Image Identification of Grayscale-Based JPEG Images for Privacy-Preserving Photo Sharing Services

Kenta Iida* and Hitoshi Kiya*
* Tokyo Metropolitan University, 6-6, Asahigaoka, Hino-shi, Tokyo, Japan
E-mail: iida-kenta2@ed.tmu.ac.jp, kiya@tmu.ac.jp

***Abstract*—We propose an image identification scheme for double-compressed JPEG images encrypted by a grayscale-based encryption method, where the encrypted JPEG images are referred to as grayscale-based JPEG images, that has been proposed for Encryption-then-Compression (EtC) systems with JPEG compression. The proposed scheme aims to identify encrypted JPEG images that are generated from an original JPEG image. To store images without any visual sensitive information on photo sharing services, grayscale-based JPEG images are generated by using the grayscale-based encryption method. The use of the grayscale-based JPEG images and feature vectors extracted from the JPEG images allows us to identify images not only recompressed multiple times but re-encrypted with different keys. In an experiment, the proposed scheme is shown to have a high identification performance, even when images are recompressed multiple times and re-encrypted with different keys.**

I. Introduction

With the rapid growth of social networking services (SNSs) and cloud computing, photo sharing via various services has greatly increased. Generally, images are uploaded and stored in a compressed form to reduce the amount of data. In the uploading process for these SNSs, it is known that service providers employ manipulation, such as recompression [?], [?]. In addition, most of the content includes sensitive information, such as personal data and copyrights [?], [?]. Thus, it is required that images on photo-sharing services be prevented from leakage and unauthorized use by service providers.

For privacy-preserving photo sharing on these services, three requirements need to be satisfied: 1) protection of visual information, 2) tolerance for recompression after encryption, and 3) identification of encrypted images. In terms of requirement 1, a lot of studies on secure and efficient communications have been reported [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?], [?]. To secure multimedia data, full encryption with provable security, such as RSA and AES, is the most secure option. However, most schemes do not consider requirement 2, although requirement 3 is considered in several schemes [?], [?], [?], [?], [?], [?]. As systems that satisfy both requirements 1 and 2, Encryption-then-Compression (EtC) systems have been developed [?], [?], [?], [?], [?], [?], [?]. We focus on EtC systems with JPEG compression to achieve the scheme which satisfies all requirements.

The images on EtC systems are classified into two types according to whether the transform to grayscale-based images, which are images generated by the transform from RGB images with three channels to gray images with one channel, are applied before the encryption. In this paper, encrypted JPEG images generated from the grayscale-based images are referred to as “grayscale-based JPEG images”, while the others are referred to as “color-based JPEG image”. It is known that grayscale-based JPEG images are more robust against various attacks such as jigsaw puzzle solver attack than color-based ones [?], [?]. Therefore, grayscale-based JPEG images are focused on in this paper.

Regarding only requirement 3, almost schemes have never been considered for grayscale-based JPEG images, although a large number of image identification and retrieval schemes that are robust against JPEG compression have been proposed for unencrypted images [?], [?], [?], [?], [?]. Due to such a situation, the identification scheme for color-based JPEG images has been recently proposed [?]. While this scheme has a high identification performance, it is reported that the performance of other schemes is degraded in the case of identification between encrypted images and the corresponding re-encrypted images. However, the identification for grayscale-based JPEG images has never been considered.

Thus, we propose an image identification scheme for grayscale-based JPEG images compressed under various coding conditions. The proposed scheme generates grayscale-based JPEG images by using grayscale-based two-layer image encryption extended from grayscale-based image encryption method [?], [?], that enables to enhance robustness against ciphertext-only attacks. To identify these images, a feature vector robust against JPEG compression is designed for this encryption. The use of the two-layer encryption and the feature vectors allows us to identify re-encrypted images without re-calculating the feature vectors. Simulation results show that the proposed scheme has a high identification performance, even when grayscale-based JPEG images are recompressed and re-encrypted.

II. Preliminaries

A. Image Identification for JPEG Images

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 under various coding conditions. We refer to the identification of these images as "image identification". Note that the aim of the image identification is not to retrieve visually similar images.

The JPEG standard is the most widely used image compression standard, and the coding procedure for grayscale images is performed as below.

1) Divide an image into non-overlapping consecutive 8×8-blocks.
2) Apply DCT to each blocks to obtain 8×8 DCT coefficients, after all pixel values in each block are shifted from [0,255] to [-128,127] by subtracting 128.
3) Quantize DCT coefficients using a quantization matrix.
4) Entropy-code using Huffman coding.

In the compression of color-based image, color transform and sub-sampling chroma components are conducted before 1), in addition to steps mentioned above.

A DC coefficient DC in each block is obtained by using the following equation, where $I(x,y)$ represents a pixel value at the position (x,y) in a block of an image I.

$$DC = \frac{1}{8}\sum_{x=0}^{7}\sum_{y=0}^{7}(I(x,y)-128) \tag{1}$$

The range of the DC coefficients is [-1024,1016]. It has been reported that the features extracted from DC coefficients are effective for negative-positive transform, block rotation and inversion in [?], in addition to recompression in the conventional schemes [?], [?]. Therefore, the DC coefficients are also used for the identification in this paper.

B. Grayscale-based EtC Image

We focus on EtC images which have been proposed for Encryption-then-Compression (EtC) systems with JPEG compression [?], [?], [?], [?], [?], [?], [?]. EtC images have not only almost the same compression performance as that of unencrypted images, but also enough robustness against various ciphertext-only attacks including jigsaw puzzle solver attacks [?]. In this paper, images generated by the transform from RGB images with three channels to gray images with one channel, as in Fig.1, are referred to "grayscale-based images", and the images encrypted by the grayscale-based image encryption [?] are called "grayscale-based EtC images" (see Fig.2). The procedure of generating grayscale-based EtC images is conducted as below (see Figs. 1, 3 and 4) [?], [?].

1) Split an image with $X \times Y$ pixels into three color channels, and then concatenate all channels to generate a grayscale-based image with $(3 \times X) \times Y$, as shown Fig. 1.
2) Divide the grayscale-based image into into non overlapping M 8×8 blocks, where $M = \lfloor \frac{3\times X}{8} \rfloor \times \lfloor \frac{Y}{8} \rfloor$.
3) Permute randomly M divided blocks by using a random integer secret key K_1.
4) Rotate and invert randomly each divided block by using a random integer secret key K_2.
5) Apply a negative-positive transform to each divided block by using a random integer secret key K_3. In this step, transformed pixel value at the position (x,y) in a block $I_{np}(x,y)$ is computed from the pixel value at the same position $I(x,y)$ in a 8×8 block of an image applied steps from 1 to 3 by

$$I_{np}(x,y) = \begin{cases} I(x,y), & b=0, \\ 255 - I(x,y), & b=1, \end{cases} \tag{2}$$

where b is a random binary value generated by K_3 under the probability $P(b)=0.5$ and $0 \le I(x,y), I_{np}(x,y) \le 255$. Note that the value of b is assigned for each block.

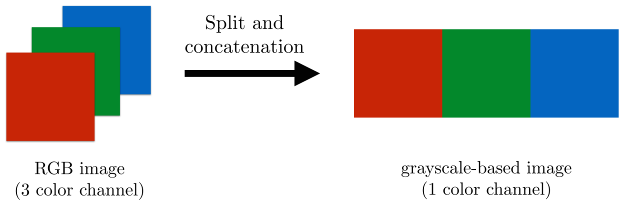


Fig. 1. Generation of grayscale-based image

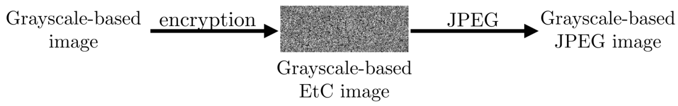


Fig. 2. Generation of grayscale-based JPEG image

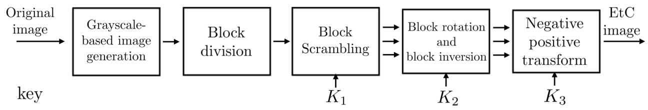


Fig. 3. Generation of grayscale-based EtC image

In this paper, the grayscale-based EtC image compressed by the JPEG standard is referred to as "grayscale-based JPEG image".

The aim of this encryption is to protect visual information of an image. The security of EtC systems has been evaluated in terms of robustness against ciphertext-only attacks including jigsaw puzzle solver attacks [?], [?], [?]. It was also confirmed from the previous researches that the grayscale-based JPEG image is more robust than the color-based one [?], [?].

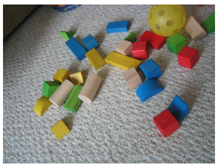
III. Proposed Scheme

In this section, a two-layer image encryption method and an identification scheme are proposed. The combination of them enables us to avoid the effects of not only recompression but also re-encryption. The notations used in the following sections are shown in Tab. I.

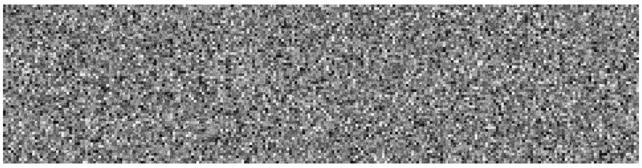
A. Two-layer Image Encryption for Image Identification

In this scheme, the permutation process is divided into two layers. Instead of step 3 in Sec. II-B, the following processes are performed in the case of applying the grayscale-based encryption.

3-1) Permute randomly M divided blocks using a random integer secret key K_0.



(a) Original image



(b) Encrypted image

Fig. 4. Example of original image and encrypted image

TABLE I
NOTATIONS USED IN THIS PAPER

O_i	ith original JPEG image
$E_i^{(j,k_0,k)}$	ith encrypted JPEG image generated from O_i with seeds k_0 and k and compressed j times (secret keys K_0 and $\mathbf{K}$ are generated from k_0 and k)
M	number of 8×8-blocks in image
$O_i(m)$	DC coefficient in mth block of image O_i $(0 \le m < M)$
$E_i^{(j,k_0,k)}(m)$	DC coefficient in mth block of image $E_i^{(j,k_0,k)}$ $(0 \le m < M)$

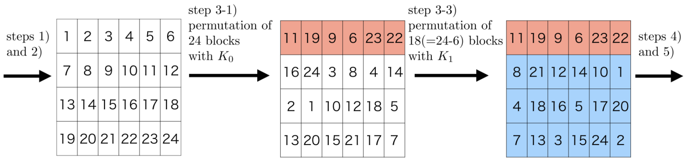


Fig. 5. Example of two-layer image encryption under $M = 24$ and $N = 6$

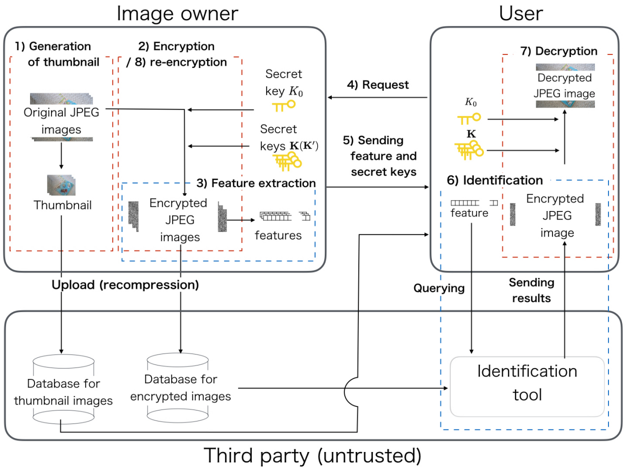


Fig. 6. Privacy-preserving photo-sharing

3-2) Select a positive integer value N.

3-3) Permute randomly the last $M - N$ blocks using a random integer secret key K_1 again.

After that, steps 4 and 5 in Sec. II-B are carried out.

An example of the encryption process under $M = 24$ and $N = 6$ is shown in Fig. 5. It can be confirmed from Fig. 5 that the first four blocks are not permuted in step 3-3 . Thus, the process in these steps does not change the positions of the first N blocks under the same K_0, even if K_1 is changed. This property plays an important role in the the proposed scheme.

B. Overview of Photo-sharing Services

So that an image owner shares JPEG images on an untrusted service without publishing the sensitive information of the original quality images, a scenario of the proposed scheme is illustrated in Fig. 6.

1) An image owner generates thumbnail JPEG images from original JPEG images, and the thumbnail images are then uploaded to a third party.
2) The image owner encrypts the original JPEG images with secret keys K_0 and $\mathbf{K} = [K_1, K_2, K_3]$ according to the two-layer image encryption. As shown in Fig. 5, the blocks of original JPEG images are permuted with the secret key K_0 , and encryption with $\mathbf{K}$ is then performed. After that, the compressed EtC images are uploaded to the third party. In this uploading process, these images may be recompressed.
3) The image owner extracts features from the encrypted JPEG images. The features are related to the uploaded thumbnail images.
4) A user selects a thumbnail image from those stored on the third party's storage, and then sends the selected images to the image owner.
5) The image owner sends the corresponding feature and the secret keys K_0 and $\mathbf{K}$ to the user.
6) The third party identifies the encrypted images corresponding to the feature received from the user, and sends the identified image to the user.
7) The user decrypts the encrypted image with K_0 and $\mathbf{K}$.
8) The image owner re-encrypts the identified image with K_0 and $\mathbf{K}' = [K_1', K_2', K_3']$ where K_1', K_2' and K_3' are different from K_1, K_2 and K_3.

Thumbnail images are not tied to corresponding encrypted images on the services because of the following two reasons. One is to prevent jigsaw solver attacks done by using visual information of a thumbnail image, which a third party uses to decrypt the corresponding encrypted image. The other is to prevent the unauthorized use of the user data. A third party makes it possible to collect the data on users, such as their preferences, from a thumbnail image corresponding to an encrypted image. Therefore, identification using encrypted images without any visual sensitive information is required for the privacy-preserving communications.

It is known that service providers usually employ manipulation such as recompression to uploaded images. Therefore, recompression is assumed in steps 1 and 2 of this scenario.

The feature used in the proposed identification scheme is designed to identify images encrypted with the different key sets $\mathbf{K}$ and $\mathbf{K}'$ under the same K_0. Thus, recalculation of features is not needed, even when images are re-encrypted.

C. Image Identification Scheme

In the proposed identification scheme, the features extracted from the first N DC coefficients in the grayscale-based images are used. The use of these features allows us to robustly identify images against recompression and re-encryption. Here, the feature extraction and the identification processes are explained.

1). Feature extraction process

In order to extract the feature vector of $E_i^{(1,k_0,k)}$, the following process is performed.

(a) Set N.
(b) Set $n := 0$.
(c) Extract the feature vector $v_{E_i^{(1,k_0,k)}}$ from the nth DC coefficient in $E_i^{(1,k_0,k)}$ as below.

$$v_{E_i^{(1,k_0,k)}}(n) = |E_i^{(1,k_0,k)}(n)|, \tag{3}$$

(d) Set $n := n + 1$. If $n < N$, return to step (c). Otherwise, the image owner halts the process for $E_i^{(1,k_0,k)}$.

In step (c), the feature vector is extracted from the the absolute values of the DC coefficients of the Y component. It is known that block rotation and inversion in the DCT domain do not change the value of the DC coefficient in each block [?]. In addition, from Eqs. (2) and (1), the absolute value of a DC coefficient is not greatly changed by a negative-positive transform as below.

$$\begin{aligned} |DC_{np}| &= |\frac{1}{8}\sum_{x=0}^{7}\sum_{y=0}^{7}((255 - I(x,y)) - 128)| \\ &= |\frac{1}{8}\sum_{x=0}^{7}\sum_{y=0}^{7}(128 - I(x,y) - 1)| \\ &= | - DC - 8|, \end{aligned} \tag{4}$$

where DC_{np} is the DC coefficient of a negative-positive transformed block. Thus, the use of DC coefficients allows us to avoid not only the effect of the recompression but also that of the encryption. In the proposed scheme, when K_0 and N are not changed, it is expected that the absolute values of DC coefficients in the first N blocks are close to those in the images encrypted with the different key sets $\mathbf{K} \neq \mathbf{K}'$. This allows us to identify re-encrypted images without re-calculating features.

2). Identification process

As shown in Fig. 6, a user obtains the feature vector corresponding to a thumbnail image $v_{E_i^{(1,k_0,k)}}$ from the image owner, and then sends the vector to the third party. The third party performs the following process to identify $E_{i'}^{(j,k_0,k')}$ with $E_i^{(1,k_0,k)}$, after extracting $v_{E_{i'}^{(j,k_0,k')}}$ from $E_{i'}^{(j,k_0,k')}$.

(a) Set N and d, where d is a parameter that determines the acceptance error.

(a) No.000 (b) No.001 (c) No.004 (d) No.005

Fig. 7. Examples of images in UKbench

(b) Set $n := 0$ and $i' = 0$.
(c) If $|v_{E_i^{(1,k_0,k)}}(n) - v_{E_{i'}^{(j,k_0,k')}}(n)| \le d$, proceed to step (d). Otherwise, the third party judges that $E_{i'}^{(j,k_0,k')}$ is not generated from O_i and proceed to step (e).
(d) Set $n := n + 1$. If $n < N$, return to step (c). Otherwise, the third party judges that $E_{i'}^{(j,k_0,k')}$ is generated from the same original image as that of $E_i^{(1,k_0,k)}$, i.e., O_i and the process for $E_i^{(1,k_0,k)}$ is halted.
(e) Set $i' := i' + 1$ and $n := 0$. If i' is not equal to the number of images stored in the database of the third party, return to step (c). Otherwise, third party judges that there is no image corresponding to $E_i^{(1,k_0,k)}$.

The distance between the absolute values of the features is used for identification under the acceptance error d in step (c). As well as the conventional schemes, this value was experimentally determined in a pre-experiment.

The use of grayscale-based JPEG images allows us to take the following advantages.

- To improve identification performance
  The selection of larger values as N allows us to improve the identification performance because step (c) is performed at more positions.
- To avoid limitation regarding color sub-sampling
  In terms of compression performances and image quality of decoded images, no color sub-sampling is required in the compression for color-based images not only by an image owner but by a third party. On the other hand, there is no limitation regarding color sub-sampling in the case of grayscale-based JPEG images.
- To enhance robustness against ciphertext-only attacks
  As mentioned in Sec. II-B, the use of grayscale-based JPEG images enables to enhance the security against ciphertext-only attacks.

IV. Simulation

A number of simulations were conducted to evaluate the performance of the proposed identification scheme. We used images (size of 480×640) in UKbench dataset [?] and an encoder and a decoder from the IJG (Independent JPEG Group) [?] in the simulations. The dataset consists of 10,200 images (4 images per 2,520 objects), and 500 images from No.000 to No.499 were chosen from the 10,200 images (see Fig. 7).

A. Simulation Conditions

Table II summarizes the conditions for generating original JPEG images and encrypted ones, where QF_I indi-

TABLE II
CONDITION TO GENERATE ORIGINAL AND ENCRYPTED JPEG IMAGES, WHERE QF_I INDICATES THE QUALITY FACTOR GENERATED FOR THE JPEG IMAGE I, $I \in \{O_i, E_i^{(1,k_0,k)}, E_i^{(1,k_0,k')}, E_i^{(2,k_0,k)}, E_i^{(2,k_0,k')}\}$.

Condition	$QF_{O_i} =$	$QF_{E_i^{(1,k_0,k)}} =$ $QF_{E_i^{(1,k_0,k')}} =$	$QF_{E_i^{(2,k_0,k)}} =$ $QF_{E_i^{(2,k_0,k')}} =$
(1)	95	95	85,80,75,70
(2)	85	85	
(3)	75	75	

cates the quality factor used for JPEG image I, $I \in \{O_i, E_i^{(1,k_0,k)}, E_i^{(1,k_0,k')}, E_i^{(2,k_0,k)}, E_i^{(2,k_0,k')}\}$. For instance, in the case of condition (1), 500 original JPEG images were generated with $QF_{O_i} = 95$ from the 500 UKbench images first. To generate $E_i^{(1,k_0,k)}$, the 500 original JPEG images were encrypted by grayscale-based method and compressed with $QF_{E_i^{(1,k_0,k)}} = 95$. Next, these 500 single-compressed encrypted images were recompressed with $QF_{E_i^{(2,k_0,k')}} = 85, 80, 75, 70$. As a result, 500 single-compressed and 2,000 double-compressed images encrypted with k were generated under each condition. As well as the generation of images encrypted with k, there were 500 single-compressed and 2,000 double-compressed JPEG images encrypted with k', $QF_{E_i^{(1,k_0,k')}} = 95$ and $QF_{E_i^{(2,k_0,k')}} = 85, 80, 75, 70$. In the simulations, the identification performances between 500 single-compressed and 2,000 double-compressed images encrypted with k were evaluated for each condition first. Also, identification between 500 single-compressed images with k and 2,000 double-compressed ones with k' was performed.

As the parameters, $N = 1440$ and $d = 150$ were selected. The grayscale-based images were divided into 14400 8×8 blocks, i.e. $M = 14400$, so that $N = 1440$ was selected as 10% of all blocks. To determine d, identification between images generated under condition (2) and $k \neq k'$ from 885 UCID images [?] was carried out. As one of the best choices, $d = 150$ was selected.

The proposed scheme was compared with four identification schemes (DC signs-based [?], sparse coding-based [?], quaternion-based [?], and iterative quantization (ITQ)-based ones [?]). In the schemes [?], [?], [?], the Hamming distances between the hash values of the encrypted images were calculated, and images that had the smallest distance were then chosen as images generated from an original image after all images were decompressed.

B. Identification Performance

Table III shows Precision value p and Recall value r,where "-" means that the scheme can not be applied. p and r are defined by

$$p = \frac{TP}{TP+FP}, \; r = \frac{TP}{TP+FN}, \quad (5)$$

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

TABLE III
IDENTIFICATION PERFORMANCE FOR DOUBLE-COMPRESSED ENCRYPTED IMAGES, WHERE "-" MEANS THAT THE SCHEME CAN NOT BE APPLIED.

scheme	condition	$k = k'$		$k \neq k'$	
		$p[\%]$	$r[\%]$	$p[\%]$	$r[\%]$
proposed ($d = 150$)	(1)	100	100	100	100
	(2)	100	100	100	100
	(3)	100	100	100	100
DC sign [?]	(1)	100	100	0	0
	(2)	100	100	0	0
	(3)	100	100	0	0
ITQ [?]	(1)	100	100	21.30	21.30
	(2)	100	100	24.00	24.00
	(3)	100	100	23.35	23.35
Sparse coding [?]	(1)	99.70	99.90	0.27	0.50
	(2)	99.85	99.95	0.29	0.50
	(3)	99.80	99.90	0.14	0.25
Quaternion [?]	(1)	-	-	-	-
	(2)	-	-	-	-
	(3)	-	-	-	-

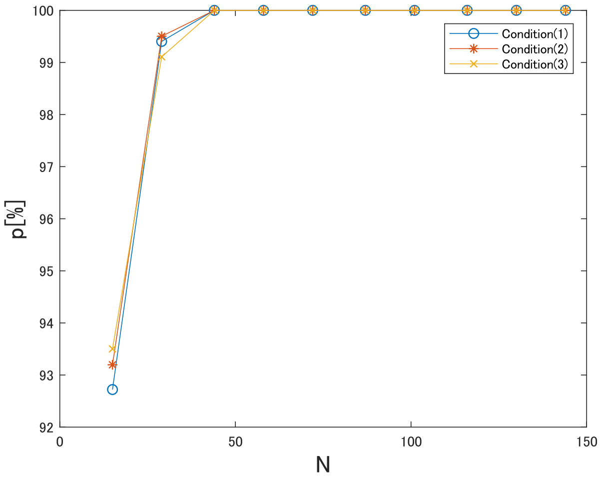


Fig. 8. Precision values under $15 \leq N \leq 144$ and $k \neq k'$

It was confirmed that all schemes had high identification performances under $k = k'$, except for quaternion-based scheme [?] because only color images are targeted in the scheme. However, only the proposed scheme achieved $r = 100\%$ and $p = 100\%$ under all conditions with $k \neq k'$; the other schemes did not.

Additionally, we confirmed the identification performances in the case that the value of N was changed. Figures 8 and 9 show that $r = 100\%$ and $p = 100\%$ was achieved under all conditions when $N \geq 44$ This means that the perfect performances were achieved, while about 99.7% in all blocks were permuted in the step 3-3).

Therefore, the proposed scheme enables to achieve a high identification performance, even when almost blocks are re-permuted.

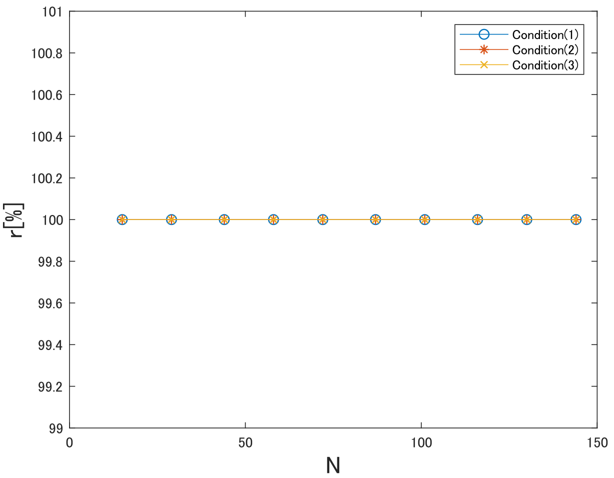


Fig. 9. Recall values under $15 \leq N \leq 144$ and $k \neq k'$

V. Conclusion

In this paper, an identification scheme for grayscale-based JPEG images was proposed. To generate grayscale-based JPEG images, images are encrypted by grayscale-based image encryption and compressed by the JPEG standard. In the encryption process, a two-layer block permutation operation is performed for the identification. The feature vector used in the proposed scheme is extracted from the DC coefficients of each block in the grayscale-based JPEG images. The use of the grayscale-based JPEG images and the feature vectors allows us to avoid not only the effect of recompression but also that of re-encryption with different keys. Simulation results showed the effectiveness of the proposed scheme, even when images were recompressed and re-encrypted by different keys for the second layer.

Acknowledgements

This work was partially supported by Grant-in-Aid for Scientic Research(B), No.17H03267, from the Japan Society for the Promotion Science.

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, 2017.

[2] T. Chuman, K. Iida, W. Sirichotedumrong, and H. Kiya, "Image manipulation specifications on social networking services for encryption-then-compression systems," *IEICE Trans. on Info. and Sys.*, vol. 102, no. 1, pp. 11–18, 2019.

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

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

[5] V. Itier, P. Puteaux, and W. Puech, "Recompression of jpeg crypto-compressed images without a key," *IEEE Trans. on Circuits and Systems for Video Technology,* https://www.doi.org/10.1109/TCSVT.2019.2894520, 2019.

[6] J. Zhou, X. Liu, O. C. Au, and Y. Y. Tang, "Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation.," *IEEE Trans. information forensics and security*, vol. 9, no. 1, pp. 39–50, 2014.

[7] T. Chuman, W. Sirichotedumrong, and H. Kiya, "Encryption-then-compression systems using grayscale-based image encryption for jpeg images," *IEEE Trans. on Information Forensics and Security*, vol. 14, no. 6, pp. 1515–1525, 2019.

[8] T. Chuman and H. Kiya, "Security evaluation for block scrambling-based image encryption including jpeg distortion against jigsaw puzzle solver attacks," *IEICE Trans. Fundamentals*, vol. E101-A, no. 12, pp. 2405–2408, 2018.

[9] W. Sirichotedumrong and H. Kiya, "Grayscale-based block scrambling image encryption using ycbcr color space for encryption-then-compression systems," *APSIPA Trans. on Signal and Information Processing, e7*, vol. 8, 2019.

[10] K. Kurihara, M. Kikuchi, S. Imaizumi, S. Shiota, and H. Kiya, "An encryption-then-compression system for jpeg/motion jpeg standard," *IEICE Trans. Fundamentals.*, vol. 98, no. 11, pp. 2238–2245, 2015.

[11] K. Kurihara, S. Shiota, and H. Kiya, "An encryption-then-compression system for jpeg standard," in *Proc. Picture Coding Symposium*, 2015, pp. 119–123.

[12] K. Iida and H. Kiya, "An image identification scheme of encrypted jpeg images for privacy-preserving photo sharing services," in *Proc. IEEE Int'l Conf. on Image Processing*, 2019 (to be published). [Online]. Available: https://arxiv.org/abs/1905.03025.

[13] K. Munadi, F. Arnia, M. Syaryadhi, and H. Kiya, "A content-based image retrieval system for visually protected image databases," in *Proc. IEEE Asia Pacific Conference on Multimedia and Broadcasting*, 2015, pp. 1–6.

[14] M.R. Ra, R. Govindan, and A. Ortega, "P3: Toward privacy-preserving photo sharing," in *Proc. USENIX Symposium on Networked Systems Design and Implementation*, 2013, vol. 13, pp. 515–528.

[15] A.A.A.M. Kamal, K. Iwamura, and H. Kang, "Searchable encryption of image based on secret sharing scheme," in *Proc. APSIPA Annual Summit and Conference*, 2017, pp. 1495–1503.

[16] H. Cheng, X. Zhang, and J. Yu, "Ac-coefficient histogram-based retrieval for encrypted jpeg images," *Springer Multimedia Tools and Applications*, vol. 75, no. 21, pp. 13791–13803, 2016.

[17] Y. Xu, J. Gong, L. Xiong, Z. Xu, J. Wang, and Y. Shi, "A privacy-preserving content-based image retrieval method in cloud environment," *Elsevier Journal of Visual Communication and Image Representation*, vol. 43, pp. 164–172, 2017.

[18] H. Cheng, X. Zhang, J. Yu, and F. Li, "Markov process-based retrieval for encrypted jpeg images," *EURASIP Journal on Information Security*, vol. 2016, no. 1, pp. 1, 2016.

[19] Z. Xia, N. N. Xiong, A.V. Vasilakos, and X. Sun, "Epcbir: An efficient and privacy-preserving content-based image retrieval scheme in cloud computing," *Elsevier Information Sciences*, vol. 387, pp. 195–204, 2017.

[20] K. Iida and H. Kiya, "Robust image identification with dc coefficients for double-compressed jpeg images," *IEICE Trans. on Info. and Sys.*, vol. 102, no. 1, pp. 2–10, 2019.

[21] K. Iida and H. Kiya, "Robust image identification for double-compressed and resized jpeg images," in *Proc. APSIPA Annual Summit and Conference*, 2018, pp. 1968–1974.

[22] 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.

[23] 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.

[24] Y. Gong, S.Lazebnik, A. Gordo, and F. Perronnin, "Iterative quantization: A procrustean approach to learning binary codes for large-scale image retrieval," *IEEE Trans. on Pattern Analysis and Machine Intelligence*, vol. 35, no. 12, pp. 2916–2929, 2013.

[25] R. L. De Queiroz, "Processing jpeg-compressed images and documents," *IEEE Trans. on Image Processing*, vol. 7, no. 12, pp. 1661–1672, 1998.

[26] "Ukbench dataset," https://archive.org/details/ukbench.

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

[28] G. Schaefer and M. Stich, "Ucid: An uncompressed color image database," in *Electronic Imaging 2004*, 2003, pp. 472–480.