ROBUST IMAGE IDENTIFICATION WITH SECURE FEATURES FOR JPEG IMAGES

Kenta Iida and Hitoshi Kiya

Tokyo Metropolitan University, Asahigaoka, Hino-shi, Tokyo 191-0065, Japan

ABSTRACT

A robust identification scheme for JPEG images is proposed in this paper. The aim is to robustly identify JPEG images 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 in principle produce any false negative matches. Features without visual information are used to achieve not only a robust identification scheme but also secure one. Conventional schemes can produce false negative matches under certain compression conditions and require the use of a secret key for secure identification. The proposed scheme is well-suited for the uploading images to social network services and for image retrieval and forensics. Simulations demonstrated the effectiveness of the proposed scheme outperformed conventional ones in terms of query performance, while maintaining reasonable security.

Index Terms— Image identification, JPEG, SNSs

1. INTRODUCTION

The growing popularity of social network services(SNSs) like Twitter and Facebook has opened new perspectives in many research fields, including the emerging area of multimedia forensics. The huge amount of images uploaded to social networks are generally stored in a compressed format as JPEG images, after being recompressed using compression parameters different from those used for the uploaded images [1, 2]. We have developed a scheme for robustly identifying JPEG images generated from the same original image under various compression conditions. It is aimed at producing evidence regarding image integrity, e.g., tamper detection. The proposed scheme does not in principle produce false negative matches. Features that do not have visual information are used to achieve not only a robust identification scheme but also secure one.

Several schemes and image hash functions have been developed for identifying compressed images [3–16]. They can be broadly classified into two types: compression-method-dependent and compression-method-independent. Image hashing-based schemes [14–16] correspond to the second type. Although they are robust against lossy compression, they can produce false negative matches. Moreover, they need to decompress images before carrying out identification. This paper focuses on the first type, which are generally strongly robust against differences in compression conditions.

Conventional compression-method-dependent schemes [7,8,10–13] not only are robust against differences in compression ratio but also do not produce false negative matches for various compression ratios, due to the use of the positive and negative signs of discrete cosine transform(DCT) coefficients. However, they need to be combined with a security technique utilizing a secret key such as the fuzzy commitment scheme [11–13], to securely protect the features that provide visible information. In addition, these schemes cannot carry out the robust identification when various initial quantization matrices are used.

Our proposed scheme can robustly identify JPEG images generated from the same original image and compressed under various compression conditions. It does this by using quantization matrices and the positions at which the DCT coefficients have zero values. Simulations demonstrated the effectiveness of the proposed scheme. It outperformed 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) Perform color transformation from RGB space to YC_bC_r space and sub-sample C_b and C_r.
2) Divide image into non-overlapping consecutive 8×8-blocks.
3) Apply DCT to each block to obtain 8×8 DCT coefficients **S**.
4) Quantize **S** using quantization matrix **Q**.
5) Entropy code using Huffman coding.

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

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

with

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

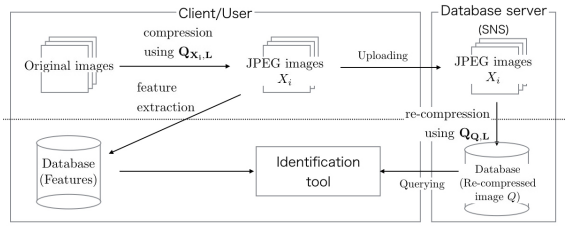
where $S(u,v)$, $Q(u,v)$, $S_q(u,v)$ and $Q_0(u,v)$ represent the (u,v)element of **S**, **Q**, $\mathbf{S_q}$ and $\mathbf{Q_0}$ respectively. The Round(x) function is used to round value x to the nearest integer value and $\lfloor x \rfloor$ denotes the integer part of x.

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

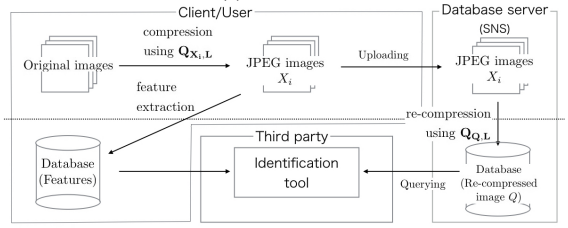
2.2. Notation and Terminology

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

- X represents JPEG compressed image X. X can be "Q" for query image and "O" for original image (all images have the same size).



(a)1st scenario



(b)2nd scenario

Fig. 1. Framework for identification

- M represents number of 8×8-blocks in an image.
- N represents number of DCT coefficients used for identification in each block ($0 < N \leq 64$).
- $X(m,n)$ indicates nth DCT coefficient in mth block in image X ($0 \leq m < M$, $0 \leq n < N$).
- $\mathbf{Q}_{\mathbf{X_i,L}}$ and $\mathbf{Q}_{\mathbf{Q,L}}$ represent luminance quantization matrices used to generate images X_i and Q respectively, and $Q_{X_i,L}(n)$ and $Q_{Q,L}(n)$ indicate nth component of $\mathbf{Q}_{\mathbf{X_i,L}}$ and $\mathbf{Q}_{\mathbf{Q,L}}$, respectively ($0 \leq n < N$).

2.3. Image Identification

Let us consider a situation in which there are two or more compressed images generated under different or the same coding conditions. They originated from the same image and were compressed using the various coding parameters including initial quantization matrices and quality factors. We refer to the identification of those images as "image identification". In other words, if the images did not originate from the same image, they are not identified. The requirement of the robustness is to robustly identify images against differences in coding conditions.

A. Scenarios

The two scenarios illustrated in Fig. 1 are considered in this paper. In the first scenario, a client/user identifies images generated from the same original image by using an identification tool. When the client/user uploads JPEG images to a database server like Twitter, the features of those images are enrolled (extracted and stored) in a database by the user/client. The uploaded images are re-compressed under different coding conditions and stored in the database server. Finally, the client/user carries out identification after extracting the features from a query image, i.e., an uploaded image.

In the second scenario, a third party identifies images. The processes to enroll the features and to upload images are the same as those in the first scenario. For the identification, a client/user sends only the features to the third party, and the third party extracts features from an uploaded image. Note that the third party should not receive any visual information of the client/user's images due to privacy concerns or copyright protection.

The proposed scheme uses features that do not provide visible information, so unprotected features can be used for both scenarios. In addition, use of these features prevents false negative matches. As a result, the proposed scheme enables a third party to carry out identification without using any sensitive data, even under the second scenario.

B. Applications

The proposed scheme is aimed at detecting images generated from the same original image as that of a query image. On social media sites like Twitter, uploaded images are generally re-compressed using coding parameters different from the uploaded ones. Therefore, the identification system is required to robustly identify images against differences in coding conditions. Target applications are:

- finding the original image of an uploaded image,
- detecting whether uploaded image has been altered,
- determining whether an uploaded image has been illegally distributed.

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

3. PROPOSED IDENTIFICATION SCHEME

The proposed image identification scheme uses a new property of DCT coefficients.

3.1. Property of DCT Coefficients

As shown by Eq.(1), quantized DCT coefficients have the following property.

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

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

and

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

This property is illustrated in Fig. 2. Images Q and X_1 were generated from the same original image using 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. Note that $Q_{Q,L}(n) < Q_{X_1,L}(n)$ is satisfied due to $Q_f > Q_{f_1}$. It is that $X_1(m,n) = 0$ if $Q(m,n) = 0$.

Therefore, the original images of images Q and X_i are different if

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

or

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

The use of Eqs.(5) and (6) for identification prevents false negative matches because they are sufficient conditions for rejection. Therefore, when either Eqs.(5) or (6) is satisfied at any position, the JPEG images are judged to 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., $Q_{X_1,L}(n) > Q_{Q,L}(n)$.

(a) Original image

(b) Images reconstructed from DCT signs

Fig. 3. Visible information reconstructed from DCT signs

Fig. 4. Example test images (384×288)

3.2. Proposed Identification Scheme

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

Feature extraction and identification processes are explained, here.

A. Feature Extraction Process

A client/user carries out the following steps in order to enroll the features of image X_i.

(a) Set values M and N.

(b) Extract luminance quantization matrix $\mathbf{Q_{X_i,L}}$ from header part of X_i.

(c) Set $m := 0$ and $n := 0$.

(d) Map DCT coefficient $X_i(m,n)$ into $x_i(m,n)$ with 1 bit:

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

(e) Set $n := n + 1$.If $n < N$, return to step (d).

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

B. Identification Process

To compare image Q with image X_i, a third party or a client/user extracts the feature set of Q, $\mathbf{F}_Q$ from Q as well as from $\mathbf{F_{X_i}}$. Under the second scenario, the third party carries out the following steps.

(a) Set values M and N.

(b) Set $m := 0$ and $n := 0$.

(c) Determine whether Eq. (5) or (6) is satisfied. If either is satisfied, judge that X_i and Q were generated from different original images and terminate process for image X_i.

(d) Set $n := n + 1$.If $n < N$, return to step (c).

(e) Set $n := 1$ and $m := m + 1$.If $m < M$, return to step (c). Otherwise, judge that X_i and Q were generated from the same original image.

Table 1. Coding conditions

database	enrolled images		query images	
	$Q_{f_i} =$	$\mathbf{Q}_0$	$Q_f =$	$\mathbf{Q}_0$
DB_1	50	IJG	40,60,85,95	IJG
DB_2	75	IJG		
DB_3	50	HVS		

As mentioned above, the proposed scheme uses only the positions of the zero values and the quantization tables. In the conventional schemes [7, 8, 11–13], the signs of the coefficients are used as features. However, these schemes have two important limitations. The first is that the initial quantization matrices used to generate X_i and Q have to be the same, and the second is that the features provide visible information, as shown in Fig. 3 [17, 18]. In contrast, the positions of the zero values do not provide any visible information.

The image-hashing based schemes that have been proposed for image retrieval [14–16] can produce false negative matches, while the proposed scheme does not in principle, as mentioned above.

4. SIMULATION

A number of simulations were conducted to evaluate the performance of the proposed scheme. We used the encoder from the IJG (Independent JPEG Group) [19] and 186 face images as test images [20] (see Fig.4). The images were compressed under various coding conditions. Table 1 summarizes the coding conditions and data base types;IJG means that the initial quantization matrix in IJG was used, and HVS means that the initial quantization matrix based on the human visual system [21] was used.

For instance, features extracted from the 186 images with $Q_{f_1} = 50$ were enrolled in database DB_1, and 744(186×4) images compressed with $Q_f = 40, 60, 85, 95$ were used as a query for DB_1, DB_2 and DB_3. Therefore, identification was performed 186×744 times for each database to evaluate the proposed scheme.

Tables 2 and 3 show the true positive rate(TPR) and false positive rate(FPR), defined by

$$TPR = \frac{TP}{TP + FN}, \; FPR = \frac{FP}{FP + TN}, \tag{8}$$

where TP, TN, FP, and FN represent the number of true positive, true negative, false positive and false negative matches, respectively. Note that $TPR = 100[\%]$ means that there were no false negative matches.

Table 2. Querying performance for images with $Q_f = 60$

scheme	database	TPR[%]	FPR[%]
proposed	DB_1	100	0
	DB_2	100	0
FCS-based [11]	DB_1	100	0
	DB_2	0	0
image hashing [14]	DB_1	98.92	0.03
	DB_2	97.85	0.04

Table 3. Querying performance for images with $Q_f = 40, 60, 85, 95$

scheme	database	TPR[%]	FPR[%]
proposed	DB_1	100	0
	DB_2	100	0
	DB_3	100	0
FCS-based [11]	DB_1	75	0
	DB_2	50	0
	DB_3	71.23	0
image hashing [14]	DB_1	98.79	0.03
	DB_2	99.33	0.03
	DB_3	98.52	0.03

The proposed scheme was compared with a state-of-art image hashing-based scheme [14] and a fuzzy commitment scheme (FCS)-based scheme [11], which are as secure as well as the proposed one. In the image hashing-based scheme, the hamming distances between the hash value of a query image and those of all images in each database are calculated after decompressing all images, and the images that have the smallest distance are taken as ones generated from the same original image as the query image.

The results in Tabs.2 and 3 suggest the following points.

A.Querying for common $\mathbf{Q_0}$ and $Q_f \geq Q_{fi}$

The performance of querying for DB_1 and $Q_f = 60$ is shown in Table 2; the images stored in DB_1 had the same $\mathbf{Q_0}$ as the queries and satisfied $Q_f \geq Q_{f_i}$. The proposed and FCS-based schemes do not produce any false negative matches, while the image hashing-based one did.

B.Querying for common $\mathbf{Q_0}$ and $Q_f < Q_{fi}$

Table 2 also shows the results of the identification between query images and images in DB_2. Only the proposed scheme identified images without any misidentification. This is because FCS-based scheme does not guarantee that there are no false negative matches under $Q_f < Q_{f_i}$.

C.Querying for non-common Q_0

Table 3 summarizes the results of querying for all databases and all query images. Note that DB_3 used HVS as the initial quantization matrix. Therefore, the images in DB_3 and the query images did not have a common $\mathbf{Q_0}$. Only the proposed scheme does not produce any false negative matches for various coding conditions.

In short, only the proposed scheme has perfect identification accuracy in all simulations.

5. CONCLUSION

Our proposed identification scheme for JPEG images uses quantization tables and the positions of zero values. It is robust against differences in coding conditions, and the features stored in the databases do not provide visual information from the original images under any coding conditions. Moreover, it does not in principle produce false negative matches. The results of simulation showed that the proposed scheme has better query performance for classification than conventional ones.

6. REFERENCES

[1] A.Viejo, J. Castellà-Roca, and G. Rufián, "Preserving the user's privacy in social networking sites," in *Trust, Privacy, and Security in Digital Business: 10th International Conference*, 2013, pp. 62–73.

[2] O. Giudice, A. Paratore, M. Moltisanti, and S. Battiato, "A classification engine for image ballistics of social data," `http://arxiv.org/abs/1610.06347`, 2016.

[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, no. 2, pp. 153–168, 2001.

[4] Z. Fan and R. L. de Queiroz, "Identification of bitmap compression history: Jpeg detection and quantizer estimation," *IEEE Trans. on Image Processing*, vol. 12, no. 2, pp. 230–235, 2003.

[5] D. Edmundson and G. Schaefer, "An overview and evaluation of jpeg compressed domain retrieval techniques," in *Proc. ELMAR-2012*, 2012, pp. 75–78.

[6] K.O. Cheng, N.F. Law, and W.C. Siu, "A fast approach for identifying similar features in retrieval of jpeg and jpeg2000 images," in *Proc. APSIPA Annual Summit and Conference*, 2009, pp. 258–261.

[7] F. Arnia, I. Iizuka, M. Fujiyoshi, and H. Kiya, "Fast and robust identification methods for jpeg images with various compression ratios," in *Proc. IEEE Int'l Conf. on Acoustics Speech and Signal Processing Proceedings*, 2006, vol. 2, pp. II–II.

[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*, 2015, pp. 38–50.

[9] T. Dobashi, O. Watanabe, T. Fukuhara, and H. Kiya, "Hash-based identification of jpeg 2000 images in encrypted domain," in *Proc. Int'l Symp. on Intelligent Signal Processing and Communications Systems*, 2012, pp. 469–472.

[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*, 2009, pp. 2065–2068.

[11] K. Iida and H. Kiya, "Secure and robust identification based on fuzzy commitment scheme for jpeg images," in *Proc. IEEE Int'l Symp. on Broadband Multimedia Systems and Broadcasting*, 2016, pp. 1–5.

[12] K.Iida and H.Kiya, "Fuzzy commitment scheme-based secure identification for jpeg images with various compression ratios," *IEICE Trans. Fundamentals*, vol. 99, no. 11, pp. 1962–1970, 2016.

[13] K. Iida, H. Kobayashi, and H. Kiya, "Secure identification based on fuzzy commitment scheme for jpeg xr images," in *Proc. EURASIP European Signal Processing Conf.*, 2016, pp. 968–972.

[14] Y. Li and P. Wang, "Robust image hashing based on low-rank and sparse decomposition," in *Proc. IEEE Int'l Conf. on Acoustics, Speech and Signal Processing*, 2016, pp. 2154–2158.

[15] Y. N. Li, P. Wang, and Y. T. Su, "Robust image hashing based on selective quaternion invariance," *IEEE Signal Processing Letters*, vol. 22, no. 12, pp. 2396–2400, 2015.

[16] Z. Tang, X. Zhang, X. Li, and S. Zhang, "Robust image hashing with ring partition and invariant vector distance," *IEEE Trans. on Information Forensics and Security*, vol. 11, no. 1, pp. 200–214, 2016.

[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*, vol. 2009, no. 1, 2009.

[18] I.Ito and H.Kiya, "A new class of image registration for guaranteeing secure data management," in *Proc. IEEE Int'l Conf. on Image Processing*, 2008, pp. 269–272.

[19] "The independent jpeg group software jpeg codec," `http://www.ijg.org/`.

[20] N. Gourier, D. Hall, and J. L Crowley, "Estimating face orientation from robust detection of salient facial structures," in *Proc. Int'l Workshop on Visual Observation of Deictic Gestures*, 2004, vol. 6.

[21] 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.