Multimed Tools Appl (2012) 57:49–66
DOI 10.1007/s11042-010-0521-3

Content distribution and copyright authentication based on combined indexing and watermarking

Shiguo Lian · Xi Chen · Jinwei Wang

Published online: 29 April 2010

Abstract Copyright issues become more and more urgent with the wide spread of multimedia content over Internet, e.g., whether the media content is copyright-protected in multimedia social networks, or whether a media content is released on Internet illegally. To solve these problems, this paper proposes a content distribution and copyright authentication system based on media index and watermarking techniques. Before media distribution, the media content is marked (by embedding the ownership information or customer identification into the media), and the robust features that can be used both for media index and content emendation is extracted from the watermarked media and registered in a feature database. Some customer may leak out his media copy over Internet directly or after slight operations, such as rotation, shearing, scaling, translation, etc. To detect whether a media over Internet is copyright-protected or not, the following work is done. Firstly, a watermark is extracted from the media and compared with the original one. If the watermark exists, then the media is copyright-protected, and the authentication process is finished. Otherwise, a robust feature is extracted from the considered media and matched with the feature database. The matching result gives the operation parameters that are used to emend the media content. After media emendation, a watermark is extracted or detected again and used to authenticate the copyright. In this system, the robust feature is not only used to search the related media contents but also to emend the media in order to improve the robustness against such operations as adding noise, compression, rotation, shearing, scaling, translation, etc. Experimental results show that the combination of media index and watermark detection can improve the detection rate greatly.

S. Lian
France Telecom R&D (Orange Labs) Beijing, Beijing 100080, People's Republic of China
e-mail: shiguo.lian@orange-ftgroup.com

X. Chen (✉)
E-Commerce Department, Nanjing University, Nanjing 210093, People's Republic of China
e-mail: chenx@nju.edu.cn

J. Wang
The 28th Research Institute, CETC, Nanjing 210007, People's Republic of China
e-mail: wjwei_2004@163.com

Keywords Content distribution · Copyright authentication · Media index · Watermark · Multimedia social network · Digital right management

1 Introduction

In nowadays, there exit more and more multimedia content sharing networks, e.g., p2p based file sharing websites, User Generated Content sharing websites, video-on-demand or live TV systems, etc. With respect to such properties as anonymous sharing and free uploading/consuming, content sharing networks are often filled with various contents. Thus, it is often possible to find the copyrighted contents (images, videos, musics or flashes, etc.) illegally spread over Internet. This case happens when the customer redistributes the received multimedia content illegally, e.g., to other customers without the permission to consuming, or to public networks. Thus, it is urgent to detect the content with copyright issues or even tell the content's illegal distributor [25].

Till now, there exist various techniques that can be used to detect or protect copyright of multimedia content, e.g., digital watermarking, digital fingerprinting, and copy detection. Watermarking technique [13] is used to protect multimedia content's ownership, which embeds the ownership information (e.g., the producer's name or ID) into multimedia content by modifying the content slightly. Later, the ownership information can be extracted and used for authentication. Generally, invisible watermarking that embeds the ownership information imperceptibly is often used for ownership protection. Digital fingerprinting [39] is the technique used to detect the illegal redistributors. It embeds different information, such as Customer ID, into multimedia content, produces a unique copy, and sends the copy to the corresponding customer. If a copy is spread to unauthorized customers, the unique information in the copy can be detected and used to trace the illegal redistributor. Recently, the concept of content-based copy detection (CBCD) [18] has been proposed as an alternative means of identifying illegal media copies. Given an image registered by the owner, the system can determine whether near-replicas of the image are available on the Internet or through an unauthorized third party. If it is found that an image is registered (i.e., it belongs to a content owner), but the user does not have the right to use it, the image will be deemed an illegal copy.

As can be seen, the existing techniques, i.e., digital watermarking, digital fingerprinting and copy detection realize different functionalities. To realize copyright authentication (detect the illegal media content and identify the illegal distributor), all the techniques should be combined together [23].

Now, there are some schemes consider to realize both copyright detection and media index. For example, the work in [6] proposes the scheme to extract the features of the key frames from the video and use the features as a key to embed the watermark. However, the features are only used for security but not for robust watermark embedding or extraction. The work in [9] presents the image indexing methods and watermarking methods in wavelet domain, respectively. However, there is no relation between the watermarking and indexing operations.

Considering that images are often operated by compression, rotation, shearing, scaling, translation, etc., to detect the watermark in the operated images is difficult. To implement robust media copyright protection, media contents' feature may be used, which can be obtained from the feature database in content index. Till now, no works have been done in copyright protection combined with content index.

This paper aims to propose a copyright authentication scheme based on both digital watermarking or fingerprinting and copy detection or media index. The media content

is marked before distribution, and the robust feature is extracted from the marked media content and registered in a feature database. To detect whether an image is released over Internet, the robust feature is computed from potential images and compared with the registered one. Additionally, the feature is used to emend the image in order to improve the watermark/fingerprint detection rate. Here, the emendation operations can recover the image from such geometric attacks as shifting, rotation, resize, etc. The paper's brightest innovation is to propose the algorithm to combine digital watermarking/fingerprinting and copy detection/media index.

The rest of the paper is arranged as follows. In Section 2, some related works are reviewed. Then, the architecture of the proposed copyright authentication system and the detailed algorithms are proposed in Section 3. In Section 4, the example based on feature points and additive watermarking is presented in detail. And, the experimental results and analysis are given in Section 5. Finally, in Section 6, the conclusions are drawn.

2 Related work

2.1 Digital watermarking

A good watermarking algorithm satisfies some performance metrics such as imperceptibility, robustness, capacity, security, oblivious detection, etc. During the past decades, many watermarking algorithms have been reported, which can be classified by different methods. According to the embedding domain, watermarking can be embedded in either temporal domain, spatial domain or frequency domain. Taking video watermarking for example, the watermark can be embedded in the frame-pixels, the motion vectors or the DCT coefficients, which obtains different performances. Spatial domain watermarking embeds information in pixels directly, such as the LSB method [33] and the perceptual model based methods [30]. Generally, these methods are often not robust to signal processing or attack, although they are efficient in computing. Frequency domain Watermarking is embedded in transformation domain, such as DCT transformation [24], wavelet transformation [35], etc. Compared with the watermarking in spatial domain, the one in frequency domain obtains some extra properties in robustness and imperceptibility. Additionally, the embedding can be done during compression, which is compatible with international data compression standard. Temporal domain Watermarking is embedded in temporal information. For example, in audios, echo property is used to hide information, which is named echo hiding [15]. In videos, the temporal sequence is partitioned into static component and motive component, with information embedded into motive component [19]. Considering that human's eyes are more sensitive to static component than to motive one, embedding in motive component can often obtain higher robustness. However, error accumulation or floating makes the watermarked videos blurred in some extent, which should be improved by error compensation.

Additionally, some synchronization algorithms are proposed to improve the robustness against various operations. The typical ones are based on robust features. For example, the corners can be used to identify an object in a robust manner [1]. It firstly detects the corners, then forms the shape matrix through a neighborhood operation of the detected corners, and uses the shape matrix to match the expected objects (such as the house). Another method uses the robust regions to realize synchronization [36]. It extracts the disks in the image as the features (that is stored) and then embeds the watermark into the image's FFT domain. The disks will be used to restore the rotated image.

2.2 Digital fingerprinting

The most serious threat to watermarking-based fingerprinting is collusion attack that fabricates a new copy by combining several copies in order to avoid the tracing. Generally, five kinds of collusion attacks are considered, i.e., averaging attack, linear combinatorial collusion attack (LCCA) [37], min-max attack, negative-correlation attack and zero-correlation attack. Since the past decade, finding new solutions resisting collusion attacks has been attracting more and more researchers. The existing fingerprinting algorithms can be classified into three categories, i.e., orthogonal fingerprint, coded fingerprint and warping-based fingerprint. In orthogonal fingerprinting [22, 34], the unique information (also named fingerprint) to be embedded is the vector independent from each other. For example, the fingerprint can be a pseudorandom sequence, and different fingerprint corresponds to different pseudorandom sequence. The orthogonal fingerprint can resist most of the proposed collusion attacks, which benefits from the orthogonal property of the fingerprints. Fingerprinting can be carefully designed in codeword form, named coded fingerprinting [7], which can detect the colluders partially or completely. Till now, two kinds of encoding methods are often referenced, i.e., the Boneh-Shaw scheme [7] and the combinatorial design based code [34]. Compared with orthogonal fingerprinting, the coded fingerprinting has some advantages. Firstly, the embedding method is not only limited to additive embedding, some other existing embedding methods are also usable. Secondly, the correct detection rate does not depend on the number of colluders. However, with respect to LCCA attacks, the coded fingerprinting is not so robust. In warping-based fingerprinting [26], the multimedia content (e.g., image or video) is desynchronized imperceptibly with some geometric operations in order to make each copy different from others. This kind of fingerprinting aims to make collusion impractical under the condition of imperceptibility. However, in this scheme, the compression ratio is often changed because of the pre-warping operations. Additionally, it is a challenge to support large number of customers by warping the content imperceptibly.

2.3 Copy detection

Image copy detector searches for all copies of a query image, and is different from content-based image retrieval (CBIR) [2] that searches for similar images. Thus, it is not usually feasible to apply existing CBIR techniques to CBCD because they may cause a considerable number of false alarms. For CBCD, the key challenge is to extract the suitable features that can obtain a good tradeoff between discriminability and robustness. The discriminability denotes the ability to distinguish different media contents. The robustness refers to the ability to survive such operations as cropping, noising, contrast changing, zoom, insertion, etc. Generally, the extracted features are compared with the registered ones, whose distance tells the repetition.

According to the methods that extract features, the CBCD algorithms can be classified into two types: global feature-based algorithms, and local feature -based algorithms. For example, the algorithm in [8] extracts the global features from wavelet transformed coefficients and color space, the one in [20] extracts the ordinal measure of DCT coefficients from the whole image, the one in [38] uses elliptical track division strategy to extract features from all the elliptical track blocks, and the one in [40] uses a sliding window to extract the block's relationship with its neighboring blocks. These global feature-based algorithms often obtain good discriminability, while bad robustness. For example, they are not robust to such operations as block cropping. Differently, local feature-based algorithms have better robustness. For example, the algorithm in [5]

computes many descriptors for each image, in which, each descriptor corresponds to one image block, and the algorithm in [17] extracts the key points from each image part. They can still identify the content even when it is tampered (e.g., cropped or modified) greatly. Their disadvantage is the high computational complexity, and the research challenge is how to determine the block size.

2.4 Drawbacks of prior arts

The digital watermarking/fingerprinting technique is often used in copyright identification, which embeds copyright information into media content imperceptibly and uses it to authenticate the copyright. For example, in the watermarking based image protection method [32], the ownership information is embedded into images before spreading them out. By detecting whether the watermark exists in the image or not, the copyright of the image spreading over Internet can be authenticated. However, considering that images are often operated by compression, rotation, shearing, scaling, translation, etc., to detect the watermark in the operated images is difficult. To implement robust media copyright protection, some extra information should be used to resist the operations. Copy detection or index aims to find some contents matching the targeted one. For example, the content index method [31] provides image index based on image feature extraction and matching. In the method, some features are extracted from an image and compared with the ones stored in a database, and thus, one or a group of matched images are found. Generally, the copy detection/index is in no relation with digital watermarking/fingerprinting. In fact, the media content's feature extracted for copy detection/index can also be used to help the detection of watermarking/fingerprinting. In this paper, we will propose the scheme combining them together, give an example based on corner features and additive watermarking, and present some experiments to show its practicability.

3 Architecture of the proposed content distribution and copyright authentication scheme

The content distribution and copyright authentication system, as shown in Fig. 1, is composed of several steps: Firstly, the content provider/producer embeds the watermarking/fingerprinting information (content provider's information or customer ID) W into the media content P before distributing it, and produces the marked media content C. Secondly, the robust feature F is extracted from media content C and registered in the feature database. Thirdly, the content provider distributes the media content C to customers. Fourthly, from Internet, the suspicious media contents are searched by copy detection or media index. Fifthly, for each suspicious media content C′, the copyright information is detected by watermark extraction and authentication.

Among the system, there are five key algorithms, i.e., media watermark embedding, robust feature extraction and registering, media distribution, copy detection/media index, and watermark extraction and authentication. They are presented in detail in the following content.

3.1 Media watermark embedding

The watermark W is embedded into the media P under the control of K, which produces the watermarked media C. Here, the watermark W represents the ownership information or customer ID. The embedding method may be the existing watermarking algorithms [11, 12]

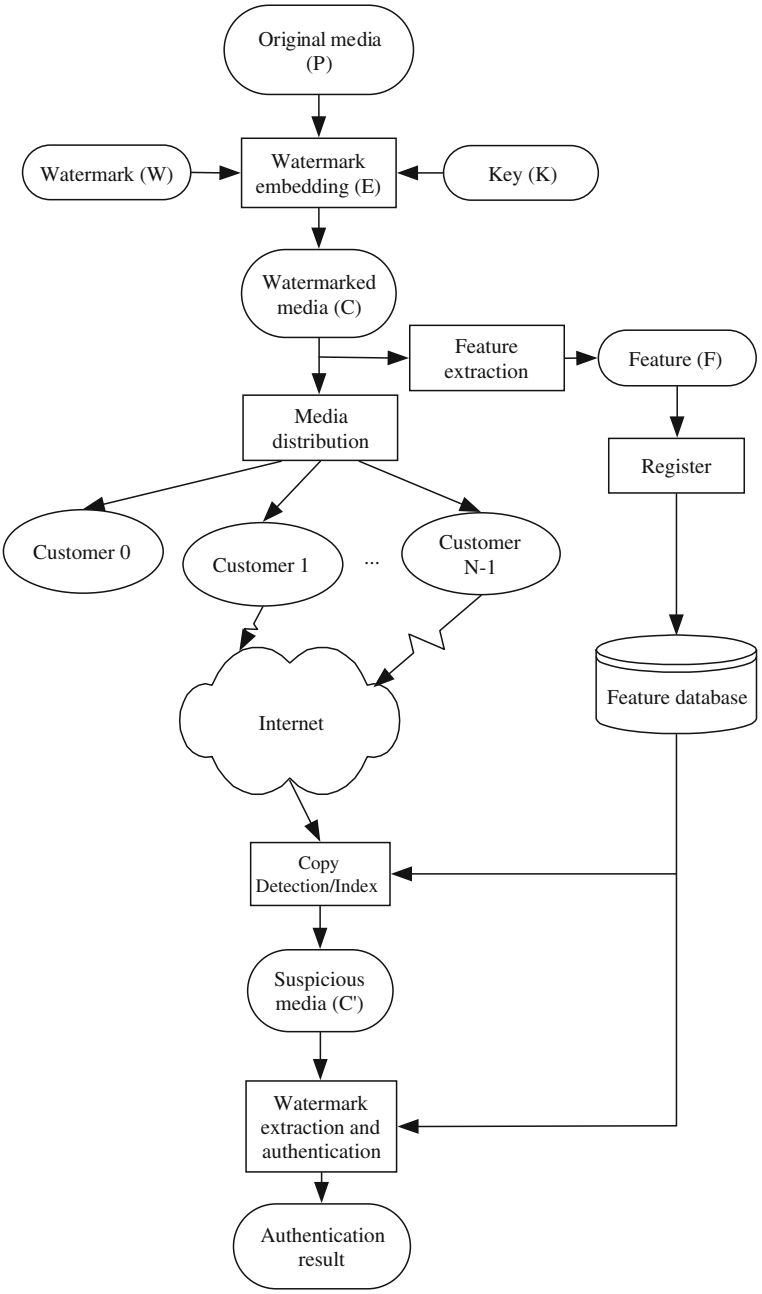

Fig. 1 Architecture of the proposed media copyright authentication system

robust to general attacks [10]. The watermarking algorithms embed watermarks into the spatial domain or frequency domain of images, videos or audios. And the algorithms are often robust to such general attacks as adding noise, compression, A/D or D/A conversion, filtering, etc. The key K controls embedding position or parameters.

3.2 Robust feature extraction and registering

The feature F is extracted from the watermarked media C and stored in the feature database D with size of M. The data structure of the feature database is shown in Table 1. The feature F should satisfy two requirements: firstly, F is robust to watermarking attacks [4], such as general attacks, rotation, shearing, translation, scaling, etc. Secondly, F can be used in media index [27, 42] and is much fewer in volumes compared with the media itself. Such feature as corner point, boundary, edge, histogram, etc [27, 42] can be used.

3.3 Media distribution

The watermarked media is distributed to customers through such means as broadcasting, multicasting, unicasting, etc. Some customers may distribute directly the received media over Internet, or distribute it after such operations as recompression, scaling, translation, etc. This media represented as C′ is then spread from one person to another freely.

3.4 Copy detection/Media index

Copy detection/Media index is to find the media content C′ similar to the ones registered in the feature database D. For each image, a robust feature F′ is extracted matched with the feature database D. The matching result gives the n ($1 \le n < M$) most matched features ($F_0, F_1, \ldots, F_{n-1}$). The n media contents corresponding to the n features are the matched results.

3.5 Watermark extraction and authentication

If some media over Internet is to be authenticated, the watermark extraction and authentication process shown in Fig. 2 is followed, which consists of two sub-steps.

Firstly, a watermark W′ is extracted from the suspicious media C′ and compared with the original watermark W. Here, the watermark extraction method is symmetric to the watermark embedding method [11, 12]. If $|W' - W| < T$ (T is the extraction threshold determined before hand), then the watermark exists, the media is copyright protected, and the authentication process is finished. Otherwise, continue to the second step.

Secondly, a robust feature F′ is extracted from the media C′ and matched with the feature database D. The matching result gives the n ($1 \le n < M$) most matched features ($F_0, F_1, \ldots, F_{n-1}$). The matching algorithm is based on the comparison between $|F - F_i|$ ($i = 0,1,\ldots,n-1$) and T_F (T_F is the threshold determined before hand). If $|F - F_i| < T_F$, the feature F_i is the matched one. Otherwise, the feature F_i is not the matched one. The n media contents corresponding to the n features are the index results. From the n indexed features, each pair (F, F_i) ($i = 0,1,\ldots,n-1$) is used to compute the changing quantity caused by attack operations, e.g. the corner matching [28], and the changing quantity is then used to emend the media from C′ to C″. For example, if F_i is different from F in rotation angle, then C′ is inverse rotated in the same angle. From the emended media C″, a watermark W″ is extracted and compared with the original watermark

Table 1 Data structure of the feature database

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

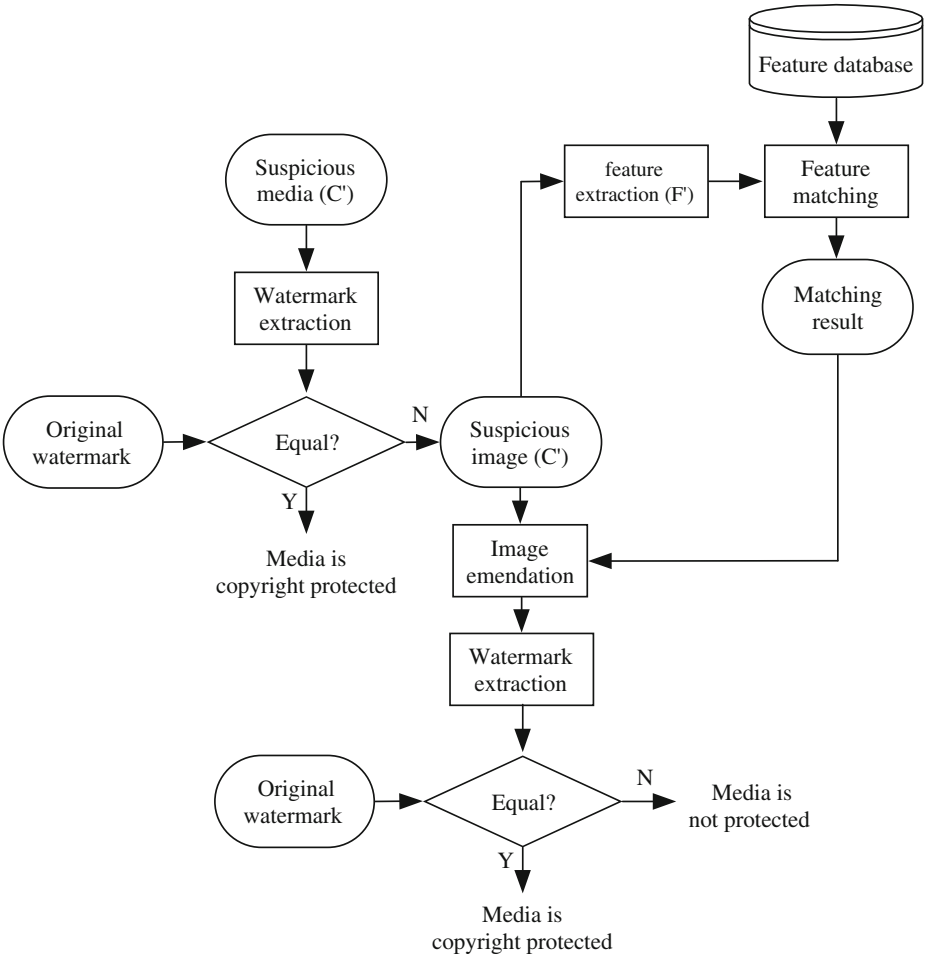

Fig. 2 Watermark extraction and authentication process

W. If $|W'-W|<T$, then the watermark exists, the media is copyright protected, and the authentication process is finished. Otherwise, continue until i = n or the watermark is detected.

4 The example based on feature points and additive watermarking

Taking corner point as the feature, an image copyright authentication method is shown in Fig. 3 and Fig. 4. Among them, Fig. 3 shows the watermark embedding and feature extraction process, and Fig. 4 is the watermark extraction and authentication process.

4.1 Watermark embedding and feature extraction

Firstly, the original image P, watermark W and key K are initialized. Here, $W = [w_0, w_1, ..., w_{m-1}]$ is Gaussian sequence.

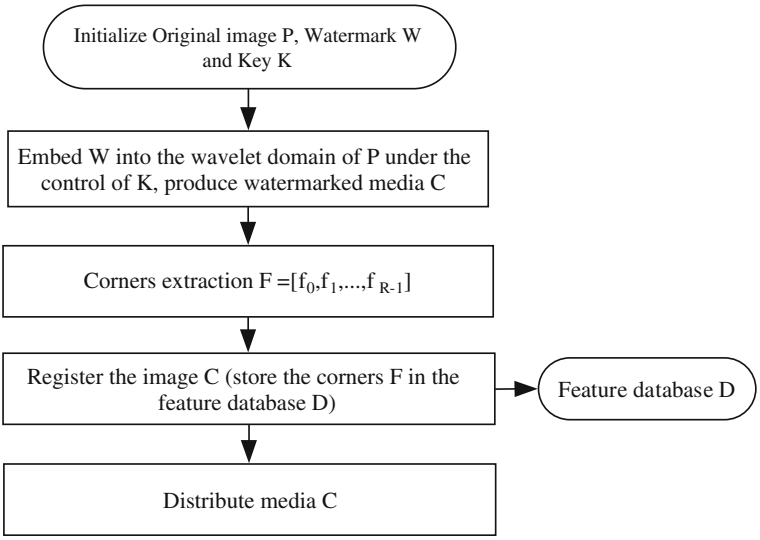

Fig. 3 Watermark embedding and feature extraction

Secondly, W is embedded into the wavelet domain of P under the control of K, which produces the watermarked media C. Here, K controls the permutation of W, and the permutation method based on pseudorandom number or chaotic map can be used. In watermark embedding, P is firstly transformed by wavelet transformation, which produces the coefficients in different subband. For example, if P is decomposed into 4 resolution levels using wavelet transformation, the produced subbands are denoted by $I^{r,s}$. Here r∈{0,1,2,3} is the resolution level, and s∈{LL,LH, HL,HH} is the orientation. Then, the watermark is embedded into the subbands according to

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

In order to keep robust, r∈{2,3} is prefer. α ($0<\alpha\leq 1$ and $1+\alpha w_i>0$) is the embedding strength, which ranges in [0,1] and can be computed by HVS [21] or set as a constant. After embedding, the subbands are inversely transformed by wavelet transformation, and the produced watermarked image is C.

Thirdly, the corners $F = [f_0,f_1,...,f_{R-1}]$ are extracted from C with the method proposed in [16]. Here, $f_i = (x_i,y_i)$ (i=0,1,…,R−1) is the coordinates of a corner point. The corner points are often robust to such geometric operations as rotation, shearing, scaling, translation, etc. Generally, for different image, the number of the extracted corner points is different. To keep coherence, only R points are selected as the feature. The selection can be random.

Fourthly, the watermarked image C is registered. That is, to store the corners F and the corresponding image name in the feature database D. The data structure of the database is shown in Table 2.

Fifthly, the watermarked and registered image C is distributed to customers.

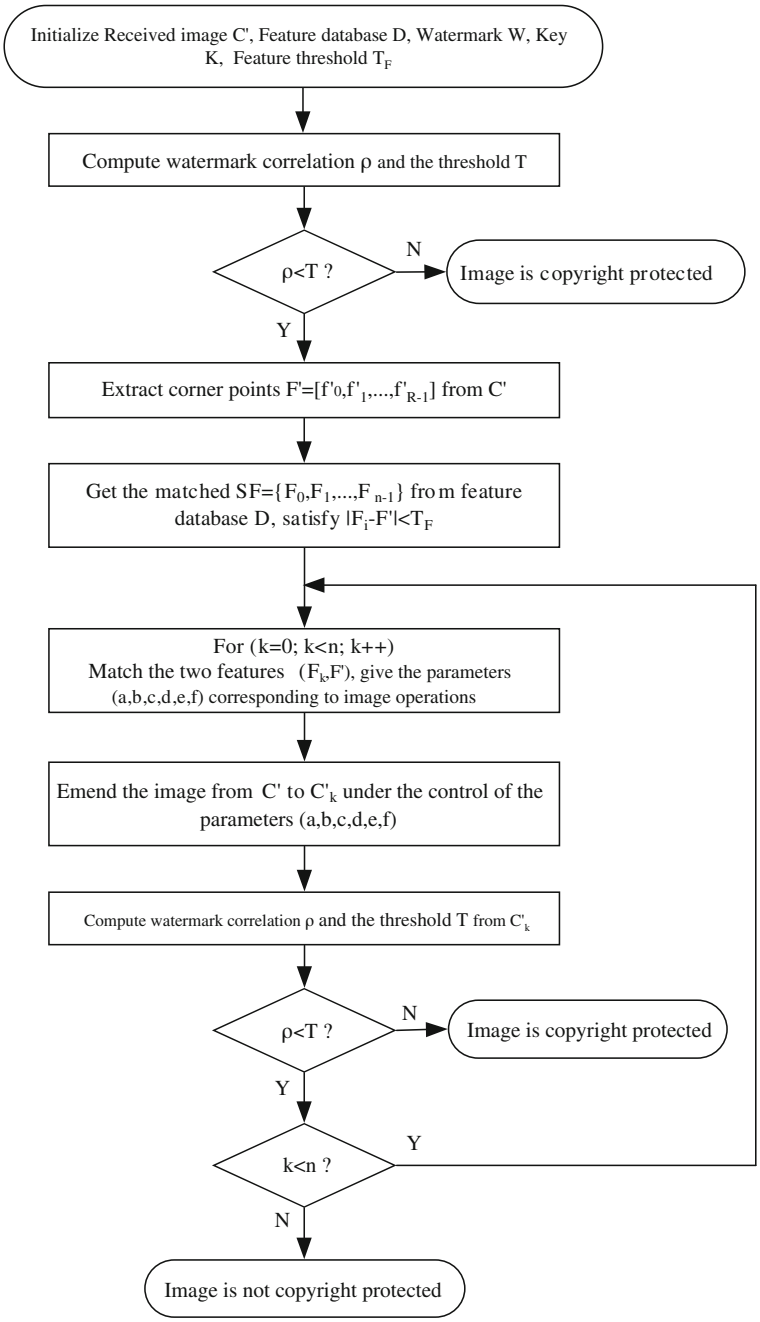

Fig. 4 Watermark extraction and authentication process

Table 2 Structure of the corner point based feature database

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

4.2 Watermark extraction and authentication

Firstly, the received image C′, feature database D, watermark W, key K and feature matching threshold T_F are initialized. Here, C′ is the operated copy of C, which has been attacked by such operations as adding noise, compression, rotation, shearing, scaling, translation, etc. T is the threshold to determine the existence of watermark. T_F is the threshold to determine the matched features.

Secondly, the watermark W is permuted under the control of K, the subbands $I'^{r,s}$ are obtained by wavelet transformation, and the correlation value

$$\rho = \frac{1}{m}\sum_{i=1}^{m}\left|I_i'^{r,s}\right|w_i \tag{2}$$

and the threshold

$$T = \frac{6}{N}\sqrt{\sum_{i=1}^{N}\left(I_i'^{r,s}\right)^2} \tag{3}$$

are computed. If $\rho \geq T$, then the watermark exists, and the authentication process is finished. Otherwise, continue to the following steps.

Thirdly, A feature $F' = [f'_0, f'_1, ..., f'_{R-1}]$ composed of R corner points is extracted from the watermarked image C′. The n most matched features $SF = \{F_0, F_1, \ldots, F_{n-1}\}$ are obtained by computing the distance $Dist(F_i, F')$ and compared with the threshold T_F. Here,

$$Dist(F_i, F') = \frac{1}{R}\sum_{j=0}^{R-1}\sqrt{\left(x_{ij} - x_j'\right)^2 + \left(y_{ij} - y_j'\right)^2}. \tag{4}$$

If $Dist(F_i, F') \leq T_F$, then the feature F_i is the matched feature. Otherwise, F_i is not the matched one. The n images corresponding to the n features in SF are the indexed images.

Fourthly, set k=0, do the following operations:

i) if k = n, there is no watermark in the image, the image is not copyright protected, and the authentication process is finished. Otherwise, continue.
ii) Match the two features (F_k, F′) by computing the parameters (a,b,c,d,e,f) of affine transformation according to

$$\begin{pmatrix} x' \\ y' \end{pmatrix} = \begin{pmatrix} a & b & c \\ d & e & f \end{pmatrix}\begin{pmatrix} x \\ y \\ 1 \end{pmatrix} = H\begin{pmatrix} x \\ y \\ 1 \end{pmatrix}. \tag{5}$$

Here, (x′,y′) and (x,y) is the corner point's coordinates in F′ and F_k, respectively. Using at least three point pairs, the parameters in H can be computed. The computing method may

be least square method [41] or the coarse matching before random sample consensus (RANSAC) method [14], etc.

iii) Using the computed parameters (a,b,c,d,e,f) to emend the image from C′ to C′$_k$. That is, these parameters are used to emend the pixel position (x′,y′) in C′ according to

$$\begin{cases} x_k^{'} = \frac{ex'-by'-ec+bf}{ea-bd} \\ y_k^{'} = \frac{dx'-ay'-cd+af}{bd-ae} \end{cases}. \quad (6)$$

Here, (x′$_k$,y′$_k$) is the pixel position in C′$_k$.

iv) From the emended image C′$_k$, the watermark correlation ρ and the watermark threshold T is computed, respectively, with the method similar to the one in the second step. If ρ≥T, then the watermark exists (image is copyright protected), and the authentication process is finished. Otherwise, continue to the following steps.

v) Do k=k+1, and go to i).

5 Experiments and performance analysis

The experiments are done to show the proposed scheme's authentication performance. The image library composed of 2000 natural images is used to simulate the images over Internet. Among them, 30 images are registered in the feature database, and 270 images are the operated versions corresponding to the 30 images. The operations include rotation, scaling, cropping, shearing, resizing, filtering, noising, etc., as shown in Table 3. Here, m=100, R=80, T_F=20, n=10, and 500 images are tested, including baboon, plane, lena, Elaine, Barbara, etc. Fig. 5 shows the corner detection results of the original and operated images. As can be seen, there are high similarities between these images' corners. Figure 6 shows

Table 3 Robustness test under the condition of various operations

Attacks	Baboon	Plane	Lena	Elaine	Barbara	Peppers	Boats	Tiffy
Rotation(15)	12	11	12	10	11	12	11	10
Scaling(6)	6	6	6	6	6	6	6	6
Rotation-Scaling(15)	11	10	12	10	12	11	12	11
Ratio(4)	4	4	4	4	4	4	4	4
Row and Col remove(4)	4	4	4	4	4	4	4	4
Shearing(3)	3	3	3	3	3	3	2	3
Cropping(8)	5	4	5	5	4	5	7	4
JPEG(4)	4	4	4	3	4	4	4	4
Sharpening(1)	1	1	1	1	1	1	1	1
Gaussian filtering(1)	1	1	1	1	1	1	1	1
Median filtering(3)	3	3	2	2	2	3	2	2
Gaussian noise(4)	4	4	4	4	4	4	4	4
Histogram(1)	1	1	1	1	1	1	1	1
Wiener filtering(2)	2	2	2	2	2	2	2	2
Valumetirc scaling(8)	8	8	8	8	8	8	8	8
Translation(6)	6	6	6	6	6	6	6	6
Stirmark(1)	0	0	0	0	0	0	0	0

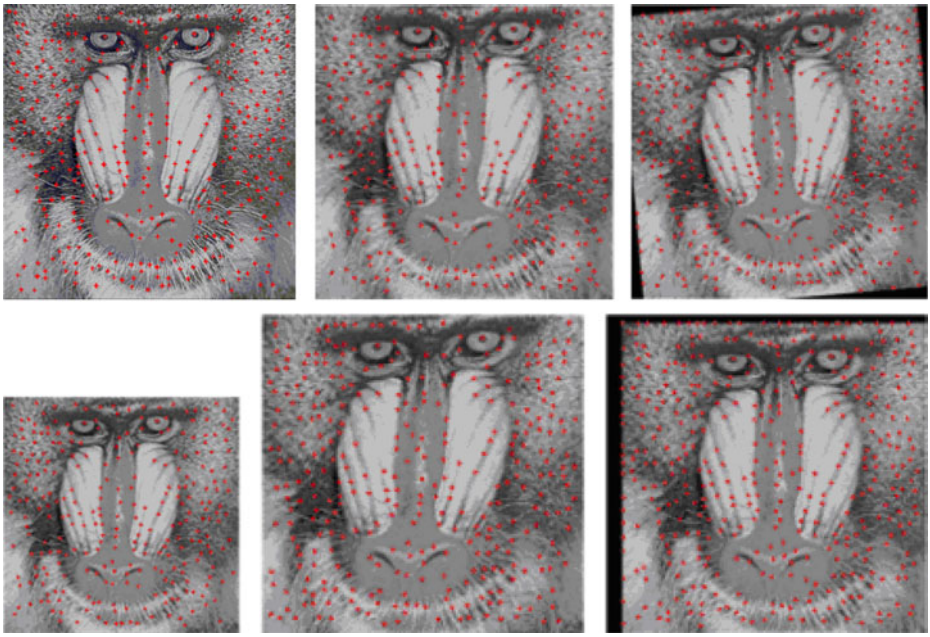

Fig. 5 Corner detection in the original and operated images (from left to right, from top to bottom: original, cropping, rotation, scaling, shearing, translation)

the result of corner point matching, from which, the rotation direction and angle can be estimated. Figure 7 shows the result of watermark detection. The high correlation value can be detected if the watermark exists in the operated media content.

Table 3 shows the robustness test under the condition of various operations. As can be seen, the scheme can survive most of the desynchronization attacks based on global geometrical transforms and the general signal processing attacks. For example, the rotation

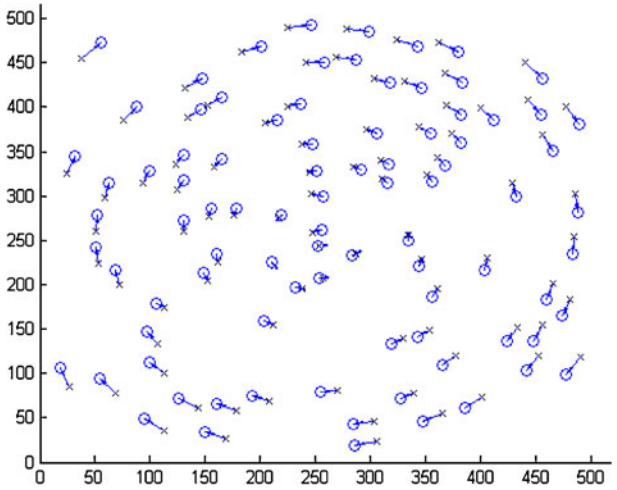

Fig. 6 Corner point matching of the rotated image

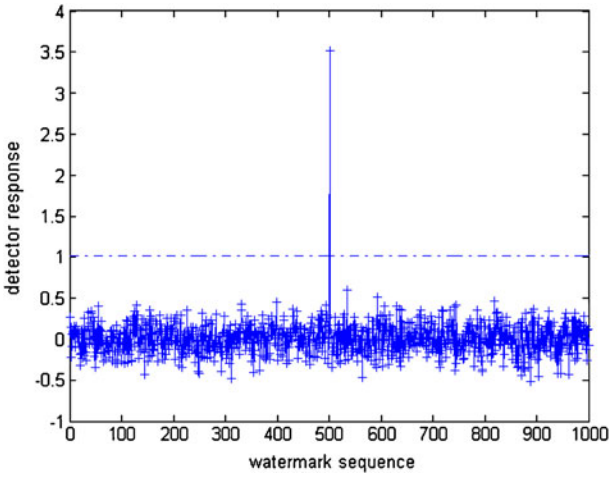

Fig. 7 Watermark detection with correlation and threshold

or rotation-scaling operation can be detected if the rotation angle is not bigger than 10°. However, after Stirmark attacks [29], the watermark is difficult to be detected. This is because the combined operations in Stirmark increase the difficulties of both corner detection and watermark detection.

Table 4 shows the detection rate of both copy detection/media index and watermark detection. Here, the detection rate denotes the ratio between the number of correctly detected images and the number of tested images. Keeping other parameters unchanged, T_F=10, 20 and 30 are tested respectively. Seen from Table 4, the smaller the T_F is, the more possible the operated image copies are missed. The more the T_F is, the more possible the unrelated images are detected by a mistake. Thus, there is a tradeoff for copy detection/media index. Here, T_F=20 gets the suitable tradeoff. Additionally, for watermark detection, the feature point based emendation increases the detection rate greatly no matter what's kind of parameter is applied. Furthermore, the bigger the T_F is, the more the matched images are detected, and the more the possibility of watermark detection is.

In this scheme, copy detection/media index is introduced to select the suspicious media copies, and then the watermark detection or image emendation is applied. To evaluate the computational cost of the proposed scheme, we compare it with the watermark-only scheme (without copy detection and emendation) and watermark-based scheme (without emendation). Set T_W be the cost of watermark detection in an image, T_M the cost of two image's feature matching, T_E the cost of an image's emendation, and T_1, T_2, T_3 the cost of n

Table 4 Detection rate of different algorithms

Parameters	Copy detection / media index	Watermark detection (without emendation)	Watermark detection (with emendation)
T_F=10	90%	64%	80%
T_F=20	95%	78%	92%
T_F=30	93%	80%	93%

Table 5 Time cost of different copyright authentication schemes

Number of images to be authenticated	Watermark-only scheme (without index and emendation)	Watermark-based scheme (with emendation)	The proposed scheme
300	15.7s	472.1s	503.8s
500	27.3s	786.6s	825.2s
2000	106.8s	3197.2s	3231.5s

images' authentication with the watermarking-only scheme, watermarking-based scheme, and the proposed scheme. Then, the costs satisfy

$$\begin{cases} T_1 = nT_W \\ T_2 = mnT_M + n_1T_W \ (n \geq n_1) \\ T_3 = mnT_M + n_1T_W + n_2(T_E + T_W)(n \geq n_1 \geq n_2) \end{cases} \tag{7}$$

where m is the size of registered image database, n is the total number of images to be authenticated, n_1 is the number of suspicious images detected by feature matching, and n_2 is the number of suspicious images that are not authenticated by watermark detection. The experiments are done to test the time cost. Here, m=100, R=80, T_F=20, n=10, and various number of images are tested. The schemes are implemented by C code, and worked in the computer of 1.20 GHz CPU/1.49 GB RAM. The results (with the metric of seconds) are shown in Table 5. As can be seen, the proposed scheme costs the most time compared with the watermark-only scheme and watermark-based scheme, while the watermark-only scheme costs the least time. This is because the feature matching and image emendation often cost more time than watermark detection. To reduce the time cost, some typical means can be adopted, e.g., the LSH-based search method [3], which will be investigated in future work.

6 Conclusions

This paper presents the content distribution and copyright authentication scheme based on both copy detection/media index and digital watermarking. Firstly, the architecture of the scheme is presented. Then, each algorithm in the architecture is proposed in detail. Thirdly, the example based on feature point and additive watermarking is presented, together with the experiments and analysis. The scheme uses copy detection/media index to get the matched media contents, and uses digital watermarking to detect the copyright information. Furthermore, the features extracted in copy detection/media index are also used to emend the media contents. Experimental results show that the emendation operation improves the watermark detection rate greatly. Although the example is based on images, the scheme can also be applied to video or audio contents. Considering that in the example, the feature points' extraction often costs much computation, some better features may be investigated in order to reduce the computational cost. Additionally, the features robust against such attack as Stirmark or combined attacks need to be studied. Furthermore, to distinguish the illegal distributors, the fingerprinting code's detection against collusion attacks will be considered in future work.

Acknowledgments The work was partially supported by France Telecom's Invenio project through the grant code of ILAB-PEK09-016, National Natural Science Foundation of China under Grant No. 70901039, National Postdoctoral Science Foundation of China under Grant No. 20090450144, and Jiangsu Postdoctoral Science Foundation under Grant No. 0901104C.

References

1. Ahmad N, Park J, Kang G, Kang J, Beak J (2007) Object retrieval approach with invariant features based on corner shapes. 2007 IEEE International Symposium on Signal Processing and Information Technology, 15–18 Dec. 2007, page(s): 825–830
2. Amsaleg L, Gros P (2001) Content-based retrieval using local descriptors: problems and issues from a database perspective. Pattern Anal Appl 4(2–3):108–124
3. Andoni A, Indyk P (2006) Near-optimal hashing algorithms for near neighbor problem in high dimensions. In Proceedings of the Symposium on Foundations of Computer Science (FOCS'06)
4. Bas P, Chassery J-M, Macq B (2002) Geometrically invariant watermarking using feature points. IEEE Trans Image Process 11(9):1014–1028
5. Berrani SA, Amsaleg L, Gros P (2003) Robust content-based image searches for copyright protection, in Proc. ACM Int. Workshop on Multimedia Databases, pp. 70–77
6. Bhardwaji A, Pandey TP, Gupta S (2001) Joint indexing and watermarking of video using color information. 2001 IEEE Fourth Workshop on Multimedia Signal Processing, Page(s):333–338
7. Boneh D, Shaw J (1998) Collusion-secure fingerprinting for digital data. IEEE Trans Inform Theory 44 (5):1897–1905
8. Chang EY, Li C, Wang J-Z, Mork P, Wiederhold G (1999) Searching near-replicas of images via clustering, in Proc. SPIE: Multimedia Storage and Archiving Systems IV, 3846: 281–92
9. Chatterji BN, Kokare M, Reddy AA, Jha RK (2003) Wavelets for content based image retrieval and digital watermarking for multimedia applications. 2003 and the Fourth Pacific Rim Conference on Multimedia. Vol. 2, 15–18 Dec. 2003, Page(s): 812–816
10. Cheng Q, Huang TS (2001) An additive approach to transform-domain information hiding and optimum detection structure. IEEE Trans Multimedia 3(3):273–284
11. Cheng Q, Huang TS (2002) Optimum detection and decoding of multiplicative watermarks in DFT domain. Proc IEEE Int Conf Acoust Speech Process 4:3477–3480
12. Cox IJ, Kilian J, Leighton T, Shamoon T (1997) Secure spread spectrum watermarking for multimedia. IEEE Trans Image Process 6(12):1673–1687
13. Cox IJ, Miller ML, Bloom JA (2002) Digital watermarking. Morgan-Kaufmann, San Francisco
14. Fishler MA, Bolles RC (1981) Random sample consensus: a paradigm for model fitting with applications to image analysis and automated cartography. Commun ACM 24(6):381–395
15. Gruhl D, Lu A, Bender W (1996) Echo hiding, pre-proceedings: information hiding. Cambridge, UK, pp. 295-316
16. Harris C, Stephens M (1988) A combined corner and edge detector. 4th Alvey Vision Conference. 147–151
17. Hsiao J-H, Chen C-S, Chien L-F, Chen M-S (2007) A new approach to image copy detection based on extended feature sets. IEEE Trans Image Process 16(8):2069–2079
18. Joly A, Buisson O (2005) Discriminant local features selection using efficient density estimation in a large database, in Proc. ACM Int. workshop on Multimedia information retrieval. New York, pp. 201–208
19. Joumaa H, Davoine F. An ICA based algorithm for video watermarking. In Proc. 2005 International Conference on Acoustics, Speech, and Signal Processing (ICASSP 2005), 2: 805–808
20. Kim C (2003) Content-based image copy detection. Signal Process Image Commun 18(3):169–184
21. Lewis AS, Knowles G (1992) Image compression using the 2-D wavelet transform. IEEE Trans Image Process 1(2):244–250
22. Lian S, Wang Z (2008) Collusion-traceable secure multimedia distribution based on controllable modulation. IEEE Trans Circuits Syst Video Technol 18(10):1462–1467
23. Lian S, Zhang Y (2009) Handbook of research on secure multimedia distribution. IGI Global (formerly Idea Group, Inc), March 2009
24. Lian S, Liu Z, Ren Z, Wang H (2007) Commutative encryption and watermarking in compressed video data. IEEE Trans Circuits Syst Video Technol 17(6):774–778
25. Lian S, Kanellopoulos D, Ruffo G (2009) Recent advances in multimedia information system security. Informatica, Slovenian Society Informatika 33(1): 3-24
26. Liu Z, Lian S, Dong Y, Wang H (2008) Desynchronized image fingerprint for large scale distribution. Proceedings of 2008 IEEE International Conference on Image Processing (ICIP2008), IEEE Publisher, October 2008, pp. 409–412
27. Minghong P, Mandal MK, Basu A (2005) Image retrieval based on histogram of fractal parameters. IEEE Trans Multimedia 7(4):597–605
28. Mokhtarian F, Suomela R (1998) Robust image corner detection through curvature scale space. IEEE Trans Pattern Anal Mach Intell 20(12):1376–1381

29. Petitcolas FAP, Anderson RJ, Kuhn MG (1998) Attacks on copyright marking systems, LNCS 1525, Springer-Verlag, ISBN 3-540-65386-4, pp. 219–239
30. Podilchuk CI, Zeng W (1998) Image-adaptive watermarking using visual models. IEEE J Sel Areas Commun 16(4):525–539
31. Sebastien G, Alexandre W, Nathalie P (2003) Image or audiovisual sequence extraction method for extraction of an image or audiovisual sequence from an image flux, wherein images are analyzed to generate a reference index and this is compares with the current index. FR2843212
32. Takeya F (2004) System for searching illegitimate use of contents. JP2004112318
33. van Schyndel RG, Tirkel AZ, Osborne CF (1994) A digital watermark. Proc IEEE Int Conf Image Process 2:86–90, Austin, Texas
34. Wang ZJ, Wu M, Trappe W, Liu KJR (2004) Group-oriented fingerprinting for multimedia forensics. EURASIP J Appl Signal Process 4:2153–2173
35. Wang J, Lian S, Liu G, Dai Y (2008) Secure multimedia watermarking authentication in wavelet domain. SPIE J Electron Imaging 17(03):033010
36. Weinheimer J, Qi X, Qi J (2006) Towards a Robust Feature-Based Watermarking Scheme. 2006 IEEE International Conference on Image Processing, Oct. 2006, pp. 1401–1404
37. Wu Y (2005) Linear combination collusion attack and its application on an anti-collusion fingerprinting. IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005 (ICASSP '05), 2:13–16
38. Wu M, Lin C, Chang C (2005) Image copy detection with rotating tolerance, In CIS 2005, Part I, LNAI 3801, Springer, pp. 464–469
39. Wu M, Trappe W, Wang ZJ, Liu R (2004) Collusion-resistant fingerprinting for multimedia. IEEE Signal Process Mag 21(2):15–27
40. Wu M-N, Lin C-C, Chang C (2006) A robust content-based copy detection scheme. Fund Inform 71 (2–3):351–366, IOS Press
41. Xue G, Lu P (2004) A counter-geometric distortions data hiding scheme using double channels in color images. The 3rd IWDW. 42–54
42. Yang Z, Cohen FS (1999) Image registration and object recognition using affine invariants and convex hulls. IEEE Trans Image Processing 8(7):934–946

Shiguo Lian got his Ph.D. from Nanjing University of Science and Technology, China. He was a research assistant in City University of Hong Kong in 2004. Since July 2005, he has been a Research Scientist with France Telecom R&D (Orange Labs) Beijing. He is the author or co-author of more than 80 refereed international journal and conference papers covering topics of secure multimedia communication, intelligent multimedia services, and ubiquitous communication. He has contributed 15 book chapters and held 16 filed patents. He authored the book "Multimedia Content Encryption: Techniques and Applications" (CRC Press, 2008), and edited 5 books. He got the Nomination Prize of "Innovation Prize in France Telecom" and "Top 100 Doctorate Dissertation in Jiangsu Province" in 2006. He is a member of IEEE Communications & Information Security Technical Committee, IEEE Multimedia Communications Technical Committee, and IEEE Technical Committee on Nonlinear Circuits and Systems. He is on the editor board of several international journals. He is the guest editor of more than 10 international journals. He is in the organization committee or the TPC member of refereed conferences, including IEEE ICC2008/2009/2010, IEEE

GLOBECOM2008/2009/2010, IEEE CCNC2009, IEEE ICCCN2009, etc. He is also the reviewer of refereed international magazines and journals.

Xi Chen received Ph.D. from Nanjing University of Science and Technology, China, in January 2006. He is an associate professor in Management School of Nanjing University and an visiting scholar of University of Washington. He authors more than 40 refereed journal/international conference papers and chapters. He authored the book "The theory of enterprise resource planning". He got the "Best Paper Awards" from Chinese Academy of System Simulation. He is the project chief of National Science Foundation and National Ministry of Education Science Foundation. His research interests include service science, E-Commerce security, information management and data authentication. He is a member of some Technical Committees, the technical committee chair and organization committee chair of refereed conferences/workshops, the peer review expert of NSFC. He is on the editor board of several international journals, and reviewer of some refereed international journals and conferences.

Jinwei Wang received the B.A.Sc. in automatic control from Inner Mongolia Electric Power College in 2000 and Ph.D. in information security from Nanjing University of Science & Technology in 2007. He was a teaching assistant at Inner Mongolia University of Technology from July 2000 to September 2002. He was a research assistant in Service Anticipation Multimedia Innovation (SAMI) Lab of France Telecom R&D Center (Beijing) from 2005 to 2006. He is now with The 28th Research Institute of CETC, China. He has published more than 20 papers in international journals and conferences. His research interests include multimedia watermarking, image processing and data authentication.