enhanced strategy the ICA analysis and synthesis  
30 functions derived in step 41 are ordered according to their three main

properties: the edge's spatial location, orientation and its frequency magnitude. They are arranged so that the parameters of these properties change continuously and smoothly. For example, the functions may be mainly ordered from low-frequency to high-frequency, but those functions with similar frequencies are ordered according to direction of their phase in the range of angles 0 to  $2\pi$  and with those functions with similar spatial locations also being placed adjacently. The purpose of this arrangement is to maximise the masking effect between components with similar characteristics. The watermark patterns will be embedded into a set of coefficients with adjacently arranged functions, and this set of coefficients is chosen such that all the coefficients are in class 2. A masking threshold can also be applied here for guaranteeing imperceptibility [6][7]. Properly choosing a certain range in this ordered function list could ensure the robustness under attacks. For example, functions within the lower-to-middle frequency range survive relatively well under image compressions. This technique provides good masking based on the known "neighbour masking" effect: the small scale watermarks cannot be seen because of other ICA components obtained through nearby ICA features with similar characteristics at a higher energy level.

Another important part of the watermark embedding stage (35) is the generation of the watermark patterns. For effective watermark embedding, it is beneficial to perform some pre-processing to format the watermark bits (0 or 1), obtained from the database 3 of Fig. 2, to produce watermark patterns with certain properties. The present embodiment employs a "spread spectrum" technique for generating the watermark patterns, which is commonly used in the fields of signal coding and watermarking. A key point of watermark pattern formulation in spread spectrum techniques is to transform narrow-band original watermark bits into wide-spectrum patterns. A private key is provided to keep the watermark pattern secure.

To make possible spread spectrum processing, in step 43 (which corresponds to unit 9 of Fig. 2) we generate several series of wide-band Gaussian distributed pseudo-random numbers, using a private key obtained from database 5 of Fig. 2, these series of numbers are modulated with respective ones of watermark bits, to transform the narrow-band original watermark bits to respective wide-spectrum patterns.

Therefore, these watermark patterns are uncorrelated to ICA coefficients on which the watermark patterns are to be embedded. This process is also known as direct-sequence Code Division Multiple Access (CDMA). This scheme also has the benefit of ensuring that the ICA-based watermarking is a secure system since only the party who has the private key is able to detect or remove the watermarks. Note that the scheme for generating the watermark patterns can be varied by optionally inserting some error-correcting codes (ECC) into the watermark bits to improve the robustness and extraction accuracy. Because of the CDMA, it is also possible to embed multiple watermark patterns onto the same portion of the ICA coefficients as long as the watermark patterns for different watermark bits are all orthogonal so that they do not interfere with each other.

Note that although the watermark bits are binary, the watermark patterns are real valued (or, rather, are one of a large number of intensity values). The total intensity of the watermark pattern is determined by a watermark strength parameter  $\alpha$ , which is used as a control variable to select a trade-off between watermark imperceptibility and robustness.

The watermark patterns generated as shown above are statistically orthogonal to each other. This is beneficial, for example, if multiple watermarks are to be embedded in the same piece of data. To improve the orthogonality of different series of random numbers orthogonal, we can

optionally pre-process the patterns by standard 2<sup>nd</sup>-order decorrelation methods, e.g. PCA, to make them uncorrelated.

Although, as discussed above, the watermark patterns used are real-valued numbers, the embodiment is not limited in this respect. For example, orthogonal binary patterns (e.g. having the values +1/-1 or having the values 1/0) can also be used. Some such known series, suitable for use in the embodiment, are referred to as "m-sequences", "hadamard sequences", or "gold sequences".

10

Although these techniques produce a limited number of purely orthogonal patterns, Fig. 8(a) illustrates a technique for making it more secure. In this technique an m-sequence is input to a unit 80 which also receives a random sequence of +1/-1 bits (which may for example be produced by applying a sign operation to a sequence of real-valued random numbers having a zero means). The unit 80 performs an individual component-wise multiplication, to generate an encoded binary sequence which can be used as a watermark pattern.

15

20 In step 44 the watermark patterns obtained in step 43 are embedded in the ICA coefficients selected in step 42 to obtain watermarked coefficients.

Assume the watermark pattern is a sequence of N numbers  $\alpha\omega_i$ , where i is an integer in the range 1 ... N and each value  $\omega_i$  is a binary value. The ICA coefficients are denoted as f(n), where n is an integer running from 1 to N' (where N' is the total number of ICA coefficients). The watermark pattern is to be embedded in selected ICA coefficients such that n runs from j+1 to j+N. One possible embedding formula which may be used is:

25

$$f'(j+i) = f(j)(1 + \alpha \cdot \omega_i) \quad (1)$$

Another embedding formula which may be used is:

$$f'(j+i) = f(j) + \alpha \cdot \omega_i \quad (2)$$

5

In either case, combining the watermarked coefficients  $f'(n)$  and those ICA coefficients  $f(n)$  which were unchanged produce final ICA coefficients  $c'$  (in the form of a matrix  $C'$ ) for each block of the watermarked image (step 45).

- 10 Note that it is important that the watermark pattern is long enough to have a good enough correlation level for robust detection. Optionally, to embed a watermark into a particular image, a number of patch blocks (e.g. 8x8 blocks) may be defined within the host data with the ICA analysis being performed block-by-block, and in step (44) any given watermark bit (0/1) is encoded in
- 15 multiple blocks. The number of blocks used is selected based on the size of the host image. Experiment shows that in the embodiment a suitable number of blocks for one watermark bit is from 50 to 100. Sometimes, the number of watermark bits is too large to keep large number of blocks for one watermark bit, e.g. if there are less than 10 blocks per watermark bit.

20

- Another way to increase the robustness is to cluster several watermark bits together to share watermark patterns. For example, one watermark bit may be embedded in two watermark patterns which respectively represent zero (0) or one (1). Two watermark bits may be embedded in four watermark patterns ,
- 25 which respectively represent 00, 01, 10 and 11. In general, for  $n$  watermark bits,  $2^n$  watermark patterns are needed to represent respective possibilities for the realisations of the watermark bits. The length of the watermark patterns increases with  $n$  (e.g. in proportion to  $2^n$ ), and so the correlation is more robust. In such a way, the detection rate for each watermark bit is
- 30 increased.

As noted above, the ICA components are not embedded in the ICA components of very small energy (e.g. those components having an intensity which is less than 1% of the intensity of the components of maximum intensity), or of very high energy (e.g. these components having an intensity more than 30% of the intensity of the components of maximum intensity).

Stage 34, the inverse ICA transform, includes a step 46 of restoring the original mean and variance of each block of the watermarked coefficients  $\mathbf{c}'$  using the values obtained in step 41. Then, in step 47, these are transformed to an intensity data matrix  $\mathbf{Z}'$  by applying the synthesis matrix  $\mathbf{A}$ , which is the inverse of analysis matrix  $\mathbf{W}$ , such that  $\mathbf{Z}' = \mathbf{A} \times \mathbf{c}'$ .

Stage 35, of post-processing in the spatial domain, includes a step 48 of reshaping the vectors in the matrix  $\mathbf{Z}$  to form 8 x 8 blocks, and then a step 49 in which each of the pixels of each block are increased by the respective local mean of that block obtained in step 38. In step 50 the blocks are arranged to form a complete image. Finally, in step 51, the global mean obtained in step 36 is added to each pixel value to obtain a final watermarked image.

We now turn to the ICA watermark detection, which is illustrated in Fig. 5. ICA watermark detection is the counterpart of the embedding process, and aims to detect the embedded watermark from the watermarked image obtained in Fig. 4 (or a version of it which has been processed in the public domain by unknown techniques).

The procedure of the detection process, as shown in Fig. 5 includes the general stages of: pre-processing to compensate for any distortion to the image while it was in the public domain (e.g. to compensate for geometric distortion, digital-to-analogue or analogue-to-digital distortion, luminance

modification) which is performed by the unit 14 in Fig. 2 (step 60); pre-processing in spatial domain (stage 61), an ICA transform (stage 62) and watermark detection (stage 63). Note that this method does not employ any knowledge of the original image 10, although it assumed that there is access to the databases 3 and 5.

The pre-processing (stage 61) is exactly same as the pre-processing procedure 31 of Fig. 4, and results in is a data matrix  $\mathbf{Z}''$ , which may or may not be the same as the watermarked data matrix  $\mathbf{Z}'$ .

In the ICA transform (stage 62) the same analysis matrix  $\mathbf{W}$  (which is available to the apparatus which does the watermark detection; either because it is another function of the same apparatus, or because the analysis matrix  $\mathbf{W}$  is transferred between the two sets of apparatus) is used to transform pre-processed image data,  $\mathbf{Z}''$ , to ICA coefficients  $\mathbf{c}'' = \mathbf{W} \times \mathbf{Z}''$  with zero mean and unit variance.

In watermark detection (stage 63), ICA coefficients are selected in step 64 by the same method as in step 42 of Fig. 4. Watermark patterns are generated in step 65 according to same key and ECC method as in step 43 of Fig. 4, but not using the parameter  $\alpha$ . In step 66 we calculate the correlation  $\delta$  of the watermark pattern  $\omega_i$  directly with the selected components  $f''$  of  $\mathbf{c}''$  according to the formula:

$$\delta = \frac{\sum_{i=1}^N f''(j+i)\omega_i}{N} \quad (3)$$

which should converge to a certain non-zero value according to the central limit theorem. We compare the correlation value  $\delta$  with a detection threshold

T. The detection threshold may be selected, for example, such that if we consider two different watermark patterns  $\omega_i^0$  and  $\omega_i^1$  then the threshold value for watermark pattern  $\omega_i^0$  may be the average value of the autocorrelation of  $\omega_i^0$  and the correlation of  $\omega_i^0$  and  $\omega_i^1$ . Conversely, the then the threshold value for watermark pattern  $\omega_i^1$  may be the average value of the autocorrelation of  $\omega_i^1$  and the correlation of  $\omega_i^0$  and  $\omega_i^1$ . This technique relies on an assumption that the similarity of one watermark pattern to itself in terms of correlation is always greater than that to the host image patch and other watermark patterns.

10

An advantage of such a correlation-based WM embedding-detection technique is that it can be performed very quickly by known processors. Additionally, it can be performed without knowing the original host image 10. It can be very accurate when detection is performed on the raw watermarked image, because we adopt the CDMA scheme. Under various attacks, like image compression, image distortion, we can normally use more coefficients to embed and detect watermark patterns to increase the extraction accuracy dramatically. It is true that the capacity of the watermark bits will be decreased at the same time, but this is a minor issue in copyright protection since only a small amount of copyright data usually has to be included in the watermark data.

15

20

Note that in other embodiments of the invention, the detection process may be a non-blind process which makes use of the original images also.

25

In the case that the watermark patterns were produced using the technique shown in Fig. 8(a), the detection steps 65 and 66 are replaced by the process shown in Fig. 8(b). In this case, the encoded binary sequence is obtained from the coefficients selected in step 64. This sequence is input to a unit 80

performing the same function as the unit 80 of Fig. 8(a). Also input to the unit 80 is the same random sequence used in Fig. 8(a). The unit 80 thus outputs the m-sequence used to produce the watermark data by cross-correlating the extracted binary sequence with the random sequence.

5

Note also that the present technique is not limited to watermarking raw images. Rather, compressed images also can be treated as the host images. This is illustrated in Fig. 6. In this watermark embedding process, two additional steps are necessary: first the compressed image is de-compressed (step 71), then the watermark embedding process is carried out (step 72), and the resultant watermarked image recompressed (step 73) to give a compressed watermarked image with proper settings of image size and quality. The compressed images may for example be in the formats JPEG, JPEG2000 etc.

15

Similarly, the corresponding watermark detection process, illustrated in Fig. 7, includes a step 75 of image de-compression, prior to a watermark detection process (step 76) which is identical to the process shown in Fig. 5.

20 Apart from image compression, other operations conventionally performed on images, such as geometric distortion, image recapturing, digital-to-analogue (DA) and analogue-to-digital (AD) conversion, etc, may also intentionally or accidentally alter the watermarked image. These operations usually can be corrected by using some standard image restoration methods as a pre-  
25 processing step before the watermark detection procedure. For example, image normalization based on spatial moments can be used for removing geometric distortion; digital filtering on different colour channels and pixel luminance has been used to remove noise introduced in an DA/AD process. These operations can be carried out according to conventional techniques.

30

We now turn to a description of two ways in which the embodiments described above may be varied within the scope of the invention. These variants may be freely combined as desired.

#### 5    1.    Watermarking the ICA coefficients by Quantization

As discussed above, in step 44 of Fig. 4 the watermark patterns are added to the selected ICA coefficients by linear addition. The present embodiment, by contrast, though in other respects identical with the embodiment of Figs. 2 to 10 5, uses a quantization method to embed the watermark patterns. The embodiment uses pre-selected individual ICA coefficients, or sets of ICA coefficients, and sets these pre-selected ICA coefficients ("reconstruction points") according to the watermark data. In the case that individual ICA coefficients are modified, this is referred to here as "scalar quantization". In 15 the case that sets of ICA coefficients are modified, this is referred to here as "vector quantization". Similarly, the detection process in this embodiment detects the watermarks by modifying step 66 of Fig. 5 by mapping the reconstruction points and determining what watermark bits are stored there. This process is referred to here as a "quantize-and-replace" strategy.

20

First, we consider a scalar quantization scheme suitable for use in the embodiment. In this technique, pairs of the ICA coefficients are chosen, and their initial magnitudes are indicated here as  $f(i)$  and  $f(j)$ . The absolute difference between them is given by

25

$$\Delta = |f(i)| - |f(j)|.$$

In order to embed one WM bit, denoted as  $w_n$  which may be 0 or 1, the coefficient pair  $f(i)$  and  $f(j)$  is modified such that the absolute distance becomes

$$\Delta' = \begin{cases} \leq -Q, & \text{when } w_n = 0 \\ \geq Q, & \text{when } w_n = 1 \end{cases}$$

where  $Q$  is a parameter controlling the detection robustness or tolerance. The changes are such that (i) the changes are as small as possible, and (2) they use self-imperceptibility feature as much as possible. Specifically, the changes are as follows:

5

$$\delta f(i) = |\Delta - Q| \times \frac{f(i)}{f(i) + f(j)} \text{ and } \delta f(j) = |\Delta - Q| \times \frac{f(j)}{f(i) + f(j)}.$$

This scheme can be simply extended to vector quantization method as follows. Among the selected ICA coefficients within one block or multiple  
10 blocks,  $2 \times m$  coefficients are chosen as  $f_1(i) \dots f_m(i)$  and  $f_1(j) \dots f_m(j)$ . The absolute difference between two groups is given by

$$\Delta = f_{total}(i) - f_{total}(j),$$

where  $f_{total}(i) = |f_1(i)| + |f_2(i)| + \dots + |f_m(i)|$  and

$f_{total}(j) = |f_1(j)| + |f_2(j)| + \dots + |f_m(j)|$ . In order to embed one WM bit,  
15 denoted as  $w_n$  which may be 0 or 1, the coefficients  $f_1(i) \dots f_m(i)$  and  $f_1(j) \dots f_m(j)$  are modified such that the absolute distance becomes

$$\Delta' = \begin{cases} \leq -Q, & \text{when } w_n = 0 \\ \geq Q, & \text{when } w_n = 1 \end{cases}$$

where  $Q$  is, again, a parameter controlling the detection robustness or tolerance. Specifically, the changes are:

20 
$$\delta f_{total}(i) = |\Delta - Q| \times \frac{f_{total}(i)}{f_{total}(i) + f_{total}(j)},$$

$$\delta f_{total}(j) = |\Delta - Q| \times \frac{f_{total}(j)}{f_{total}(i) + f_{total}(j)}, \text{ and}$$

$$\delta f_l(i) = \delta f_{total}(i) \times \frac{|f_l(i)|}{f_{total}(i)} \text{ and } \delta f_l(j) = \delta f_{total}(j) \times \frac{|f_l(j)|}{f_{total}(j)} \text{ for } l=1, \dots, m.$$

Note that the coefficients' modification in vector quantization can be smaller than those in scalar quantization for the same robustness parameter value  $Q$ . Thus, vector quantization provides better imperceptibility and better robustness

In the detection stage, the WM bit  $w_n$  is simply detected by comparing the coefficient pair or two coefficient groups. Specifically, if  $|f(i)| \leq |f(j)|$  (in the case of scalar quantization) or  $f_{total}(i) \leq f_{total}(j)$  (in the case of vector quantization) then this implies that  $w_n = 0$ . Conversely, if  $|f(i)| > |f(j)|$  (in the case of scalar quantization) or  $f_{total}(i) > f_{total}(j)$  (in the case of vector quantization) then this implies that  $w_n = 1$ .

The technique explained here can be easily extended to embedding multiple watermark bits in one quantize-and-replace step. For example, consider three of the selected ICA coefficients having respective intensities  $f(i)$ ,  $f(j)$  and  $f(k)$ . These three intensities may be modified so that they are each at least  $Q$  apart, and such that the order of the intensities encodes the watermark bit. For example, if the highest modified intensity is written as H, the lowest modified intensity is written as L, and the other modified intensity is written as M, then the correspondence of the watermark bits to be encoded ( $w_n$ ) may be as given in Table 1.

| $w_n$ | $f(i)$ | $f(j)$ | $f(k)$ |
|-------|--------|--------|--------|
| 00    | H      | M      | L      |
| 01    | M      | H      | L      |
| 10    | H      | L      | M      |
| 11    | L      | H      | M      |

|    |   |   |   |
|----|---|---|---|
| XX | M | L | H |
| XX | L | M | H |

Table 1

In Table 1, XX means a pattern reserved for future use. In other words, there never are occasion on which the value of the ICA coefficients are quantized such that  $f(k)$  becomes the highest.

5

Contrary to linear additive methods, these various quantization methods are non-linear. They can utilize the high-energy coefficients even though the original image is not available. This scheme treats both high and low magnitude coefficients with equal weight.

10

The strategy of energy sorting in step 42 is suitable in this embodiment, since the quantization scheme suppresses the image self-noise (interference), so that it is desirable to use the high-energy ICA coefficients. Significant features imply good self-masking effect for quantization changes. Because of their large magnitude, a large quantization tolerance is available to enlarge the distance between reconstruction points but still keep the imperceptibility of the watermarking. Additionally, these significant features have less distortion under imaging operations, e.g. compression. The embodiment therefore performs its equivalent of step 42 by sorting the ICA coefficients in order of their average energy, and the watermark patterns may be embedded in the ICA coefficients of class 1 and the highest energy components in class 2 in Figure 7, e.g. 1<sup>st</sup>-10<sup>th</sup> ICA coefficients.

20

## 2. Use of a private key to select ICA components for embedding

25

It is advantageous is to preserve the security of embedded watermark, although the scheme of watermark embedding is usually required to be

disclosed to public. In order to do this, the above scheme needs to use a private key to protect its security. In the present embodiment a private key is used to generate a sequence of pseudo-random numbers, in a way similar to the spread spectrum technique for generating the watermarks described above. In this embodiment, pseudo-random numbers are not necessarily used to make the watermark patterns, but alternatively or additionally are used to select, from the ICA coefficients selected in step 42, the ICA coefficients where the watermark embedding quantize-and-replace process will place and which class the coefficients belong to, i.e.  $i$ ,  $j$  or  $k$ . For example, suppose the first 10 ICA features in energy order list are selected for this quantization watermark embedding. Based on a private key, two random number sequences with one odd number and another even number may be generated, e.g. a group 1 which is 1, 5, 9, 3, 5, 7, 7, 1, ... and a group 2 which is 8, 2, 8, 6, 2, 4, 10, 4, .... Corresponding items from these two series are paired (e.g. 1 with 8, 5 with 2, etc.). Each pair of odd and even numbers is the selected coefficients for quantization embedding in each block, where odd number belongs to group  $i$  and even is group  $j$ . For a different private key, the sequence is different, and therefore the watermarking is secure from attacks.

Although the above variants of the embodiment of Figs. 2 to 5 have been described in detail, many other variants of the embodiments are possible within the scope of the invention and their implementation will be clear to a skilled reader. As an example, the techniques described above may be extended to watermarking data which is audio data or video data, making use of known ICA techniques for these forms of data.

The present invention be applied to many areas. For example, it can be used for copyright protection: embedding copyright information as a watermark into the host image to be protected, so that the copyright information can be extracted later to claim the ownership of the host image. Also it can be used

for image authentication: the embedded watermark information can also be used to identify any alteration in the image itself and altered locations by detecting the existence of ICA-based WM patterns. Also it can be used for data hiding in image: information such as a description, related knowledge about the image or indexing data can be embedded as a watermark so that such information is protected and attached. Also, it can be used image transaction tracking: the transaction path of the image can be traced by embedding a watermark into the image whenever it is transmitted, and extracting this data later.

Two particularly useful applications of the present invention are:

- to provide a first watermark on multi-media data such as a movie (i.e. a watermark-based copyright protection scheme on commercial movies to trace the unauthorized camera recording), and

- to embed metadata into multi-media data for extra/hidden information transfer.

### References

The disclosure of the following documents is incorporated by reference:

[1] B. A. Olshausen and D. J. Field, "Sparse Coding with an Overcomplete Basis Set: A Strategy employed by V1?", Vision Res., 37(23), 1997.

[2] A. J. Bell and T. J. Sejnowski, "The 'Independent Components' of Natural Scenes are Edge Filters", Vision Res., 37(23):3327-3338, 1997.

[3] B. A. Olshausen and D. J. Field. "Emergence of Simple-Cell Receptive-Field Properties by Learning a Sparse Code for Natural Images", Nature, 381:607-609, 1996.

[4] John Wiley, L. A. Olzak, and J. P. Thomas, "Handbook of Perception and Human Performance. Volume 1: Sensory Processes and Perception. Chapter 7: Seeing Spatial Patterns." University of California, Los Angeles, California,

1986.

[5] G. E. Legge, "Spatial Frequency Masking in Human Vision: Binocular Interactions", J. Opt. Soc. Am. A, 69(6):838-847, June 1979.

[6] H. R. Wilson, D. K. McFarlane, and G. C. Phillips, "Spatial Frequency  
5 Tuning of Orientation Selective Units Estimated by Oblique Masking", Vision Research, 23(9):873-847, 1983.

[7] J. H. van Hateren and A. van der Schaaf, "Independent Component Filters of Natural Images compared with Simple Cells in Primary Visual Cortex", Proc. Royal Soc. Lond. B, 265:359-366, 1998.

10 [8] A. Hyvarinen, "Fast and Robust Fixed-point Algorithms for Independent Component Analysis", IEEE Transactions on Neural Networks, 10(3):626-634, May 1999.

[9] US patent application 10/900739, filed 27 July 2004 and published as US  
20050025337, claiming priority from Singapore patent application 200304195-  
15 1, filed on 29 July 2003.

### Claims

1. A method for generating watermarked data, including the steps of:
  - (i) performing an ICA analysis of a plurality of digital data objects to derive (i) ICA basis functions indicative of respective features shared between the plurality of data objects, and (ii) an ICA inverse transform;
  - (ii) using the ICA basis functions to transform at least one data object into a transformed data object,
  - (iii) modifying at least a portion of the transformed data object using a watermark pattern, and
  - (iv) decoding the data using the ICA inverse transform to obtain the watermarked data.
2. A method according to claim 1 in which the at least one data object is one of said plurality of data objects.
3. A method according to claim 1 in which the at least one data object obeys at least one similarity condition in relation to each of the plurality of data objects.
4. A method according to any preceding claim in which the ICA analysis is performed using multiple patches of the data selected at random from each of the plurality of data objects.
5. A method according to any preceding claim in which the data objects are respective images, and the watermarked data is a watermarked image.
6. A method according to any preceding claim including a selection step, before step (i), of selecting said plurality of data objects from a database of data objects according to at least one similarity criterion.

7. A method according to claim 6 in which said selection step is a clustering algorithm performed on data objects in the database and based on said at least one similarity criterion.

5

8. A method of detecting the presence of the watermark pattern in watermarked data derived from a method according to any preceding claim, the detecting method comprising:

- (a) encoding the watermarked data using said ICA basis functions, and
- 10 (b) detecting said a watermark pattern within the encoded watermarked data.

9. An apparatus for embedding a watermark in data, including:

- (a) a database storing a plurality of digital data objects, and
- 15 (b) a processor arranged to:
  - (i) perform an ICA analysis of a plurality of data objects within the database to derive (i) ICA basis functions indicative of respective features shared between the plurality of data objects, and (ii) an ICA inverse transform;
  - (ii) use the ICA basis functions to transform at least one data object in
  - 20 the database into a transformed data object,
  - (iii) modify at least a portion of the transformed data object using a watermark pattern, and
  - (iv) decode the data using the ICA inverse transform to obtain the watermarked data.

25

10. An apparatus according to claim 9 in which the processor is arranged to employ one of said plurality of data objects as said at least one data object.

11. An apparatus according to claim 9 in which the processor is arranged to employ, as said at least one data object, at least one data object which

30

obeys at least one similarity condition in relation to the plurality of data objects.

12. An apparatus according to claim 11 in which the processor is arranged  
5 to perform said ICA analysis using multiple patches of the data selected at random from each of the plurality of digital data objects.

13. An apparatus according to any of claims 9 to 12 in which the data  
10 objects stored in the database are images, and the watermarked data is a watermarked image.

14. An apparatus according to any of claims 9 to 12 in which the processor  
is arranged to perform a selection step, before step (i), of selecting said  
plurality of digital data objects from a database of digital data objects  
15 according to at least one similarity criterion.

15. An apparatus according to claim 14 in which said selection step is a  
clustering algorithm performed on digital data objects in the database and  
based on said at least similarity criterion.  
20

16. An apparatus for detecting the presence of the watermark pattern in  
watermarked data derived from a method according to any of claims 1 to 7,  
the apparatus comprising:

- (a) a database storing the ICA basis functions; and
- 25 (b) a processor arranged to:
  - (i) encode the watermarked data using said ICA basis functions, and
  - (ii) detect said a watermark pattern within the encoded watermarked data.