

(51) International Patent Classification:
G06T 1/00 (2006.01) **G06F 17/30** (2006.01)(21) International Application Number:
PCT/IB2009/056042(22) International Filing Date:
18 December 2009 (18.12.2009)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
PCT/CN2008/002029
22 December 2008 (22.12.2008) CN(71) Applicant (for all designated States except US):
FRANCE TELECOM [FR/FR]; 6, Place d'Alleray,
F-75015 Paris (FR).

(72) Inventors; and

(75) Inventors/Applicants (for US only): **LIAN, Shiguo** [CN/
CN]; 10F, South Twr, Raycom Info Tech Park C, 2 Sci-
ence Institute South RD, Beijing 100080 (CN). **LIU,**
Zhongxuan [CN/CN]; 10F, South Twr, Raycom Info
Tech Park C, 2 Science Institute South Road, Haidian,Beijing 100080 (CN). **DONG, Yuan** [CN/CN]; 10F,
South Tower Raycom InfoTech Park C, 2 Science Insti-
tute South Road, Beijing, 100080 (CN).(74) Agent: **FRANCE**
TELECOM/FTR&D/PIV/BREVETS; BORNIER Ray-
nald, 38-40 Rue du Général Leclerc, F-92794 Issy
Moulineaux Cedex 9 (FR).(81) Designated States (unless otherwise indicated, for every
kind of national protection available): AE, AG, AL, AM,
AO, AT, AU, AZ, BA, BB, BG, BH, BR, BW, BY, BZ,
CA, CH, CL, CN, CO, CR, CU, CZ, DE, DK, DM, DO,
DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, GT,
HN, HR, HU, ID, IL, IN, IS, JP, KE, KG, KM, KN, KP,
KR, KZ, LA, LC, LK, LR, LS, LT, LU, LY, MA, MD,
ME, MG, MK, MN, MW, MX, MY, MZ, NA, NG, NI,
NO, NZ, OM, PE, PG, PH, PL, PT, RO, RS, RU, SC, SD,
SE, SG, SK, SL, SM, ST, SV, SY, TJ, TM, TN, TR, TT,
TZ, UA, UG, US, UZ, VC, VN, 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,

[Continued on next page]

(54) Title: A METHOD OF AND APPARATUS FOR AUTHENTICATING DATA CONTENT

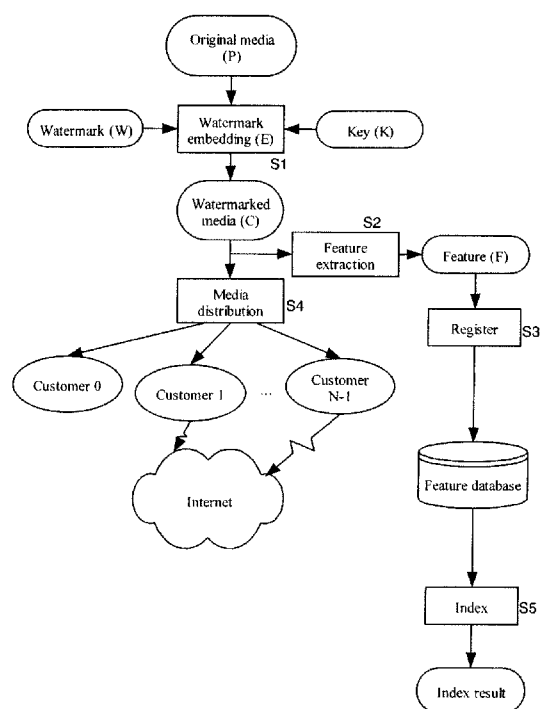


FIG. 2A

(57) Abstract: A method of watermarking data content for distribution, the method comprising: embedding auxiliary identification information in a data content; extracting a feature from the data content embedded with the auxiliary identification information; storing the extracted feature in a feature database, the extracted feature being associated with identification data identifying the data content from which the feature has been extracted, wherein the extracted feature stored in the feature database may be used to identify a detected data content and to determine operation parameters for rectifying the detected data content such that auxiliary identification information may be extracted therefrom for authentication of the detected data content. A method of authenticating data content the method comprising the steps of extracting a feature from a data content; comparing the extracted feature with a plurality of features stored in a feature database in order to determine at least one matching feature from the plurality of stored features wherein each of the stored features has been extracted from a corresponding data content embedded with auxiliary identification information prior to distribution of said data content; determining a transform relationship between the extracted feature and the matching feature; rectifying the data content according to the determined transform relationship; and extracting auxiliary identification information from the rectified data content so that the auxiliary identification information may be used for authentication of the data content.



TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HR, HU, IE, IS, IT, LT, LU, LV, MC, MK, MT, NL, NO, PL, PT, RO, SE, SI, SK, SM, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

— of inventorship (Rule 4.17(iv))

Published:

— with international search report (Art. 21(3))

— before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments (Rule 48.2(h))

Declarations under Rule 4.17:

- as to applicant's entitlement to apply for and be granted a patent (Rule 4.17(ii))
- as to the applicant's entitlement to claim the priority of the earlier application (Rule 4.17(iii))

A METHOD OF AND APPARATUS FOR AUTHENTICATING DATA CONTENT

FIELD OF THE INVENTION

The present invention relates to a method of authenticating data content. Particularly, but not exclusively the invention relates to a method of authenticating watermarked media content and a method of indexing media content.

BACKGROUND OF THE INVENTION

Watermarking is a technique that is regularly used in copyright protection to determine the ownership or media data content or to detect the origin of physical or electronic media that has been illegally redistributed. The technique involves embedding auxiliary identification information indicating ownership or customer ID into media data content in the form of a media signal before the media data content is distributed. Generally the embedded watermark is in the form of machine readable code and should be invisible and unobtrusive and not interfere with the protected media content. The media content may be image, video or audio data. It may also include other types of media objects including documents, software, multi-dimensional graphics models and surface textures of objects. For example, referring to Figure 1a a media content provider distributes media content such as a television program to a number of customers. One of the customers then redistributes his copy to others via the internet. The problem is then how to determine if the media data content which has been subsequently detected originates from that content provider. The next problem involves determining which customer was responsible for redistributing the media data content over the Internet.

JP2004112318, for example, describes a watermarking based image protection method in which the ownership information is embedded into images before they are distributed. By detecting whether or not the watermark exists in an image or not, the copyright of the image distributed over Internet can be authenticated. However, considering that operations such as compression, rotation, shearing, scaling, translation, and the like are often performed on the images successfully detecting the watermark in the operated images is becoming increasingly difficult. Prior art

techniques suffer the drawback that embedded watermark are often not robust to such geometrical transformations or desynchronisation operations.

Another requirement in media content distribution is content indexing. Content indexing refers to the finding specific data files from within a number of data files stored in a database.

FR2843212 describes a content index method based on image feature extraction and matching. In the described method, a feature of an image is extracted and compared with the features extracted from images stored in a database or with features directly stored in a database, to find one or more matching images. For media related services, often both content index and copyright protection are required. Currently the two functionalities are performed independently

SUMMARY OF THE INVENTION

Accordingly, it would be advantageous to provide a method of authenticating content data which implements both a copyright protection technique and a content indexing functionality. It would also be desirable to provide a method of authenticating data content with improved robustness to desynchronisation operations.

To better address one or more of the foregoing concerns, in accordance with a first aspect of the invention there is provided a method of watermarking data content for distribution, the method comprising: embedding auxiliary identification information in a data content; extracting a feature from the data content embedded with the auxiliary identification information; storing the extracted feature in a feature database, the extracted feature being associated with identification data identifying the data content from which the feature has been extracted, wherein the extracted feature stored in the feature database is usable to identify a detected data content and to determine operation parameters for rectifying the detected data content such that auxiliary identification information is extractable therefrom for authentication of the detected data content.

By a method of watermarking is meant a method in which auxiliary data is embedded in a data content for authentication or identification purposes. The auxiliary

identification information may be a digital watermark. The data content may be a digital media content such as image, audio or video data. The feature may be a feature or a group of features.

- 5 The extracted feature may be a corner point based feature. Such features are more robust to desynchronisation operations.

The auxiliary identification information may be embedded into the wavelet domain of the data content. For example embedding the auxiliary identification information may
 10 include transforming the data content by wavelet transformation to obtain sub-bands $I^{r,s}$ where $r \in \{0,1,2,3\}$ is the resolution level, and $s \in \{LL, LH, HL, HH\}$ is the orientation; and wherein the auxiliary information is embedded into the sub-bands according to the expression:

$$I_i^{r,s} (i = 0,1,\dots,m-1) = \begin{cases} I_i^{r,s} (1 + \alpha w_i) & s \neq LL \\ I_i^{r,s} & otherwise \end{cases}$$

- 15 where α represents the embedding strength where $(0 < \alpha \leq 1)$; $1 + \alpha w_i > 0$).

Preferably $r \in \{2,3\}$ in order to provide a more robust auxiliary identification information.

- 20 A second aspect of the invention provides a method of authenticating data content the method comprising extracting a feature from a data content; comparing the extracted feature with a plurality of features stored in a feature database in order to determine at least one matching feature from the plurality of stored features wherein each of the stored features has been extracted from a corresponding data content
 25 embedded with auxiliary identification information prior to distribution of said data content; determining a transform relationship between the extracted feature and the matching feature; rectifying the data content according to the determined transform relationship; and extracting auxiliary identification information from the rectified data content so that the auxiliary identification information is usable for authentication of
 30 the data content.

Matching the extracted feature with the matching feature may comprise determining the difference $\text{Dist}(F, F')$ between the extracted Feature F' and a matching feature F_i according to the expression

$$\text{Dist}(F_i, F') = \frac{1}{R} \sum_{j=0}^{R-1} \sqrt{(x_{ij} - x'_j)^2 + (y_{ij} - y'_j)^2}$$

5 and comparing $\text{Dist}(F, F')$ to a predetermined feature matching threshold T_F .

Determining a transform relationship between the extracted feature and the matching feature may include determining a transformation according to:

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = H \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$$

where, (x', y') and (x, y) correspond to the corner point coordinates of the extracted feature F' and the matching feature F_k , respectively.

15 The data content may be rectified or emended by rectifying a pixel position (x', y') in the data content according to:

$$\begin{cases} x'_k = \frac{ex' - by' - ec + bf}{ea - bd} \\ y'_k = \frac{dx' - ay' - cd + af}{bd - ae} \end{cases}$$

where, (x'_k, y'_k) is the corresponding pixel position in the rectified data content.

Authentication of the auxiliary information may include

computing a correlation value for correlating the extracted auxiliary information to a known auxiliary information according to the expression

$$\rho = \frac{1}{m} \sum_{i=1}^m |I_i^{r,s}| w_i$$

computing a threshold according to

$$T = \frac{6}{N} \sqrt{\sum_{i=1}^N (I_i^{r,s})^2}$$

- 5 and determining if $\rho \leq T$ to authenticate the auxiliary information.

A third aspect of the invention provides an apparatus for embedding authentication information in data content for distribution, the apparatus comprising:

- 10 an embedder for embedding auxiliary identification information in a data content;
- a feature extractor for extracting a feature from the data content embedded with the auxiliary identification information;
- a feature database for storing the extracted feature, the extracted feature
- 15 being associated with identification data identifying the data content from which the feature has been extracted,
- wherein the extracted feature stored in the feature database is usable to identify a detected data content and to determine operation parameters for rectifying the detected data content such that auxiliary identification data is extractable
- 20 therefrom for authentication of the detected data content.

The feature extractor may be operable to extract a corner point based feature from the data content embedded with the auxiliary identification information.

- 25 A fourth aspect of the invention provides an apparatus for authenticating data content the apparatus comprising
- a feature extractor for extracting a feature from a data content;
- a processor for
- comparing the extracted feature with a plurality of features stored in a
- 30 feature database in order to determine at least one matching feature from the

plurality of stored features wherein each of the stored features has been extracted from a corresponding data content embedded with auxiliary identification information prior to distribution of said data content;

determining a transform relationship between the extracted feature and the matching feature; and

rectifying the data content according to determined transform relationship; the apparatus further comprising

an extractor for extracting auxiliary identification information from the rectified data content so that the auxiliary identification information is usable for authentication of the data content.

A fifth aspect of the invention provides an method of data content authentication comprising, prior to distribution of a first data content, embedding auxiliary identification information in the first data content; extracting a first feature from the first data content embedded with the auxiliary identification information; storing the extracted first feature in a feature database, the extracted first feature being associated with identification data identifying the first data content from which the first feature has been extracted, and distributing the first data content; and on detection of a second data content after distribution, extracting a second feature from the second data content; comparing the second feature with the first feature stored in the feature database in order to determine if the second feature matches the first feature; and if it is determined that the second feature matches the first feature determining a transform relationship between the second feature and the first feature; rectifying the second data content according to the determined transform relationship; and extracting auxiliary identification information from the rectified second data content so that the auxiliary identification information is usable for authentication of the second data content.

A sixth aspect of the invention provides a system for authenticating data content, the system comprising an embedder for embedding auxiliary identification information in a data content; a first feature extractor for extracting a first feature from the data content embedded with the auxiliary identification information; a feature database for storing the extracted feature, the extracted feature being associated with identification data identifying the data content from which the feature has been

extracted, a second feature extractor for extracting a second feature from distributed data content; a processor for comparing the second feature with the first feature stored in the feature database in order to determine if the second feature matches the first feature; and if it is determined that the second feature matches the first feature the processor being operable to determine a transform relationship between the second feature and the first feature; rectifying the second data content according to the determined transform relationship; and a watermark extractor for extracting auxiliary identification information from the rectified second data content so that the auxiliary identification information is usable for authentication of the second data content. The first feature extractor and the second feature extractor may be the same feature extractor or separate feature extractors.

Aspects of the invention provide a mechanism which combines both copyright protection and media content index since a feature extracted from watermarked media content can be used for media content indexing in a database as well as for rectifying a watermarked media content, which has been detected after distribution, for media content authentication. Moreover, the extracted feature stored in the feature database improves the watermarking algorithm's robustness. Since the data content is emended or rectified according to the determined transformation undergone by the feature extracted from the data content, a watermark can thereby be extracted from the rectified or emended data content and thus used for authentication purposes.

The methods according to the invention may be computer implemented. The methods may be implemented in software on a programmable apparatus. They may also be implemented solely in hardware or in software, or in a combination thereof.

Since the present invention can be implemented in software, the present invention can be embodied as computer readable code for provision to a programmable apparatus on any suitable carrier medium. A tangible carrier medium may comprise a storage medium such as a floppy disk, a CD-ROM, a hard disk drive, a magnetic tape device or a solid state memory device and the like. A transient carrier medium may include a signal such as an electrical signal, an electronic signal, an optical

signal, an acoustic signal, a magnetic signal or an electromagnetic signal, e.g. a microwave or RF signal.

BRIEF DESCRIPTION OF THE DRAWINGS

Embodiments of the invention will now be described, by way of example only, and
5 with reference to the following drawings in which:-

Figure 1A is a schematic view of a media content being distributed to the public;

Figure 1B is a flow chart illustrating a method of authenticating media content
10 according to the prior art;

Figure 2A is a flowchart illustrating a method of embedding a watermark in media content according to an embodiment of the invention;

15 Figure 2B is a flowchart illustrating a method of authenticating media content according to an embodiment of the invention;

Figure 3A is a flowchart illustrating a method of embedding a watermark in media content according to a particular embodiment of the invention;

20

Figure 3B is a flowchart illustrating a method of authenticating media content according to a particular embodiment of the invention;

Figure 4 is an example of an image highlighting corner features;

25

Figure 5 is an example of an original image and corresponding operated images;

Figure 6A is a graphical illustration of an example of corner point matching between features in an original image and features in a rotated original image;

30

Figure 6B is a graphical illustration of watermark detection with watermark correlation and threshold; and

Figure 7 is a table illustrates the example of the results of a robustness test under the conditions of various attacks.

5 DETAILED DESCRIPTION

A method of authenticating content data according to an embodiment of the invention will be described with reference to Figures 2A to 4B.

10 With reference to Figures 2 and 3, the method of authenticating content data includes five principal steps:

- media watermark embedding;
- robust feature extraction and registration;
- media distribution;
- 15 ▪ watermark extraction and authentication; and
- media indexing.

Referring to Figure 2A step S1 of the method according to the first embodiment of the invention comprises embedding a watermark W into media data content P under the control of a key K to generate watermarked media C . Key K controls the watermark embedding position or parameters. In this embodiment of the invention, the watermark W represents the ownership information or customer ID. The embedding method may be performed according to existing watermarking algorithms such as, for example, those described in documents Cox et al.: Secure Spread Spectrum

20 Watermarking for Multimedia. IEEE Trans. on Image Processing, Vol. 6, No. 12. (1997) 1673-1687, or Cheng et al.: Optimum Detection and Decoding of Multiplicative Watermarks in DFT Domain. Proceedings of IEEE International Conference on Acoustics, Speech and Processing, Vol. 4. (2002) 3477-3480. Preferably, a method which is more robust to robust to general attacks such as the method described in

25 Cheng et al. An Additive Approach to Transform-Domain Information Hiding and Optimum Detection Structure. IEEE Transactions on Multimedia, Vol. 3, No. 3, pp. 273-284, 2001, is implemented. These watermarking algorithms embed a watermark

30 into the spatial domain or frequency domain of image, video or audio content data.

Such algorithms are often robust to general attacks such as adding noise, compression, A/D or D/A conversion, filtering, etc.

In step S2 a feature F is extracted from the watermarked media C and in step S3 stored and registered in a feature database D having a size M . In the feature database D , the feature F is associated with data representing the watermarked media content C from which it has been extracted. An example of a data structure of the feature database is shown in Table 1.

Name of media signal	Feature
Lena	F_0
Bus	F_1
...	...
Scene	F_{M-1}

Table 1: Example of a data structure of the feature database

In Table 1, the first column represents the names of media signals, for example, Lena is the name of an image. And the second column represents the features which are extracted from the media signals, for example, F_0 is extracted from the signal named Lena.

The feature F should satisfy two requirements: firstly, feature F should be robust to watermarking attacks, such as general geometrical attacks including rotation, shearing, translation, scaling, etc operations. Secondly, feature F should be usable in media indexing and be of a smaller data volume compared to the media data content itself. A feature as such as corner point, boundary, edge, histogram, may, for example, be used to this end.

In step S4 the watermarked media is distributed to a number N of customers by means such as broadcasting, multicasting, unicasting, etc. Some customers may directly distribute the received media over Internet, or distribute it after operations such as recompression, scaling, translation, etc have been performed on the

watermarked media content C. This distributed media content represented as C' may then be distributed freely from one person to another.

Authentication of detected media content will now be described with reference to Figure 2B. If media content C' is subsequently detected the steps of authentication of the detected media content are carried out. In step S6 a watermark W' is extracted from the detected media content C' and compared in step S7 with the original watermark W. In this embodiment the watermark extraction method is symmetric to the watermark embedding method of step S1. If the difference $|W'-W|$ between the original watermark W and the extracted watermark W' is less than T_W where T_W corresponds to a predetermined watermark matching threshold, then the watermark W' is authenticated, the media content C' is deemed as being copyright protected, and the authentication process terminates. From the identification of W' matching W the origin of the detected media content C' may be determined, as well as the identity of the customer to whom that media content C' was distributed to.

If $|W'-W| > T$ then the process continues to step S8 where a feature F' is extracted from the detected media content C'. In step S9 the extracted feature F' is compared with features F_i stored in the feature database D. The results from the comparison provide the n ($1 \leq n < M$) most matched features ($F_0, F_1, \dots, F_{n-1}$) where M is the number of features F_i stored in the feature database D. The matching algorithm is based on the comparison $|F'-F_i|$ between the extracted feature F' and the stored feature F_i where $i=0,1,\dots,n-1$ and T_F where T_F corresponds to a predetermined feature comparison threshold. If the difference $|F'-F_i|$ between the extracted feature F' and the stored feature F_i is less than T_F , i.e. $|F'-F_i| < T_F$, the feature F_i is deemed to be a matching feature. Otherwise, the feature F_i is not deemed to be matched.

The n media contents associated with the n features correspond to the matching index results. From the n indexed features, each pair of matching features (F', F_i) ($i=0,1,\dots,n-1$) is used to compute the transformation from F_i to F' caused by attack operations, by for example corner matching, and the determined transformation is then used accordingly to rectify or emend the media content from C' to C'' in step S10. For example, if F_i is different to F' in terms of rotation angle, then C' is inverse rotated by the same angle in order to provide the original watermarked media

content. From the rectified media C'' , a watermark W'' can be extracted in step S11 and compared with the original watermark W in step S12. If the difference $|W'-W|$ between the extracted watermark W' and the original watermark W is less than T_w , i.e. $|W'-W| < T_w$ then the watermark W is deemed to exist in the detected media

5 content, and the media content is deemed to be copyright protected. The authentication process then terminates. Otherwise, steps S8 to S10 are repeated feature by feature F_i until $i=n$ or the original watermark W is detected. From the identification of W' the origin of the detected media content C' may be determined, as well as the identity of the customer to whom that media content C' was distributed to

10 In step S5 of Figure 2A the media index created using the registered Features F_i is used to find the original media content C corresponding to C' from feature database D. When robust feature F' is extracted from the received media C' in step S7 and matched with the feature database D in step S9 of the feature extraction process the
15 matching result gives the n ($1 \leq n < M$) most matched features ($F_0, F_1, \dots, F_{n-1}$). The n media contents corresponding to the respective n features constitute the index results.

20 In a particular embodiment of the invention a corner point is used as the extracted feature. An image ownership protection and index method using corner point features is illustrated in Fig. 3A, which depicts the process of watermark embedding and Figure 3B which illustrates the feature extraction process, the watermark extraction and the authentication processes.

25 With reference to Figure 3A the watermark embedding and feature extraction process according to this particular embodiment of the invention includes an initial step S21 in which the original media content which in this embodiment comprises an image P , a watermark W and a key K are initialized. In this particular embodiment, the watermark W to be embedded in the image P , is a Gaussian sequence
30 $W=[w_0, w_1, \dots, w_{m-1}]$. In step S22 watermark W is embedded into the wavelet domain of image P under the control of key K , resulting in watermarked media C . In this embodiment, key K controls the permutation of the watermark W . A permutation method based on pseudorandom numbers or a chaotic map may be used. In the watermark embedding step S22, the image P is firstly transformed by wavelet

transformation, which produces coefficients in different sub-band. For example, if image P is decomposed into 4 resolution levels by wavelet transformation, the produced sub-bands are denoted by $I^{r,s}$ where $r \in \{0,1,2,3\}$ is the resolution level, and $s \in \{LL, LH, HL, HH\}$ is the orientation; L – Low frequency, H – High frequency. Here,
 5 LL, LH, HL and HH denote 4 different frequency bands divided by wavelet transformations.

In watermark embedding step S22 the watermark W is embedded into the sub-bands according to the expression:

$$I_i^{r,s} (i = 0,1,\dots,m-1) = \begin{cases} I_i^{r,s} (1 + \alpha w_i) & s \neq LL \\ I_i^{r,s} & otherwise \end{cases}$$

10 where m represents the length of watermark sequence, w_i is the i-th watermark value in the watermark sequence. In order to keep the watermark robust, preferably $r \in \{2,3\}$

α represents the embedding strength where $(0 < \alpha \leq 1)$; $1 + \alpha w_i > 0$), which ranges

15 from $[0,1]$ and can be computed by a human visual system (HVS) such as described in A. S. Lewis, and G. Knowles: Image Compression Using the 2-D Wavelet Transform. IEEE Transactions on Image Processing, Vol. 1, No. 2. (1992) 244-250; or set as a constant.

20 After embedding, the sub-bands are inversely transformed by wavelet transformation, and the produced watermarked image is C.

In step S23, by studying the pixels of the image C the corner features $F=[f_0, f_1, \dots, f_{R-1}]$ can be extracted from image C using for example a corner and edge detection
 25 method such as, for example, that described in C. Harris and M. Stephens: A Combined Corner and Edge Detector. 4th Alvey Vision Conference. (1988) 147-151; or H. Moravec: Obstacle Avoidance and Navigation in the Real World by a Seen Robot Rover. Technical Report CMU-RI-TR-3. Robotics Institute, Carnegie-Mellon University. (1980).

Edges are generally points where there is a boundary (or an edge) between two image regions. In practice, edges are usually defined as sets of points in the image which have a strong gradient magnitude. Corner points are typically points of the image where the difference between adjacent pixels is generally high in all directions.

- 5 A corner can be defined as the intersection of two edges and may also be defined as a point for which there are two dominant and different edge directions in a local neighbourhood of the point.

- 10 $f_i=(x_i,y_i)$ ($i=0,1,\dots,R-1$) correspond to the co-ordinates of a corner point. The corner points are generally robust to geometric operations such as rotation, shearing, scaling, translation, etc. Typically, for different images, the number of the extracted corner points differs. In order to maintain coherence, only R corner points are selected as the feature F . The selection can be random.

- 15 Figure 4A illustrates the selection of a number of corner points $f_i=(x_i,y_i)$ in an image.

In step S24, the watermarked image C is registered by storing the corner points $f_i=(x_i,y_i)$ of feature F and the corresponding image name in the feature database D .

- 20 An example of the data structure of the database is shown in Table 2.

Name of media content	Feature
Lena	$f_{00} f_{01} \dots f_{0R-1}$
Bridge	$f_{10} f_{11} \dots f_{1R-1}$
...	...
Scene	$f_{M-10} f_{M-11} \dots f_{M-1R-1}$

Table 2

- 25 In step S25, the watermarked and registered image C is distributed to customers.

The watermark embedding and feature extraction process according to this particular embodiment will now be described with Figure 3B

In step S31, image C' is detected. Here, image C' is the operated copy of image C, which has been attacked by operations such as adding noise, compression, rotation, shearing, scaling, translation, etc. T_w is a threshold used to determine the existence of a watermark. T_F is the threshold used to determine the matching features.

5

In step S32, the watermark W' in image C' is permuted under the control of key K. The sub-bands of the watermark W' are obtained by wavelet transformation, and the correlation value:

$$\rho = \frac{1}{m} \sum_{i=1}^m |I_i^{r,s}| w_i$$

10

and the watermark threshold:

$$T_w = \frac{6}{N} \sqrt{\sum_{i=1}^N (I_i^{r,s})^2} \quad \text{are computed.}$$

- 15 In step S33 the computed correlation value ρ for watermark W' is compared to the threshold T_w . If $\rho \geq T_w$, then the watermark W' is deemed as existing, and the authentication process terminates.

- Otherwise, if $\rho < T_w$ then the following steps of the process are carried out. In step 20 S34, a feature $F' = [f'_0, f'_1, \dots, f'_{R-1}]$ composed of R corner points is extracted from the watermarked image C'. In step S35 the n closest matching features $SF = \{F_0, F_1, \dots, F_{n-1}\}$ are obtained by computing the distance $\text{Dist}(F_i, F')$ and comparing with the threshold T_F .

- 25 The extracted feature F' and the stored features F_i are compared according to the expression:

$$\text{Dist}(F_i, F') = \frac{1}{R} \sum_{j=0}^{R-1} \sqrt{(x_{ij} - x'_j)^2 + (y_{ij} - y'_j)^2}$$

If $Dist(F_i, F') \leq T_F$ then the feature F_i is deemed to be a matching feature.

Otherwise, F_i is deemed as not matching. The n images corresponding to the n features in SF correspond to the indexed images.

- 5 In step S36 k is set to 0, (where k is the matching feature number of the n matching features ranges from 0 to $n-1$) and the following operations are performed:

For $k=0$ to $k=n-1$ two features (F_k, F') are matched by computing the parameters (a, b, c, d, e, f) of an affine transformation according to:

10

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = H \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$$

where, (x', y') and (x, y) correspond to the corner point coordinates of F' and F_k , respectively.

15

Using at least three point pairs, the parameters of H can be computed. The computing method may be least square method, such as described in G. Xue and P. Lu: A Counter-Geometric Distortions Data Hiding Scheme Using Double Channels in Color Images. The 3rd IWDW. (2004) 42-54; or a coarse matching before random sample consensus (RANSAC) method such as described in M. A. Fishler and R. C. Bolles: Random Sample Consensus: A Paradigm for Model Fitting with Applications to Image Analysis and Automated Cartography. The Communications of the ACM, Vol. 24, No. 6. (1981) 381-395.

20

25

In step S37 the computed parameters (a, b, c, d, e, f) are then used to rectify the image from C' to C'_k . That is, these parameters are used to emend the pixel position (x', y') in C' according to:

$$\begin{cases} x'_k = \frac{ex' - by' - ec + bf}{ea - bd} \\ y'_k = \frac{dx' - ay' - cd + af}{bd - ae} \end{cases}$$

where, (x'_k, y'_k) is the pixel position in corresponding image C'_k .

- 5 In step S38 from the emended image C'_k , a watermark correlation ρ and a watermark threshold T is computed, respectively, according to a similar method to that of step S32.

10 In step S39 if the watermark correlation $\rho < T$, then the watermark is deemed as existing i.e. the image is copyright protected, and the authentication process is terminated.

Otherwise, if $\rho \geq T$, the following steps are then performed:

- 15 k is set to $k=k+1$, and the process returns to step S36 until $K = n$. If k reaches n in step S40 then it is deemed that there is no watermark in the image and thus determined that the image is not copyright protected. The authentication process then terminates.

- 20 An example of results of the process are shown in Figures 5 to 7. In this example, $m=1000$, $R=80$, $TF=20$ $n=10$, and the test image includes baboon, plane, lena, Elaine, Barbara, etc. Fig. 5 shows the corner detection results of the original and operated images where i) is the original image, ii) a cropped image iii) a rotated image, iv) a scaled image v) a sheared image and vi) a translated image. Figure 6A
25 graphically illustrates the result of corner point matching of a rotated image and Figure 6B illustrates watermark detection with correlation and threshold. Figure 7 presents a table showing the robustness test under the condition of various attacks. The table of Figure 7 illustrates that the scheme can survive the desynchronization attacks of global geometrical transform and general signal processing attacks. For

example, the angle range against the rotation attack and the rotation-scaling one is up to 10 degrees.

The embodiments of the invention provide the advantage that a mechanism for both copyright protection and media content index is provided since the extracted feature can be used for content index as well as for media content authentication. Moreover, the extracted feature stored in the feature database improves the watermarking algorithm's robustness.

Embodiments of the invention find application in the distribution of media content data by media service providers to customers where both copyright protection and content index functionalities are required.

Although the present invention has been described hereinabove with reference to specific embodiments, the present invention is not limited to the specific embodiments, and modifications will be apparent to a skilled person in the art which lie within the scope of the present invention.

For example, although in the preceding embodiment the media data content is constituted of an image, it will be appreciated that in alternative embodiments of the invention the media content data may be any audio, video or image data content.

While in the foregoing embodiments of the invention, a corner point based feature is used, it will be appreciated that in alternative embodiments of the invention other features such as boundary, edge or histogram features may be used .

Many further modifications and variations will suggest themselves to those versed in the art upon making reference to the foregoing illustrative embodiments, which are given by way of example only and which are not intended to limit the scope of the invention, that being determined solely by the appended claims. In particular the different features from different embodiments may be interchanged, where appropriate.

In the claims, the word "comprising" does not exclude other elements or steps, and

the indefinite article "a" or "an" does not exclude a plurality. The mere fact that different features are recited in mutually different dependent claims does not indicate that a combination of these features cannot be advantageously used. Any reference signs in the claims should not be construed as limiting the scope of the invention.

CLAIMS

1. A method of watermarking data content for distribution, the method comprising:

5 embedding auxiliary identification information in a data content;
extracting a feature from the data content embedded with the auxiliary identification information;

storing the extracted feature in a feature database, the extracted feature being associated with identification data identifying the data content from which the
10 feature has been extracted,

wherein the extracted feature stored in the feature database is usable to identify a detected data content and to determine operation parameters for rectifying the detected data content such that auxiliary identification information is extractable therefrom for authentication of the detected data content.

15 2. A method according to claim 1, wherein the extracted feature comprises a corner point based feature.

3. A method according to claim 1 wherein the auxiliary identification
20 information is embedded into the wavelet domain of the data content.

4. A method according to claim 1, wherein embedding the auxiliary identification information includes transforming the data content by wavelet transformation to obtain sub-bands $I^{r,s}$ where $r \in \{0,1,2,3\}$ is the resolution level, $s \in \{LL, LH, HL, HH\}$ is
25 the orientation L – Low frequency, H – High frequency. LL, LH, HL and HH denoting 4 different frequency bands divided by wavelet transformations; and wherein the auxiliary information is embedded into the sub-bands according to the expression:

$$30 \quad I_i^{r,s} (i = 0,1,\dots,m-1) = \begin{cases} I_i^{r,s} (1 + \alpha w_i) & s \neq LL \\ I_i^{r,s} & otherwise \end{cases}$$

where α represents the embedding strength where:

$$(0 < \alpha \leq 1);$$

$$1 + \alpha w_i > 0$$

m represents the length of watermark sequence, w_i is the i-th watermark value in the watermark sequence.

- 5 5. A method according to claim 4 wherein $r \in \{2, 3\}$.
6. A method of authenticating data content the method comprising the steps of
 extracting a feature from a data content;
 comparing the extracted feature with a plurality of features stored in a
 10 feature database in order to determine at least one matching feature from the
 plurality of stored features wherein each of the stored features has been extracted
 from a corresponding data content embedded with auxiliary identification information
 prior to distribution of said data content;
 determining a transform relationship between the extracted feature and the
 15 matching feature;
 rectifying the data content according to the determined transform
 relationship; and
 extracting auxiliary identification information from the rectified data content
 so that the auxiliary identification information may be used for authentication of the
 20 data content.
7. A method according to claim 6, wherein matching the extracted feature with
 the matching feature comprises determining the difference $\text{Dist}(F, F')$ between the
 extracted Feature F' and a matching feature F_i according to the expression:

$$\text{Dist}(F_i, F') = \frac{1}{R} \sum_{j=0}^{R-1} \sqrt{(x_{ij} - x'_j)^2 + (y_{ij} - y'_j)^2}$$

and comparing $\text{Dist}(F, F')$ to a predetermined feature matching threshold T_F .

8. A method according to claim 6, wherein determining a transform relationship
 30 between the extracted feature and the matching feature includes determining a
 transformation according to

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix} \begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = H \begin{pmatrix} x \\ y \\ 1 \end{pmatrix}$$

where, (x', y') and (x, y) correspond to the corner point coordinates of the extracted feature F' and the matching feature F_k , respectively.

- 5 9. A method according to claim 8, wherein the data content is rectified by rectifying a pixel position (x', y') in the data content according to

$$\begin{cases} x'_k = \frac{ex' - by' - ec + bf}{ea - bd} \\ y'_k = \frac{dx' - ay' - cd + af}{bd - ae} \end{cases}$$

where, (x'_k, y'_k) is the corresponding pixel position in the rectified data content.

10

10. A method according to claim 6, wherein authentication of the auxiliary information comprises

computing a correlation value for correlating the extracted auxiliary information to a known auxiliary information according to the expression

15

$$\rho = \frac{1}{m} \sum_{i=1}^m |I_i^{r,s}| w_i$$

computing a watermark threshold T_w according to the expression

$$T_w = \frac{6}{N} \sqrt{\sum_{i=1}^N (I_i^{r,s})^2}$$

- 20 and determining if $\rho \leq T_w$ to authenticate the auxiliary information.

11. An apparatus for watermarking data content for distribution, the apparatus comprising:

an embedder for embedding auxiliary identification information in a data content;

a feature extractor for extracting a feature from the data content embedded with the auxiliary identification information;

5 a feature database for storing the extracted feature, the extracted feature being associated with identification data identifying the data content from which the feature has been extracted,

wherein the extracted feature stored in the feature database may be used to identify a detected data content and to determine operation parameters for rectifying
10 the detected data content such that auxiliary identification data may be extracted therefrom for authentication of the detected data content.

12. An apparatus according to claim 11, wherein the feature extractor is operable to extract a corner point based feature from the data content embedded
15 with the auxiliary identification information.

13. An apparatus for authenticating data content the apparatus comprising
a feature extractor for extracting a feature from a data content;
a processor for
20 comparing the extracted feature with a plurality of features stored in a feature database in order to determine at least one matching feature from the plurality of stored features wherein each of the stored features has been extracted from a corresponding data content embedded with auxiliary identification information prior to distribution of said data content;
25 determining a transform relationship between the extracted feature and the matching feature; and
rectifying the data content according to the determined transform relationship; the apparatus further comprising
an extractor for extracting auxiliary identification information from the
30 rectified data content so that the auxiliary identification information may be used for authentication of the data content.

14. A system for authenticating data content, the system comprising

an embedder for embedding auxiliary identification information in a data content;

a first feature extractor for extracting a first feature from the data content embedded with the auxiliary identification information;

5 a feature database for storing the extracted first feature , the extracted feature being associated with identification data identifying the data content from which the feature has been extracted,

a second feature extractor for extracting a second feature from distributed data content;

10 a processor for

comparing the second feature with the first feature stored in the feature database in order to determine if the second feature matches the first feature; and if it is determined that the second feature matches the first feature the processor being operable to determine a transform relationship between the second feature and the first feature;

15 rectifying the second data content according to the determined transform relationship; and

a watermark extractor for extracting auxiliary identification information from the rectified second data content so that the auxiliary identification information is
20 usable for authentication of the second data content.

15. A computer program product for a data-processing device, the computer program product comprising a set of instructions which, when loaded into the data-processing device, causes the device to perform the steps of the method according
25 to claim 1 or claim 6.

16. A computer-readable medium carrying one or more sequences of instructions of the computer program product of claim 15.

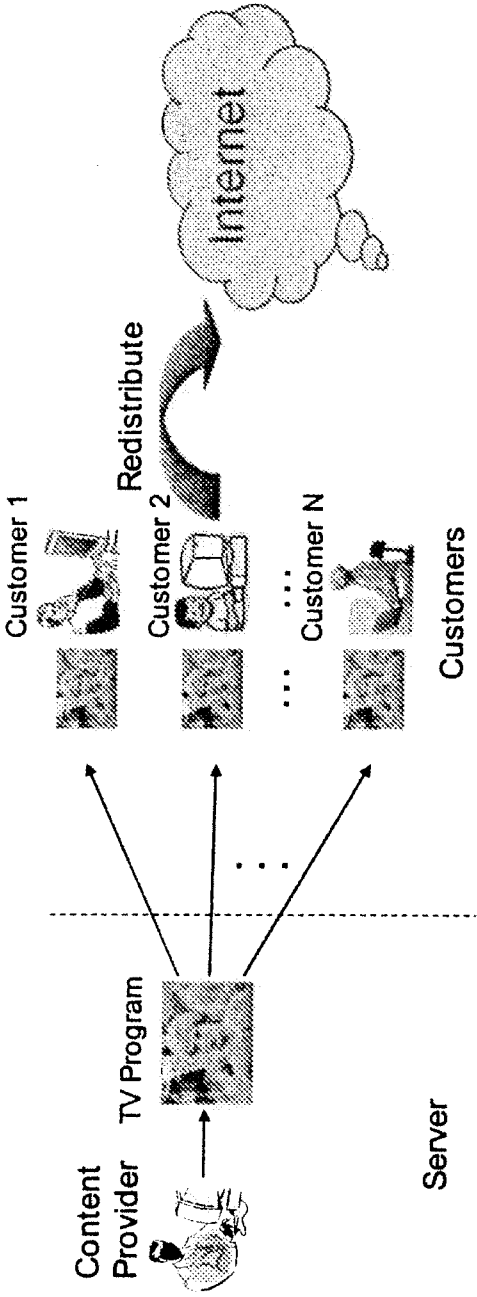


FIG. 1A

2/10

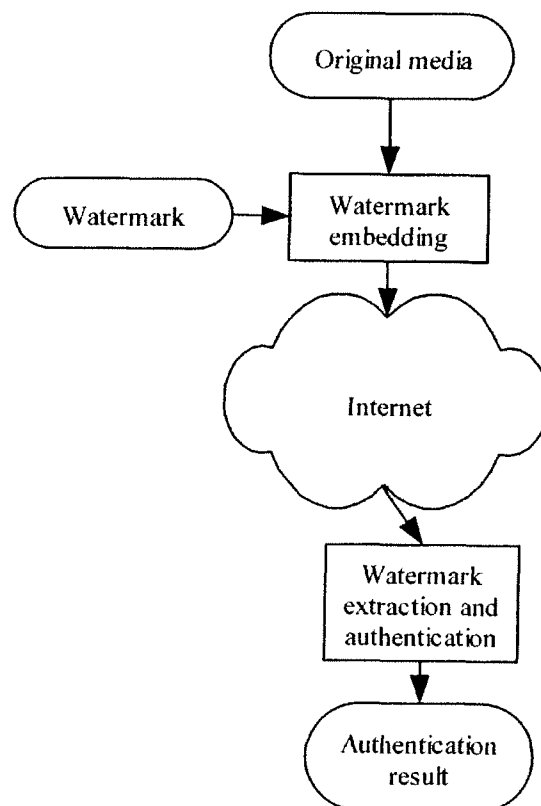


FIG. 1B

3/10

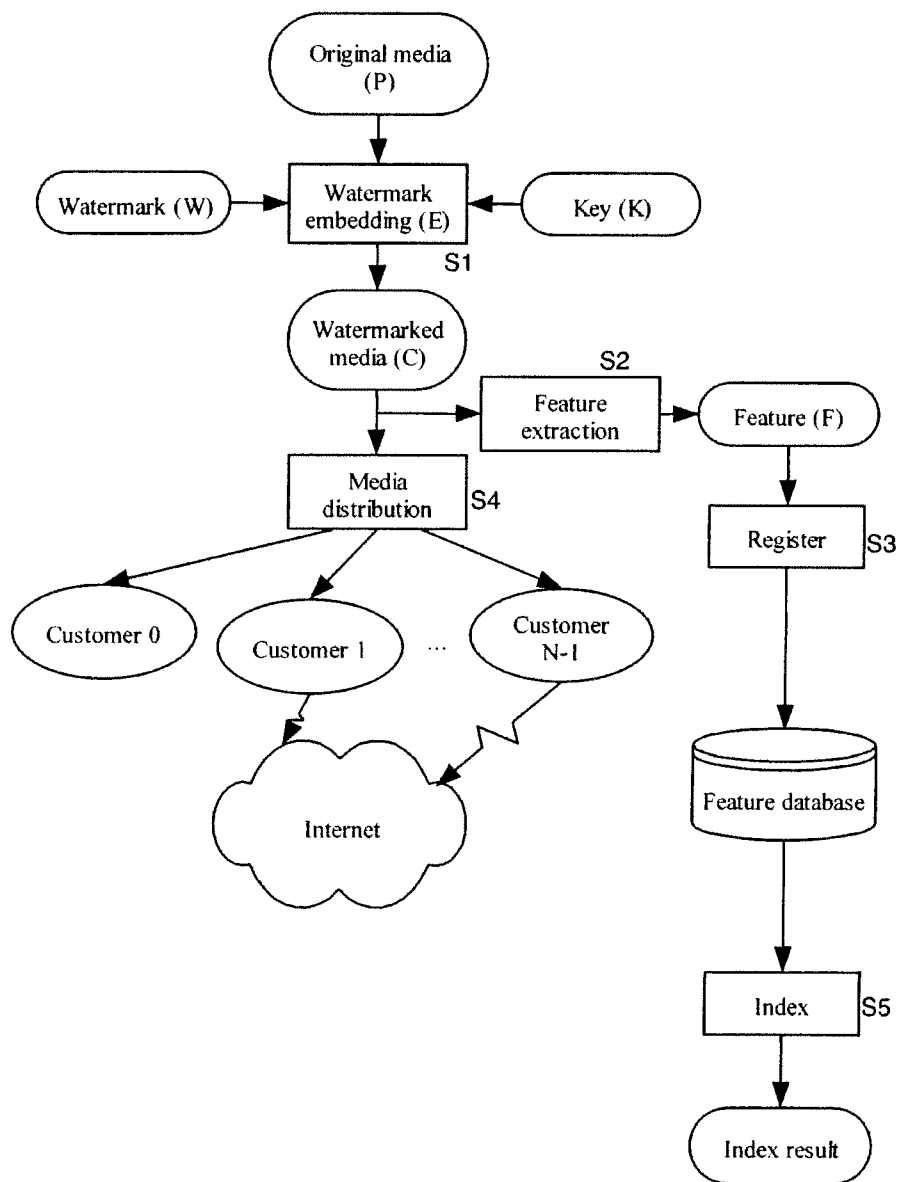


FIG. 2A

4/10

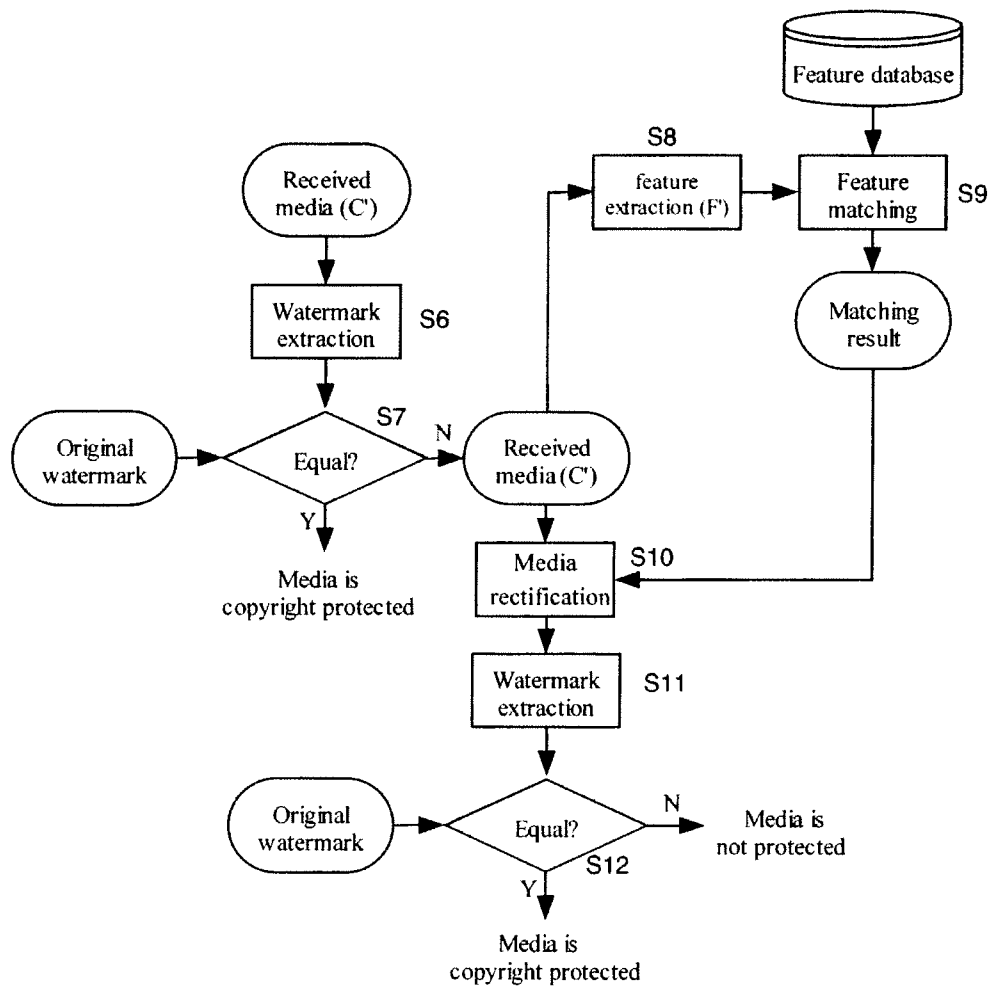


FIG. 2B

5/10

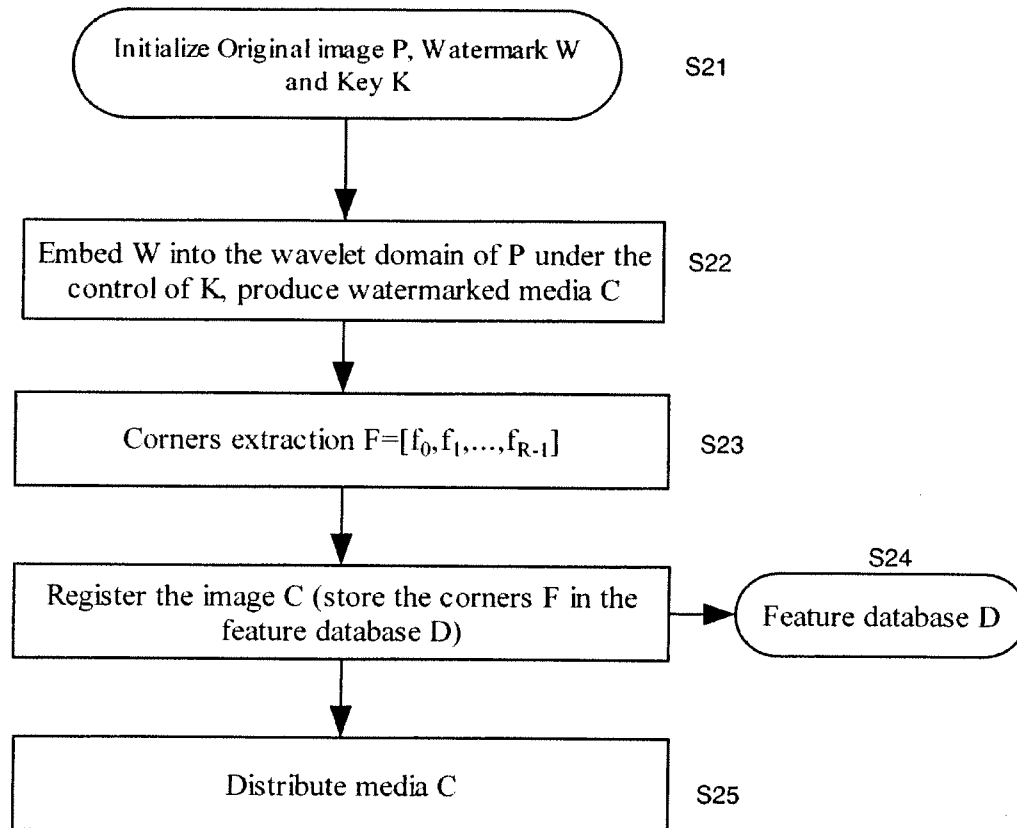


FIG. 3A

6/10

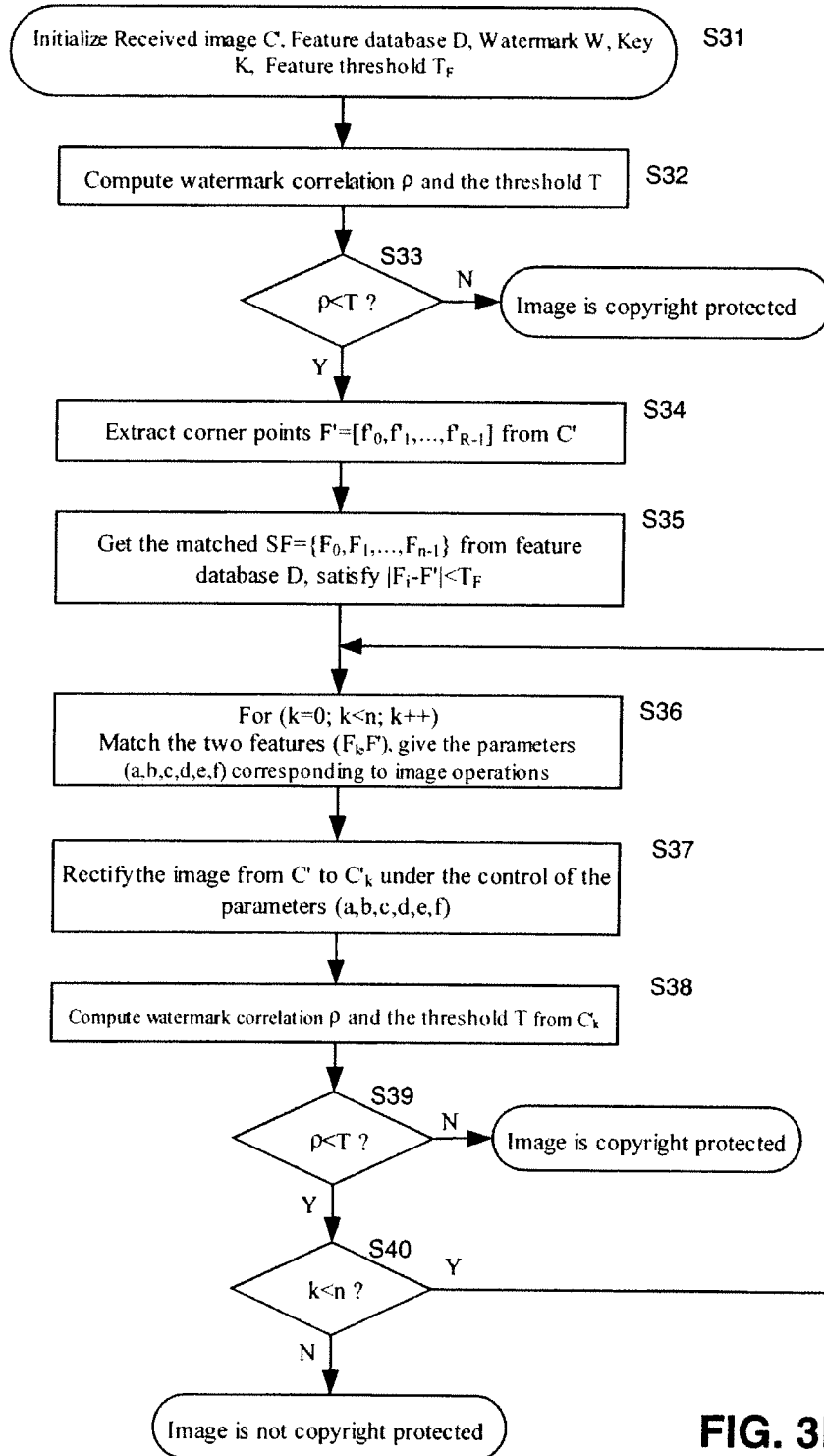


FIG. 3B

7/10

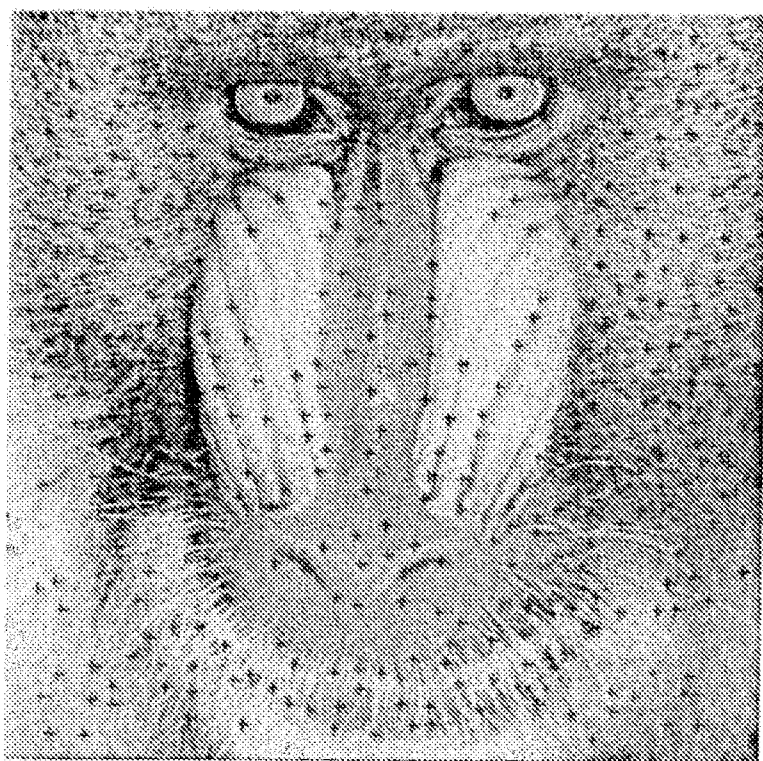


FIG. 4

8/10

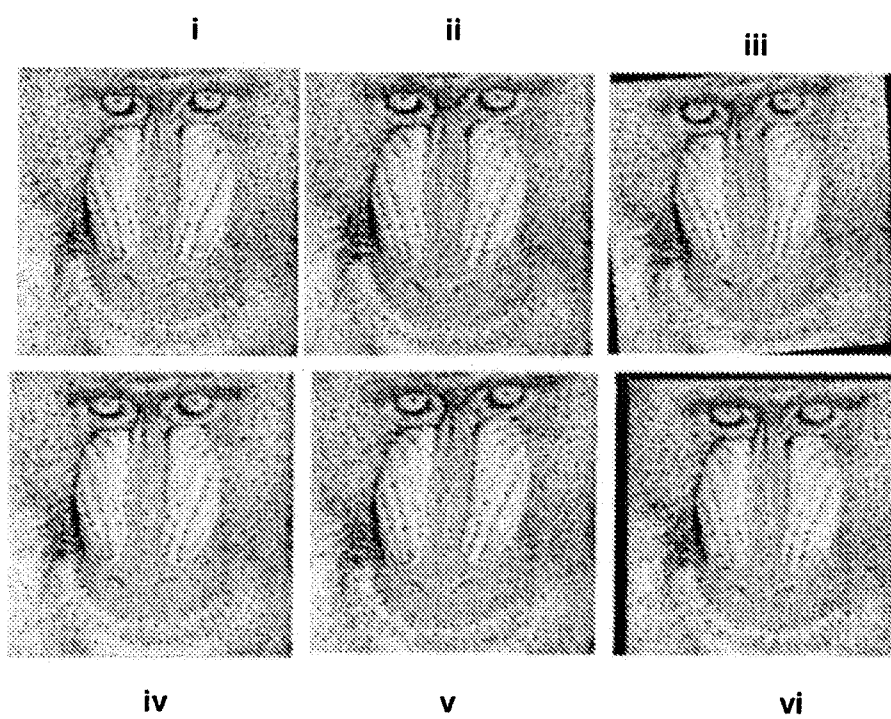


FIG. 5

9/10

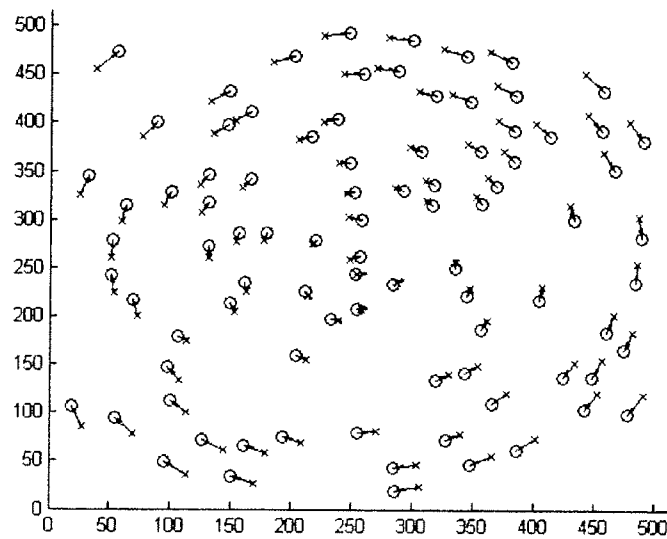


FIG. 6A

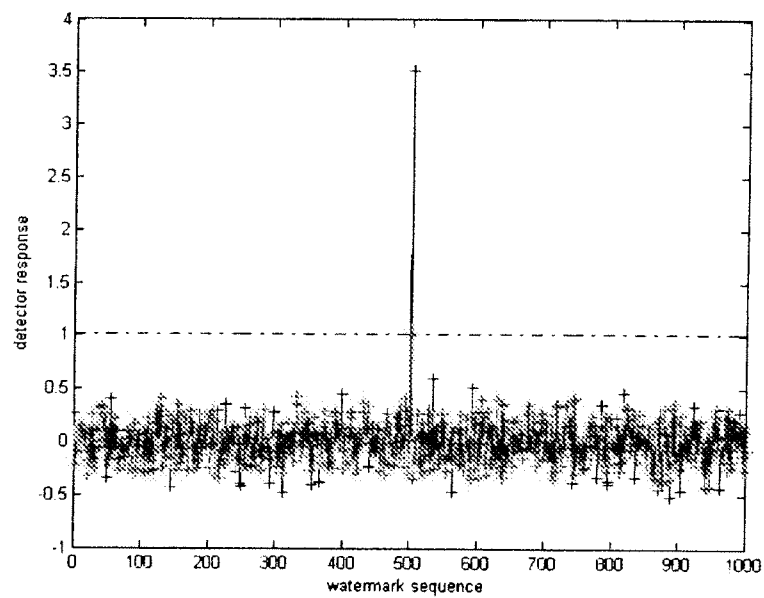


FIG. 6B

10/10

Types of the Attacks	baboon	plane	lena	elaine	barbara	house	peppers	lake	boats	tiffany
rotation(15)	12	11	12	10	11	12	12	12	11	10
scaling(6)	6	6	6	6	6	6	6	6	6	6
rotation-scaling(15)	11	10	12	10	12	11	11	11	12	11
ratio(4)	4	4	4	4	4	4	4	4	4	4
GLGT(2)	2	2	2	2	2	2	2	2	2	2
row and col removal(4)	4	4	4	4	4	4	4	4	4	4
shearing(3)	3	3	3	3	3	3	3	3	2	3
cropping(8)	5	4	5	5	4	5	5	5	7	4
JPEG(4)	4	4	4	3	4	4	4	4	4	4
sharpening(1)	1	1	1	1	1	1	1	1	1	1
Gaussian filtering(1)	1	1	1	1	1	1	1	1	1	1
median filtering(3)	3	3	2	2	2	2	3	3	2	2
FMLR(1)	1	1	1	1	1	1	1	1	1	1
Gaussian noise(4)	4	4	4	4	4	4	4	4	4	4
histogram(1)	1	1	1	1	1	1	1	1	1	1
Wiener filtering(2)	2	2	2	2	2	2	2	2	2	2
valumetric scaling(8)	8	8	8	8	8	8	8	8	8	8
translation(6)	6	6	6	6	6	6	6	6	6	6
Summark(1)	0	0	0	0	0	0	0	0	0	0

FIG. 7

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2009/056042

A. CLASSIFICATION OF SUBJECT MATTER

INV. G06T1/00 G06F17/30
ADD.

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)

G06T G06F

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

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

EPO-Internal, WPI Data

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	WO 03/013142 A1 (AMINO HOLDINGS LTD [GB]; GILBERT MARTYN [GB]; WANG KEITH [GB]) 13 February 2003 (2003-02-13) abstract page 2, line 6 - page 8, line 15 page 10, line 7 - page 11, line 31	1-16
Y	EP 1 345 160 A2 (SEIKO EPSON CORP [JP]) 17 September 2003 (2003-09-17) paragraph [0004] - paragraph [0005] paragraph [0011] - paragraph [0013] paragraph [0016] paragraph [0032] - paragraph [0033] paragraph [0035] paragraph [0040] ----- -/--	1,3-7, 10,11, 13-16

☒ Further documents are listed in the continuation of Box C.

☒ See patent family annex.

* Special categories of cited documents :

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

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

"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)

"O" document referring to an oral disclosure, use, exhibition or other means

"P" document published prior to the international filing date but later than the priority date claimed

"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention

"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone

"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art.

"&" document member of the same patent family

Date of the actual completion of the international search

13 May 2010

Date of mailing of the international search report

21/05/2010

Name and mailing address of the ISA/

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

Authorized officer

Zamuner, Umberto

INTERNATIONAL SEARCH REPORT

International application No
PCT/IB2009/056042

C(Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JOHNSON N F ET AL: "RECOVERY OF WATERMARKS FROM DISTORTED IMAGES" INFORMATION HIDING. INTERNATIONAL WORKSHOP PROCEEDINGS, XX, XX, vol. 1768, 1 September 1999 (1999-09-01), pages 318-332, XP008002242 abstract page 320, paragraph 2.1 page 321, paragraph 3 - page 328, paragraph 4.1 -----	1,2,6,8, 9,12-16
A	WO 00/39954 A1 (KENT RIDGE DIGITAL LABS [SG]; SUN QIBIN [SG]; WU JIANKANG [SG]; DENG H) 6 July 2000 (2000-07-06) page 17, line 18 - page 19, line 5 -----	1-16

INTERNATIONAL SEARCH REPORT

Information on patent family members

International application No

PCT/IB2009/056042

Patent document cited in search report	Publication date	Patent family member(s)	Publication date
WO 03013142	A1	13-02-2003	NONE
EP 1345160	A2	17-09-2003	CN 1445722 A 01-10-2003 US 2003174859 A1 18-09-2003
WO 0039954	A1	06-07-2000	GB 2366112 A 27-02-2002 US 6678389 B1 13-01-2004