

# Secure and Robust Identification Based on Fuzzy Commitment Scheme for JPEG Images

Kenta Iida\* and Hitoshi Kiya\*

\*Tokyo Metropolitan University, Hino, Tokyo, 191-0065, Japan

Email:iida-kenta1@ed.tmu.ac.jp, kiya@tmu.ac.jp

phone number:81-42-585-8454

**Abstract**—A secure identification scheme for JPEG images is proposed in this paper. The aim is to robustly identify JPEG images which are generated from the same original image under various compression levels in security. A property of the positive and negative signs of DCT coefficients is employed to achieve a robust scheme. The proposed scheme is robust against a difference in compression levels, and does not produce false negative matches in any compression level. Conventional schemes that have this property are not secure. To construct a secure identification system, we propose a novel identification scheme that consists of new error correction technique with 1-bit parity and a fuzzy commitment scheme, which is a well-known biometric cryptosystem. The experimental results show the proposed scheme is effective for not only still images, but also video sequences in terms of the querying such as false positive, false negative and true positive matches, while keeping a high level of the security.

**Index Terms**—JPEG, fuzzy commitment scheme, Image Identification

## I. INTRODUCTION

The use of images and video sequences has greatly increased recently because of the rapid growth of the Internet and multimedia systems. It is often necessary to identify a certain image in a database that has a large number of digital images in various types of applications. The image database generally consists of images in a compressed form to reduce the amount of data. In addition, most of the contents include sensitive information such as personal data and copyright [1], [2]. “Identification” in this work is defined as an operation for finding an image that is identical to a given original image from an image database. In this paper, a robust scheme for identifying JPEG images securely is proposed.

In previous search, several identification schemes and image hashing schemes have been developed for image authentication [3]–[15]. According to a difference in the features extracted from the images, they are classified into two types: compression method-depend, compression method-independent. This paper focuses on the former one that generally has strong robustness against JPEG compression. The schemes described in [3]–[7] were proposed for the JPEG standard, and the schemes described in [7]–[11] were developed for the JPEG 2000 and JPEG XR standards. The schemes are robust against a difference in compressed levels, and does not produce false negative matches in any compression level. However, most of

conventional schemes [3]–[9] fail in the encrypted domain, since the same image could result in different bit content at different compression level. A number of schemes for JPEG 2000 images tried to construct a secure identification system, but they can not protect header information [10], [11].

Because of such situations, this paper proposes a robust scheme for identifying compressed images in security. The strategy to robustly identify JPEG images is to notice that the polarity of DCT coefficients are preserved in the compressed images as well as the conventional one [6]. Moreover, to achieve secure identification, a new error correction technique with 1-bit parity is combined with a fuzzy commitment scheme, which is a well-known secure protocol for biometric template protection [15], [16]. The experimental results show the proposed scheme is effective for not only still images, but also video sequences in terms of the querying such as false negative and true positive matches, while keeping a high level of the security.

## II. PRELIMINARIES

### A. JPEG Encoding

The JPEG standard is the most widely used image compression standard. JPEG encoding procedure can be summarized as follows.

- 1) Performing color transform from RGB space to  $YC_bC_r$  space and sub-sampling the  $C_b$  and  $C_r$ .
- 2) Dividing an image into non-overlapping consecutive  $8 \times 8$ -blocks.
- 3) Applying DCT to each block to obtain  $8 \times 8$  DCT coefficients  $\mathbf{S}$ .
- 4) Quantizing  $\mathbf{S}$  with a quantization matrix  $\mathbf{Q}$ .
- 5) Entropy coding using Huffman coding.

In step 4), a quantization matrix  $\mathbf{Q}$  with  $8 \times 8$  components is used to obtain a matrix  $\mathbf{S}_q$  from  $\mathbf{S}$  as below.

$$S_q(u, v) = \text{round} \left( \frac{S(u, v)}{Q(u, v)} \right), 1 \leq u \leq 8, 1 \leq v \leq 8 \quad (1)$$

with

$$Q(u, v) = Q_0(u, v) * \frac{Q_f}{50} \quad (2)$$

where  $S(u, v)$ ,  $Q(u, v)$ ,  $S_q(u, v)$  and  $Q_0(u, v)$  represent the  $(u, v)$ element of  $\mathbf{S}$ ,  $\mathbf{Q}$ ,  $\mathbf{S}_q$  and  $\mathbf{Q}_0$  respectively.  $\text{Round}(x)$  is

the function to round off the value  $x$  to the nearest integer value.

Quality factor  $Q_f (1 \leq Q_f \leq 100)$  is a parameter to control the matrix  $\mathbf{Q}$ . All components of an initial quantization matrix  $\mathbf{Q}_0$  are positive numbers as well as  $Q_f$ .

### B. Notations and Terminologies

Several notations and terminologies used in the following sections are listed here.

- $X$  represents an image  $X$ .  $X$  can be “ $Q$ ” for image  $Q$  and “ $O$ ” for the original image, where all images have the same size.
- $M$  represents the number of  $8 \times 8$ -blocks in an image.
- $N$  represents the number of DCT coefficients used for identification in each block.  $0 < N \leq 64$ .
- $X(m, n)$  represents the  $n$ th DCT coefficient in the  $m$ th block in image  $X$ .  $1 \leq m \leq M$ ,  $1 \leq n \leq N$ .
- $\text{sgn}(y)$  represents the sign of a real value  $y$  as

$$\text{sgn}(y) = \begin{cases} 1, & y > 0, \\ 0, & y = 0, \\ -1, & y < 0. \end{cases} \quad (3)$$

### III. PROPOSED IDENTIFICATION SCHEME

A secure and robust image identification scheme is proposed.

#### A. Property of DCT Coefficients

It is verified from Eq.(1) that quantized DCT coefficients have the following property [6].

- When JPEG images  $Q$  and  $X_i$  are generated from the same original image  $O$ , the positive and negative signs of DCT coefficients of the two images are equivalent in the corresponding location, even though  $Q_f \neq Q_{f_i}$ , where  $Q_f$  and  $Q_{f_i}$  are quality factors used to generate  $Q$  and  $X_i$  respectively. Namely, the relation is given as

$$\text{sgn}(Q(m, n)) = \text{sgn}(X_i(m, n)) \quad (4)$$

where this property does not apply in zero value coefficients.

The above property is illustrated in Figure 1, where images  $Q$  and  $X_1$  are generated from the same original image  $O$ . It is confirmed the positive and negative signs of DCT coefficients of the two images are equivalent in the corresponding location, except for the case in zero value coefficients.

Note that  $X_1(m, n) = 0$  is satisfied if  $Q(m, n) = 0$  due to  $Q_{f_i} \geq Q_f$ . Moreover, when two JPEG images have the different original images as  $Q$  and  $X_2$ , the signs of the DCT coefficients are not always equivalent in the corresponding location.

The aim of the proposed scheme is to securely identify  $X_i$  that satisfies the following condition for  $1 \leq m \leq M$  and  $1 \leq n \leq N$ ,

$$\begin{cases} \text{sgn}(Q(m, n)) = \text{sgn}(X_i(m, n)), & \text{if } X_i(m, n) \neq 0 \\ X_i(m, n) = 0, & \text{if } Q(m, n) = 0 \end{cases} \quad (5)$$

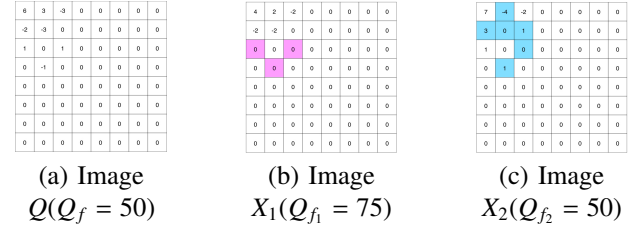


Fig. 1. Examples of quantized DCT coefficients in a block. Image  $X_1$  has the same signs of coefficients as image  $Q$  except for zero-values.  $X_2$  has different original ones.

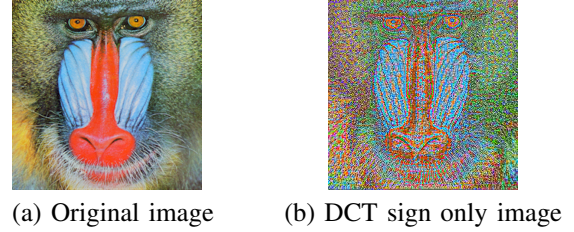


Fig. 2. Visible information of DCT signs

under the assumption  $Q_{f_i} \geq Q_f$ . This condition does not generate any false negative matches because it is a necessary condition for the identification.

Note that Eq.(4) is not satisfied in the case of zero value coefficients. Therefore, a new error correction coding technique is required for the identification.

#### B. Proposed Identification System

Figure 3 shows the proposed identification system with the fuzzy commitment scheme. A new error correction technique is also proposed for this system.

##### 1) Scenario

DCT signs are sensitive data because they provide visible information, although they have important properties for the identification. Figure 2(a) is an original image and (b) shows the DCT sign only image reconstructed by using the DCT signs [17].

Image  $X_i$  with a quality factor  $Q_{f_i}$  is sent to client to be enrolled in a database. After client extracts some features (DCT signs) from  $X_i$ , to protect both  $X_i$  and the features, a commitment  $\sigma$  and a hash value  $h(c)$  are calculated by using a secret code  $S$  and an error correcting code respectively. The set of  $\sigma$  and  $h(c)$  is sent to an authentication server. Note that only the protected set is enrolled in the database. On the other hand, the image  $Q$  with  $Q_f$  is sent to client to identify images generated from the same original image. Client extracts features from  $Q$  and error-correction decoding is carried out to obtain  $c''$  by using the features and  $\sigma$ . The hash value  $h(c'')$  is then calculated and compared with  $h(c)$  in the encrypted domain.

##### 2) Enrollment Process

In order to securely enroll features of image  $X_i$ , the following steps are carried out.

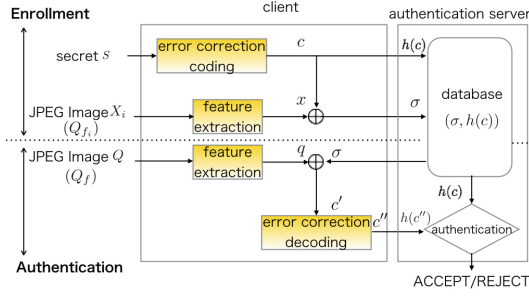


Fig. 3. Proposed identification system

- Set the values  $M$  and  $N$ , where the zig-zag manner scan is used to map  $8 \times 8$  DCT coefficients to a  $1 \times 64$  vector in each block, and the  $N$  signs are extracted from the DC coefficient to  $N$ th low frequency one.
- Set  $m := 1$  and  $n := 1$ .
- Extract a DCT sign from  $X_i(m, n)$  and map it to a codeword  $x(m, n)$  with 2 bits as

$$x(m, n) = \begin{cases} (00)_2, \text{sgn}(X_i(m, n)) = 1, \\ (01)_2, \text{sgn}(X_i(m, n)) = 0, \\ (11)_2, \text{sgn}(X_i(m, n)) = -1. \end{cases} \quad (6)$$

- Select randomly a 1-bit secret code  $s(m, n) \in S = \{(0)_2, (1)_2\}$  and map it to a 2-bit error-correcting codeword  $c(m, n) \in C = \{(00)_2, (11)_2\}$  respectively, by adding 1-bit parity to  $s(m, n)$ . For instance,  $s(m, n) = (1)_2$  is mapped to  $c(m, n) = (11)_2$ . Note that the Hamming weight of  $c(m, n)$ , denoted by  $W_H(c(m, n))$  is either two or zero.
- Calculate a commitment codeword  $\sigma(m, n)$  as

$$\sigma(m, n) = x(m, n) \oplus c(m, n) \quad (7)$$

where  $\oplus$  denotes the bit wise XOR operation.

- Set  $n := n + 1$ . If  $n \leq N$ , proceed to step(c).
- Set  $n := 1$  and  $m := m + 1$ . If  $m \leq M$ , proceed to step(c). Otherwise, generate codewords  $c$  and  $\sigma$  by connecting each component as below.

$$\sigma = \begin{cases} \sigma(1, 1) \parallel \dots \parallel \sigma(1, N) \parallel \dots \parallel \sigma(M, N), & \text{if } N \neq 1, \\ \sigma(1, 1) \parallel \sigma(2, 1) \parallel \dots \parallel \sigma(M, 1), & \text{otherwise.} \end{cases} \quad (8)$$

$$c = \begin{cases} c(1, 1) \parallel \dots \parallel c(1, N) \parallel \dots \parallel c(M, N), & \text{if } N \neq 1, \\ c(1, 1) \parallel c(2, 1) \parallel \dots \parallel c(M, 1), & \text{otherwise.} \end{cases} \quad (9)$$

- Calculate a hash value  $h(c)$  for  $c$  and send  $h(c)$  and  $\sigma$  to an authentication server. The set is stored in the server.

Table I summarizes the relation among codewords.  $\sigma(m, n)$  is mapped to an element of  $C$  for  $x(m, n) = (00)_2, (11)_2$ . Otherwise, for  $x(m, n) = (01)_2$ ,  $\sigma(m, n)$  is mapped to a codeword which is not an element of  $C$ . As a result,  $W_H(\sigma(m, n))$  becomes an odd.

### 3) Authentication Process

In order to compare image  $Q$  with image  $X_i$ , the following steps are carried out.

- Set the values  $M$  and  $N$ .

- Set  $m := 1$  and  $n := 1$ .
- Request the authentication server to send the commitment  $\sigma$ .
- Extract a DCT sign from  $Q(m, n)$  and map it to a codeword  $q(m, n)$  with 2-bits as

$$q(m, n) = \begin{cases} (00)_2, \text{sgn}(Q(m, n)) = 1, \\ (01)_2, \text{sgn}(Q(m, n)) = 0, \\ (11)_2, \text{sgn}(Q(m, n)) = -1. \end{cases} \quad (10)$$

- Compute  $c'(m, n)$  as

$$c'(m, n) = \sigma(m, n) \oplus q(m, n) \quad (11)$$

and apply error correction decoding to  $c'(m, n)$  to obtain  $c''(m, n)$  (see III-C).

- Set  $n := n + 1$ . If  $n \leq N$ , proceed to step(d).
- Set  $n := 1$  and  $m := m + 1$ . If  $m \leq M$ , proceed to step(d). Otherwise, generate a codeword  $c''$  by connecting each component as below:

$$c'' = \begin{cases} c''(1, 1) \parallel \dots \parallel c''(1, N) \parallel \dots \parallel c''(M, N), & \text{if } N \neq 1, \\ c''(1, 1) \parallel c''(2, 1) \parallel \dots \parallel c''(M, 1), & \text{otherwise,} \end{cases} \quad (12)$$

and compute a hash value  $h(c'')$  and send it to the authentication server.

- Output "ACCEPT" if  $h(c'') = h(c)$ .

### C. Error Correction Decoding

$c'(m, n)$  is mapped to  $c''(m, n)$  for error correction as shown in step (e). Let us explain the error correction decoding in more detail. The proposed codeword  $c(m, n)$  is designed to satisfy the condition:

$$c(m, n) \begin{cases} = c''(m, n), & \text{if } \text{sgn}(X_i(m, n)) = \text{sgn}(Q(m, n)) \\ & \text{and } X_i(m, n) \neq 0, \\ = c''(m, n), & \text{if } \text{sgn}(X_i(m, n)) = 0, \\ \neq c''(m, n), & \text{otherwise.} \end{cases} \quad (13)$$

#### A. $W_H(\sigma(m, n))$ is an even

When  $W_H(\sigma(m, n))$  is an even,  $c'(m, n)$  is mapped to  $c''(m, n) = c'(m, n)$  (see Table II). Since  $W_H(c(m, n))$  is absolutely an even,  $W_H(\sigma(m, n)) = W_H(x(m, n) \oplus c(m, n))$  must be an even for  $\text{sgn}(X_i(m, n)) = 1$  or  $-1$  from Eq.(6). Thus  $c'(m, n) = \sigma(m, n) \oplus q(m, n)$  is equal to  $c(m, n)$  under  $\text{sgn}(X_i(m, n)) = \text{sgn}(Q(m, n))$  as Eq.(13).

TABLE I  
RELATION AMONG CODEWORDS

$\text{sgn}(X_i(m, n))$	$x(m, n)$	$s(m, n)$	$c(m, n)$	$\sigma(m, n)$
1	$(00)_2$	$(0)_2$	$(00)_2$	$(00)_2$
		$(1)_2$	$(11)_2$	$(11)_2$
-1	$(11)_2$	$(0)_2$	$(00)_2$	$(11)_2$
		$(1)_2$	$(11)_2$	$(00)_2$
0	$(01)_2$	$(0)_2$	$(00)_2$	$(01)_2$
		$(1)_2$	$(11)_2$	$(10)_2$

TABLE II  
ERROR CORRECTION

	Error correction decoding	
$W_H(\sigma(m, n))$	$c''(m, n) =$	$c(m, n) = c''(m, n)?$
even	$c'(m, n)$	yes, if $\text{sgn}(X_i(m, n)) = \text{sgn}(Q(m, n))$
odd	$c'(m, n) \oplus (01)_2,$ for $\text{sgn}(Q(m, n)) = 1$	yes
	$c'(m, n) \oplus (10)_2,$ for $\text{sgn}(Q(m, n)) = -1$	
	$c'(m, n),$ for $\text{sgn}(Q(m, n)) = 0$	

$c'(m, n) = c(m, n)$  is not guaranteed under  $\text{sgn}(X_i(m, n)) \neq \text{sgn}(Q(m, n))$ .

B.  $W_H(\sigma(m, n))$  is an odd

Since  $W_H(\sigma(m, n))$  is an odd for only  $X_i(m, n) = 0$  from Eq.(6),  $c'(m, n)$  is able to be mapped to  $c''(m, n) = c(m, n)$  by the operations in Table II. For example,  $c''(m, n)$  is mapped to  $c'(m, n) \oplus (01)_2$  for  $\text{sgn}(Q(m, n)) = 1$  ( $q(m, n) = (00)_2$ ) because of  $c'(m, n) = x(m, n) \oplus c(m, n) \oplus q(m, n) = (01)_2 \oplus c(m, n) \oplus (00)_2 = (01)_2 \oplus c(m, n)$ . Similarity,  $c'(m, n)$  is mapped to  $c''(m, n) = c'(m, n) \oplus (10)_2$  for  $\text{sgn}(Q(m, n)) = -1$  and  $c'(m, n)$  is mapped to  $c''(m, n) = c'(m, n)$  for  $\text{sgn}(Q(m, n)) = 0$ .

The above mapping operations do not guarantee to provide the correct relation  $c''(m, n) = c(m, n)$  in any other cases such as  $\text{sgn}(X_i(m, n)) \neq \text{sgn}(Q(m, n))$ .

IV. EVALUATION FOR SECURITY

Several attacks have been introduced in [16] for the fuzzy commitment scheme, and studies on security analysis have been also considered in [15], [16]. In this section, to evaluate the safety of proposed scheme, we assume that attackers intend to deliver the brute force attack on  $h(c)$ . The aim of the attack is to obtain DCT signs from information enrolled in the database by estimating  $c$ . In this case, the simplest approach is to calculate  $h(c)$  for all possible  $c$ . The number of generable codewords  $c$  in an image is given as  $2^{M \times N}$ .

The other approach is to estimate  $c$  from each  $\sigma(m, n)$ . When  $W_H(\sigma(m, n))$  is an odd, it is satisfied from Eqs.(6) and (7) that  $c(m, n)$  can be decided as  $c(m, n) = \sigma(m, n) \oplus (01)_2$ . On the other hand, when  $W_H(\sigma(m, n))$  is an even, it is impossible to decide whether  $\text{sgn}(X_i(m, n))$  has 1 or -1. In this case, attackers have to calculate  $h(c)$  for  $2^{M \times N - L}$  codewords  $c$  where  $L$  is the number of zero coefficients in an image. Therefore, when  $2^{M \times N - L}$  is larger than  $2^{256}$ , i.e.

$$M \times N - L > 256, \quad (14)$$

the key space of the proposed scheme is larger than that of the 256-bits key. As described later, Eq.(14) can be easily satisfied.

V. SIMULATION

To evaluate the performance of the proposed scheme, several simulations are conducted.



Fig. 4. Four examples of images with 388×374

TABLE III  
SELECTION OF  $N$  FOR STILL IMAGES IN DATABASES  $D_1(Q_{f_1} = 50)$  AND  $D_2(Q_{f_2} = 90)$

database	$N$	$TP$	$TN$	$FP$	$FN$	$TPR[\%]$	$FPR[\%]$	$\min(M \times N - L)$
$D_1$	1	160	25139	301	0	100	1.18	2367
	4	160	25440	0	0	100	0	4428
	16	160	25440	0	0	100	0	11178
	64	160	25440	0	0	100	0	14944
$D_2$	1	320	24992	288	0	100	1.41	2347
	4	320	25280	0	0	100	0	4262
	16	320	25280	0	0	100	0	10038
	64	320	25280	0	0	100	0	12031

A. Simulation condition

We used 80 still images and two video sequences compressed by PVRG JPEG codec [18] in the simulations. The original uncompressed versions were not included in the simulations. Identification was accomplished by querying each query image respectively. The hash function SHA-256 was used in the simulations.

B. Evaluation for Still Images

Figure 4 shows examples of 80 fingerprint images [19] used in the simulation. They were compressed with six different quality factors to generate 480 compressed images. The sets  $(\sigma, h(c))$  generated from images compressed with  $Q_{f_1} = 50$  were enrolled in the database  $D_1$ , and the sets of images compressed with  $Q_{f_2} = 90$  were enrolled in the  $D_2$ . As a query image, images compressed with  $Q_f = 20, 40, 60$  and  $80$  were used respectively.

Querying results are shown in Table III. The table summarizes the number of true positive (TP), true negative (TN), false positive (FP) and false negative (FN) matches. The table also shows the true positive rate (TPR) and false positive rate (FPR) defined by

$$TPR = \frac{TP}{TP + FN}, FPR = \frac{FP}{FP + TN}. \quad (15)$$

It is confirmed that there were not any false negative matches for both databases under all  $N$ . Moreover, larger  $N$  provides higher recognition accuracy. In particular, for  $N \geq 4$ , querying for each database resulted in a perfect identification. Note that these performances are the same as those of using DCT signs without secure protection, and thus the proposed scheme does not provide any degradation of the querying performance.

Besides, the Table illustrates the minimum value of  $M \times N - L$  in all images. It is confirmed that the condition Eq.(14) was satisfied even for  $N = 1$ .

C. Evaluation for Videos

Two video sequences shown in Fig.5 were used to confirm the effectiveness of the proposed scheme. Originally, there

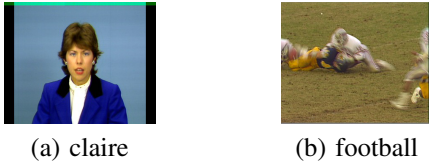


Fig. 5. Examples of video sequences with 360×288

TABLE IV  
SELECTION OF  $N$  FOR VIDEO SEQUENCES IN DATABASES  $D_1(Q_{f_1} = 50)$  AND  $D_2(Q_{f_2} = 90)$

database	$N$	$TP$	$TN$	$FP$	$FN$	$TPR[\%]$	$FPR[\%]$	$\min(M \times N - L)$
$D_1$	1	120	14274	6	0	100	0.042	2311
	4	120	14280	0	0	100	0	4236
	16	120	14280	0	0	100	0	7027
	64	120	14280	0	0	100	0	7576
$D_2$	1	240	14146	14	0	100	0.099	2273
	4	240	14158	2	0	100	0.014	3625
	16	240	14159	1	0	100	0.007	5392
	64	240	14159	1	0	100	0.007	5602

were 30 uncompressed consecutive frames for each video sequences. All video frames were compressed with six different quality factors i.e.  $Q_f=20, 40, 50, 60, 80$  and  $90$ . As a result, 180 compressed frames were generated from each sequence, and 360 compressed frames were totally used in the simulation. The sets  $(\sigma, h(c))$  generated from frames compressed with  $Q_{f_1} = 50$  were enrolled in the database  $D_1$  and the sets of frames compressed with  $Q_{f_2} = 90$  were enrolled in the  $D_2$ . As a query frame, 240 frames generated from the video sequences by using  $Q_f=20, 40, 60$  and  $80$  were used. Therefore,  $240 \times 60$  authentication process were performed for each database to evaluate the proposed scheme.

Querying results for videos are shown in Table IV. It is confirmed from these results that there were not any false negative matches for both databases under all  $N$ , and a larger  $N$  provides higher recognition accuracy as well as the results for still images.

Besides, the table illustrates the minimum value of  $M \times N - L$  in all frames in each database. We can see that the condition Eq.(14) was satisfied even for  $N = 1$ .

## VI. CONCLUSION

This paper proposed a robust system for identifying JPEG images in security. The property of the positive and negative signs of DCT coefficients was considered to construct a robust identification system. Moreover, to achieve a secure system, a new error correction technique was combined with a fuzzy commitment scheme. In principle, the proposed scheme does not produce false negative matches in any compression ratio, while images and the features are protected. The experimental results showed that the proposed scheme is effective for not only still images, but also video sequences in term of the retrieval performance such as false negative and true positive matches.

## REFERENCES

[1] C. T. Huang, L. Huang, Z. Qin, H. Yuan, L. Zhou, V. Varadharajan and C. C. J. Kuo, "Survey on securing data storage in the cloud," *APSIPA Trans. on Signal and Information Processing*, vol.3, e7, May 2014.

[2] R. L. Lagendijk, Z. Erkin and M. Barni, "Encrypted signal processing for privacy protection: Conveying the utility of homomorphic encryption and multiparty computation," *IEEE Signal Processing Mag.*, vol 30, no.1, pp.82-105, January 2013.

[3] C. Y. Lin and S. F. Chang, "A robust image authentication method distinguishing JPEG compression from malicious manipulation," *IEEE Trans. on Circuits and Systems for Video Technology*, vol.11, pp.153-168, February 2001.

[4] Z. Fan and R. L. de Queiroz, "Identification of bitmap compression history: JPEG detection and quantizer and estimation," *IEEE Trans. on Image Processing*, vol.12, pp.230-235, February 2003.

[5] D. Edmundson and G. Schaefer, "An overview and evaluation of JPEG compressed domain retrieval techniques," in *Proc. Int'l. Symposium ELMAR-2012*, pp.75-78, September 2012.

[6] F. Arnia, I. Iizuka, M. Fujiyoshi and H. Kiya, "Fast method for Joint Retrieval and Identification of JPEG Coded Images Based on DCT sign," in *Proc. IEEE Int'l. Conf. on Image Processing*, vol.II, pp.229-232, September 2007.

[7] K. O. Cheng, N. F. Law and W. C. Siu, "A Fast Approach for Identifying Similar Features in Retrieval of JPEG and JPEG 2000 Images," in *Proc. APSIPA Annual Summit and Conf.*, pp.258-261, October 2009.

[8] A. Chaker, M. Kaaniche, A. Benazza-Benyahia and M. Antonini, "An efficient statistical-based retrieval approach for JPEG2000 compressed Images," in *Proc. European Signal Processing Conf.*, pp.1830-1834, September 2015.

[9] H. Kobayashi, S. Imaizumi and H. Kiya, "A Robust Identification Scheme for JPEG XR Images with Various Compression Ratios," in *Proc. Pacific Rim Symposium on Image and Video Technology*, November 2015.

[10] O. Watanabe, T. Iida, T. Fukuhara and H. Kiya, "Identification of JPEG 2000 Images in Encrypted Domain for Digital Cinema," in *Proc. IEEE Int'l. Conf. on Image Processing*, vol.2, no.MA.PJ.8, pp.2065-2068, November 2009.

[11] T. Dobashi, O. Watanabe, T. Fukuhara and H. Kiya, "Hash-based Identification of JPEG2000 Images in Encrypted Domain," in *Proc. IEEE Int'l. Symposium on Intelligent Signal Processing and Communication Systems*, no.D2.4, pp.469-472, November 2012.

[12] A. Swaminathan, Y. Mao and M. Wu, "Robust and secure image hashing," *IEEE Trans. on Information Forensics and Security*, vol.1, pp.215-230, June 2006.

[13] J. Ouyang, G. Coatrieux and H. Shu, "Robust hashing for image authentication using quaternion discrete Fourier transform and log-polar transform," *Digital Signal Processing*, vol.41, pp.98-109, June 2015.

[14] A. Kadyrov and M. Petrou, "The Trace transform and its applications," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol.23, pp.811-828, August 2001.

[15] A. Juels and M. Wattenberg, "A fuzzy commitment scheme," in *Proc. ACM Conf. on Computer and Communications Security*, pp.28-36, November 1999.

[16] C. Rathgeb and A. Uhl, "A survey on biometric cryptosystems and cancelable biometrics," *EURASIP Journal on Information Security*, 2011:3, September 2011.

[17] I. Ito and H. Kiya, "One-time key based phase scrambling for phase-only correlation between visually protected images," *EURASIP Journal on Information Security*, 2009:841045, January 2009.

[18] PVRG (Portable Video Research Group)- JPEG codec, ver1.2(1994).

[19] FVC2004, <http://bias.csr.unibo.it/fvc2004/download.asp>.