Secure Identification Based on Fuzzy Commitment Scheme for JPEG XR Images

Kenta Iida*, Hiroyuki Kobayashi† and Hitoshi Kiya*
*Tokyo Metropolitan University, Hino, Tokyo, 191-0065, Japan
Email:iida-kenta1@ed.tmu.ac.jp, kiya@tmu.ac.jp
†Tokyo Metropolitan College of Industrial Technology, Shinagawa, Tokyo, 140-0011, Japan
Email:hkob@s.metro-cit.ac.jp

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

***Index Terms*—JPEG XR, 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 for various applications in content authentication, database search and watermarking. 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 XR images securely is proposed.

So far, several identification schemes and image hash functions have been developed for authenticating images [3]–[14]. They can be broadly classified into two types according to a difference in extracted features: compression method-depended type, to which the proposed scheme corresponds, and compression method-independent type. This paper focuses on the former one, that has generally strong robustness against a difference in compressed levels. The schemes described in [3]–[6] have been proposed for the JPEG standard, and the schemes described in [7]–[10] have been developed for the JPEG 2000 and JPEG XR standards. Most of these schemes not only are robust against a difference in compressed levels but also do not produce false negative matches in any compression level. However, the conventional schemes [3]–[8] do not consider to identify images in secure, since it is impossible to avoid the effect of compression levels. A number of schemes for JPEG 2000 images have tried to construct secure identification systems, but they can not protect header information in codestreams [9], [10]. In addition, these schemes can not be applied to other compression standards such as JPEG and JPEG XR.

Because of such a situation, for the first time, this paper proposes a secure scheme for identifying JPEG XR compressed images. The strategy to robustly identify JPEG XR images is to notice that the polarity of lapped biorthogonal transform (LBT) coefficients are preserved in the compressed images as well as in the conventional one [8]. Moreover, to achieve secure identification, a new error correction technique with1-bit parity is combined with a fuzzy commitment scheme that is a well-known secure protocol for biometric template protection [15], [16]. The error correction allows to avoid the effect of a different in compression levels. The experimental results show the proposed scheme has a high query performance, while keeping a high level of the security.

II. Preliminaries

A. JPEG XR Encoding

The JPEG XR standard supports lossy and lossless coding for still images and videos. It is available for not only images with 8 bits, but also images with over 8 bits and floating point representation. Therefore, the proposed scheme is widely available for many kinds of images including high dynamic range ones. The following is the encoding procedure [17].

(1) Performing a color conversion.
(2) Dividing an image into macroblocks which are non-overlapped consecutive 16×16 pixels, and then each macroblock into blocks which are consecutive 4×4 pixels.
(3) Applying two basic operators i.e. core transform and optional overlap filtering to each macroblock, where core transformations are hierarchically executed twice as shown in Fig.1.
(4) Applying a coefficient quantization approach controlled by quantization parameters (QPs).
(5) Performing entropy encoding.

978-0-9928-6265-7/16/$31.00 ©2016 IEEE

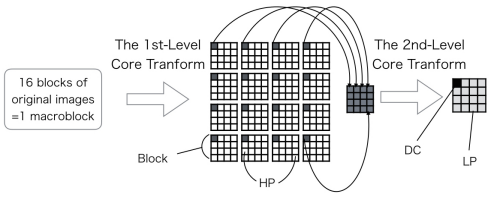


Fig. 1. Core transform

In step (3), one temporally DC coefficient and 15 HP coefficients are obtained for each block by the 1st-level core transform, and 16 temporally DC coefficients are gathered from each macroblock as shown in Fig.1. By applying the 2nd-level core transform to them, one DC coefficient, 15 LP coefficients and 15×16 HP coefficients are calculated for each macroblock. The core transform is referred to as lapped biorthogonal transform (LBT), so that the transform coefficients are often called LBT coefficients, which consist of DC, LP and HP ones.

The overlap filtering may be used to reduce blocking artifacts. There are three overlapping-modes: mode 0, mode 1 and mode 2. For instance, 1st-level and 2nd-level overlapping filtering are performed when mode 2 is chosen.

B. Notations and Terminologies

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

- X represents an image.X can be "Q" for a query image and "O" for the original image, where all images have the same size.
- M represents the number of macroblocks in an image.
- N represents the number of coefficients in a 4×4 core transform, and the number of blocks in a macroblock,where $N = 16$.
- B represents the number of blocks in an image.
- $DC_X(m)$ indicates the DC coefficient of the m^{th} macroblock in image X. $0 \leq m < M$.
- $LP_X(m,n)$ indicates the n^{th} LP coefficient of the m^{th} macroblock in image X. $0 \leq m < M$, $1 \leq n < N$
- $HP_X(b,n)$ indicates the n^{th} HP coefficient of the b^{th} block in image X. $0 \leq b < B$, $1 \leq n < N$.
- $\mathrm{sgn}(y)$ represents the sign of a real value y as

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

- $L_X(j)$ represents LBT coefficients sequence given as

$$L_X(j) = \begin{cases} DC_X(j), 0 \leq j < M, \\ LP_X(m,n), M \leq j < MN, \\ \quad m = \mathrm{mod}(j,M), n = \lfloor (j-M)/M \rfloor, \\ HP_X(b,n), MN \leq j < P, \\ \quad b = \mathrm{mod}(j-MN, B), \\ \quad n = \lfloor (j-MN)/B \rfloor + 1, \end{cases} \quad (2)$$

where $\mathrm{mod}(x,d)$ denotes the reminder when x is divided by d, and $\lfloor x \rfloor$ denotes the integer part of x. The length of $L_X(j)$ is $P = MN + B(N-1)$, (see Fig.2).

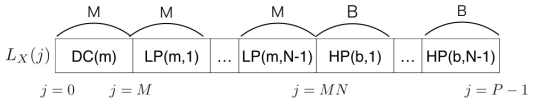


Fig. 2. LBT coefficients sequence

628	-8	-7	0
2	-3	1	-6
0	1	-2	-1
-8	-10	5	-1

(a) Image $Q(QP = 100)$

300	-3	-3	0
1	-1	0	-3
0	0	-1	0
-3	-4	2	0

(b) Image $X_1(QP_1 = 120)$

279	2	-6	9
28	-1	6	-9
-32	11	-1	5
-24	-10	4	-1

(c) Image $X_2(QP_2 = 100)$

Fig. 3. Examples of quantized LBT 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.

- L represents the number of LBT coefficients used for identification in an image. For instance, $L = M$ corresponds the number of DC coefficients.

III. Proposed Identification Scheme

A secure and robust image identification scheme is proposed.

A. Property of LBT coefficients

Quantized LBT coefficients have the following property [8].

- When JPEG XR images Q and X_i are generated under the same overlapping mode from the same original image O, the positive and negative signs of LBT coefficients of the two images are equivalent in the corresponding location, even though $QP \neq QP_i$, where QP and QP_i are quantization parameters used to generate Q and X_i respectively. Namely, the relation is given as

$$\mathrm{sgn}(L_Q(j)) = \mathrm{sgn}(L_{X_i}(j)), (0 \leq j < P) \quad (3)$$

where this property does not apply in zero value coefficients.

The above property is illustrated in Fig.3, where images Q and X_1 are generated from the same original image O. It is confirmed that the positive and negative signs of LBT coefficients of two images are equivalent in the corresponding location, except for the case in zero value coefficients. Note that Eq.(3) is not satisfied in the case of zero value coefficients. Therefore, a new error correction coding technique is required to avoid the effect.

LBT signs are sensitive data because they provide visible information as shown in Fig.4, although they have important properties for the identification. Figure 4(a) is an original image and (b) shows the LBT sign only image reconstructed by using the LBT signs of the image [18].

B. Scenario

Figure 5 shows the proposed identification system based on the fuzzy commitment scheme [15]. A new error correction technique is also proposed for this system.

(a) Original image

(b) LBT sign only image

Fig. 4. Visibility of LBT signs

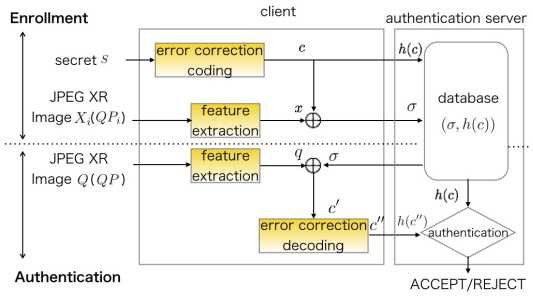


Fig. 5. Proposed identification system

Image X_i with a quantization parameter QP_i is sent to client to be enrolled in a database. After client extracts some features(LBT signs) from X_i, to protect both X_i and the features, a commitment σ and a hash value $h(c)$ are calculated by using a secret code S and an error correcting code respectively, where $h(\cdot)$ is a hash function. The set of σ 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 QP 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 σ. The hash value $h(c'')$ is then calculated and compared with $h(c)$ in the encrypted domain.

C. Proposed Identification System

Enrollment and authentication processes consist of the following steps.

1) Enrollment Process

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

(a) Set the value L.
(b) Set $j := 0$.
(c) Extract a LBT sign from $L_{X_i}(j)$ and map it to a codeword $x(j)$ with 2 bits as

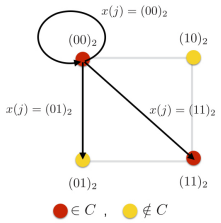
$$x(j) = \begin{cases} (00)_2, \mathrm{sgn}(L_{X_i}(j)) = 1, \\ (01)_2, \mathrm{sgn}(L_{X_i}(j)) = 0, \\ (11)_2, \mathrm{sgn}(L_{X_i}(j)) = -1. \end{cases} \quad (4)$$

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

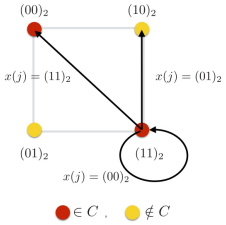
$$\sigma(j) = x(j) \oplus c(j), \quad (5)$$

TABLE I
RELATIONSHIP AMONG CODEWORDS

$\mathrm{sgn}(L_{X_i}(j))$	$x(j)$	$s(j)$	$c(j)$	$\sigma(j)$
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	$(01)_2$	$(0)_2$	$(00)_2$	$(01)_2$
		$(1)_2$	$(11)_2$	$(10)_2$



(a) $c(j) = (00)_2$



(b) $c(j) = (11)_2$

Fig. 6. Examples of $\sigma(j) = x(j) \oplus c(j)$

where $\oplus$ denotes the bit wise XOR operation.
(f) Set $j := j + 1$.If $j < L$, proceed to step(c). Otherwise, generate codewords c and σ by connecting each component as below.

$$\sigma = \begin{cases} \sigma(0)||\ldots||\sigma(L-1), L \neq 1, \\ \sigma(0), L = 1, \end{cases} \quad (6)$$

$$c = \begin{cases} c(0)||\ldots||c(L-1), L \neq 1, \\ c(0), L = 1. \end{cases} \quad (7)$$

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

Table I summaries the relationship among codewords. Figure 6 also illustrates examples of the relationship between $c(j)$ and $\sigma(j)$. $\sigma(j)$ is mapped to an element of C for $x(j) = (00)_2$ or $(11)_2$. Otherwise, for $x(j) = (01)_2$, $\sigma(j)$ is not an element of C. Namely, $W_H(\sigma(j))$ becomes an odd.

2) Authentication Process

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

(a) Set the value L.
(b) Set $j := 0$.
(c) Request the authentication server to send the commitment σ.
(d) Extract a LBT sign from $L_Q(j)$ and map it to a codeword $q(j)$ with 2-bits as

$$q(j) = \begin{cases} (00)_2, \mathrm{sgn}(L_Q(j)) = 1, \\ (01)_2, \mathrm{sgn}(L_Q(j)) = 0, \\ (11)_2, \mathrm{sgn}(L_Q(j)) = -1. \end{cases} \quad (8)$$

(e) Compute $c'(j)$ as

$$c'(j) = \sigma(j) \oplus q(j) \quad (9)$$

and apply error correction decoding to $c'(j)$ to obtain $c''(j)$(see III-D).
(f) Set $j := j + 1$.If $j < L$, proceed to step(d). Otherwise, generate a codeword c'' by connecting each component

TABLE II
ERROR CORRECTION

	Error correction decoding	
$W_H(\sigma(j))$	$c''(j) =$	$c(j) = c''(j)$?
even	$c'(j)$	yes, if $\mathrm{sgn}(L_{X_i}(j)) = \mathrm{sgn}(L_Q(j))$
odd	$c'(j) \oplus (01)_2$, for $\mathrm{sgn}(L_Q(j)) = 1$	yes
	$c'(j) \oplus (10)_2$, for $\mathrm{sgn}(L_Q(j)) = -1$	
	$c'(j)$, for $\mathrm{sgn}(L_Q(j)) = 0$	

as below:

$$c'' = \begin{cases} c''(0)||\ldots||c''(L-1), L \neq 1, \\ c''(0), L = 1, \end{cases} \quad (10)$$

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

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

D. Error Correction Decoding

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

$$c(j) \begin{cases} = c''(j), \text{if } \mathrm{sgn}(L_{X_i}(j)) = \mathrm{sgn}(L_Q(j)) \\ \qquad \text{and } L_{X_i}(j) \neq 0, \\ = c''(j), \text{if } \mathrm{sgn}(L_{X_i}(j)) = 0, \\ \neq c''(j), \text{otherwise.} \end{cases} \quad (11)$$

1) $W_H(\sigma(j))$ is an even
When $W_H(\sigma(j))$ is an even, $c'(j)$ is mapped to $c''(j) = c'(j)$(see Table II). Since $W_H(c(j))$ is absolutely an even, $W_H(\sigma(j)) = W_H(x(j) \oplus c(j))$ must be an even for $\mathrm{sgn}(L_{X_i}(j)) = 1$ or -1 from Eq.(4). Thus $c'(j) = \sigma(j) \oplus q(j)$ is equal to $c(j)$ under $\mathrm{sgn}(L_{X_i}(j)) = \mathrm{sgn}(L_Q(j))$ as Eq.(11). $c'(j) = c(j)$ is not guaranteed under $\mathrm{sgn}(L_{X_i}(j)) \neq \mathrm{sgn}(L_Q(j))$.

2) $W_H(\sigma(j))$ is an odd
Since $W_H(\sigma(j))$ is an odd for only $L_{X_i}(j) = 0$ from Eq.(4), $c'(j)$ is able to be mapped to $c''(j) = c(j)$ by the operations in Table II. For example, $c''(j)$ is mapped to $c'(j) \oplus (01)_2$ for $\mathrm{sgn}(L_Q(j)) = 1 (q(j) = (00)_2)$ because of $c'(j) = x(j) \oplus c(j) \oplus q(j) = (01)_2 \oplus c(j) \oplus (00) = (01) \oplus c(j)$.

The above mapping operations do not guarantee to provide the correct relation $c''(j) = c(j)$ in any other cases such as $\mathrm{sgn}(L_{X_i}(j)) \neq \mathrm{sgn}(L_Q(j))$.

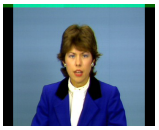
IV. EVALUATION FOR SECURITY

For the fuzzy commitment scheme, some 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 LBT 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^L.

The other approach is to estimate c from each $\sigma(j)$. When $W_H(\sigma(j))$ is an odd, it is satisfied from Eqs.(4) and (5) that $c(j)$ can be decided as $c(j) = \sigma(j) \oplus (01)_2$. On the other hand, when $W_H(\sigma(j)$ is an even, it is impossible to decide whether $\mathrm{sgn}(L_{X_i}(j))$ has 1 or -1. In this case, attackers have to calculate $h(c)$ for 2^{L-Z} codewords c where Z is the number of zero coefficients in an image. Therefore, when 2^{L-Z} is larger than 2^{256}, i.e.

$$L - Z > 256 \quad (12)$$

the key space of the proposed scheme is larger than that of the 256-bits key. As described later, Eq.(12) can be easily satisfied.



(a) claire

(b) football

Fig. 7. Examples of video sequences with 360×288

TABLE III
SELECTION OF L FOR VIDEO SEQUENCES IN DATABASES $D_1(QP_1 = 50)$AND $D_2(QP_2 = 90)$ UNDER OVERLAPPING MODE $OM = 2$

database	L	TP	TN	FP	FN	TPR[%]	FPR[%]	min$(L-Z)$
D_1	M	120	14242	38	0	100	0.26	1130
	MN	120	14280	0	0	100	0	5384
	P	120	14280	0	0	100	0	13150
D_2	M	240	13644	516	0	100	3.64	855
	MN	240	14062	98	0	100	0.69	1918
	P	240	14111	49	0	100	0.35	2080

V. SIMULATION

We evaluate the effectiveness of the proposed scheme by a number of simulations. Two video sequences shown in Fig.7 were used to confirm the effectiveness of the proposed scheme. The hash function SHA-256 was used in the simulations.

A. Querying performance

The aim of using video sequences is to show that the proposed scheme does not offer any false negative matches, even if frames are not visually distinguishable. Originally, there were 30 uncompressed consecutive frames for each video sequence. All video frames were compressed with six different quantization parameters i.e. QP=20, 40, 50, 60, 80 and 90 under each overlapping mode (OM). 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 $QP_1 = 50$ were enrolled in the database D_1 and the sets of frames compressed with $QP_2 = 90$ were enrolled in the D_2. As a query frame, 240 frames generated from the video sequences by using QP=20, 40, 60 and 80 were used. The original uncompressed versions were not included in the simulation. Therefore, 240×60 authentication process were performed for each database to evaluate the proposed scheme.

TABLE IV
COMPARISON WITH OTHER METHODS

method	$QP = 20$		$QP = 60$		$QP = 80$	
	TPR[%]	FPR[%]	TPR[%]	FPR[%]	TPR[%]	FPR[%]
image hashing	61.67	1.38	58.33	1.58	58.33	1.50
Triple feature	1.67	1.67	1.67	1.67	1.67	1.67

Querying results for the videos in each database under $OM = 2$ 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. Besides, the table shows the true-positive-Rate(TPR) and false-positive-Rate(FPR), defined by

$$TPR = \frac{TP}{TP + FN}, FPR = \frac{FP}{FP + TN}. \quad (13)$$

It is confirmed that there were not any false negative matches for both databases under every L. Moreover, larger L provides higher recognition accuracy. Note that these performances are the same as those of using LBT signs without secure protection [8], and thus the proposed protection scheme does not provide any degradation of the querying performance.

Besides, the tables illustrate the minimum value of $L - Z$ in all images. It is confirmed that the condition Eq.(12) was satisfied even for $L = M$. We also confirmed querying results under $OM = 0$ and 1 had the same trends as in Table. III.

B. Comparison with other methods

The proposed scheme were compared with two schemes, i.e. image hashing-based and triple feature-based ones. In the image hashing-based scheme [13], the hamming distances between the hash value of a query image and those of all images in each database are calculated, and then images in each database that have the smallest distance are chosen as the images generated from the same original image as the query, after decompressing all images. Besides, in the triple feature-based scheme, after decompressing all images, triple features are extracted from images in each database, and then the values are compared with that of a query image. Images having the closest triple feature value are chosen as the images generated from the same original image as the query, where the triple feature is a well-known robust feature [14] and it has been applied as an efficient retrieval scheme.

Querying results under the same condition as A for video sequences in D_2 are shown in Table IV. It is confirmed that $TPR = 100\%$ is not always satisfied for two methods. It means that the methods generate false negative matches, while there were not any false negative matches in the case of using the proposed scheme. In addition, they can not also protect the features of images.

VI. CONCLUSION

This paper proposed a robust scheme for identifying JPEG XR images in security. To construct a robust identification system, a property of the positive and negative signs of LBT coefficients was considered. Moreover, to protect the features of images, a new error correction technique was combined with a fuzzy commitment scheme. In principle, the proposed scheme does not not only produce false negative matches in any compression ratio, but also can protect images and the features. The experimental results showed the proposed scheme is robust against JPEG XR compression, while keeping a high level of security.

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 Image 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 signs," *IEEE Int'l. Conf. on Image Processing*, vol.II, no.MP-P1.10, pp.229-232, September 2007.

[7] A.Chaker, M.Kaaniche, A.Benazza-Benyahia and M.Antonini, "An Efficient Stastical-Based Retrieval Approach for JPEG2000 Compressed Images," in Proc. European Signal Processing Conf., pp.1870-1874, September 2015.

[8] 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.

[9] 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*, pp.2065-2068, November 2009.

[10] 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.

[11] 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.

[12] 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.

[13] B.Yang, F.Gu and X.Niu, "Block mean value based image perceptual hashing," in *Proc. Int'l. Conf. on Intelligent Information Hiding and Multimedia Signal Processing*, pp.167-172, December 2006.

[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] F.Dufaux,G.J.Sullivan and T.Ebrahimi, "The JPEG XR Image Coding Standard," *IEEE Signal Processing Magazine*, vol.26, pp.195-199, November 2009.

[18] 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.