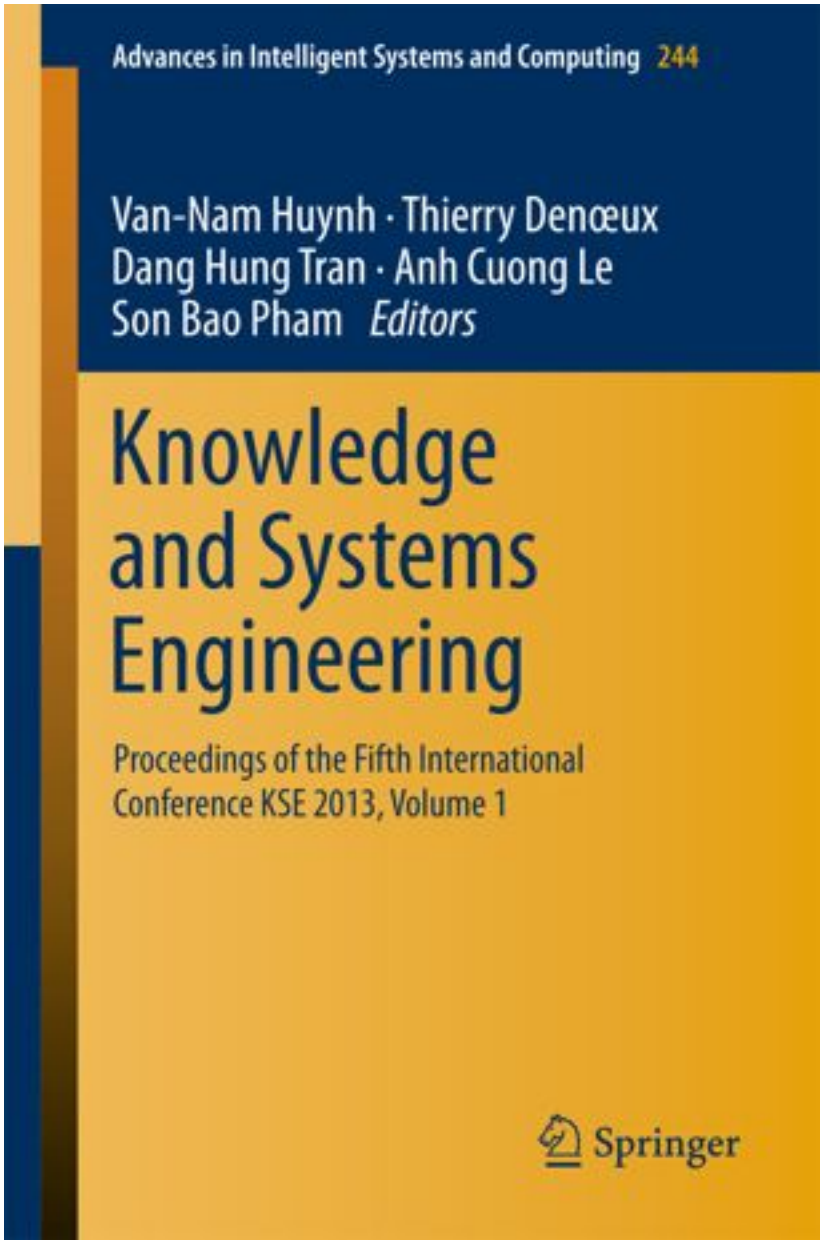
Advances in Intelligent Systems and Computing 244
Van-Nam Huynh · Thierry Denœux
Dang Hung Tran · Anh Cuong Le
Son Bao Pham Editors
Knowledge and Systems Engineering
Proceedings of the Fifth International Conference KSE 2013, Volume 1
Springer

Incomplete Encryption Based on Multi-channel AES Algorithm to Digital Rights Management

Ta Minh Thanh, Munetoshi Iwakiri

Abstract DRM (Digital Rights Management) systems is the promising technique to allow the copyrighted content to be commercialized in digital format without the risk of revenue loss due to piracy. However, traditional DRMs are achieved with individual function modules of cryptography and watermarking. Therefore, all digital contents are temporarily disclosed with perfect condition via decryption process in the user side and it becomes the risk of illegal redistribution. In this paper, we propose an incomplete encryption based on multi-channel AES algorithm (MAA) to control the quality of digital contents as a solution in DRM system. We employed the multi-channel AES algorithm in the incomplete cryptography to imitate multimedia fingerprint embedding. Our proposed method can trace the malicious users who redistribute the digital contents via network. We make this scenario more attractive for users by preserving their privacy.

1 Introduction

1.1 Overview

Advances in computer and network technologies have made easily to copy and distribute the commercially valuable digital content, such as video, music, picture via

Ta Minh Thanh
Department of Network Security, Le Quy Don Technical University, 100 Hoang Quoc Viet, Cau Giay, Hanoi, Vietnam, and Department of Computer Science, Tokyo Institute of Technology, 2-12-2, Ookayama, Meguro-ku,Tokyo, 152-8552, Japan
e-mail: taminhjp@gmail.com;thanhtm@ks.cs.titech.ac.jp

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

global digital networks. It enables an e-commerce model, that consists of selling and delivering digital versions of content online. The main point of concern for such a business is to prevent illegal redistribution of the delivered content.

DRM systems were created to protect and preserve the owner's property right for the purpose to protect their intellectual property [1, 2, 3]. A common approach to protect a DRM system against tampering is to use a hardware based protection, often implemented in set-top-boxes. However, the biggest disadvantage of hardware based DRM systems are inflexibility and high cost. It requires a large investment cost from the service provider and time consuming for market. Additionally, hardware based DRM systems are expensive for customers. At a time where a lot of pirated contents are available on the Internet, hardware based solutions have the hard time creating value for the users. In order to reduce the developed cost, software based DRM [4, 5, 6] is proposed instead of hardware based DRM. The advantage of software based DRM is that they can be easily distributed to the users via networks and do not need to create additional installation costs. Most users would prefer a legal way to easily access content without huge initial costs or long term commitment. The problem with software based DRM system is that they are assumed to be insecure. Especially, such kind of software based DRM technologies are manipulated by encryption and watermark method separately. Therefore, original content is disclosed temporarily inside a system in the user's decryption [7]. In that case, users can save original contents without watermark information and distribute via network.

1.2 Our contributions

In this paper, we focus on a strategy for the construction of software based DRM system that is far more secure than existing software based DRM system. We describe a design and implementation of DRM technique based on multi-channel AES algorithm (MAA). Our method will deteriorate the quality of original contents to make trial contents for distribution to widely users via network. The quality of the trial contents will be controlled with a fingerprinted key at the incomplete decoding process, and the user information will be fingerprinted into the incomplete decoded contents simultaneously.

This paper is organized as follows. The related techniques are reviewed in Section 2. The implementation of DRM based on MAA is explained in Section 3. The experimental results with JPEG (Joint Photographic Experts Group) algorithm are given in Section 4 and the conclusion is summarized in Section 5.

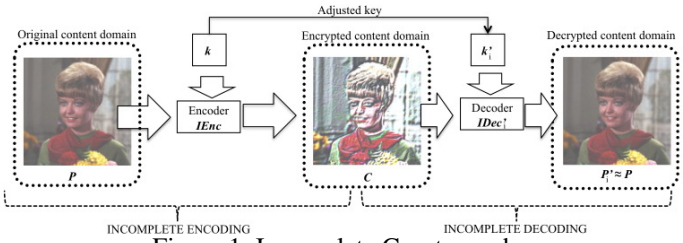

Figure 1: Incomplete Cryptography.

2 Preliminaries

2.1 Incomplete Cryptography

The incomplete cryptography consists two steps: the incomplete encoding and the incomplete decoding (**Fig. 1**).

In the incomplete encoding process, content P is encoded based on the incomplete encoder function $IEnc$ with encoder key k to make the scrambled content C (trial content).

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

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 another incomplete decryption function $IDec'_i \neq D$ and a decoded key $k'_i \neq k$. Key k'_i is adjusted based on k to allow content owner making i decoded contents P'_i.

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

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

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

2.2 DRM system based on incomplete cryptography

The idea of the DRM system based on the incomplete cryptography is presented in this subsection. 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 the 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, producer 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 the encoder key k based on the incomplete cryptography. Here, 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 that is distributed via network, user R decides to purchase a digital content. Then, R has to register his/her individual information. This information will be used as the fingerprinted information (w_m) and embedded into the content. When T receives the purchaser's agreement, T sends a fingerprinted key k_i' to the user R. k_i' is the incomplete decoding key and it is prepared individually to each user based on w_m.

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 fingerprinted 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 fingerprinting information from P_i' and compare with his user database. If the fingerprinting information matches his database, the user is a legal user. Conversely, if the fingerprinting information is a different from his database, the user is an illegal user. Furthermore, it can specify to trace the source of pirated copies. The purpose of this proposed method is to informs the producer about the existence of fingerprinting which can exactly identify users, and limit the illegal redistribution in advance.

3 The proposed MAA algorithm

The main idea of the proposed method is that utilizes the complete cryptography to implement the incomplete cryptography. Suppose that the complete cryptography $\mathbb{E}$ is selected and has the encryption function *CEnc* and the decryption function *CDec* with secret share key $\{k_1, k_2\}$. Here, we present the algorithm to implement the incomplete cryptography using $\mathbb{E}$. As shown in **Fig. 2**, the proposed MAA method consists of two processes: the incomplete encoding, the incomplete decoding.

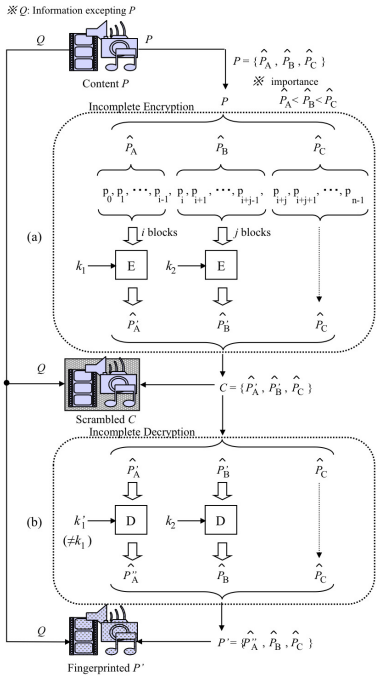

Figure 2: Overview of MAA algorithm.

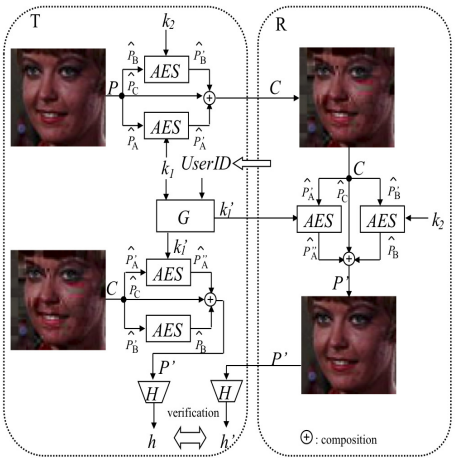

Figure 3: Using AES for MAA algorithm.

3.1 Incomplete encoding

The incomplete encoding is shown in Fig. 2(a). This process is implemented in the producer side by T. There are four steps in this process.

Step 1. Extract the important elements P from the digital content and split P into n blocks as shown in Fig. 2(a). Moreover, block $p_0 \sim p_{n-1}$ are grouped to make three groups $\widehat{P_A}, \widehat{P_B}, \widehat{P_C}$, respectively. The importance of three groups can be expected that is $\widehat{P_A} < \widehat{P_B} < \widehat{P_C}$.

$$P = \{p_0, \cdots, p_{i-1}, \cdots, p_{i+j-1}, \cdots, p_{n-1}\} \Rightarrow P = \{\widehat{P_A}, \widehat{P_B}, \widehat{P_C}\} \tag{3}$$

Step 2. Extract $\widehat{P_A}$ and $\widehat{P_B}$ to encode a part of P.

Step 3. Encode $\widehat{P_A}$ and $\widehat{P_B}$ by using the encoder function $CEnc$ with key pair $\{k_1, k_2\}$.

$$\widehat{P'_A} = CEnc(k_1, \widehat{P_A}); \;\; \widehat{P'_B} = CEnc(k_2, \widehat{P_B}) \tag{4}$$

Step 4. Merge $\{\widehat{P'_A}, \widehat{P'_B}\}$ with $\widehat{P_C}$ to make the scrambled content $C = \{\widehat{P'_A}, \widehat{P'_B}, \widehat{P_C}\}$.

In incomplete encoding, the most important group $\widehat{P_C}$ is not encoded to disclose P for users. It means that C can be simply recognized a part of P (even if C is not decoded). C is distributed widely to users as trial content via network.

3.2 Incomplete decoding

Fig. 2(b) shows the detail of the incomplete decoding. This process is executed in the user side by R. Suppose that R had finished the purchasing process and the decoded key $\{k_1', k_2\}$ is delivered by producer T. In order to obtain the high quality content, R uses the decoded key $\{k_1', k_2\}$ with decoder function $CDec$ to decode the trial content C. This algorithm is shown as the following.

Step 1. Extract three groups $\{\widehat{P_A'}, \widehat{P_B'}, \widehat{P_C}\}$ from C.

Step 2. Decode $\{\widehat{P_A'}, \widehat{P_B'}\}$ by using $IDec$ and $CDec$ with $\{k_1', k_2\}$ to obtain $\{\widehat{P_A''}, \widehat{P_B}\}$.

$$\widehat{P_A''} = IDec(k_1', \widehat{P_A'}); \;\; \widehat{P_B} = CDec(k_2, \widehat{P_B'}) \tag{5}$$

Since $k_1' \neq k_1$ then $\widehat{P_A''} \neq \widehat{P_A}$. Note that, k_1' is the decoded key that is generated based on the individual user information w_m. Therefore, $\widehat{P_A''}$ can be expected to imitate multimedia fingerprint embedding for each user.

Step 3. Merge $\{\widehat{P_A''}, \widehat{P_B}\}$ with $\widehat{P_C}$ to make the decoded content $P' = \{\widehat{P_A''}, \widehat{P_B}, \widehat{P_C}\}$.

In the incomplete decoding, because of $\widehat{P_A}$ has the lowest level of importance, then even $\widehat{P_A'}$ is decoded to $\widehat{P_A''}$, we still obtain the incomplete decoded content P' with high quality.

In addition, by controlling the decoder key pair $\{k_1', k_2\}$, producer T can not only control the quality of the digital content P' for the legal user, but also distinguish the legal user by using the hash value h_i of P'.

3.3 Using AES encryption for MAA

Fig. 3 explains how to implement AES[8] encryption in the proposed MAA.

First, T extracts $\{\widehat{P_A}, \widehat{P_B}\}$ from P and encrypts $\{\widehat{P_A}, \widehat{P_B}\}$ by using AES encryption with key pair $\{k_1, k_2\}$ to obtain $\{\widehat{P_A'}, \widehat{P_B'}\}$. T degrades the quality of P by merging $\{\widehat{P_A'}, \widehat{P_B'}\}$ into $\widehat{P_C}$ to obtain the trial content C. C is distributed to many users via network.

After receiving the purchasing agreement of R, T creates the decoded key $\{k_1', k_2\}$ based on the key generation function G with key k_1 and the UserID w_m. T sends decoded key $\{k_1', k_2\}$ to R. In this paper, function G is bitwise XOR (eXclusive OR) and is described as $\oplus$. It means that $k_1' = k_1 \oplus w_m$.

R uses $\{k_1', k_2\}$ with AES decryption to decode $\{\widehat{P_A'}, \widehat{P_B'}\}$. Here, $\widehat{P_A'}$ is incomplete decoded, whereas $\widehat{P_B'}$ is complete decoded. After that, $\{\widehat{P_A''}, \widehat{P_B}\}$ will be replaced $\{\widehat{P_A'}, \widehat{P_B'}\}$ in C to obtain $P' = \{\widehat{P_A''}, \widehat{P_B}, \widehat{P_C}\}$ with high quality.

In our proposed MAA method, since k_1' is created based on the UserID w_m and function G, it is clear that k_1' is also changed according to UserID w_m. Therefore, the hash value h of P' can be used as the identity of the legal user.

4 Application on JPEG algorithm

In this section, we explain the mechanism to create the scrambled content for the trial content and the incomplete decoded content. We implemented the fundamental method based on the standard JPEG (Joint Photographic Experts Group) algorithm[10].

4.1 MAA using AES algorithm in JPEG

Let P be the DCT table of the Y component or UV component that is extracted from JPEG image. $\{\widehat{P_A}, \widehat{P_B}\}$ are created by collecting some bits from DC coefficient of P. $\widehat{P_C}$ is AC coefficients of P. In order to encode P, AES encryption[1] with ten rounds is employed for the implementation of MAA. The detail of MAA is explained as following.

4.1.1 Trial content creation

The trial content is obtained based on the incomplete encoding of MAA as following,

Step 1. Extract DC coefficient from DCT table and convert to binary array. As shown in **Fig. 4**, DC coefficient = "13" and its binary array is $\{0,0,0,0,1,1,0,1\}$.

Step 2. Let $\widehat{P_A}$ be i bits LSB (Least Significant Bit) of DC coefficient and $\widehat{P_B}$ be next continuos j bits. In example of Fig. 4, $i = 2$ and $j = 3$;

$$\widehat{P_A} = \{0,1\}; \widehat{P_B} = \{0,1,1\} \tag{6}$$

Step 3. Repeat Step 2 for collecting all $\{\widehat{P_A}, \widehat{P_B}\}$ to obtain 256-bit array $\{\widetilde{P_A}, \widetilde{P_B}\}$.

Step 4. Encrypt $\{\widetilde{P_A}, \widetilde{P_B}\}$ obtained in Step 3 by AES encryption with the encoded key $\{k_1, k_2\}$.

Step 5. Repeat Step 1 $\sim$ Step 4 until all DCT tables are encrypted. After encryption, the encoded bit array $\{\widetilde{P'_A}, \widetilde{P'_B}\}$ are collected.

Step 6. Split $\{\widetilde{P'_A}, \widetilde{P'_B}\}$ to make the encrypted i bits of $\widehat{P'_A}$ and j bits of $\widehat{P'_B}$, respectively. Then, restore $\widehat{P'_A}$ and $\widehat{P'_B}$ into the position of $\widehat{P_A}$ and $\widehat{P_B}$ to obtain the trial content C. In **Fig. 4**, since $i = 2$ and $j = 3$ then $\widehat{P'_A}$ and $\widehat{P'_B}$ became $\{0,0\}$ and $\{1,1,0\}$, respectively.

According to incomplete encoding, DC coefficient = "13" in Fig. 4 is encrypted to "24". Therefore, the trial content C is generated with low quality, then C can disclose P.

[1] http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf

4.1.2 Fingerprinted content creation

In this process, user R uses the decoded key $\{k'_1, k_2\}$ to decode the trial content C. k'_1 is generated based on w_m that belongs to legal user identity. According to the AES decryption, R can decrypt $\{\widetilde{P'_A}, \widetilde{P'_B}\}$ by using $\{k'_1, k_2\}$. The detail of this process is shown in **Fig. 5**.

Step 1. Extract DC coefficient from DCT table of trial content C and convert to binary array. In example **Fig. 5**, DC coefficient = "24" and its binary array is $\{0,0,0,1,1,0,0,0\}$.

Step 2. Extract $\widehat{P'_A}$ from i bits LSB (Least Significant Bit) of DC coefficient and $\widehat{P'_B}$ from next continuos j bits. In our example, $i = 2$ and $j = 3$.

$$\widehat{P'_A} = \{0,0\}; \widehat{P'_B} = \{1,1,0\} \tag{7}$$

Step 3. As the incomplete encoding, repeat Step 2 for collecting all $\{\widehat{P'_A}, \widehat{P'_B}\}$ to obtain 256-bit array $\{\widetilde{P'_A}, \widetilde{P'_B}\}$.

Step 4. Decode the obtained $\{\widetilde{P'_A}, \widetilde{P'_B}\}$ in Step 3 by AES decryption with encoded key $\{k'_1, k_2\}$. Here, since $k'_1 \neq k_1$ then $\widetilde{P''_A} \neq \widetilde{P_A}$.

Step 5. Repeat Step 1 $\sim$ Step 4 until all DCT tables are decrypted. After decryption, the decoded bit array $\{\widetilde{P''_A}, \widetilde{P_B}\}$ are collected.

Step 6. Split $\{\widetilde{P''_A}, \widetilde{P_B}\}$ to make the decrypted i bits of $\widehat{P''_A}$ and j bits of $\widehat{P_B}$, respectively. Then, restore $\widehat{P''_A}$ and $\widehat{P_B}$ into the position of $\widehat{P'_A}$ and $\widehat{P'_B}$ to obtain the fingerprinted content P'. In Fig. 5, since $i = 2$ and $j = 3$ then $\{\widehat{P''_A}, \widehat{P_B}\}$ became $\{1,0\}$ and $\{0,1,1\}$, respectively.

According to the incomplete decoding, DC coefficient = "24" in Fig. 5 is encrypted to "14". It is clear that two LSBs ($\widehat{P_A}$) of each DC coefficient are changed according to the user identity w_m. Namely, producer T can decide the decoded key pair $\{k'_1, k_2\}$ to control the decoded content P' based on user identity w_m. Therefore, when a producer verifies the legal user of content P, he/she can extract the hash information h from P' to detect the legal user. In this paper, we use 256-bit hash value for legal user verification.

4.2 Implementation and evaluation

4.2.1 Experimental environment

All experiments were performed by incomplete encoding and incomplete decoding on JPEG images using the Vine Linux 3.2 system. In order to generate the encryption key k_1, k_2, k'_1 of AES encryption, we used function *rand*() of GCC version

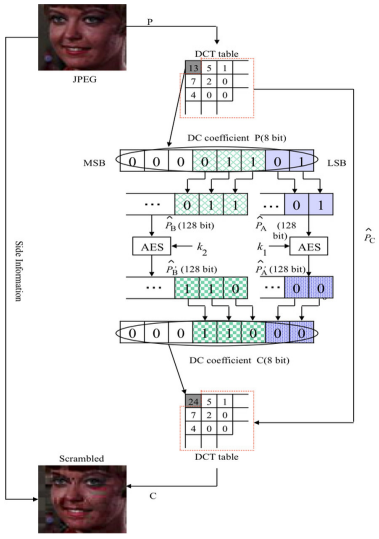

Figure 4: The encoding a part of DC coeff.

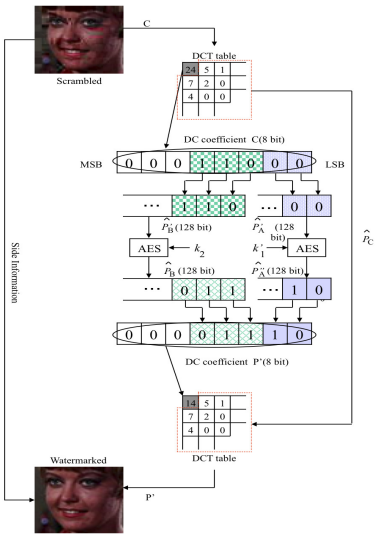

Figure 5: The decoding a part of DC coeff.

3.3.2[2] with $seed = 1$. Additionally, the ImageMagick version 6.6.3-0[3] was used to convert and view the experimental JPEG images. The encryption keys are employed in our experiments as following,

$$k_1 = \{\texttt{53564df05d23565c31153e1b5a3b3f1a}\}$$
$$k_2 = \{\texttt{5a13584b3d62404d2d1b2a4f315d2531}\}$$
$$k_1' = \{\texttt{53564df05d23565c31153e1b5a3b3f1b}\}$$

Note that, we suppose $w_m = 1$ and $k_1' = k_1 \oplus w_m$.

4.2.2 Experimental image

The four test images are the 8-bit RGB images of SIDBA (Standard Image Data BAse) international standard image (Girl, Airplane, Parrots, Couple) of size 256×256 pixels. Here, all images were compressed with quality 75 (the lowest $0 \leftrightarrow 100$ the highest) to make experimental JPEG images for evaluation of the proposal method. We also randomly generated the w_m to assign as the userID and the decoded key k_1' is created based on w_m.

[2] http://gcc.gnu.org/

[3] http://www.imagemagick.org/script/

Table 1: PSNR[dB] of experimental images.

Method		P	C	P'	$h[bits]$
$AES_{1,3}$	Airplane	30.20	24.74	30.06	256
	Girl	32.71	25.99	32.51	256
	Parrots	34.25	26.29	33.97	256
	Couple	34.06	26.26	33.82	256
$AES_{2,3}$	Airplane	30.20	19.40	29.73	256
	Girl	32.71	20.91	31.83	256
	Parrots	34.25	20.60	33.13	256
	Couple	34.06	20.82	32.99	256
$AES_{3,3}$	Airplane	30.20	13.31	28.28	256
	Girl	32.71	16.87	30.12	256
	Parrots	34.25	14.09	30.55	256
	Couple	34.06	18.51	30.71	256

4.2.3 Evaluation of image quality

We used PSNR (Peak Signal to Noise Ratio) [11] to evaluate the JPEG image quality.

The PSNR of $M \times N$ pixels images of $g(i,j)$ and $g'(i,j)$ is calculated with

$$PSNR = 20\log\frac{255}{MSE} \quad [\text{dB}] \tag{8}$$

$$MSE = \sqrt{\frac{1}{MN}\sum_{i=0}^{M-1}\sum_{j=0}^{N-1}\{g(i,j)-g'(i,j)\}^2}$$

$(MSE : Mean\ Square\ Error)$.

In these experiments, PSNRs were calculated with RGB pixel data of original image and the JPEG image. A typical value for PSNR in a JPEG image (quality 75) is about 30dB [11].

4.2.4 Results and analysis

Here, we present some results concerning incomplete encoding, incomplete decoding on JPEG images and discussion the power of MAA method.

Let $AES_{i,j}$ indicate the algorithm of MAA in which i and j bits are extracted from DC coefficient and they are assigned to $\widehat{P}_A$ and $\widehat{P}_B$. For instance, in the example of Fig. 4 and Fig. 5, we can indicate MAA as $AES_{2,3}$. In this paper, we implemented three methods $AES_{1,3}$, $AES_{2,3}$ and $AES_{3,3}$ based on YUV component. Results and analysis

The experimental results of PSNR values are shown in **Table. 1**. In these experiments, we encrypted $4 \sim 6$ bits to create the trial content C, and used $1 \sim 3$ bits to fingerprint the legal user in the decoded content P'. As the results of $AES_{3,3}$ method, the PSNR values of the incomplete encoded images C are around 15dB. We recog-

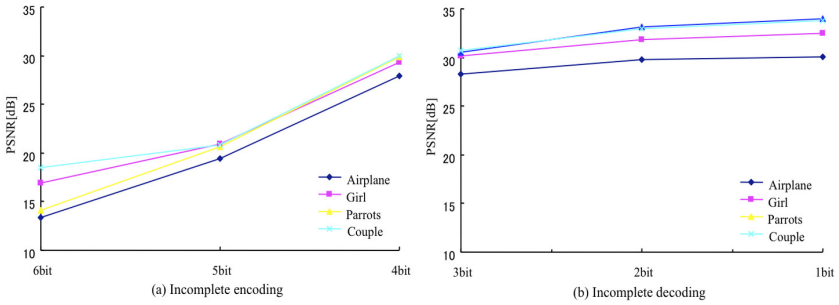

Figure 6: The PSNR of experimental JPEG images.

Table 2: PSNR[dB] of $AES_{1,3}$ method.

Method		P	C	P'	$h[bits]$
$AES_{1,3}$, UV comp.	Airplane	30.20	25.79	30.10	256
	Girl	32.71	27.15	32.56	256
	Parrots	34.25	27.67	34.06	256
	Couple	34.06	27.58	33.91	256
$AES_{1,3}$ Y comp.	Airplane	30.20	27.90	30.16	256
	Girl	32.71	29.34	32.65	256
	Parrots	34.25	29.91	34.17	256
	Couple	34.06	29.98	33.97	256
$AES_{1,3}$ YUV comp.	Airplane	30.20	24.74	30.06	256
	Girl	32.71	25.99	32.51	256
	Parrots	34.25	26.29	33.97	256
	Couple	34.06	26.26	33.82	256

nized that the images C of $AES_{3,3}$ are not suitable for the trial image. However, the incomplete encoded images C of $AES_{1,3}$ and $AES_{2,3}$ are very suitable for the trial image. Additionally, **Fig. 6** shows the relationship of i and j bits with the PSNR value of image. According these results, we could understand that in order to make the appropriate trial image, total bits $(i+j)$ can be encrypted from 2 to 5 bits (see Fig. 6(a) to confirm the PSNR: 20dB–25dB); and in order to obtain the appropriate fingerprinted image, only i bits can be incompletely decrypted from 1 to 3 bits (see Fig. 6(b) to confirm the PSNR over than 30dB). And from these results, it is clear that $AES_{1,3}$ method gave us the best results in our experiments.

Next, for confirming the effect of Y component and UV component separately, we implemented $AES_{1,3}$ method based on Y component, UV component, and YUV component, respectively. The experimental results are shown in **Table. 2**. According to the Table. 2, we confirmed that when we manipulated the UV component, the image deterioration was extremely more conspicuous than that when we applied to the Y component. Therefore, we can make the trial content (scrambled content) efficiently with drawing up on least UV component. However, because the image deterioration is not conspicuous when implementing Y component, there is an advantage to incompletely decode i bits into the decoded content under the maintaining its quality.

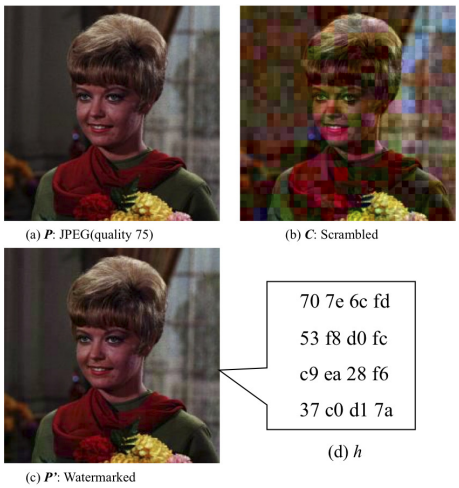

Figure 7: An example Girl image (UV component).

Fig. 7 is an experimental sample of Girl images in the UV component. According to the results in Fig. 7, it is possible to produce the trial content (see Fig. 7(b)) and the incomplete decoded content (see Fig. 7(c)) based on MAA. Furthermore, the hash value can be extracted as Fig. 7(d). It is easy to confirm that we can not distinguish the original image and the fingerprinted image. This implied that the proposed MAA method achieved image transparence.

In order to decode the trial content, producer needs to send individual k_1' to each user for incompletely decoding i bits of LSB. Based on k_1', i of LSB in the decoded image P' are randomly changed. Therefore, the hash value $h(i)$ of each P_i can be employed for identification the legal user. $h(i)$ is also saved into the producer's database for comparing with $h'(i)$ of the suspected image. In our experiment, since we used 256-bit hash value to distinguish the legal user, then our system can distinguish 2^{256} users. Here, we tried to decode the trial Girl image with 5 decoded key $k_1'(k_1'(1) \sim k_1'(5))$ and extract 5 hash values $h(1) \sim h(5)$. We obtained the following hash values

$$
\begin{aligned}
h(1) &= \{\texttt{b20460b286726d1903e2ff3eba4bd677}\} \\
h(2) &= \{\texttt{315f681571049c47095f5a0322208ffd}\} \\
h(3) &= \{\texttt{dce8d9da05971e319366db5ca87e2461}\} \\
h(4) &= \{\texttt{2e6c1ca5b1439e62e4c962e3aa033770}\} \\
h(5) &= \{\texttt{f97d0109646ded9b7af798d0a24bcf53}\}
\end{aligned}
$$

Obviously, every hash values are unique. Therefore, hash value of P' can be used as the legal user's identification.

According to the above results, we have established the DRM system based on the proposed MAA method. Trial content is created to disclose the original content

and distributed widely to users. In the incomplete decode process, we changed the i bits in LSB of the quantized DCT coefficient itself by a devised decryption key. Thus, the original content is not decoded temporarily inside the system. Therefore, we conclude that the above technical problem by the conventional DRM system is solved by using the incomplete cryptography system.

5 Conclusion

In this paper, we have presented a scheme of digital content distribution system based on multi-channel AES algorithm (MAA). This approach integrates the encoding process and fingerprinting progress of DRM technology. Therefore, we can eliminate the problem of the present DRM technology and manage the legal user effectively.

One of the lessons learned from this paper is that in order to make the scrambled image and the incomplete decoded image for JPEG, it is possible to process the Y component and UV component flexibly. Also, another lesson is that we can control the incomplete decoded image quality using a specialized key individually. Subsequently, the hash value is extracted from the fingerprinted image using this approach for distinguishing the legal user. The fingerprinted images are in good visual quality and have high PSNR values. The effectiveness of the proposed scheme has been demonstrated with the aid of experimental results. Therefore, we conclude that proposed MAA method is useful for the rights management technology in illegal content distribution via network.

References

1. W. Shapiro and R. Vingralek, “How to manage persistent state in DRM systems,” In Security and privacy in DRM, vol. 2320 of LNCS, pp. 176–191, 2002.
2. A. Kiayias and M. Yung, “Breaking and repairing asymmetric public-key traitor tracing,” In Digital Rights Management, vol. 2320 of LNCS, pp. 32–50, 2003.
3. C. Serrao, D. Naves, T. Barker, M. Balestri, and P. Kudumakis, “Open SDRM ? an open and secure digital rights management solution,” 2003.
4. H. Chang and Mikhail J. Atallah, “Protecting Software Code by Guards,” In DRM f01: ACM CCS-8 Workshop on Security and Privacy in Digital Rights Management, pp.160–175, 2002.
5. S.Emmanuel and M.S.Kankanhalli,“A Digital Rights Management Scheme for Broadcast Video,” Multimedia System 8, pp. 444–458, 2003.
6. A.Seki and W.Kameyama,“A Proposal on Open DRM System Coping with Both Benefits of Rights-Holders and Users,” IEEE conf. on Image Proceedings, Vol. 7, pp.4111–4115, 2003.
7. C. Lin, P. Prangjarote, L. Kang, W. Huang, Tzung-Her Chen: “Joint fingerprinting and decryption with noise-resistant for vector quantization images,” Journal of Signal Processing,” vol. 92, no. 9, pp. 2159–2171, 2012.
8. Federal Information Processing Standards Publication: Announcing the ADVANCED ENCRYPTION STANDARD (AES), FIPS(2001).

9. T. Tachibana, M. Fujiyoshi, H. Kiya, “A method for lossless watermarking using hash function and its application for broadcast monitoring”, IEICE Technical report, ITS 103(640), vol. 103,no. 643, pp.13–18(2004) (in Japanese).
10. T.84, “Digital Compression and Coding of Continuous-tone still Images - Requirements and Guidelines, International Telecommunication Union,” 1992.
11. M. Iwakiri and Ta Minh Thanh, “Fundamental Incomplete Cryptography Method to Digital Rights Management Based on JPEG Lossy Compression,” The 26th IEEE International Conf. on AINA, pp.755–762, 2012.