A Scrambling Method for JPEG Coded Images Enabling Image Retrieval from Scrambled Images

Ryo HOSAKA[1], Fitri Arnia[2], Masaaki FUJIYOSHI[1], and Hitoshi KIYA[1]
[1]Department of Information and Communication Systems Engineering, Tokyo Metropolitan University
6–6 Asahigaoka, Hino-shi, Tokyo 191–0065, Japan
[2]Jurusan Teknik Elektro, Universitas Syiah Kuala
JI.T. Nyak Arif, Banda Aceh, Nanggröe Aceh Darussalam 23111, Indonesia
E-mail : [1]hosaka-ryo@sd.tmu.ac.jp, [1]mfujiyoshi@m.ieice.org, [1]kiya@eei.metro-u.ac.jp

Abstract: This paper proposes a scrambling method for JPEG coded images and an image retrieval method for scrambled JPEG images. The proposed scrambling and retrieval methods utilizes the positive and negative sign of discrete cosine transformed coefficients. The proposed method scrambles a JPEG coded image without decoding the JPEG codestream. Moreover, this proposed method never changes the coding efficiency by scrambling. The proposed retrieval method compares a query image and scrambled images without descrambling and without decoding. This method is able to retrieve the same image as the query image but with the different compression ratio. Simulation results show the effectiveness of the proposed method.

1. Introduction

Nowadays, a large volume of digital images are stored whole world wide. In general, stored images are coded by image compression techniques such as JPEG (Joint Photographic Expert Group) [1]. To manage JPEG compressed images easily, many image retrieval methods has proposed [2–8]. Methods using the similarity measurement based on the positive and negative sign of discrete cosine transformed (DCT) coefficients efficiently retrieve images without decoding JPEG codestreams [6–8].

Meanwhile, a scrambling technique is often applied to stored images, in particular, medical images and camera surveillance images, for security and privacy protection [9–12]. Then, an image retrieval method for scrambled images and/or a scrambling method which does not effect conventional retrieval methods are desired.

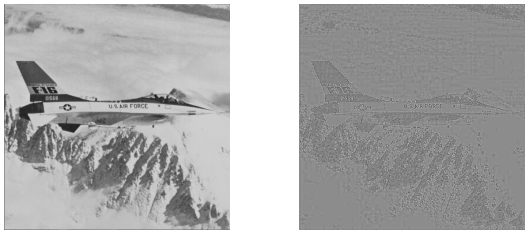
This paper proposes a method that scrambles JPEG coded images and also retrieves images from scrambled images.By using the proposed scrambling algorithm that never changes the characteristics used in the proposed retrieval method, it retrieves images from scrambled images. This method directly scrambles codestreams so that the coding efficiency never changes.

2. DCT Coefficient Signs and JPEG Codestream Structure

This section briefly describes the characteristices of DCT coefficient signs (DCS) and JPEG codestream structure.

2.1. DCT Coefficient Signs (DCS)

The DCT coefficient signs (DCS) of an image has much information of the image [6, 13, 14]. Fig. 1 shows an image and its DCS image. That is, applying the DCT to Fig. 1 (a), extracting the DCS, and applying the inverse DCT to the DCS generates Fig. 1 (b). Figure 1 shows that the DCS has much information of the original image to identify the image.



(a) Original Image. (b) DCS Image.

Figure 1. DCS Image.

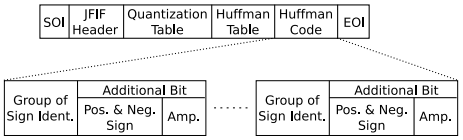


Figure 2. An example of JPEG codestream.

Furthermore, since a scalar quantization of DCT coefficients that is used in JPEG compression never inverts DCS, DCS is robust to JPEG compression. This DCS characteristics is utilized in DCS-based image retrieval methods [6–8] so that they retrieve not only images the same as the query image but also images with different compression ratio.

2.2. JPEG Codestream

The DCS's are directly obtained from a JPEG codestream without decoding the stream. Fig. 2 shows the structure of a JPEG codestream that is generated from a grayscale image and with Huffman encoder. The start of image (SOI) marker is the head of a JPEG codestream. The JPEG file interchange format (JFIF) header contains information such as the image size. The next two entities are the quantization table for scalar quantization and the Huffman table for entropy encoding. Then, the entropy-coded quantized DCT coefficients are put. The end of image (EOI) marker follows the last byte of a codestream.

An entropy code consists of a Huffman code and an additional bits. The Huffman code represents the amplitude, whereas the positive and negative sign is represented by the most significant bit of the additional bits. Thus, a DCS is di-

rectly obtained from a codestream as a bit. Moreover, a modification of an amplitude often changes the codestream length, whereas the sign modification never changes the length. The difference between DC coefficients of two consecutive DCT blocks is encoded, whereas AC coefficients are directly encoded.

3. Proposed Method

This section proposes a scrambling method for JPEG coded images and image retrieval method for scrambled JPEG coded images. Firstly, the assumptions and requirements are summarized. Secondly, two processes in the proposed method are described; the image scramble and the image retrieval. Then, the features and an application example of the proposed method are introduced.

3.1. System Description

The assumptions and requirements of the proposed method are summarized below.

1. System
   (a) A query image and images in a database have the same size.
   (b) A query image and images in a database are coded by JPEG.
2. Scrambling
   (a) All JPEG coded images in a database are scrambled.
   (b) Scrambling never affects the coding efficiency.
   (c) A scrambled codestream is losslessly descrambled to the original codestream.
3. Retrieval
   (a) Images are directly retrieved from scrambled images without descrambling.
   (b) A query codestream and codestreams in a database are never decoded.

3.2. Scrambling

This section describes the scrambling algorithm for image database $\mathbf{D}$, which contains D images composed of M of 8×8-pixels DCT blocks. Fig. 3 shows the principle of this algorithm.

1. Pseudo random matrix $\mathbf{r_D}$ is generated with $p_\mathbf{D}$ to scramble images in $\mathbf{D}$, where $p_\mathbf{D}$ is the ratio of the number of -1 to 64. That is,

$$\mathbf{r_D} = \left\{ r_\mathbf{D}(m,n) \;\middle|\; r_\mathbf{D}(m,n) \in \{-1,1\} \right\}, \quad m = 0,1,\ldots,M-1, \quad n = 0,1,\ldots,63 \tag{1}$$

2. DCS's of I_d, the d-th image in $\mathbf{D}$, are multiplied by $\mathbf{r_D}$, where $d = 0,1,\ldots,D-1$.
3. DCS's randomly inverted in Step. 2 are put back to I_d to generate its scrambled version I'_d.

Since DCS's are randomly inverted by multiplying by pseudo random matrix $\mathbf{r_D}$, decoding I'_d gives a scrambled image. This scrambling algorithm never affects the coding efficiency.

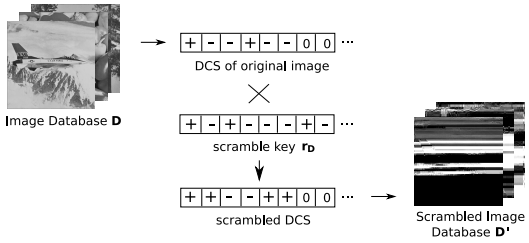


Figure 3. Proposed scrambling.

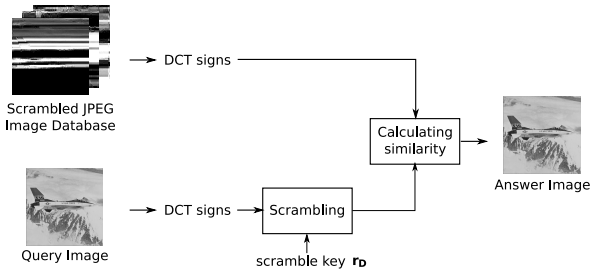


Figure 4. Proposed retrieval.

3.3. Retrieval

The proposed retrieval algorithm has three steps; 1) scrambling query image I_Q composed of M of DCT blocks, 2) calculating similarity between the query and an image of the database, and 3) returning answer images. Fig. 4 shows the principle of this retrieval algorithm.

3.3.1. Scrambling the Query Image

Query image I_Q is scrambled as following process:

1. DCS's of I_Q are multiplied by pseudo random matrix $\mathbf{r_D}$.
2. DCS's randomly inverted in Step. 1 are put back to I_Q to form its scrambled version, I'_Q.

3.3.2. Calculating Similarity

Similarity $\mu_{Q,d}$ between I'_Q, the scrambled query image, and I'_d, the d-th scrambled image in $\mathbf{D}$, is accomplished by following equations[1] [7, 8]:

$$\mu_{Q,d} = \frac{1}{M} \sum_{m=0}^{M-1} \chi_{Q,d}(m), \tag{2}$$

$$\chi_{Q,d}(m) = \frac{\sum_{n=0}^{63} s'_Q(m,n) s'_d(m,n)}{\sum_{n=0}^{63} \left| s'_Q(m,n) s'_d(m,n) \right|}, \tag{3}$$

where $s'_Q(m,n)$ and $s'_d(m,n)$ are the n-th DCS in the m-th DCT block in I'_Q and I'_d, respectively.

The denominator of $\chi_{Q,d}(m)$ in Eq. (3) represents the number of coefficients that are non-zero in both I'_Q and I'_d. The numerator of $\chi_{Q,d}(m)$ is the summation of the following; 1 for coefficients of which both I'_Q and I'_d have the same DCS, -1

[1] For similar image retrieval, the denominator in Eq. (3) is changed to $\Sigma_{n=0}^{63} \left| s'_Q(m,n) \right|$ [8].

for coefficients of which the DCS of I'_Q differs from that of I'_d, and 0 for coefficients of which I'_Q and/or I'_d are zero. $\chi_{Q,d}(m)$ reaches its maximum value one when DCS's of all non-zero coefficients in I'_Q are the same as these of I'_d.

3.3.3. Answering

The proposed retrieval algorithm returns I'_d's whose $\mu_{Q,d} = 1$ as duplicated images [7, 8]. Meanwhile, I'_d's whose $\mu_{Q,d}$ are W largest are returned as W of similar images [8]. According to the request, I'_d's to be answered are losslessly descrambled to I_d's by multiplying by $\mathbf{r_D}$.

3.4. Features

This section describes two major features of the proposed method.

3.4.1. Retrieval without Descrambling

The characteristics used for image retrieval is an special form of the DCT sign phase correlation [13, 14]. In Eq. (3), $s'_Q(m,n)s'_d(m,n)$ is given as

$$\begin{aligned} s'_Q(m,n)s'_d(m,n) &= \{s_Q(m,n)r_{\mathbf{D}}(m,n)\}\{s_d(m,n)r_{\mathbf{D}}(m,n)\} \\ &= s_Q(m,n)s_d(m,n)r^2_{\mathbf{D}}m,n. \end{aligned} \quad (4)$$

According to $r_{\mathbf{D}} \in \{-1,1\}$ in Eq (1),

$$s'_Q(m,n)s'_d(m,n) = s_Q(m,n)s_d(m,n). \quad (5)$$

That is, the proposed method never changes the characteristics for the image retrieval, whereas scrambling is applied to images. Consequently, the proposed retrieval algorithm directly acquires images from scrambled images without descrambling images.

3.4.2. Processes without Decoding

The proposed method scrambles images by the inversion of DCS and retrieves images by the DCS-based similarity measure. Since a DCS is independently encoded as a bit in a JPEG codestream, as described in Sect. 2.2, the proposed scrambling never affects the coding efficiency. Moreover, DCS's are directly obtained from a JPEG codestream without decoding, so similarity calculation in the proposed retrieval algorithm is fast.

3.5. Application Example

This section describes an example for medical systems that utilizes the above mentioned features. The proposed method improves security of such medical systems that already have access control functionalities for security.

Fig. 5 shows the system description. A medical organization has its own key to scramble medical images of patients for protecting patients' privacy. A medical worker who wants to obtain identical or similar images of a query image scrambles the query image with the key. The scrambled query image is input to the system, and the system calculates similarities between the query and database images without descrambling any image. The system gives scrambled answer images to the medical worker, and he/she descrambles the received images with the key.

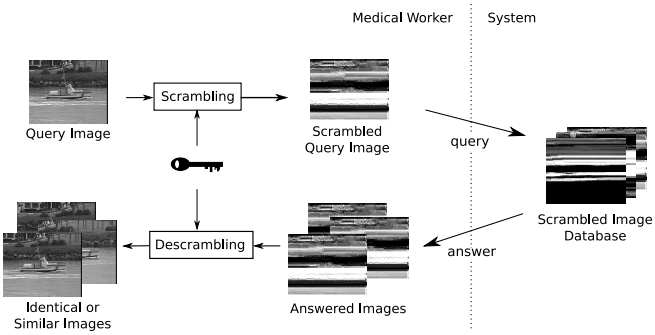


Figure 5. Application example.

Table 1. Image database **D**.

Images	grayscale, 288×352 pixels, 8 bits/pixel
image no.0–100	sequence "coastguard"
image no.101–200	sequence "container"
image no.201–300	sequence "hall monitor"
Q-factor	50 and 200
the number of images D	600

4. Experimental Results

Database **D** constructed under the conditions shown in Table 1 and query images shown in Table 2 are used for performance evaluation. Fig. 6 shows some images in **D**.

4.1. Scramble

Fig. 7 shows scrambled images with $p_{\mathbf{D}} = 0.5$. From Fig. 7, it is found that the proposed method effectively scrambles images.

4.2. Retrieval

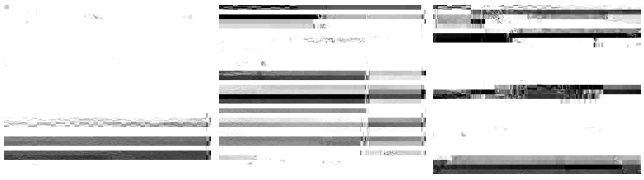
Similarities between I_{Q_1} and non-scrambled database **D** are shown in Fig. 8 with respect to each Q-factor, whereas Fig. 9 shows that for I'_{Q_1} and scrambled database. It is confirmed that the similarity used in the proposed method is independent of scrambling from Figs. 8 and 9.

Table 2. Query image I_Q.

Query image	Image (Q-factor: 50)
I_{Q_1}	frame no.30 of "coastguard"
I_{Q_2}	frame no.30 of "container"
I_{Q_3}	frame no.30 of "hall monitor"

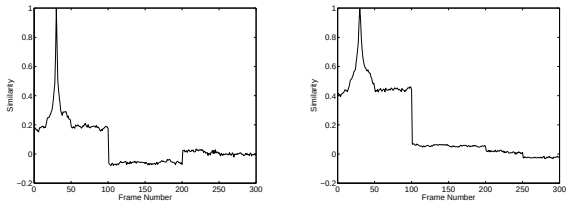
(a) coastguard. (b) container. (c) hall monitor.

Figure 6. Some images in database **D**.



(a) coastguard. (b) container. (c) hall monitor.

Figure 7. Scrambled version of Fig. 6 (DCS inversion ratio $p_{\mathbf{D}} = 0.5$).



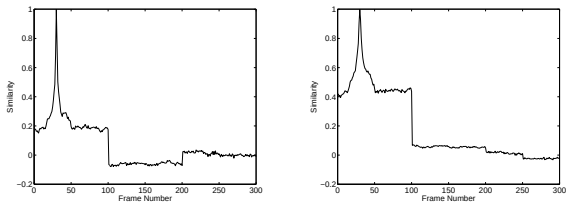
(a) Q-factor: 50. (b) Q-factor: 200.

Figure 8. Similarities $\mu_{Q,d}$'s for non-scrambled database **D**.

On the other hand, Fig. 10 shows similarities I_{Q_1} and scrambled database, with respect to each Q-factor. From Fig. 10, non-scrambled query images and scrambled query images with different $\mathbf{r_D}$ mark low similarities. Consequently, by setting adequate threshold, the proposed method is able to reject illegal search with no key and different key.

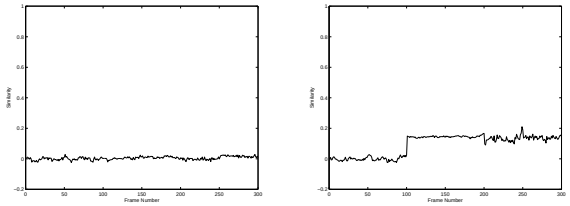
5. Conclusions

This paper has proposed a scrambling method for JPEG coded images and image retrieval from scrambled images. The proposed method utilizes DCS for both scrambling and retrieval so that it retrieves images from scrambled images without descrambling and decoding.



(a) Q-factor: 50. (b) Q-factor: 200.

Figure 9. Similarities $\mu_{Q,d}$ for scrambled database.



(a) Q-factor: 50. (b) Q-factor: 200.

Figure 10. Similarities $\mu_{Q,d}$ for non-scrambled query image and scrambled database.

References

[1] Information technology — Digital compression and coding of continuous-tone still images — Requirement and guidelines, ISO/IEC International Standard 10918-1, 1992.

[2] M. Shneier and M. Abdel-Mottaleb, "Exploiting the JPEG compression scheme for image retrieval," IEEE Trans. Pattern Anal. Mach. Intell., vol.18, no.8, pp.849–853, Aug. 1996.

[3] A.R. McIntyre and M.I. Heywood, "Exploring content-based image indexing techniques in compressed domain," Proc. IEEE Canadian Conf. Elect. & Comp. Eng., vol.2, pp.957–962, May 2002.

[4] J. Jiang, A. Armstrong, and G.C. Feng, "Web-based image indexing and retrieval in JPEG compressed domain," Multimedia Syst., vol.9, no.5, pp.424–432, Mar. 2004.

[5] C.-C. Chang, J.-C. Chuang, and Y.-S. Hu, "Retrieving digital images from JPEG compressed image database," J. Image and Vision Computing, vol.22, no.6, pp.471–484, Jun. 2004.

[6] J. Bracamonte, M. Ansorge, F. Pellandini, and P.A. Farine, "Efficient compressed domain target image search and retrieval," Proc. ACM CIVR, pp.154–163, Singapore, Jul. 2005.

[7] Fitri Arnia, I. Iizuka, M. Fujiyoshi, and H. Kiya, "Fast image identification methods for JPEG images with different compression ratios," IEICE Trans. Fundamentals, vol.E89-A, no.6, pp.1585–1593, Jun. 2006.

[8] Fitri Arnia, I. Iizuka, M. Fujiyoshi, and H. Kiya, "DCT sign-based similarity measure for JPEG image retrieval," IEICE Trans. Fundamentals, vol.E90-A, no.9, pp.1976–1985, Sept. 2007.

[9] M. Takayama, K. Tanaka, A. Yoneyama, and Y. Nakajima, "A video scrambling scheme applicable to local region without data expansion," Proc. IEEE ICME, pp.1349–1352, Toronto, Ontario, Canada, Jul. 2006.

[10] F. Dufaux and T. Ebrahimi, "Scrambling for video surveillance with privacy," Proc. IEEE Workshop PRIV, Jun. 2006.

[11] I. Kitahara, K. Kogure, and H. Hagita, "Stealth vision for protecting privacy," Proc. IAPR ICPR, pp.404–407, Cambridge, England, the U.K., Aug. 2004.

[12] K. Yabuta, H. Kitazawa, and T. Tanaka, "A new concept of real-time security camera monitoring with privacy protection by masking moving objects," Proc. IS&T/SPIE Electronic Imaging, San Jose, CA, the U.S., Jan. 2006.

[13] I. Ito and H. Kiya, "DCT sign-only correlation with application to image matching and the relationship with phase-only correlation," Proc. IEEE ICASSP, vol.I, pp.1237–1240, Apr. 2007.

[14] I. Ito, M. Fujiyoshi, and H. Kiya, "Relationship between Signs of DCT coefficients and phase-only correlation," IEICE Trans. Fundamentals, vol.J90-A, no.7, pp.567–577, Jul. 2007.