PAPER Special Section on Enriched Multimedia — Potential and Possibility of Multimedia Contents for the Future —

Robust Image Identification without Visible Information for JPEG Images

Kenta IIDA[†], ***Student Member and*** **Hitoshi KIYA**[†a)], ***Fellow***

SUMMARY A robust identification scheme for JPEG images is proposed in this paper. The aim is to robustly identify JPEG images that are generated from the same original image, under various compression conditions such as differences in compression ratios and initial quantization matrices. The proposed scheme does not provide any false negative matches in principle. In addition, secure features, which do not have any visual information, are used to achieve not only a robust identification scheme but also secure one. Conventional schemes can not avoid providing false negative matches under some compression conditions, and are required to manage a secret key for secure identification. The proposed scheme is applicable to the uploading process of images on social networks like Twitter for image retrieval and forensics. A number of experiments are carried out to demonstrate that the effectiveness of the proposed method. The proposed method outperforms conventional ones in terms of query performances, while keeping a reasonable security level.

key words: *image identification, JPEG, social networks*

1. Introduction

The growth of popularity of social networks(SNs) like twitter and Facebook have opened new perspectives in many research fields, including the emerging area of Multimedia Forensics. The huge amount of images have been uploaded on social networks, and generally stored in a compressed form as JPEG images, after being re-compressed with different compression parameters from those of uploaded images [1]–[5].

This paper proposes a new robust identification scheme for JPEG images that are generated from the same original image, under various compression parameters, aiming at producing evidence on the integrity of images e.g. tamper detection. The proposed scheme allows not only to identify JPEG images under the use of different initial quantization matrices and quality factors but also to provide no visible information.

So far, several identification schemes and image hash functions have been developed for compressed images [6]–[20]. 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. Image hashing-based schemes [18]–[20] which correspond to the latter one have the robustness against the lossy compression, but it is not guaranteed that the identification is performed without any false negative matches. Moreover, they need to decompress images before carrying out the identification. This paper focuses on the former one, that has generally a strong robustness against a difference in compression parameters.

Conventional schemes [10], [11], [13]–[16] not only are robust against a difference in compressed ratios but also do not produce false negative matches in various compression ratios, due to the use of the positive and negative signs of DCT coefficients. However, they need to be combined with a security technique with a secret key such as the fuzzy commitment scheme [14]–[16], to securely protect the features which have some visible information. In addition, the security technique is not useful for the robust identification when various initial quantization matrices and quality factors are used.

Due to such situations, this paper proposes a robust scheme for identifying images compressed under the various compression parameters. The strategy to robustly identify JPEG images is to notice quantization matrices and the positions in which DCT coefficients have zero values. A number of experiments are carried out to demonstrate the effectiveness of the proposed method. The proposed method outperforms conventional ones in terms of query performances, without providing any visual information.

2. Preliminaries

2.1 JPEG Encoding

The JPEG standard is the most widely used image compression standard. The 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 8×8-blocks.
3) Applying DCT to each block to obtain 8×8 DCT coefficients **S**.
4) Quantizing **S** with a quantization matrix **Q**.
5) Entropy coding using Huffman coding.

In step 4), a quantization matrix **Q** with 8×8 components is used to obtain a matrix $\mathbf{S_q}$ from **S**, for example as below.

$$S_q(u,v) = \mathrm{round}\left(\frac{S(u,v)}{Q(u,v)}\right),\ 0 \le u \le 7,\ 0 \le v \le 7 \quad (1)$$

Manuscript received April 5, 2017.
Manuscript revised August 26, 2017.
Manuscript publicized October 16, 2017.

[†]The authors are with the Tokyo Metropolitan University, Asahigaoka, Hino-shi, 191–0065 Japan.
a) E-mail: kiya@tmu.ac.jp

DOI: 10.1587/transinf.2017MUP0005

with

$$Q(u,v) = \begin{cases} \text{round}\left(\frac{Q_0(u,v)*\lfloor\frac{5000}{Q_f}\rfloor}{100}\right), & 1 \le Q_f < 50, \\ \text{round}\left(\frac{Q_0(u,v)*(200-2*Q_f)}{100}\right), & 50 \le Q_f \le 100, \end{cases} \quad (2)$$

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. Round(x) is the function to round the value x to the nearest integer value and $\lfloor x \rfloor$ denotes the integer part of x.

Quality factor $Q_f (1 \le Q_f \le 100)$ is a parameter to control the matrix $\mathbf{Q}$. Large Q_f results in a high quality image. All components of an initial quantization matrix $\mathbf{Q_0}$ are positive numbers as well as Q_f. The data regarding initial quantization matrices are included in a header part of the JPEG codestream.

2.2 Notations and Terminologies

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

- X represents a JPEG compressed image X. X can be "Q" for a query image Q and "O" for an original image, where all images have the same size.
- M represents the number of 8×8-blocks in an image.
- N represents the number of DCT coefficients used for identification in each block. $0 < N \le 64$.
- $X(m,n)$ indicates the nth DCT coefficient in the mth block in image X. $0 \le m < M$, $0 \le n < N$.
- $\mathbf{Q_{X_i,L}}$ and $\mathbf{Q_{Q,L}}$ indicate the luminance quantization matrices used to generate images X_i and Q respectively, and $Q_{X_i,L}(n)$ and $Q_{Q,L}(n)$ indicate the nth component of $\mathbf{Q_{X_i,L}}$ and $\mathbf{Q_{Q,L}}$ respectively. $0 \le n < N$.

2.3 Image Identification

Let us consider that there are two or more compressed images, which are generated under the different or the same coding parameters. Those images are originated from the same images and compressed by the various coding parameters including initial quantization matrices and quality factors. In this paper, the identification of those images is referred to as image identification. In other words, if the images do not originate from the same image, they are unidentifiable from each other. The requirement of the robustness is to robustly identify images against a difference in coding parameters.

A. Scenario

The scenario is considered in this paper, as shown in Fig. 1. In this scenario, a client/user identifies images by using an identification tool. When the client/user uploads JPEG images to a database server like Twitter, the features of these images are extracted and then stored in a database by the client/user. The uploaded images are re-compressed under different coding parameters and then are stored in a database server. Finally, the client/user carries out the identification after extracting the features from a query i.e. an uploaded image.

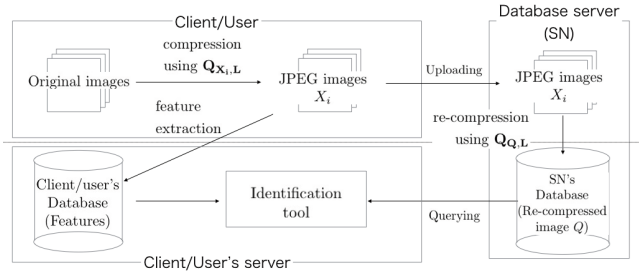


Fig. 1 Scenario

In addition to re-compression, it is known that SN providers often resize uploaded images, if certain conditions are satisfied [2]–[5]. For instance, when the filesize of images is larger than 3MB or the size of images is larger than 4096×4096, uploaded images will be resized in Twitter [5]. If both conditions are not satisfied, unresized images can be downloaded by adding "orig" to the URL for image view, even when displayed images are resized. The proposed scheme aims to identify images which have the same size.

Moreover, PNG images are uploaded to SNs in some cases. At this time, the images are also compressed by the JPEG standard and then stored in SN's database. Therefore, the client/user can extract the features from images.

The proposed scheme uses features without any visible information, so that unprotected features can be used for the scenario without any secret keys. Therefore, even when the features are leaked from a client/user's database, it is not required to protect the features. In addition, the features enable to avoid false negative matches.

B. Applications

In this paper, the proposed scheme aims to specify images generated from the same original image as that of a query. In social networks like Twitter, uploaded images are re-compressed by using different coding parameters from those of the uploaded images in general. Therefore, the identification system is required to robustly identify images against a difference in coding parameters. The target applications of the proposed scheme are shown, for example, as below.

- To find the original image of an uploaded image.
- To verify whether an alternation for an uploaded image is made or not.
- To confirm whether an uploaded image is illegally distributed.

Note that the proposed scheme does not aim to retrieve visually similar images to a query.

3. Proposed Identification Scheme

A robust image identification scheme is proposed by using a new property of DCT coefficients.

3.1 Property of DCT Coefficients

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

- When two JPEG images Q and X_i are generated from the same original image O, $Q(m,n)$ and $X_i(m,n)$ satisfy the condition:

$$Q(m,n)=0, \text{ for } Q_{X_i,L}(n)\leq Q_{Q,L}(n) \text{ and } X_i(m,n)=0 \tag{3}$$

and

$$X_i(m,n)=0, \text{ for } Q_{X_i,L}(n)\geq Q_{Q,L}(n) \text{ and } Q(m,n)=0. \tag{4}$$

The above property is illustrated in Fig. 2. Two images Q and X_1 are generated from the same original image under a common initial matrix $\mathbf{Q_0}$ and $Q_f > Q_{f_1}$, where Q_f and Q_{f_1} are quality factors used to generate images Q and X_1 respectively. It is confirmed that $X_1(m,n) = 0$ has to be satisfied if $Q(m,n) = 0$.

Therefore, the original images of two images Q and X_i have to be different original images if

$$Q(m,n)\neq 0, \text{ for } Q_{X_i,L}(n)\leq Q_{Q,L}(n) \text{ and } X_i(m,n)=0 \tag{5}$$

or

$$X_i(m,n)\neq 0, \text{ for } Q_{X_i,L}(n)\geq Q_{Q,L}(n) \text{ and } Q(m,n)=0. \tag{6}$$

In the proposed scheme, Eqs. (5) and (6) are used for the identification. The identification can be performed without any false negative matches by using them, because Eqs. (5) and (6) are sufficient conditions for the rejection. Therefore, when either Eqs. (5) or (6) is satisfied at any one of the positions, it is judged that the JPEG images have different original images.

$Q(m,n)$

-5	0	-1	0	0	-1	0	0
2	-1	0	0	0	0	0	0
1	0	0	0	0	0	0	0
1	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

(a) Image $Q(Q_f = 50)$

$X_1(m,n)$

-4	0	0	0	0	0	0	0
2	-1	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0
0	0	0	0	0	0	0	0

(c) Image $X_1(Q_{f_1} = 40)$

Fig. 2 Examples of quantized DCT coefficients in a block, where images X_1 and Q with a common initial quantization matrix $\mathbf{Q_0}$ are generated from the same original image. $X_1(m,n) = 0$ if $Q(m,n) = 0$ due to $Q_{f_1} < Q_f$ i.e. $Q_{X_1,L}(n) > Q_{Q,L}(n)$

3.2 Proposed Identification Scheme

In the proposed scheme, the positions of zero values and the quantization matrix $\mathbf{Q}$ are extracted from each JPEG codestream as features. These features are used for the identification, based on Eqs. (5) and (6).

Feature extraction and identification processes are explained, here.

A. Feature Extraction Process

In order to enroll features of image X_i, a client/user carries out the following steps.

(a) Set the values M and N.
(b) Extract the luminance quantization matrix $\mathbf{Q_{X_i,L}}$ from the header part of X_i.
(c) Set $m := 0$ and $n := 0$.
(d) Map a DCT coefficient $X_i(m,n)$ into $x_i(m,n)$ with 1 bit as

$$x_i(m,n) = \begin{cases} 0, & X_i(m,n) \neq 0, \\ 1, & X_i(m,n) = 0. \end{cases} \tag{7}$$

(e) Set $n := n + 1$. If $n < N$, proceed to step(d).
(f) Set $n := 1$ and $m := m + 1$. If $m < M$, proceed to step(d). Otherwise, store $\mathbf{Q_{X_i,L}}$ and x_i as the feature set $\mathbf{F}_{X_i}$ in the a client/user's database.

B. Identification Process

In order to compare image Q with image X_i, a client/user extracts the feature set of Q, $\mathbf{F}_Q$ from Q as well as $\mathbf{F_{X_i}}$. The client/user carries out the following steps.

(a) Set the values M and N.
(b) Set $m := 0$ and $n := 0$.
(c) Confirm whether Eq. (5) or (6) is satisfied. If either Eq. (5) or (6) is satisfied, the client/user judges that X_i and Q are generated from different original images and the process for image X_i is halted.
(d) Set $n := n + 1$. If $n < N$, proceed to step(c).
(e) Set $n := 1$ and $m := m + 1$. If $m < M$, proceed to step(c). Otherwise, the client/user judges that X_i and Q are generated from the same original image.

As mentioned above, the proposed scheme is required to use only the positions of zero values and quantization tables. In the conventional schemes [10], [11], [14]–[16], the signs of coefficients are used as features. However, they have two important limitations. The first limitation is that the coding parameters used to generate X_i and Q are limited, and the second one is that the features have some visible information as shown in Fig. 3 [21], [22]. On the other hand, the positions of zero values do not provide any visible information, compared to the features used in [10], [11], [14]–[16]. Besides, the proposed scheme can identify images under various coding conditions, although schemes which

(a) Original image (b) Images reconstructed from DCT signs

Fig. 3 Visible information of DCT signs

consider the protection of the information [14]–[16] had the limitation regarding initial quantization matrices and quality factors.

Moreover, several image-hashing schemes have been proposed for image retrieval [18]–[20]. However, they can not guarantee that there are not any false negative matches as shown later, although the proposed scheme guarantees it in principle.

4. Simulation

A number of simulations were conducted to evaluate the performance of the proposed scheme. We used two initial quantization matrices and two datasets: Uncompressed Color Image Database (UCID) [23] and Head Pose Image Database (HPID) [24] (see Figs. 4 and 5). UCID consists of 1338 images which have two different sizes, where 885 images have 384×512 and 453 images have 512×384 as sizes. In the simulations, 885 images with the size of 384×512 were used. HPID consists of face images of 15 persons and there are 186 images per person. We used 186 images of "Person01".

The images were compressed under various coding parameters. Table 1 summarizes the compression conditions, where IJG means to use the default initial quantization matrix in the encoder from IJG (Independent JPEG Group) [25], and HVS means to use the initial quantization matrix based on the human visual system [26] respectively.

In Table 1, features enrolled in the database $DB_{UCID,1}$ were extracted from 885 images in UCID under $Q_{f_1} = 50$ and IJG. Similarly, features in $DB_{UCID,2}$ were extracted from images with $Q_{f_2} = 75$ and IJG, and ones in $DB_{UCID,3}$ were extracted from images with $Q_{f_3} = 50$ and HVS. 885×4=3540 images generated from 885 images in UCID under $Q_f = 40, 60, 85, 95$ and IJG were used as query images. Therefore, 885×3540 identification process were performed for each database generated from images in UCID to evaluate the proposed scheme. As well as the identification for images in UCID, we carried out 186×744 identification process for each database generated from images in HPID. In the proposed scheme, the features were extracted from only Y components to avoid the effect of a difference in subsampling the C_b and C_r. The simulations were run on a PC with Intel Core i7-5820K CPU and a main memory of 16Gbytes.

4.1 Identification Performance for UCID

The identification for each database which consists of 885 images in UCID was performed. Tables 2 and 3 show the true positive rate(TPR), false positive rate(FPR) and Precision value, defined by

$$TPR = \frac{TP}{TP + FN}, \tag{8}$$

$$FPR = \frac{FP}{FP + TN}, \tag{9}$$

$$Precision = \frac{TP}{TP + FP}, \tag{10}$$

where TP, TN, FP and FN represent the number of true pos-

Fig. 4 Examples of images in UCID with 384×512

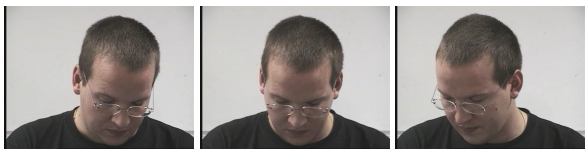


Fig. 5 Examples of images in HPID with 288×384

Table 1 Conditions used to generate JPEG images

dataset	enrolled images			query images	
	database	Q_{f_i} =	$\mathbf{Q_0}$	Q_f=	$\mathbf{Q_0}$
UCID	$DB_{UCID,1}$	50	IJG	40,60,85,95	IJG
	$DB_{UCID,2}$	75	IJG		
	$DB_{UCID,3}$	50	HVS		
HPID	$DB_{HPID,1}$	50	IJG	40,60,85,95	IJG
	$DB_{HPID,2}$	75	IJG		
	$DB_{HPID,3}$	50	HVS		

Table 2 Querying performance for common $\mathbf{Q_0}$ and $Q_f = 60$ (UCID)

method	database	TPR[%]	FPR[%]	Precision[%]
proposed	$DB_{UCID,1}$	100	0	100
	$DB_{UCID,2}$	100	0	100
FCS-based [14]	$DB_{UCID,1}$	100	0	100
	$DB_{UCID,2}$	0	0	0
image hashing [18]	$DB_{UCID,1}$	100	0	100
	$DB_{UCID,2}$	100	0	100
SIMPLE descriptors [27]	$DB_{UCID,1}$	100	0	100
	$DB_{UCID,2}$	100	0	100

Table 3 Querying performance for including non-common $\mathbf{Q_0}$ and $Q_f < Q_{f_i}$ (UCID)

method	database	TPR[%]	FPR[%]	Precision[%]
proposed	$DB_{UCID,1}$	100	0	100
	$DB_{UCID,2}$	100	0	100
	$DB_{UCID,3}$	100	0	100
FCS-based [14]	$DB_{UCID,1}$	75	0	100
	$DB_{UCID,2}$	50	0	100
	$DB_{UCID,3}$	25	0	100
image hashing [18]	$DB_{UCID,1}$	100	0	100
	$DB_{UCID,2}$	100	0	100
	$DB_{UCID,3}$	100	0	100
SIMPLE descriptors [27]	$DB_{UCID,1}$	99.46	0.00	99.46
	$DB_{UCID,2}$	99.69	0.00	99.69
	$DB_{UCID,3}$	99.66	0.00	99.66

itive, true negative, false positive and false negative matches respectively. Note that $TPR = 100[\%]$ means that there are no false negative matches.

The proposed scheme was compared with the state-of-art image hashing-based scheme [18], the SIMPLE descriptors-based scheme [27] and the fuzzy commitment scheme (FCS)-based scheme [14]. In the scheme [18], the hamming distances between the hash value of a query image and those of all images in each database are calculated, and then images that have the smallest distance are chosen as the images generated from the same original image as the query, after decompressing all images. In the scheme [27], after indexing all images in each database, image retrieval is performed by using a query image and the index, and then images that have the highest values are chosen as the images generated from the same original image as the query, where SURF(speeded up robust features) and CEDD(color and edge directivity descriptors) were used as local and global descriptors respectively in the simulations. The results in Tables 2 and 3 suggest the following points.

A. Querying for Common $\mathbf{Q_0}$ and $Q_f \geq Q_{f_i}$

The performance of querying for $DB_{UCID,1}$ and $Q_f = 60$ is shown in Table 2, where images enrolled in $DB_{UCID,1}$ have the same $\mathbf{Q_0}$ as that of queries and satisfy $Q_f \geq Q_{f_i}$. Under this condition, all schemes did not provide any false negative matches. Note that the results for $DB_{UCID,2}$ in the case using FCS-based scheme did not have the same trend because the scheme does not guarantee that there are no false negative matches under $Q_f < Q_{f_i}$.

B. Querying for Including Non-common $\mathbf{Q_0}$ and $Q_f < Q_{f_i}$

Table 2 also shows the results of the identification between query images and images in $DB_{UCID,2}$. The proposed and image hashing-based schemes identified images without any misidentification, although FCS-based one provided some false negative matches. Table 3 summarizes the results of querying for all databases and all query images, where $FPR = 0.00$ indicates $FP \neq 0$ although $FPR = 0$ indicates $FP = 0$. It is confirmed that there were not any false negative and false positive matches in the case of using proposed and image hashing-based schemes.

4.2 Identification Performance for HPID

The simulations for 186 images in HPID were also conducted. The images are face images of a person that include some variations of panning and tilt angles as shown in Fig. 5, so that they are very similar.

Table 4 shows the results of the identification. In the simulations, the proposed scheme resulted in the perfect performance in terms of identification accuracy, although other schemes provided some false negative and false positive matches. This is because the proposed scheme can identify images without misidentification in principal, even if two images are very similar. Note that the proposed scheme has a probability of producing false positive matches. When identifying images compressed with a quite low quality factor, false positive matches might increase if most of DCT coefficients had zero values. In the simulation, even when JPEG images were compressed with a very low quality factor i.e., $Q_f = 40$, those images had still some non-zero AC coefficients. As a result, there were no false positive matches in this case. It is known that quality factors used for the recompression in Twitter and Facebook are larger than 70 [2], [5]. Therefore, it is expected that false positive matches will not dramatically increase in the proposed scheme for identifying images uploaded to SNs.

Table 4 Querying performance for including non-common $\mathbf{Q_0}$ and $Q_f < Q_{f_i}$(HPID)

method	database	TPR[%]	FPR[%]	Precision[%]
proposed	$DB_{HPID,1}$	100	0	100
	$DB_{HPID,2}$	100	0	100
	$DB_{HPID,3}$	100	0	100
FCS-based [14]	$DB_{HPID,1}$	75	0	100
	$DB_{HPID,2}$	50	0	100
	$DB_{HPID,3}$	71.10	0	100
image hashing [18]	$DB_{HPID,1}$	98.79	0.03	94.11
	$DB_{HPID,2}$	99.33	0.03	95.11
	$DB_{HPID,3}$	98.52	0.03	94.83
SIMPLE descriptors [27]	$DB_{HPID,1}$	72.04	0.15	72.04
	$DB_{HPID,2}$	95.83	0.02	95.83
	$DB_{HPID,3}$	88.84	0.06	88.84

4.3 Image Tamper Localization

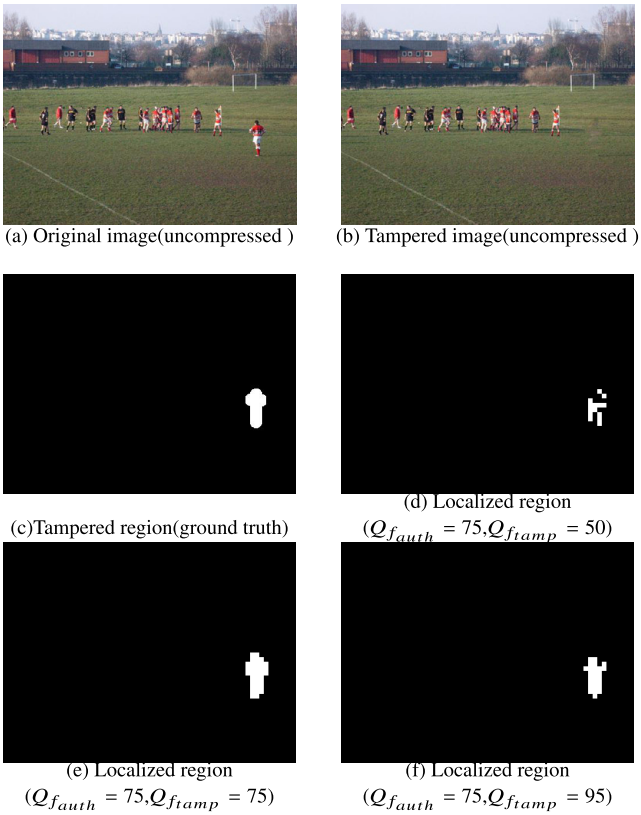
The proposed method can be easily extended for image tamper localization because the identification is performed by using the positions of zero values in each block. For the evaluation, we prepared the image shown in Fig. 6 (b) by manipulating an original image in Fig. 6 (a), where the tampered region is shown in Fig. 6 (c). To localize the tampered regions, these images were compressed by JPEG. In this paper, "authentic image" and "tampered image" are defined as the JPEG image generated from the original image (Fig. 6 (a)) and the JPEG image generated from the image (Fig. 6 (b)) respectively. The following notations are used in this section.

- Tp indicates the number of the blocks correctly detected as tampered blocks.
- Fp indicates the number of the blocks falsely detected as tampered blocks.
- Fn indicates the number of the blocks falsely detected as not tampered blocks.
- Precision(Tam) and recall are defined by

$$Precision(Tam) = \frac{Tp}{Tp + Fp}, \tag{11}$$

$$Recall = \frac{Tp}{Tp + Fn}. \tag{12}$$

$Precision(Tam) = 100[\%]$ means that there are not any blocks falsely detected as tampered blocks. Note that $Precision(Tam)$ is the percentage of the tampered



(a) Original image(uncompressed)
(b) Tampered image(uncompressed)
(c)Tampered region(ground truth)
(d) Localized region ($Q_{f_{auth}}$ = 75,$Q_{f_{tamp}}$ = 50)
(e) Localized region ($Q_{f_{auth}}$ = 75,$Q_{f_{tamp}}$ = 75)
(f) Localized region ($Q_{f_{auth}}$ = 75,$Q_{f_{tamp}}$ = 95)

Fig. 6 Images used for evaluating the performance of tamper localization

Table 5 Results for tamper localization with $Q_{f_{auth}}$ = 75

$Q_{f_{auth}}$	$Q_{f_{tamp}}$	$Precision(Tam)$[%]	$Recall$[%]	F_1[%]
75	95	100	74.29	85.25
	75	100	97.14	98.55
	50	100	40.00	57.14

blocks among the blocks judged to be tampered, although some tampered blocks might not be judged to be tampered.

- F_1 score is defined by

$$F_1 = 2 \times \frac{Precision(Tam) \times Recall}{Precision(Tam) + Recall}. \quad (13)$$

- $Q_{f_{auth}}$ and $Q_{f_{tamp}}$ represent the quality factors used to generate authentic and tampered images respectively.

In the simulation, the performance of tamper localization is evaluated in 8×8 block unit because tamper localization by the proposed scheme is limited to the detection of 8×8 block unit. Note that the definition of $Precision(Tam)$ is different from that of $Precision$ in the previous sections.

When the authentic and tampered images were generated with $Q_{f_{auth}} = 75$ and $Q_{f_{tamp}} = 50, 75, 95$, tamper localized regions are shown in Fig. 6 (d), (e) and (f) respectively. In addition, Table 5 shows $Precision(Tam)$, $Recall$ and F_1 scores. Note that all images were generated by using IJG. It is confirmed that there were not any blocks falsely detected as tampered blocks. Especially, when $Q_{f_{auth}} = 75$ and $Q_{f_{tamp}} = 75$, $Recall$ had the highest value, i.e., the most of tampered blocks were detected. This is because both Eqs. (5) and (6) were used for tamper localization when $Q_{f_{auth}} = Q_{f_{tamp}}$, although either of the equations was used when $Q_{f_{auth}} \neq Q_{f_{tamp}}$.

Table 6 Results for tamper localization with common initial quantization matrix

$Q_{f_{auth}}$	$Q_{f_{tamp}}$	$Precision(Tam)$[%]	$Recall$[%]	F_1[%]
75	95	100	74.29	85.25
	85	100	85.71	92.31
	75	100	97.14	98.55
	60	100	57.14	72.73
	50	100	40.00	57.14
	40	100	28.86	37.21
50	95	100	74.29	85.25
	85	100	74.29	85.25
	75	100	80.00	88.89
	60	100	85.71	92.31
	50	100	94.29	97.06
	40	100	48.57	65.38

Table 7 Results for tamper localization with non-common initial quantization matrix

$Q_{f_{auth}}$	$Q_{f_{tamp}}$	$Precision(Tam)$[%]	$Recall$[%]	F_1[%]
50	95	100	65.71	79.31
	85	100	82.86	90.63
	75	100	85.71	92.31
	60	100	88.57	93.94
	50	100	88.57	93.94
	40	100	77.14	87.10

Besides, Tables 6 and 7 show the results in the case of using that the various parameters like the initial quantization matrices and the quality factors. Under all conditions, tamper regions were localized without falsely detecting the blocks as not tampered ones. In addition, $Recall$ values had the same trend as the values in Table 5.

FCS-based and image-hashing based schemes can not localize the tampered regions, although they can judge whether an alternation for an image is made or not. In addition, most image retrieval methods such as SIMPLE descriptors-based one can not be also applied to tamper localization. Therefore, the proposed scheme is more effective than other schemes in terms of not only the querying performances but also tampered detection, in the case of identifying JPEG images uploaded to SNs.

5. Conclusion

A robust identification scheme for JPEG images was proposed in this paper. By using quantization tables and the positions of zero values for the identification, the proposed scheme is robust against a difference in various coding parameters, and the features enrolled in the databases do not provide any visual information of original images. Besides, the proposed scheme does not produce false negative matches under any level and any tables in principle. The experimental results showed that the proposed scheme has a better query performance for classification tests than conventional ones. Moreover, the proposed scheme can be easily extended for image tamper localization. In addition, it has been confirmed that any blocks are not falsely detected as tampered blocks in the simulation.

References

[1] R. Caldelli, R. Becarelli, and I. Amerini, "Image origin classification based on social network provenance," IEEE Trans. Information Forensics and Security, vol.12, no.6, pp.1299–1308, June 2017.
[2] M. Moltisanti, A. Paratore, S. Battiato, and L. Saravo, "Image manipulation on facebook for forensics evidence," Int'l Conf. on Image Analysis and Processing, vol.9280, pp.506–517, 2015.
[3] J. Hiney, T. Dakve, K. Szczypiorski, and K. Gaj, "Using facebook for image steganography," Int'l Conf. on Availability, Reliability and Security, pp.442–447, 2015.
[4] O. Giudice, A. Paratore, M. Moltisanti, and S. Battiato, "A classification engine for image ballistics of social data," Computing Research Repository, vol.abs/1610.06347, 2016.
[5] T. Chuman, K. Iida, and H. Kiya, "Image manipulation analysis on social networking service for encryption-then-compression systems," in IEICE Technical Report (Enriched Multimedia), vol.117, no.201, pp.1–6, Sept. 2017.
[6] C.-Y. Lin and S.-F. Chang, "A robust image authentication method distinguishing jpeg compression from malicious manipulation," IEEE Trans. Circuits Syst. Video Technol., vol.11, no.2, pp.153–168, Feb. 2001.
[7] Z. Fan and R.L. de Queiroz, "Identification of bitmap compression history: Jpeg detection and quantizer estimation," IEEE Trans. Image Process., vol.12, no.2, pp.230–235, Feb. 2003.
[8] D. Edmundson and G. Schaefer, "An overview and evaluation of jpeg compressed domain retrieval techniques," Proceedings ELMAR-2012, pp.75–78, Sept. 2012.
[9] K. Cheng, N. Law, and W. Siu, "A fast approach for identifying similar features in retrieval of jpeg and jpeg2000 images," Asia-Pacific Signal and Information Processing Association, Annual Summit and Conference, pp.258–261, Oct. 2009.
[10] F. Arnia, I. Iizuka, M. Fujiyoshi, and H. Kiya, "Fast and robust identification methods for jpeg images with various compression ratios," IEEE International Conference on Acoustics Speech and Signal Processing Proceedings, pp.II-397–II-400, May 2006.
[11] H. Kobayashi, S. Imaizumi, and H. Kiya, "A robust identification scheme for jpeg xr images with various compression ratios," Pacific-Rim Symposium on Image and Video Technology, vol.9431, pp.38–50, 2015.
[12] T. Dobashi, O. Watanabe, T. Fukuhara, and H. Kiya, "Hash-based identification of jpeg 2000 images in encrypted domain," Intelligent Signal Processing and Communications Systems (ISPACS), International Symposium on, pp.469–472, 2012.
[13] O. Watanabe, T. Iida, T. Fukuhara, and H. Kiya, "Identification of jpeg 2000 images in encrypted domain for digital cinema," IEEE International Conference on Image Processing (ICIP), pp.2065–2068, Nov. 2009.
[14] K. Iida and H. Kiya, "Secure and robust identification based on fuzzy commitment scheme for jpeg images," IEEE International Symposium on Broadband Multimedia Systems and Broadcasting (BMSB), pp.1–5, June 2016.
[15] K. Iida and H. Kiya, "Fuzzy commitment scheme-based secure identification for jpeg images with various compression ratios," IEICE Trans. Fundamentals of Electronics, Communications and Computer Sciences, vol.99, no.11, pp.1962–1970, 2016.
[16] K. Iida, H. Kobayashi, and H. Kiya, "Secure identification based on fuzzy commitment scheme for jpeg xr images," European Signal Processing Conference (EUSIPCO), pp.968–972, Aug. 2016.
[17] K. Iida and H. Kiya, "Codestream level secure identification for jpeg 2000 images under various compression ratios," Asia-Pacific Signal and Information Processing Association, Annual Summit and Conference, pp.1–6, 2016.
[18] Y. Li and P. Wang, "Robust image hashing based on low-rank and sparse decomposition," International Conference on Acoustics, Speech and Signal Processing (ICASSP), pp.2154–2158, March 2016.
[19] Y.N. Li, P. Wang, and Y.T. Su, "Robust image hashing based on selective quaternion invariance," IEEE Signal Process. Lett., vol.22, no.12, pp.2396–2400, Dec. 2015.
[20] Z. Tang, X. Zhang, X. Li, and S. Zhang, "Robust image hashing with ring partition and invariant vector distance," IEEE Trans. Inf. Forensics Security, vol.11, no.1, pp.200–214, Jan. 2016.
[21] I. Ito and H. Kiya, "One-time key based phase scrambling for phase-only correlation between visually protected images," EURASIP Journal on Information Security, vol.2009, no.1, 2009.
[22] I. Ito and H. Kiya, "A new class of image registration for guaranteeing secure data management," IEEE Int'l Conf. on Image Processing (ICIP), pp.269–272, 2008.
[23] G. Schaefer and M. Stich, "Ucid: An uncompressed color image database," Electronic Imaging 2004, pp.472–480, 2003.
[24] N. Gourier, D. Hall, and J.L. Crowley, "Estimating face orientation from robust detection of salient facial structures," Int'l Workshop on Visual Observation of Deictic Gestures, pp.1–9, 2004.
[25] "The independent jpeg group software jpeg codec." http://www.ijg.org/.
[26] C.-Y. Wang, S.-M. Lee, and L.-W. Chang, "Designing jpeg quantization tables based on human visual system," Signal Processing: Image Communication, vol.16, no.5, pp.501–506, 2001.
[27] C. Iakovidou, N. Anagnostopoulos, A. Kapoutsis, Y. Boutalis, M. Lux, and S.A. Chatzichristofis, "Localizing global descriptors for content-based image retrieval," EURASIP Journal on Advances in Signal Processing, vol.2015, no.1, p.80, 2015.

Kenta Iida received his B.Eng. degree from Tokyo Metropolitan University, Japan in 2016. He is a Master course student at Tokyo Metropolitan University, Japan. His research interests include image processing, biometrics, and multimedia security. He is a student member of IEEE and IEICE.

Hitoshi Kiya received his B.Eng. and M.Eng. degrees from Nagaoka University of Technology, Japan, in 1980 and 1982, respectively, and his D.Eng. degree from Tokyo Metropolitan University in 1987. In 1982, he joined Tokyo Metropolitan University as an Assistant Professor, where he became a Full Professor in 2000. From 1995 to 1996, he attended the University of Sydney, Australia as a Visiting Fellow. He was/is the Chair of IEEE Signal Processing Society Japan Chapter, an Associate Editor for IEEE Trans. Image Processing, IEEE Trans. Signal Processing and IEEE Trans. Information Forensics and Security, respectively. He also served as the President of IEICE Engineering Sciences Society (ESS), the Editor-in-Chief for IEICE ESS Publications, and a Vice President of APSIPA, He currently serves as the President-Elect of APSIPA and Regional Director-at-Large for Region 10 of IEEE Signal processing Society. He received IEEE ISPACS Best Paper Award in 2016, IWAIT Best Paper Award in 2014and 2015, ITE Niwa-Takayanagi Best Paper Award in 2012, the Telecommunications Advancement Foundation Award in 2011, and IEICE Best Paper Award in 2008. He is a Fellow of IEEE, IEICE and ITE.