Nonspecific DCT-block Fingerprinting based on Incomplete Cryptography for DRM system

Ta Minh Thanh
Department of Network Security
Le Quy Don Technical University
100 Hoang Quoc Viet, Cau Giay,
Hanoi, Vietnam.
Email: taminhjp@gmail.com

Munetoshi Iwakiri
Department of Computer Science
National Defense Academy
1-10-20, Hashirimizu, Yokosuka-shi,
Kanagawa, 239-8686, Japan.
Email: iwak@nda.ac.jp

***Abstract*—In the present digital world, Digital Rights Management (DRM) is essential to enforce persistent data protection right from the moment it is published. In spite of a need for DRM there are significant weaknesses in the current technology. Generally, DRM system is achieved with individual function modules of cryptography, fingerprinting and so on. In this typical system flow, all digital contents are temporarily disclosed with perfect condition via decryption process. This paper describes the elemental idea of a DRM method which is composed of an incomplete cryptography based on nonspecific DCT-block (Discrete Cosine Transform) and user fingerprinting mechanism to control the quality of digital contents. There are two fundamental steps in our proposed cryptography: incomplete encoding and incomplete decoding. These two steps will create the scrambled content using as trial content and fingerprinted content is used to prevent unauthorized duplication or business of digital contents, respectively. Experimental results on standard JPEG (Joint Photographic Experts Group) format show that the proposed method is suitable for DRM in the network distribution system.**

I. Introduction

Due to the advent of network and computer technology, there has been an explosion in the use of digital media through electronic commerce and online services. Since digital media are easily reproduced and manipulated, anyone is potentially capable of incurring considerable financial loss to the media producers and content providers. Thus the need for an effective rights management system where only legitimate consumers can have access to digital content [1], [2], [3].

A DRM system usually contains encryption and key management, access control, copy control, identification, tracing and billing mechanisms. Access control must be done using an adaptable set of usage rules that define what the user can do with the content. Copy control is used to prevent making unauthorized copies of the content and usually hard to achieve. Identification and trace can be used as a last resort to follow the source of pirated copies and enable legal action [4], [5], [6].

In recent researches, the fingerprinting information such as user's information is embedded into the content to prove legal users or trace the source of pirated copies. However, conventional DRM technologies are manipulated by encryption and fingerprinting method separately. Therefore, original content is disclosed temporarily inside a system in the user's decryption (key management process) [3]. In that case, users save original contents without watermark information and distribute via network.

In this paper, we present a new DRM technique based on an incomplete cryptography system using nonspecific DCT-block in encoding and decoding process, which can hold promise for a better compromise between encryption and fingerprinting for emerging digital rights management applications. The proposed method will deteriorate the quality of original contents to make trial contents for distribution to wide users via network. The quality of trial contents will be controlled with a watermarked key at the incomplete decoding process, and user information will be embedded into the incomplete decoded contents simultaneously.

The rest of the paper is organized as follows: in Section 2, we briefly review the incomplete cryptography system. The implementation of fingerprinting method based on nonspecific DCT-block using incomplete cryptography is explained in Section 3. Experimental results on JPEG algorithm are presented in Section 4 to demonstrate the performance of proposed method in the network distribution system. Finally, we conclude in Section 5.

II. Overview of incomplete cryptography

The proposed incomplete cryptography[7] consists two steps: the incomplete encoding and the incomplete decoding.

In the incomplete encoding process, content P is encoded based on the encoder function E with encoder key k to make the scrambled content C.

$$C = E(k, P) \tag{1}$$

Here, C can be simply recognized as a part of P (even if C is not decoded). This feature is called $incomplete\ confidentiality$.

On the other hand, the incomplete decoding process is different from the complete decoding process. C is decoded by using a decryption function $D' \neq D$ and a decoded key $k' \neq k$.

$$P' = D'(k', C) \tag{2}$$

978-1-4673-4352-7/12/$31.00 ©2012 IEEE

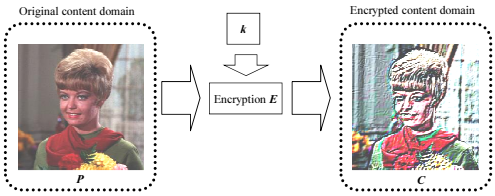

Fig. 1. Scrambled method based on incomplete cryptography.

Since P' is decoded by another decryption function D' with key k', it will be deferent from original content P. Therefore, the relationship of P and P' is $P' \neq P$ in incomplete cryptography system. This feature is called *incomplete decode*.

The main contribution of incomplete cryptography is that the quality of P' can be controlled with a particular key k'. And when C is decoded with k', P' is not only decoded with slight distortion, but also watermarked with individual user information that is used as fingerprinting information. It is the elemental mechanism of fingerprinting based on the incomplete cryptography system.

III. The Fingerprinting Method Based on Nonspecific DCT Block

Since the incomplete cryptography has incomplete confidentiality and incomplete decode feature, it makes no value to a secret transmission system. However, the incomplete cryptography is able to manipulate the contents via an information transmission system so far as the distortion level permits. Especially, if features of the incomplete cryptography are implemented to a DRM system, the incomplete encoding (make scrambled content) and the incomplete decoding (make watermarked content) processes are required to resolve the above mentioned problem. The scrambled algorithm and watermarked algorithm are explained in the following subsections.

A. Scrambled method

The scrambled content is used as trial contents, which is delivered to users via network. The scrambled content has an important role in user's decision of purchase. The basic idea of the scrambled algorithm is shown in **Fig.1**. Suppose P is a JPEG image in the domain of original contents, k is an encoder key and E is an encoder function. E will encode a part of P and degrade the quality of P. To create the scrambled content C, we choice the nonspecific DCT blocks Q_t that is randomly chosen by key t. By encoding the DCT coefficients in Q_t, the quality of P is degraded. This randomization is expected to increase the security of the system and makes guessing difficult. Commonly used randomization in selecting the DCT-block are - selecting all even blocks for encryption, selecting all odd blocks for encryption or selecting $10\%, 15\%, 20\%, 25\%, \cdots, 100\%$ blocks and so on. These are obviously good but chances of guessing are more. The randomization approach proposed in this paper places itself far from these guesses.

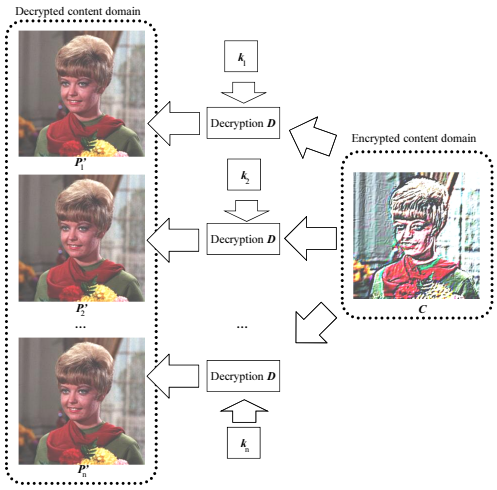

Fig. 2. Watermarking based on incomplete cryptography.

B. Fingerprinted method

In the proposed method, the decoded content P'_i is different from the original content P. Assume that a user R can decode C to P'_i that closes the quality of P, then we can propose a watermarked algorithm to control quality of P'_i [7]. The watermarked algorithm is explained as follows (see **Fig.2**).

Suppose a user R receives a decoder key k'_i from producer T and decodes scrambled C. Here, if $k'_i \neq k$, it is clear to decode $P'_i \neq P$. But, as shown in Fig.2, if quality of P'_i is sufficient for the user, even if $k'_i \neq k$, user can not sense the distortion which is inserted into P such as copyright protection codes. k'_i is also used to embedded the user information into the chosen blocks Q_t at random positions in Q_t. Using k'_i, we present a fingerprinted method that embeds the user information in the least significant bits (LSB) of randomly chosen locations in Q_t for distinguishing the legal users.

Thus, T can control the quality of P'_i (watermarked contents) with a particular key k'_i (watermarked key). Then, when the user decodes C using k'_i to make P'_i, P'_i is not only decoded with slight deterioration, but also watermarked with particular information (i.e. user information). It is the elemental mechanism of watermarking based on the incomplete cryptography system.

C. Proposed DRM based on incomplete cryptography

A DRM system requires to enable the distribution of original contents safely and smoothly, as well as to enable the secondary use of contents under rightful consents. When a DRM system is constructed using incomplete cryptography to implement a content distribution system, it is not only the safety distribution method to users, but also the solution of the conventional DRM problem.

Before distribution, T has a digital content P and needs to be sent to users as much as possible. Thus, T creates a scrambled content C with encryption key k based on incomplete cryptography. The result of the encryption process, C is to disclose a part of P. It means that C is maintained over

the minimum quality of P. T distributes C to users widely via network as a trial content.

After trial C, R decides to purchase a digital content. Then, R has to register his/her individual information. This information will be used as the watermarked information (w_m) and to be embedded into the content. When T receives the purchaser's agreement, T sends a watermarked key k_i' to the user R. k_i' is the incomplete decoding key and it is prepared individually to each user.

R decodes C using k_i' and obtains the high quality content P_i'. In this decoding process, ID information (w_m) of user will be embedded in P_i' as the copyright information.

Therefore, when a producer wishes to check whether the users is a legal user, he/she can extract the watermarking information from P_i' and compare with his user database. If the watermarking information matches his database, the user is a legal user. Conversely, if the watermarking information is a different from his database, the user is an illegal user.

$Note\ that$, in this study, robustness is not the major concern. Therefore, we derive analytic bounds of the embedded signals to achieve the highest transparency and ensure that our technique can trace the traitor exactly.

IV. Simulation results

In this section, we explain the mechanism to create the scrambled content for a trial content. Then, an algorithm to make the watermarked key is used to decode the scrambled content, then the user information is embedded into the decoded content at the incomplete decoding process with the key. We implemented the most fundamental method based on the standard JPEG algorithm[9].

To make scrambled and incomplete decoding contents of JPEG, and we have selected the quantized DCT coefficients in DCT-block to implement the incomplete cryptography. There are two reasons for this choice. First, it is easy to control the image quality which stored in the quantized DCT coefficients as digital data. The second reason is flexibility of making a variation of content by selecting a luminance component (Y component) and two chrominance components (UV component) in the quantized DCT coefficients.

A. Incomplete encoded method

First, various parameters such as the side information, entropy code, and so on, are extracted from JPEG data. Suppose that the DCT-block Q_t that is chosen by random key t will be scrambled and specified coefficient P is selected from the quantized DCT coefficients in Q_t. We proposed a new watermarking method to control significant bits of DCT coefficient for making scrambled and incomplete decoding content. In this method, lower bits except for most significant bit(MSB) of "1" in P are encoded by a random code to scramble JPEG image. The scrambled method is described as follows:

Step 1. A random key t is generated to choice quantized DCT-block Q_t.

Step 2. A 8-bit of key k is generated to scramble a quantized DCT coefficient P in Q_t.

Step 3. A shift coefficient m can be obtained using the following calculation.

$$m \leftarrow 8 - \lfloor \log_2(|P|) \rfloor \tag{3}$$

where the symbol $\lfloor . \rfloor$ is the floor function. k is shifted m bits to prepare the encryption key k_m.

$$k_m \leftarrow k \gg m \tag{4}$$

Step 4. The significant bits of P are encoded with using k_m to make scrambled content C. The scrambled content C is given by,

$$C \leftarrow P \oplus k_m \tag{5}$$

where the symbol $\oplus$ is the XOR function.

In the scrambled method, the scrambled content C is disclose a part of P because the exception MSB of P is encoded. C is widely distributed to users as a trial content via network.

B. Incomplete decoded method

T generates a decryption key k_m' and sends it to R. The incomplete decoded method is described as follows.

Step 1. T extracts 1-bit w from $userID$ and defines the least significant bit (LSB) of key k_m as

$$k_m' \leftarrow \begin{cases} k_m \oplus (P \ \& \ 0 \times 01) & (\text{if } w = 0) \\ k_m \oplus (\overline{P} \ \& \ 0 \times 01) & (\text{if } w = 1) \end{cases} \tag{6}$$

where the symbol $\&$ is the AND function and the symbols $\overline{P}$ is NOT function of P.

Step 2. T prepares watermarked key k_m' based on **Step 1**, and delivers to R.

Step 3. R decodes the scrambled C by using k_m' and obtains incomplete decode content P'.

$$P' \leftarrow C \oplus k_m' \tag{7}$$

In the decoding process, user information ($userID$) is embedded into the LSB of quantized DCT coefficient P' at some particular position of DCT tables. The advantage of incomplete cryptography is that when decoding the scrambled content C, watermarking information is simultaneously embedded into the decoding content. Therefore, it is possible to implement the watermarked process while decoding.

Additionally, when a producer verifies the legal user of content P, he/she can extract the user information from LSB of a particular DCT coefficient using a random key t for detecting DCT-block Q_t and a secret key k_s for extraction fingerprinting bit. In this paper, k_s is the LSB of each pixels in P'.

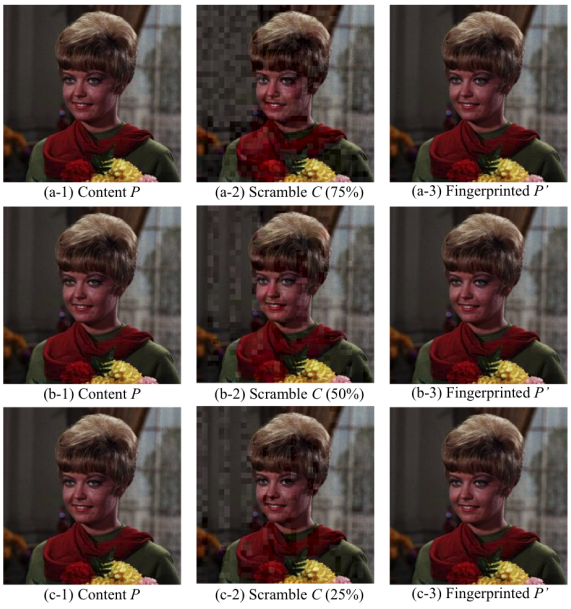

Fig. 3. Examples of images (Girl, quality: 75).

TABLE I
EXPERIMENTAL RESULTS (PSNR[DB] AND EMBEDDED BITS).

Image	Block[%]	P	C	P'	Emb.[bit]
Girl	25	32.71	28.00	32.82	3117
Girl	50	32.71	24.48	31.07	6607
Girl	75	32.71	21.62	30.39	9801
Aerial	25	30.20	25.77	29.27	3863
Aerial	50	30.20	22.77	28.27	8397
Aerial	75	30.20	22.47	27.59	12584
Couple	25	34.06	28.05	33.01	3106
Couple	50	34.06	25.40	32.14	6447
Couple	75	34.06	16.63	31.42	9735

C. Simulation results

To prove the efficiency of proposed method, we used Girl, Aerial, Couple (256×256, 8-bit color) image in SIDBA[1] database and create JPEG image with quality 75. We also used PSNR (Peak Signal to Noise Ratio) [7] to evaluate the JPEG image quality. To generate the encryption k and random key t, we used function $rand()$ of GCC version 3.3.2 with $seed = 1$ and $seed = 2$. We also applied the proposed method for 25%, 50%, 75% DCT-block, respectively, in each JPEG image to control the quality of experimental image.

Assume that a quantized DCT coefficient in random DCT-block Q_t is $P = 21$; then P can be expressed as binary bits $P = 10101_2$. As in the scrambled method, we generate an encoded key k, and set that as $k = 31(k = 11111_2)$ for example. For encoding P, we calculate $m = 8 - \lfloor \log_2(|21|) \rfloor = 4$ (see formula (3)). m is used to create $k_m = k \gg m = 31 \gg 4$; then, $k_m = 00001_2$. Finally, following (5), $C = P \oplus k_m = 10101_2 \oplus 00001_2 = 10100_2 (C = 20)$ is scrambled. To illustrate the decoded process, let us assume the watermark bit as $w = 1$, then $k'_m = k_m \oplus (\overline{P} \ \& \ 0 \times 01) = 00001_2 \oplus (\overline{10101_2} \ \& \ 0 \times 01) = 00001_2$ (see formula (6)). If k'_m is used to decode C, we can obtain $P' = C \oplus k'_m = 10100_2 \oplus 00001_2 = 10101_2$. It means that the watermark bit $w = 1$ is embedded into LSB of P'. To extract the watermark from the watermarked JPEG image, it can be extracted from LSB (as the extract key k_s) of P' and compare with $userID$ to confirm the illegal user.

The experimental results are shown in **Fig.3** and **Tab.I**. We see that the fingerprinted JPEG images (Fig.3 (a-3), (b-3), (c-3)) are not distinguishable from the original JPEG images (Fig.3 (a-1), (b-1), (c-1)). The scrambled JPEG images (Fig.3 (a-2), (b-2), (c-2)) are degraded about 20dB, and they seem appropriate as trial content. We calculate PSNR value of the output JPEG images in every processes and extracted the watermark information (embedded binary data) perfectly from the incomplete decode JPEG images. In our method, we extracted LSB of quantized DCT coefficients. In addition, from results of Tab.I, we recognized that we can easily control the quality of trial image by utilizing the number of DCT-block (25%, 50% or 75%)

[1] http://vision.kuee.kyoto-u.ac.jp/IUE/IMAGE_DATABASE/STD_IMAGES

V. CONCLUSION

In this paper, we have established the novel DRM system integrated with fingerprinting based on incomplete cryptography system. And, the original content is not decoded temporarily inside the system. Thus, we conclude that the above technical problem by the conventional DRM system is solved by using the incomplete cryptography system. The effectiveness of the proposed scheme has been demonstrated with the aid of experimental results. Therefore, we conclude that proposal method is useful for the rights management technology in illegal content distribution via network.

REFERENCES

[1] S. Michiels, K. Verslype, W. Joosen, and B. D. Decker, "Towards a software architecture for drm," in DRM 05: Proceedings of the 5th ACM workshop on Digital rights management. New York, NY, USA: ACM, 2005, pp. 65–74.
[2] S. Subramanya and B. Yi, "Digital rights management," Potentials, IEEE, vol. 25, pp. 31–34, 2006.
[3] DRM technology, "Advanced Image Seminar 2003," The Institute of Image Electronics Engineers of Japan, 2003.
[4] F.Hartung and F.Ramme, "Digital Rights Management and Watermarking of Multimedia Content for M-Commerce Applications," IEEE Communications Magazine, Selected Papers from ISS2000, pp. 77–84, 2000.
[5] E.T.Lin, A.M.Eskicioglu, R.L.Lagendijk, and E.J.Delp, "Advances in Digital Video Content Protection," Proc. of the IEEE, Vol. 93, No. 1, pp. 171–183, 2005.
[6] A.Seki and W.Kameyama, "A Proposal on Open DRM System Coping with Both Benefits of Rights-Holders and Users," IEEE conference on Image Proceedings, Vol. 7, pp.4111–4115, 2003.
[7] I. Munetoshi, Ta Minh Thanh, "Fundamental Incomplete Cryptography Method to Digital Rights Management Based on JPEG Lossy Compression," The 26th IEEE International Conference on Advanced Information Networking and Applications (AINA-2012), 2012.
[8] I. Munetoshi, Ta Minh Thanh, "Incomplete Cryptography Method Using Invariant Huffman Code Length to Digital Rights Management," The 26th IEEE International Conference on Advanced Information Networking and Applications (AINA-2012), 2012.
[9] The International Telegraph and Telephone Consultative Committee Information Technology - Digital Compression and Coding of Continuous-tone still Images - Requirements and Guidelines, International Telecommunication Union, 1992.