SIP (2019), vol. 8, e7, page 1 of 15 © The Authors, 2019.

doi:10.1017/ATSIP.2018.33

ORIGINAL PAPER

Grayscale-based block scrambling image encryption using YCbCr color space for encryption-then-compression systems

WARIT SIRICHOTEDUMRONG AND HITOSHI KIYA

A novel grayscale-based block scrambling image encryption scheme is presented not only to enhance security, but also to improve the compression performance for Encryption-then-Compression (EtC) systems with JPEG compression, which are used to securely transmit images through an untrusted channel provider. The proposed scheme enables the use of a smaller block size and a larger number of blocks than the color-based image encryption scheme. Images encrypted using the proposed scheme include less color information due to the use of grayscale images even when the original image has three color channels. These features enhance security against various attacks, such as jigsaw puzzle solver and brute-force attacks. Moreover, generating the grayscale-based images from a full-color image in YCbCr color space allows the use of color sub-sampling operation, which can provide the higher compression performance than the conventional grayscale-based encryption scheme, although the encrypted images have no color information. In an experiment, encrypted images were uploaded to and then downloaded from Twitter and Facebook, and the results demonstrated that the proposed scheme is effective for EtC systems and enhances the compression performance, while maintaining the security against brute-force and jigsaw puzzle solver attacks.

Keywords: Image encryption, Jigsaw puzzle, EtC system, JPEG

Received 29 August 2018; Revised 18 December 2018

I. INTRODUCTION

The use of images and video sequences has greatly increased because of the rapid growth of the Internet and widespread use of multimedia systems. While many studies on secure, efficient, and flexible communications have been reported [1–4], full encryption with provable security (like RSA and AES) is the most secure option for securing multimedia data. However, there is a trade-off between security and other requirements such as low processing demand, bitstream compliance, and signal processing in the encrypted domain. Several perceptual encryption schemes have been developed to achieve these trade-offs [5–11].

Image encryption prior to image compression is required in certain practical scenarios such as secure image transmission through an untrusted channel provider. Encryption-then-Compression (EtC) systems [3, 12–21] are used in such scenarios. In this paper, we focus on EtC systems with JPEG compression although the traditional way of securely transmitting images is to use a Compression-then-Encryption (CtE) system. Since most studies on EtC systems assumed the use of a proprietary compression scheme incompatible with international compression standards such as JPEG [3, 14, 15, 22–24], block scrambling-based image encryption schemes, which are compatible with international standards, have been proposed for EtC systems [16–21].

A lot of image encryption methods [3, 11–26] have been proposed for securing image data. However, some of them do not consider the compression to the encryption schemes. A hybrid compression–encryption algorithm [11] has been proposed to jointly consider both compression and encryption. In this algorithm, an image is compressed and encrypted at the same time. Moreover, various compression-friendly algorithms [3, 11–13, 25, 26] have been studied although they do not consider applying them to applications with JPEG compression, such as Social Network Services (SNS) and Cloud Photo Storage Services (CPSS). In [3, 14, 15], the compression methods for EtC systems have been proposed, but they are not applicable to EtC systems with JPEG compression. Therefore, the works [16–21] only focus on EtC systems with JPEG compression.

In this paper, we present a novel grayscale-based image encryption scheme for EtC systems that enhances security compared with the conventional color-based scheme [16–19]. A grayscale image is an image with a range of shades of gray without color information, where the

Tokyo Metropolitan University, 6-6 Asahigaoka, Hino-shi, Tokyo, 191-0065, Japan

Corresponding author:
Hitoshi Kiya
Email: kiya@tmu.ac.jp

darkest possible shade is black, and the lightest possible shade is white. In contrast, a grayscale-based image is artificially generated from three color channels of a color image, and pixels in the image have color information. Therefore, the original color image can be reconstructed from the grayscale-based image. Although the conventional grayscale-based image encryption scheme [20, 21] , which is an extension of the color-based EtC systems [15–19], has been proposed to enhance the robustness against several attacks, such as brute-force and jigsaw puzzle solver attacks [27–29], and also avoid the effect of color subsampling, the compression performance is degraded compared with the color-based image encryption scheme [15–19]. This is because a grayscale-based image is generated from RGB components of a full-color image, so the correlation between RGB color channels is not used.

Consequently, we aim to propose a novel grayscale-based encryption scheme that has almost the same compression performance as non-encrypted images as well as the color-based scheme. We also consider a JPEG quantization table which is especially designed for grayscale-based images. We evaluated the performance of the proposed scheme in terms of the compression performance and security. The results showed that the proposed scheme has almost the same compression performance as the color-based scheme while having almost the same robustness against ciphertext-only attacks as the conventional grayscale-based encryption.

The rest of paper is organized as follows. Section II provides a review of the color-based and conventional grayscale-based image encryption schemes used in EtC systems. Section III presents the proposed grayscale-based image encryption and the new quantization table for grayscale-based images. Extensive experimental results including the compression performance and robustness against jigsaw puzzle solver attacks are given in Section IV. Concluding remarks are in Section V.

II. RELATED WORKS

In this section, the color-based block scrambling image encryption scheme [15–19] and the conventional grayscale-based image encryption scheme [20] are summarized. Moreover, the security of both schemes is described.

A) Image encryption for EtC systems

Block scrambling-based image encryption schemes [15–20] were proposed for EtC systems, in which a user wants to securely transmit an image I to an audience or a client via, SNS or CPSS providers, as shown in Fig. 1. The privacy of the image to be shared can be controlled by the user unless the user does not give the secret key K to the providers, although the image is generally recompressed by the providers. In contrast, in CtE systems, the disclosure of non-encrypted images is required before the recompression.

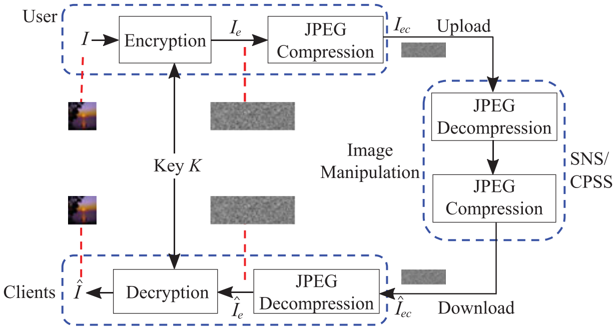


Fig. 1. EtC system.

B) Color-based image encryption

In the previous works [15–19], a full-color image (I_{RGB}) with $X \times Y$ pixels is divided into non-overlapping blocks each with $B_x \times B_y$; then four block scrambling-based encryption steps are applied to the divided blocks as follows (see Fig. 2).

1) Randomly permute the divided blocks by using a random integer generated by a secret key K_1.
2) Rotate and invert each block randomly (see Fig. 3) by using a random integer generated by a key K_2.
3) Apply negative–positive transformation to each block by using a random binary integer generated by a key K_3, where K_3 is commonly used for all color components. In this step, a transformed pixel value in the i-th block B_i, p', is calculated using

$$p' = \begin{cases} p & (r(i) = 0) \\ p \oplus (2^L - 1) & (r(i) = 1) \end{cases}, \qquad (1)$$

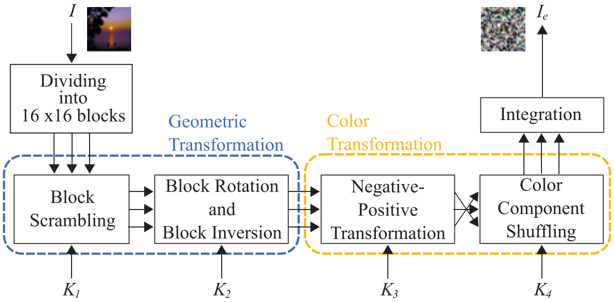
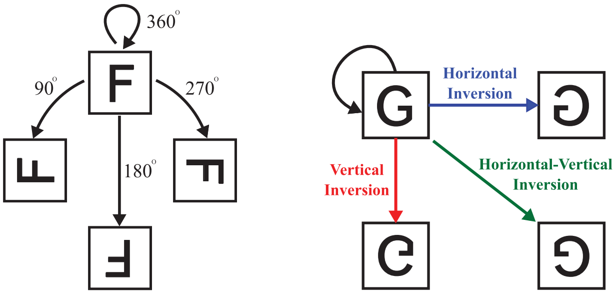

I
Dividing into 16 x16 blocks
Geometric Transformation
Color Transformation
I_e
Integration
Block Scrambling
Block Rotation and Block Inversion
Negative-Positive Transformation
Color Component Shuffling
K_1
K_2
K_3
K_4

Fig. 2. Color-based block scrambling image encryption.



(a) Block rotation (b) Block inversion

Fig. 3. Block rotation and inversion. (a) Block rotation, (b) block inversion

Table 1. Permutation of color components for a random integer. For example, if the random integer is equal to 2, the red component is replaced by the green one, and the green component is replaced by the red one while the blue component is not replaced.

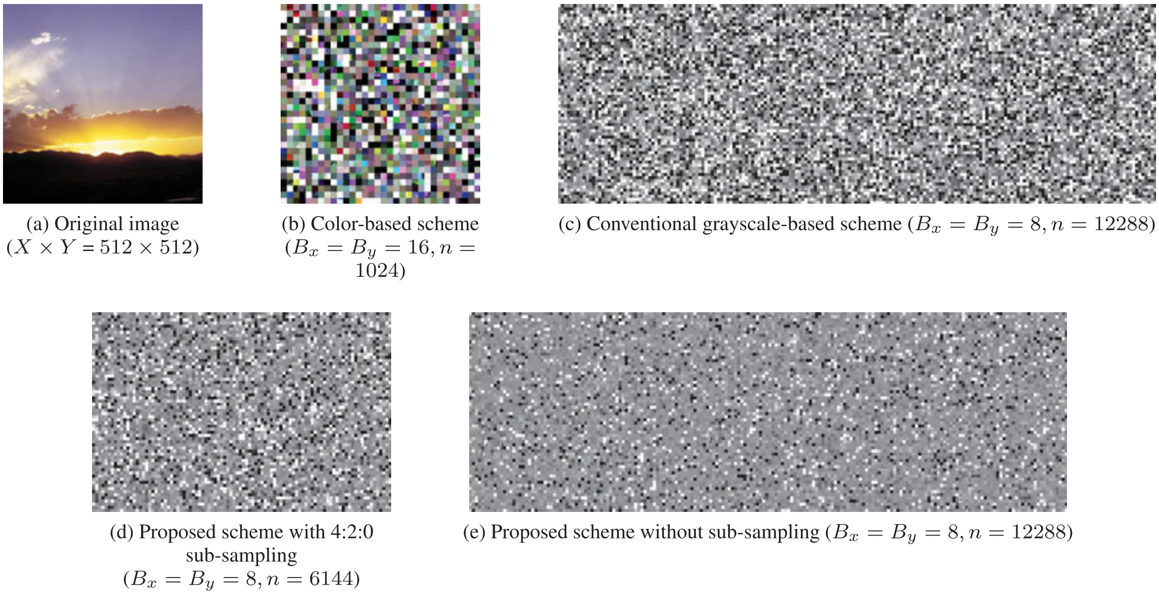
	Three color channels		
Random integer	R	G	B
0	R	G	B
1	R	B	G
2	G	R	B
3	G	B	R
4	B	R	G
5	B	G	R

where $r(i)$ is a random binary integer generated by K_3, $p \in B_i$ is the pixel value of the original image with L bit per pixel, and $\oplus$ is the bitwise exclusive-or operation. The value of occurence probability $P(r(i)) = 0.5$ is used to invert bits randomly.

4) Shuffle three color components in each block by using an integer randomly selected from six integers generated by a key K_4 as shown in Table 1.

An example of an encrypted image with $B_x = B_y = 16$ is shown in Fig. 4(b) where Fig. 4(a) is the original one.

Although images encrypted by using the color-based image encryption scheme are compatible with the JPEG standard and have almost the same compression performance as non-encrypted ones when using $B_x = B_y = 16$, there is a limitation that the scheme cannot achieve. The possible smallest block size of the scheme is 16 × 16 to avoid the effect of color sub-sampling. As shown in Fig. 5, if 4:2:0 color sub-sampling is applied to an encrypted image, each 8 × 8-block in the sub-sampled chroma components consists of four 4 × 4-blocks from different 8 × 8-block, which have low correlation among the blocks. As a result, block distortion is generated due to the interpolation of the sub-sampled chroma components with discontinuous pixel values. An example of the decrypted images including block distortion, where the JPEG quality factor (Q_{f_u}) of uploaded images was equal to 100, is shown in Fig. 6. If the block size is smaller than 16 × 16 pixels, such as 8 × 8 pixels, the compression performance decreases and some block distortion is generated. This is because when color sub-sampling is applied to the chroma components (C_b and C_r) of a color image in a JPEG encoder, the interpolation is carried out to the sub-sampled chroma components (C_b' and C_r') to reconstruct the spatial resolution as that of the original image in a decoder.


(a) Original image ($X \times Y = 512 \times 512$)

(b) Color-based scheme ($B_x = B_y = 16, n = 1024$)

(c) Conventional grayscale-based scheme ($B_x = B_y = 8, n = 12288$)

(d) Proposed scheme with 4:2:0 sub-sampling ($B_x = B_y = 8, n = 6144$)

(e) Proposed scheme without sub-sampling ($B_x = B_y = 8, n = 12288$)

Fig. 4. Examples of images encrypted by using the color-based, conventional grayscale-based, and proposed schemes. n is the number of divided blocks. (a) Original image ($X \times Y = 512 \times 512$), (b) color-based scheme ($B_x = B_y = 16, n = 1024$), (c) conventional grayscale-based scheme ($B_x = B_y = 8, n = 12288$), (d) proposed scheme with 4:2:0 sub-sampling ($B_x = B_y = 8, n = 6144$), (e) proposed scheme without sub-sampling ($B_x = B_y = 8, n = 12288$).

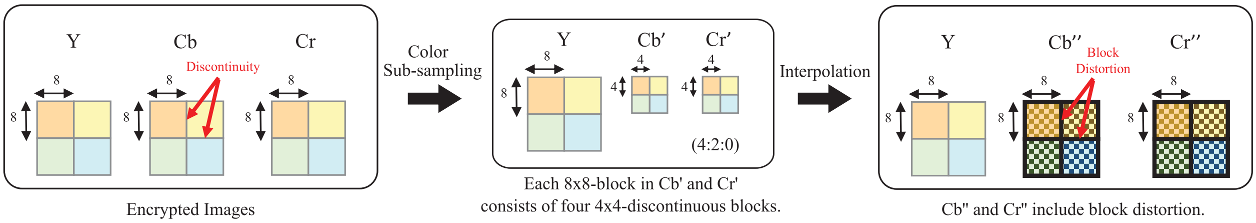
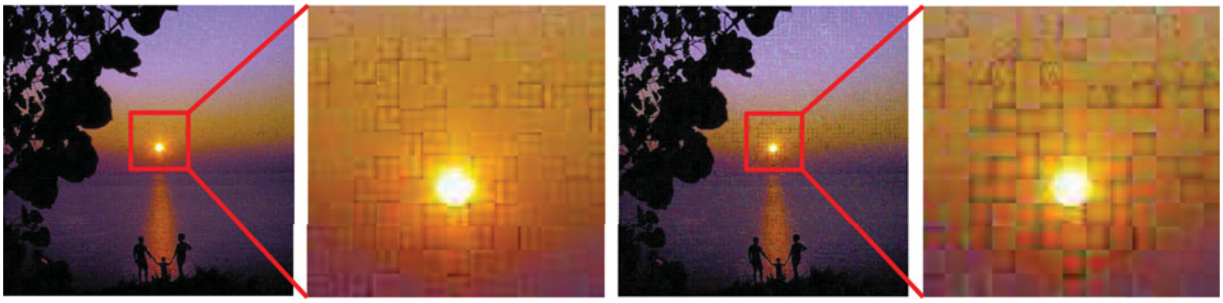

Y
Cb
Cr
8
8
Discontinuity
Encrypted Images
Color Sub-sampling
Y
Cb′
Cr′
8
4
(4:2:0)
Each 8x8-block in Cb' and Cr' consists of four 4x4-discontinuous blocks.
Interpolation
Y
Cb″
Block Distortion
Cr″
8
Cb" and Cr" include block distortion.

Fig. 5. Sub-sampling in JPEG encoder and interpolation of chroma components in JPEG decoder.



(a) Downloaded from Twitter (PSNR=29.44dB)

(b) Downloaded from Facebook (PSNR=26.93dB)

Fig. 6. Example of the decrypted images with the color-based scheme including block distortion ($B_x = B_y = 8, Q_{f_u} = 100$, and 4:2:0 sub-sampling). (a) Downloaded from Twitter (PSNR=29.44dB), (b) downloaded from Facebook (PSNR = 26.93 dB).

C) Grayscale-based image encryption

A conventional grayscale-based image encryption has been proposed to avoid the effect of color sub-sampling by encrypting I_{RGB} into the encrypted image (I_e) which consists of only one color channel [20]. In order to generate I_e, four processing steps are carried out as follows (see Fig. 7).

1) Split I_{RGB} into three RGB channels, i_R, i_G, and i_B and concatenate all channels to generate a conventional grayscale-based image (I_g^{RGB}) with $3(X \times Y)$ pixels as shown in Fig. 8.
2) Divide I_g^{RGB} into blocks each with $B_x \times B_y$ and then randomly permute the divided blocks by using a random integer generated by a secret key K_1.
3) Rotate and invert each block randomly by using a random integer generated by a key K_2.
4) Apply negative–positive transformation to each block by using a random binary integer generated by a key K_3. This step is carried out by using the same process as Step 3 of the color-based image encryption in Section II.B.

Since images encrypted by using the grayscale-based image encryption contain only one color channel, the encrypted images can avoid the effect of color sub-sampling. Therefore, the scheme allows us to use 8×8 as the block size, which is smaller than that with the color-based one, as shown in Fig. 4(c). Moreover, the number of blocks is larger because the block size is smaller, and the number of pixels of encrypted images is larger. As a result, the scheme enhances the security against various attacks [20] and also provides the robustness against color sub-sampling due to the use of grayscale-based images. However, the compression performance of the conventional grayscale-based scheme decreases, because the correlation between RGB color channels is not used.

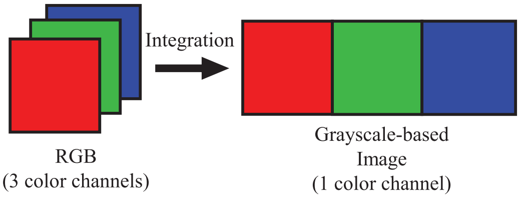


Fig. 8. Conventional grayscale-based image generation.

D) Security against ciphertext-only attacks

Security mostly refers to protection from adversarial forces. The proposed scheme aims to protect the visual information which allow us to identify an individual, a time, and the location of the taken photograph. Untrusted providers and unauthorized users are assumed as the adversary. This paper considers both brute-force and jigsaw puzzle solver attacks as ciphertext-only attacks.

1) Brute-force attack

In the conventional color-based encryption scheme, if an image with $X \times Y$ pixels is divided into blocks with $B_x \times B_y$ pixels, the number of blocks n is given by

$$n = \left\lfloor \frac{X}{B_x} \right\rfloor \times \left\lfloor \frac{Y}{B_y} \right\rfloor, \tag{2}$$

where $\lfloor \cdot \rfloor$ is a function that rounds down to the nearest integer. The four block scrambling-based processing steps are then applied to the divided image.

The key space of the block scrambling (Step 1) $N_{scr}(n)$, which is the number of permutation of n blocks, is given by

$$N_{scr}(n) = {}_nP_n = n!. \tag{3}$$

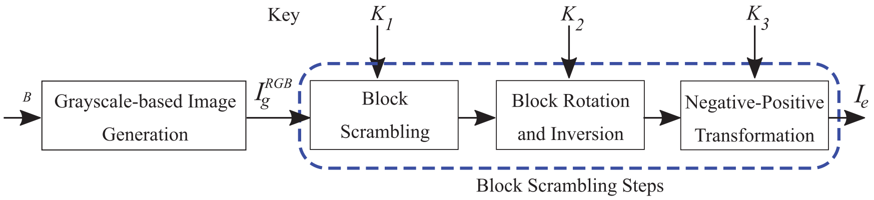

Key
K_1
K_2
K_3
B
Grayscale-based Image Generation
I_g^{RGB}
Block Scrambling
Block Rotation and Inversion
Negative-Positive Transformation
I_e
Block Scrambling Steps

Fig. 7. Conventional grayscale-based encryption.

Similarly, the key spaces of other encryption steps are given as

$$N_{rot}(n) = 4^n,\ N_{inv}(n) = 4^n,\ N_{rot\&inv}(n) = 8^n \tag{4}$$

$$N_{np}(n) = 2^n,\ N_{col}(n) = \left({}_3P_3\right)^n = 6^n \tag{5}$$

where $N_{rot}(n)$ and $N_{inv}(n)$ are the key spaces of the block rotation and block inversion, and $N_{rot\&inv}(n)$ is the key space of the encryption combining them (Step 2). Note that $N_{rot\&inv}$ is the key space considering the collision between block rotation and inversion. Namely, rotating pieces 180 degrees is the same operation as inverting them horizontally and vertically. $N_{np}(n)$ and $N_{col}(n)$ are the key spaces of the negative–positive transformation (Step3) and color component shuffling (Step 4), respectively. Consequently, the key space of images encrypted by using all the proposed encryption steps, $N_A(n)$, is represented by

$$\begin{aligned} N_A(n) &= N_{scr}(n) \cdot N_{rot\&inv}(n) \cdot N_{np}(n) \cdot N_{col}(n) \\ &= n! \cdot 8^n \cdot 2^n \cdot 6^n. \end{aligned} \tag{6}$$

In comparison, since an image encrypted by using the conventional grayscale-based image encryption scheme is generated from I_g^{RGB} with $3(X \times Y)$ pixels, the number of blocks of the grayscale-based scheme (n_g) is three times larger than that of the color-based scheme. n_g is given by

$$n_g = 3n. \tag{7}$$

Unlike the color-based scheme, color shuffling is not carried out by the conventional grayscale-based encryption scheme. Thus, the key space of the grayscale-based image encryption is calculated by

$$\begin{aligned} N_B(n) &= N_{scr}(3n) \cdot N_{rot\&inv}(3n) \cdot N_{np}(3n) \\ &= 3n! \cdot 8^{3n} \cdot 2^{3n} \gg N_A(n), \end{aligned} \tag{8}$$

where n is the number of blocks calculated from I with $X \times Y$ pixels in accordance with equation (2). Although the color shuffling is not applied to the scheme, the number of blocks is larger, as shown in equation (8). Therefore, the grayscale-based image encryption enhances the robustness against brute-force attacks.

2) Jigsaw puzzle solver attack

The extended jigsaw puzzle solvers for block scrambling-based image encryption [27–29] have been proposed to assemble encrypted images including rotated, inverted, negative–positive transformed, color component shuffled blocks. It has been shown that assembling encrypted images becomes difficult when the encrypted images are under the following conditions [27–30].

- Number of blocks is large.
- Block size is small.
- Encrypted images include JPEG distortion.
- Encrypted images have less color information.

Since most conventional jigsaw puzzle solvers utilize color information to assemble puzzles, reducing the number of color channels in each pixel makes assembling encrypted images much more difficult. Thus, the grayscale-based encryption scheme has a higher security level than that of the color-based scheme because it provides a large number of blocks, the small block size, and less color information.

III. PROPOSED GRAYSCALE-BASED ENCRYPTION

In this section, we present a new grayscale-based block scrambling image encryption using YCbCr color space which aims not only to enhance security, but also to improve the compression performance of encrypted images.

A) Image encryption procedure

To generate an encrypted image (I_e), the following steps are carried out (see Fig. 9).

1) Transform an RGB color image (I_{RGB}) with $X \times Y$ pixels into an image in YCbCr color space (I_{YCbCr}) as in [31]. Note that I_{YCbCr} consists of three individual channels which can be represented by i_Y, i_{Cb}, and i_{Cr}.
2) Generate a proposed grayscale-based image (I_g) from I_{YCbCr}. This paper considers two types as I_{YCbCr}:
   (a) I_g *without color sub-sampling*: As shown in Fig. 10(a), i_Y, i_{Cb}, and i_{Cr} are combined into I_{YCbCr} with $3(X \times Y)$ pixels.

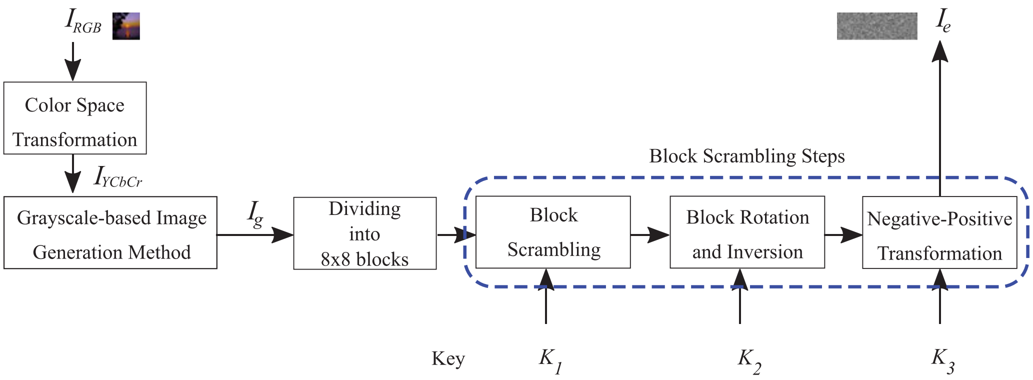
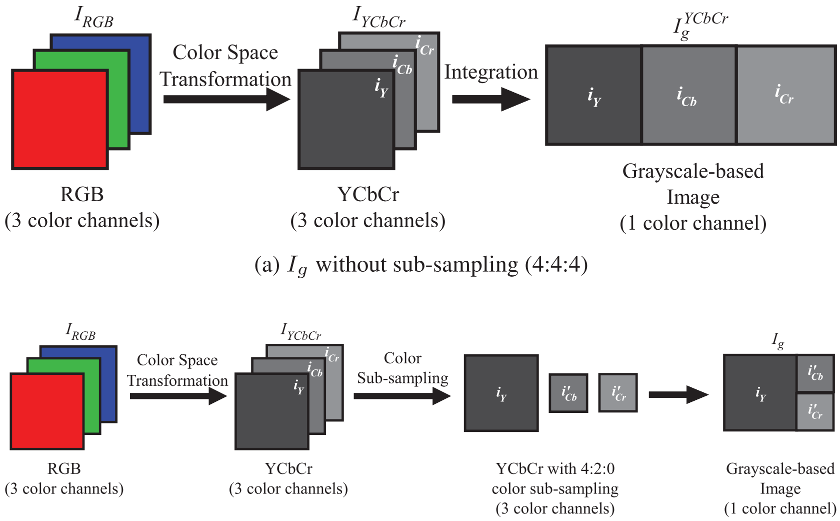

I_{RGB}
I_e
Color Space Transformation
I_{YCbCr}
Block Scrambling Steps
Grayscale-based Image Generation Method
I_g
Dividing into 8x8 blocks
Block Scrambling
Block Rotation and Inversion
Negative-Positive Transformation
Key
K_1
K_2
K_3

Fig. 9. Proposed grayscale-based image encryption.



(a) I_g without sub-sampling (4:4:4)

(b) I_g with 4:2:0 sub-sampling

Fig. 10. Proposed grayscale-based image generation. (a) I_g without sub-sampling (4:4:4), (b) I_g with 4:2:0 sub-sampling.

(b) I_g *with 4:2:0 color sub-sampling:* As shown in Fig. 10(b), i_{Cb} and i_{Cr} are sub-sampled to produce the sub-sampled chrominance (i'_{Cb} and i'_{Cr}) using the same method as in [26]. Then, i_Y, i'_{Cb}, and i'_{Cr} are combined into I_g with $3/2(X \times Y)$ pixels.

3) Divide I_g into blocks each with $B_x \times B_y$ and then randomly permute the divided blocks by using a random integer generated by a secret key K_1.
4) Rotate and invert each block randomly by using a random integer generated by a key K_2.
5) Apply negative–positive transformation to each block by using a random binary integer generated by a key K_3.

An example of images encrypted by using the proposed scheme is shown in Figs 4(d) and 4(e).

B) Image decryption procedure

As shown in Fig. 1, to reproduce a decrypted image ($\hat{I}$) from an encrypted JPEG image ($\hat{I}_{ec}$), JPEG decompression is performed to $\hat{I}_{ec}$. As a result, the decompressed image ($\hat{I}_e$) is generated. Then, the following steps are carried out to decrypt $\hat{I}_e$ using the corresponding secret key K (see Fig. 11).

1) Divide $\hat{I}_e$ into blocks, each with $B_x \times B_y$.
2) Apply inverse negative–positive transformation to each block with key K_3.
3) Inversely rotate and invert each block with key K_2
4) Assemble blocks based on key K_1 to produce the grayscale-based image ($\hat{I}_g$)
5) Reconstruct the color image in YCbCr color space ($\hat{I}_{YCbCr}$) from $\hat{I}_g$
6) Transform $\hat{I}_{YCbCr}$ to RGB color space
7) Integrate RGB components to generate $\hat{I}$

There are two methods used for reconstructing $\hat{I}_{YCbCr}$ from $\hat{I}_g$ in Step (5):

- I_g *without sub-sampling:* When I_g was generated according to Fig. 10(a), $\hat{I}_g$ is separated into three color channels.

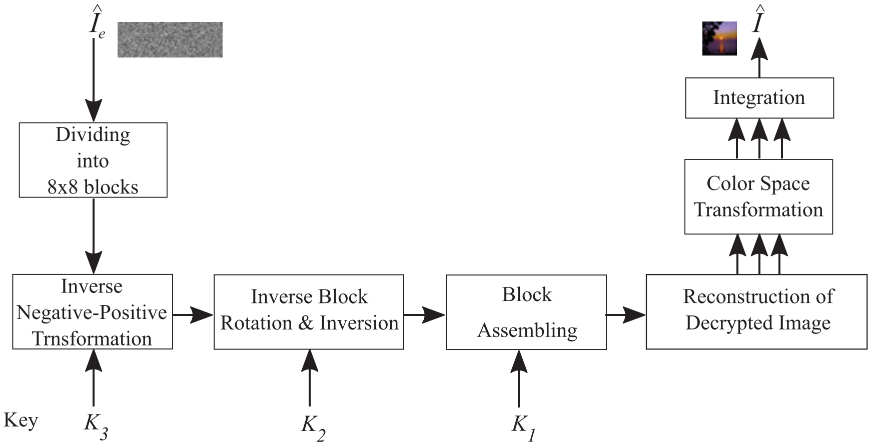
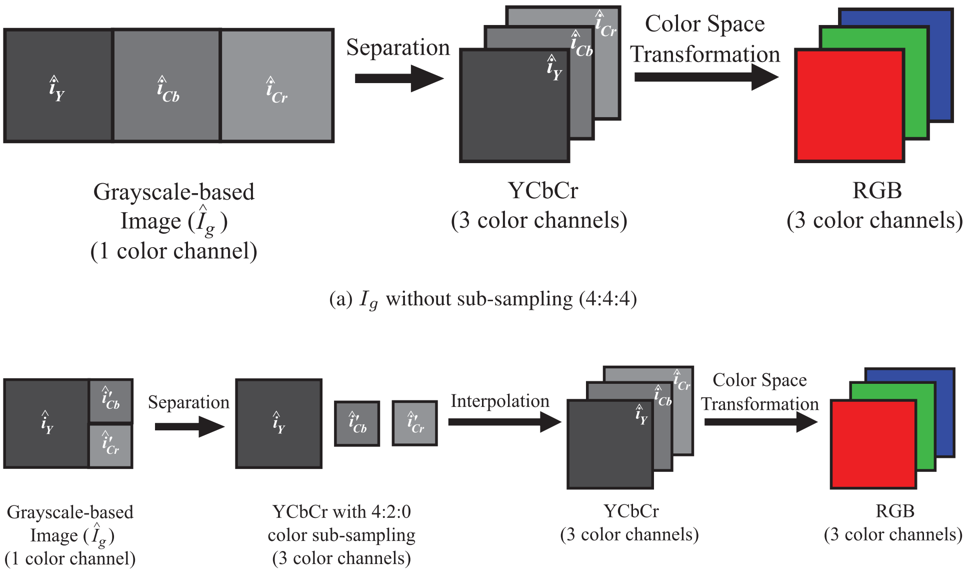

$\hat{I}_e$
Dividing into 8x8 blocks
Inverse Negative-Positive Trnsformation
Inverse Block Rotation & Inversion
Block Assembling
Reconstruction of Decrypted Image
Color Space Transformation
Integration
$\hat{I}$
Key
K_3
K_2
K_1

Fig. 11. Proposed grayscale-based image decryption procedure.



(a) I_g without sub-sampling (4:4:4)

(b) I_g with 4:2:0 sub-sampling

Fig. 12. Reconstruction of decrypted images. (a) I_g without sub-sampling (4:4:4), (b) I_g with 4:2:0 sub-sampling.

Then, the three channels are integrated into $\hat{I}_{YCbCr}$, as shown in Fig. 12(a).

- I_g *with 4:2:0 sub-sampling*: When I_g was generated according to Fig. 10(b), $\hat{I}_g$ is separated into one luminance ($\hat{i}_Y$) and two sub-sampled chrominance components ($\hat{i}'_{Cb}$ and $\hat{i}'_{Cr}$), as shown in Fig. 12(b). Then, $\hat{i}'_{Cb}$ and $\hat{i}'_{Cr}$ are interpolated to increase the spatial resolution as in [32]. Eventually, the luminance and interpolated chrominance components are integrated into $\hat{I}_{YCbCr}$.

C) Compression of grayscale-based image

This paper focuses on JPEG lossy compression, although the JPEG standard supports both lossy and lossless compressions, and the block scrambling-based image encryption schemes are applicable to lossless compression as discussed in [19]. This is because most JPEG compression applications, especially SNS and CPSS providers, utilize lossy compression.

JPEG softwares, such as Independent JPEG Group (IJG) software [32], generally utilize two default quantization tables to quantize i_Y, i_{Cb}, and i_{Cr} of I_{YCbCr} called the luminance quantization table (Y-table), and the chrominance quantization table (CbCr-table), although image-dependent quantization tables can be designed by users [33]. However, grayscale-based images do not correspond to luminance or chrominance. Therefore, we propose a new quantization table called G-table to improve the compression performance of I_g.

In JPEG compression, all pixel values in each block of I_g are mapped from $[0, 255]$ to $[-127, 128]$ by subtracting 128, then each block is transformed using Discrete Cosine Transform (DCT) to obtain DCT coefficients.

The DCT coefficients are employed to generate G-table. Let $DCT_m(i, j)$ be the DCT coefficient of the m^{th} block at the position (i, j) where $1 \le i \le 8$ and $1 \le j \le 8$. Considering every block of I_g, the absolute value of $DCT_m(i, j)$ is calculated, and the arithmetic mean of $|DCT_m(i, j)|$ is expressed by

$$c(i, j) = \frac{1}{n_g} \sum_{m=1}^{n_g} |DCT_m(i, j)| \tag{9}$$

where I_g consists of n_g blocks.

As a set of grayscale-based images which consists of N_I images is utilized to determine G-table, we define $c_k(i, j)$ as $c(i, j)$ of the k^{th} image and calculate the average of every $c(i, j)$ from N_I grayscale-based images. The average $\bar{c}(i, j)$ is calculated as follow.

$$\bar{c}(i, j) = \frac{1}{N_I} \sum_{k=1}^{N_I} c_k(i, j) \tag{10}$$

To obtain G-table, $q(i, j)$ represents the quantization step size at (i, j) and is derived from the ratio between $\bar{c}(1, 1)$ and $\bar{c}(i, j)$. The step size can be calculated by

$$q(i, j) = \left\lceil \frac{\bar{c}(1, 1)}{\bar{c}(i, j)} \right\rceil + \epsilon \tag{11}$$

where ϵ is set to 16 for adjusting the Y-table step size at (1, 1) as for IJG software [32].

To design G-table for grayscale-based images, we employed 1338 images with 512 × 384 pixels from Uncompressed Color Image Database (UCID) [34]. Grayscale-based images were generated from all images in the dataset. Then, the grayscale-based images were compressed by using IJG software [32] to obtain the DCT coefficients. To design G-table for I_g without sub-sampling, the DCT coefficients were calculated whereas $n_g = 9216$, $N_I = 1338$, and $\epsilon = 16$. On the other hand, G-table for I_g with 4:2:0 sub-sampling was designed by using $n_g = 4608$. As a result, two types of

17	26	32	39	46	54	67	90
26	35	42	50	56	65	80	105
34	43	51	58	65	75	91	118
42	53	60	68	76	86	103	131
50	62	69	77	86	98	116	145
61	73	81	90	99	112	133	164
76	90	99	108	118	133	157	192
98	116	126	136	147	165	193	233

(a) I_g without sub-sampling

17	26	32	40	47	56	70	92
26	36	43	52	59	69	84	110
34	44	52	61	70	80	98	125
43	54	63	72	82	95	113	142
52	65	74	84	95	109	129	159
63	78	88	99	110	126	149	182
79	97	109	119	132	150	176	213
102	124	137	149	164	183	213	254

(b) I_g with 4:2:0 sub-sampling

Fig. 13. G-table. (a) I_g without sub-sampling, (b) I_g with 4:2:0 sub-sampling.

G-table designed for I_g without sub-sampling and with 4:2:0 sub-sampling were designed as shown in Fig. 13.

D) Security against ciphertext-only attacks

The proposed scheme is grayscale-based image encryption, so it provides the higher security level than the color-based image encryption scheme in both brute-force and jigsaw puzzle solver attacks as well as the conventional grayscale-based encryption.

In I_g without color sub-sampling, the number of pixels of I_g is the same as the conventional one. This means that the number of blocks is also identical. As a result, the key space of this type is equal to that with the conventional one in equation (8).

In contrast, I_g with 4:2:0 sub-sampling has $3/2(X \times Y)$ pixels, so $n_g = (3/2)n$. As a result, the key space of this type ($N_{P_{sub}}(n)$) is given by

$$N_{P_{sub}}(n) = \frac{3}{2}n! \cdot 8^{(3/2)n} \cdot 2^{(3/2)n} \gg N_A(n). \qquad (12)$$

As described in Section IV, images encrypted by using the proposed scheme can provide almost the same robustness against jigsaw puzzle solver attacks as the conventional grayscale-based encryption.

E) Robustness against image recompression

In Table 2, we summarize the relationship between uploaded and downloaded JPEG images of typical SNS and CPSS providers in terms of sub-sampling ratios, the quality factor (Q_f), and the maximum resolutions [35]. Q_{f_u} and Q_{f_d} denote the uploaded and downloaded quality factors, respectively.

Providers do not resize uploaded images when the resolution of uploaded images is less than or equal to the maximum resolution that each provider decided. For example, if the resolution of an image uploaded to Twitter is not larger than 4096 × 4096 pixels, the uploaded image is not resized. In this paper, we assume that the image resolution is less than or equal to the maximum resolution of each provider as well as in [17, 19, 35].

The quality of images downloaded from SNS and CPSS providers is generally degraded due to recompression forced by the providers. As shown in Table 2, a color JPEG image uploaded to Facebook is always recompressed into the new JPEG image with 4:2:0 color sub-sampling. Therefore, images encrypted by the color-based scheme are affected by the recompression, even when they were compressed with 4:4:4 sub-sampling. In comparison, when grayscale-based images are uploaded to Facebook, the color sub-sampling is not carried out, although they are recompressed with

Table 2. Relationship between uploaded JPEG files and downloaded ones in terms of sub-sampling ratios and the maximum resolutions. Providers do not resize uploaded images when their resolutions are less than or equal to the maximum resolutions, e.g. the maximum resolutions of Twitter and Tumblr are 4096 × 4096 and 1280 × 1280, respectively [29].

	Uploaded JPEG file		Downloaded JPEG file	
Provider (maximum resolution)	Sub-sampling ratio	Q_{f_u}	Sub-sampling ratio	Q_{f_d}
		Low	No recompression	
	4:4:4	High	4:2:0	85
		1,2,…,84	No recompression	
Twitter (up to 4096 × 4096 pixels)	4:2:0	85,86,…,100	4:2:0	85
		1,2,…,84	No recompression	
	(Grayscale)	85,86,…,100	(Grayscale)	85
	4:4:4			
Facebook (HQ, up to 2048 × 2048 pixels)	4:2:0	1,2,…,100	4:2:0	71,72,…,85
Facebook (LQ, up to 960 × 960 pixels)	(Grayscale)		(Grayscale)	71
	4:4:4			
Google Photos (HQ, up to 16 Megapixels)	4:2:0	1,2,…,100	4:4:4	66,…,90
	(Grayscale)		(Grayscale)	
Tumblr (up to 1280 × 1280 pixels)	4:4:4			
Google+	4:2:0	1,2,…,100	No recompression	
Flickr	(Grayscale)			

Table 3. Parameters used for uploaded JPEG images

Type	Color sub-sampling	Block size	Quantization Table
Non-encrypted	4:4:4 (no sub-sampling) 4:2:0	(non-encrypted)	
	4:4:4 (no sub-sampling)	16 × 16	IJG standard table
Color-based Conventional Grayscale-based	4:2:0		
	(no sub-sampling)	8 × 8	G-table
Proposed Grayscale-based			

different quality factors from those of uploaded images. Images encrypted by using the proposed scheme are not affected by the effect of color sub-sampling due to the use of grayscale-based images as described in [20].

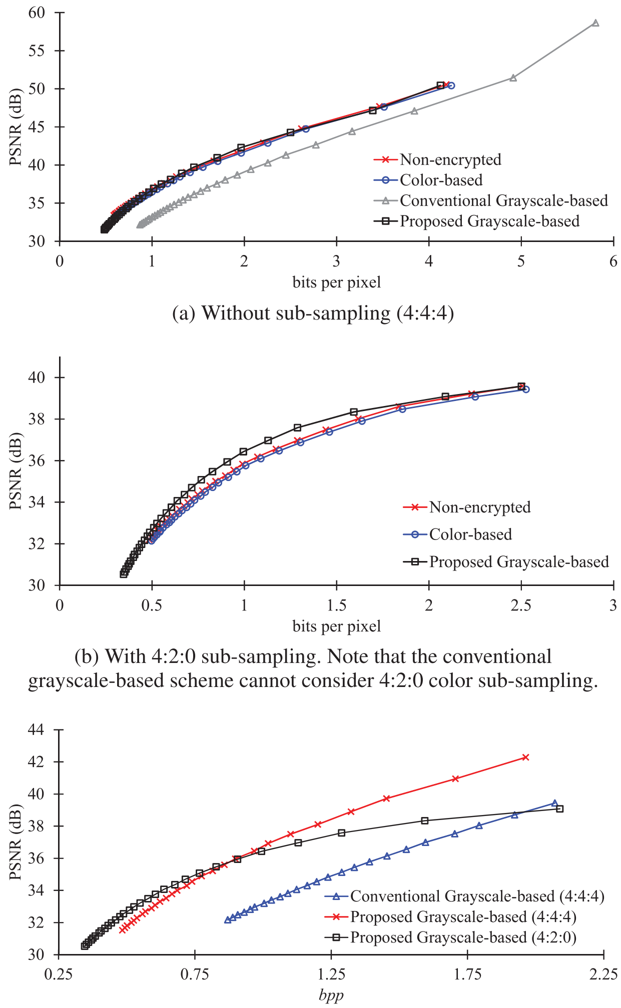
IV. EVALUATION

In this section, the effectiveness of the proposed method is discussed by conducting a number of simulations.

A) Compression performance

To evaluate the compression performance of the proposed scheme, we utilized 30 images from CSIQ dataset (512 × 512) [36]. All images in the dataset were encrypted by using the proposed scheme with $B_x = B_y = 8$. Then, all encrypted images were compressed with specific quality factors, $Q_f \in [70, 100]$, using the JPEG standard from IJG software [32]. Rate-distortion (RD) curves, which are the average peak signal-to-noise ratio (PSNR) values of all images per bits per pixel (*bpp*), were used for evaluating the compression performance. The parameters used in the experiment are shown in Table 3. Two types of G-table in Fig. 13 were used to quantize the DCT coefficients of grayscale-based images, while the IJG standard tables were employed for images encrypted by the color-based encryption scheme and non-encrypted ones.

Figure 14 shows RD curves of JPEG compressed images without any encryption and with encryption. As shown in Fig. 14(a), when images were compressed without sub-sampling, the images encrypted by using the proposed method had higher PSNR values than those with the conventional grayscale-based encryption scheme, and moreover, had almost the same RD curves as the non-encrypted ones and the color-based scheme.



(a) Without sub-sampling (4:4:4)

(b) With 4:2:0 sub-sampling. Note that the conventional grayscale-based scheme cannot consider 4:2:0 color sub-sampling.

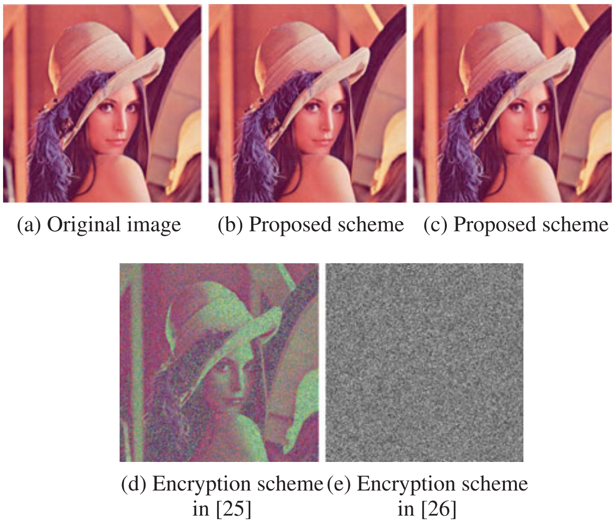
(c) Comparison between the proposed scheme with 4:2:0 sub-sampling and the conventional one

Fig. 14. R-D curves of uploaded JPEG images. (a) Without sub-sampling (4:4:4), (b) with 4:2:0 sub-sampling. Note that the conventional grayscale-based scheme cannot consider 4:2:0 color sub-sampling. (c) Comparison between the proposed scheme with 4:2:0 sub-sampling and the conventional one.

Regarding 4:2:0 color sub-sampling, the conventional grayscale-based scheme cannot consider 4:2:0 color sub-sampling because the conventional grayscale-based images consist of RGB color components. As shown in Fig. 14(b), when 4:2:0 sub-sampling was carried out, the proposed scheme provided slightly higher PSNR values, compared with non-encrypted images and the color-based scheme.

In order to clearly compare the difference between the conventional scheme and the proposed one, RD curves in a low *bpp* range were plotted in Fig. 14(c). The result showed that the proposed scheme can provide higher PSNR values than the conventional one. In addition, the proposed scheme with 4:2:0 sub-sampling is useful for the low *bpp* range. Therefore, the proposed scheme enables us to maintain almost the same image quality as non-encrypted images.

Moreover, other conventional encryption methods are considered in terms of compression performance. There are various encryption methods which can maintain an image format after encrypting as well as the proposed scheme. However, they are not suitable to EtC systems with JPEG compression, because they do not consider using JPEG compression. We numerically compared the encryption methods [25, 26] with the proposed scheme. Figures 15(d)


(a) Original image (b) Proposed scheme (c) Proposed scheme

(d) Encryption scheme in [25] (e) Encryption scheme in [26]

Fig. 15. Decrypted images after compressing and decompressing encrypted ones ($Q_f = 90$). (a) Original image ($X \times Y = 512 \times 512$), (b) proposed scheme without color sub-sampling (PSNR = 35.72 dB), (c) proposed scheme with 4:2:0 color sub-sampling (PSNR = 33.93 dB), (d) encryption scheme in [25] (PSNR = 10.32 dB, sub-sampling ratio = 4 : 2 : 0), (e) encryption scheme in [26].

and 15(e) indicate decrypted images after compressing and decompressing encrypted ones, where Fig. 15(a) is the original one. The image quality of decrypted images heavily decreased due to JPEG compression as shown in Figs 15(d) and 15(e) , because they do not consider using JPEG compression as well as most other conventional encryption methods. The proposed scheme can maintain the high quality of images as shown in Figs 15(b) and 15(c). Note that Fig. 15(e) is a grayscale image [26], so the PSNR value is not listed.

B) Robustness against image recompression

We uploaded images encrypted by using the proposed scheme to Twitter and Facebook, and then downloaded them, as well as images encrypted using color-based scheme [15–19] with $B_x = B_y = 16$, and non-encrypted images to confirm the effectiveness of the proposed scheme.

1) Experimental conditions

An experiment was carried out for evaluating robustness against image recompression and color sub-sampling forced by providers. In the experiment, the same dataset and parameters for JPEG compression as in Section IV.A were utilized. According to Fig. 1, the following procedure was conducted.

1) Generate encrypted image I_e from original image I.
2) Compress encrypted image I_e with Q_{fu}.
3) Upload encrypted JPEG image I_{ec} to SNS providers
4) Download recompressed JPEG image $\hat{I}_{ec}$ from the providers.
5) Decompress encrypted JPEG image $\hat{I}_{ec}$.
6) Decrypt decompressed image $\hat{I}_e$.
7) Compute the PSNR value between original image I and decrypted image $\hat{I}$.

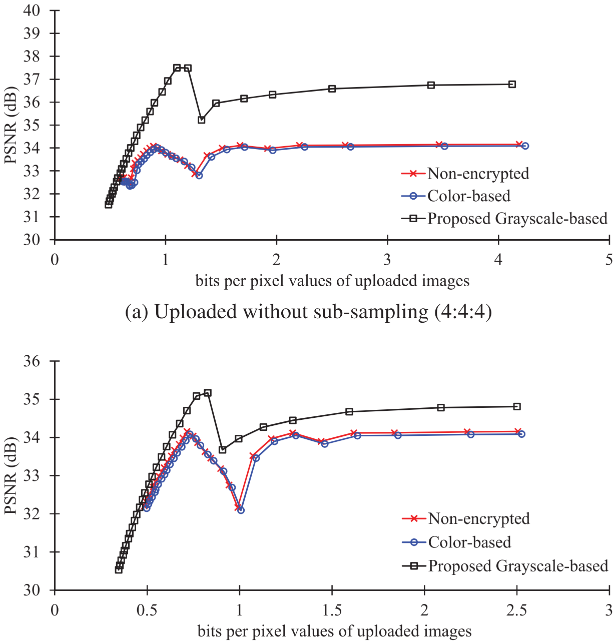
To compare PSNR values in (7), original image I was also compressed without any encryption, then uploaded and downloaded. The downloaded images were decompressed, and then, the average PSNR values of 30 images per Q_{fu} were calculated.

This paper focuses on Twitter and Facebook, which recompress uploaded JPEG images under their conditions as shown in Table 2.

2) Experimental results

Figure 16 shows the quality of images downloaded from Twitter, where the values in horizontal axis are *bpp* values of uploaded images. Although the color-based scheme could maintain almost the same PSNR values as non-encrypted images, the proposed scheme offered slightly higher PSNR values in both sub-sampling ratios, as shown in Figs 16(a) and 16(b). This is because color JPEG images are affected by 4:2:0 color sub-sampling carried out by Twitter while grayscale-based images can avoid the effect of color sub-sampling.

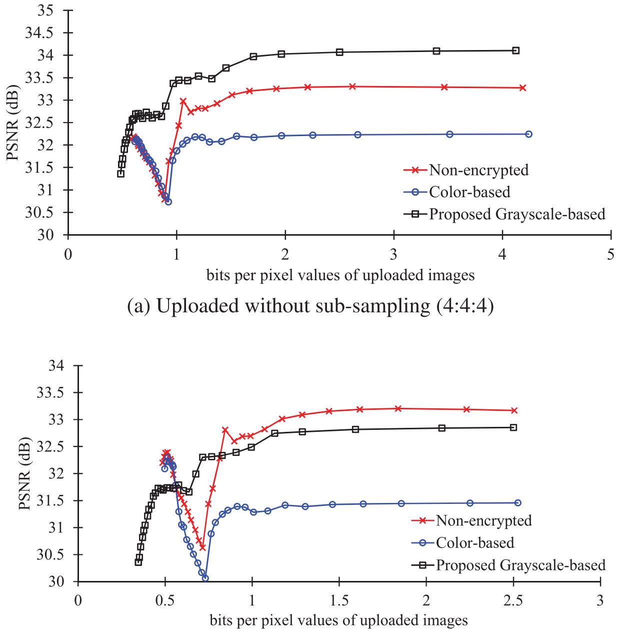
Figure 17 shows the quality of images downloaded from Facebook, where the horizontal axis refers to *bpp* values of uploaded images. As shown in Fig. 17(a), when images were compressed with 4:4:4 sub-sampling, the quality of images encrypted by the color-based scheme were heavily degraded compared with the non-encrypted ones. In comparison, the images encrypted by the proposed scheme provided higher PSNR values than those encrypted by the color-based scheme and non-encrypted images. This is because the proposed scheme is not affected by 4:2:0 sub-sampling carried out by Facebook, although color JPEG images are affected by 4:2:0 sub-sampling. When images were compressed with 4:2:0 sub-sampling, the proposed scheme provided higher



(a) Uploaded without sub-sampling (4:4:4)

(b) Uploaded with 4:2:0 sub-sampling

Fig. 16. R-D curves of downloaded JPEG images from Twitter. (a) Uploaded without sub-sampling (4:4:4), (b) uploaded with 4:2:0 sub-sampling.



(a) Uploaded without sub-sampling (4:4:4)

(b) Uploaded with 4:2:0 sub-sampling

Fig. 17. R-D curves of downloaded JPEG images from Facebook. (a) Uploaded without sub-sampling (4:4:4), (b) uploaded with 4:2:0 sub-sampling.

image quality than the color-based image encryption, as shown in Fig. 17(b). However, when $bpp > 1$, PSNR values of images encrypted by the proposed scheme are slightly lower than non-encrypted ones, but the decrypted images did not include any block artifacts. This is because every grayscale JPEG image uploaded to Facebook is recompressed to the new grayscale JPEG image with $Q_{f_d} = 71$ while Facebook recompresses JPEG color JPEG images with $Q_{f_d} \in [71, 85]$, as shown in Table 2. Note that the PSNR values of images encrypted by the color-based scheme were much lower than those of the proposed scheme and non-encrypted ones. The reason is that the images encrypted by the color-based scheme included block artifacts due to the influence of color sub-sampling.

Consequently, the proposed scheme is shown to have robustness against image recompression and color sub-sampling caused by providers as the conventional grayscale-based scheme [20, 21].

C) Robustness against jigsaw puzzle solver attacks

We evaluated the robustness against jigsaw puzzle solver attacks in terms of the difficulty of assembling encrypted images.

1) Experimental conditions

The following three measures [37, 38] were used to evaluate the results.

Direct comparison (D_c): represents the ratio of the number of pieces which are in the correct position. D_c for image I_d, namely, $D_c(I_d)$ is calculated as

$$D_c(I_d) = \frac{1}{n}\sum_{i=1}^{n} d_c(i), \tag{13}$$

$$d_c(i) = \begin{cases} 1, & \text{if } I_d(i) \text{ is in the correct position} \\ 0, & \text{otherwise} \end{cases}$$

where $I_d(i)$ represents the position of a piece i in image I_d.

Neighbor comparison (N_c): is the ratio of the number of correctly joined blocks. N_c for image I_d, namely, $N_c(I_d)$ is calculated as

$$N_c(I_d) = \frac{1}{N_{bou}}\sum_{k=1}^{N_{bou}} n_c(k), \tag{14}$$

$$n_c(k) = \begin{cases} 1, & \text{if } b_k \text{ is joined correctly} \\ 0, & \text{otherwise} \end{cases}$$

where N_{bou} is the number of boundaries among pieces in I_d, and b_k is the kth boundary in I_d. For an image with $u \times v$ blocks, there are $N_{bou} = 2uv - u - v$ boundaries in the image.

Largest component (L_c): is the ratio of the number of the largest joined blocks that have correct adjacencies to the number of blocks in an image. L_c for image I_d, namely, $L_c(I_d)$ is calculated as

$$L_c(I_d) = \frac{1}{n}\max_j\{l_c(I_d, j)\}, j = 1, 2, \ldots, m \tag{15}$$

where $l_c(I_d, j)$ is the number of blocks in the jth partial correctly assembled area, and m is the number of partial correctly assembled areas.

In the measures, $D_c, N_c, L_c \in [0, 1]$, a larger value means a higher compatibility.

We utilized 20 images from resized Ultra-Eye dataset (256×144) [39]. Thirty different encrypted images were produced from each image by using different 30 keys. The encrypted images were assembled by using the jigsaw puzzle solver, and the image that had the highest sum of D_c, N_c, and L_c was chosen. This procedure was carried out independently, and the average D_c, N_c, and L_c for the 20 images were calculated.

2) Experimental results

Table 4 shows the robustness against the extended jigsaw puzzle solver attack [27–29]. The scores for assembling both types of the proposed scheme were much lower than those of the color-based scheme and equal to those with conventional one. This is because images encrypted with the proposed scheme have a large number of encrypted blocks and no color information in the blocks.

Figures 18(g) and 18(k) are images assembled from Figs 18(b) and 18(f), respectively, while Fig. 18(a) is the original one. Comparing Figs 18(g) and 18(h), it obviously shows that the difficulty of assembling encrypted images depends on the block size. Since most conventional jigsaw puzzle solvers employ color information for assembling puzzles, reducing color channels of each pixel makes assembling

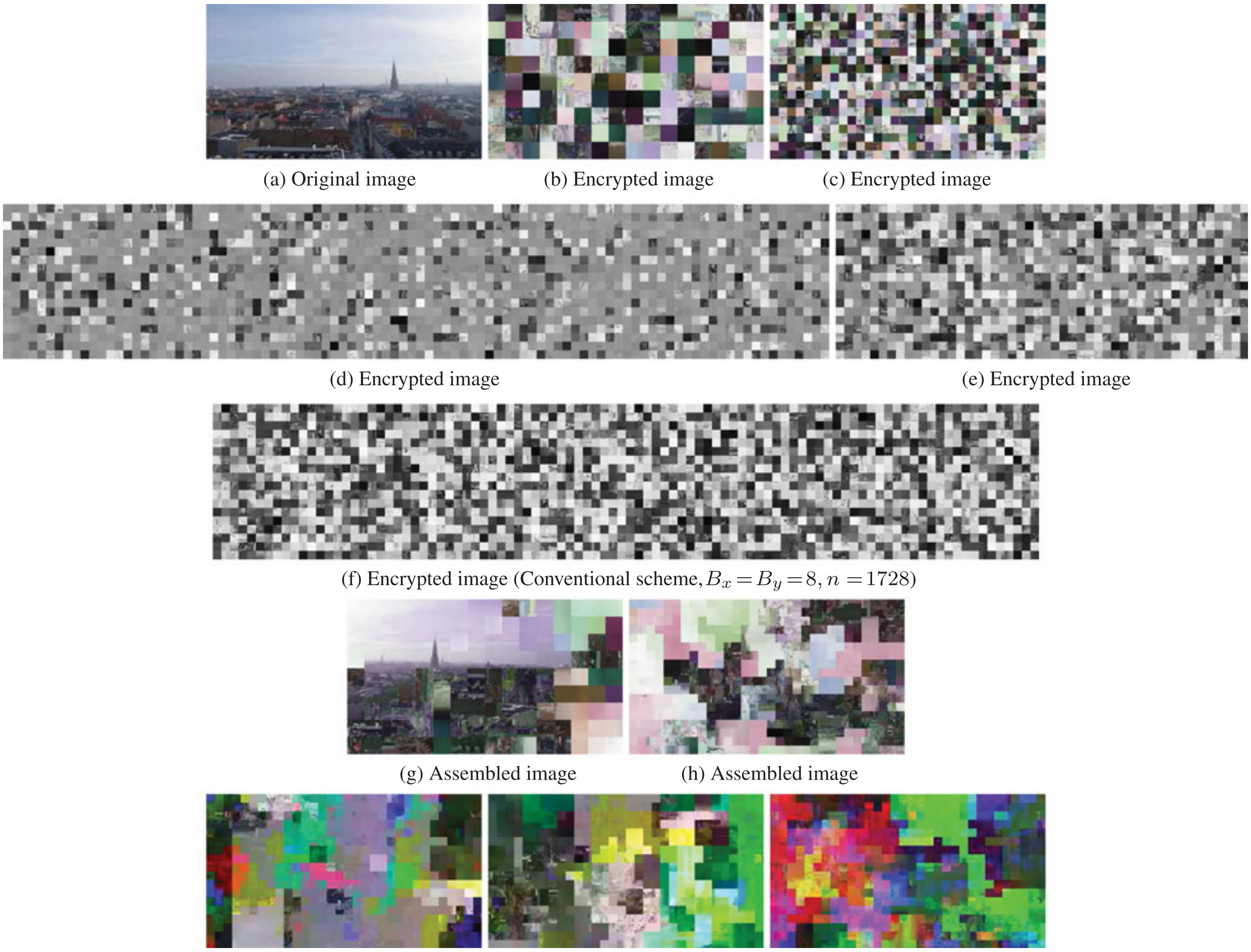
Table 4. Security evaluation of the color-based, conventional, and proposed scheme against the extended jigsaw puzzle solver [27–29].

Encryption type	Color channel	Block size	D_c	N_c	L_c
Color-based scheme [16, 17]	RGB	16 × 16	0.035	0.202	0.223
Conventional scheme [20]	Grayscale	8 × 8	0.000	0.000	0.002
Proposed scheme with sub-sampling	Grayscale	8 × 8	0.000	0.000	0.002
Proposed scheme without sub-sampling	Grayscale	8 × 8	0.000	0.000	0.002

puzzles harder. As shown in Figs 18(i) and 18(j), it is more difficult to assemble the image encrypted by the proposed grayscale-based image encryption because the encrypted image has only one color channel.

Figure 19 shows the running time to assemble encrypted images by using the jigsaw puzzle solver [27–29], where the average time of 20 images from resized Ultra-eye dataset [39] were plotted. We compared the running time to assemble images encrypted with the color-based scheme ($B_x = B_y = 16$), the conventional scheme ($B_x = B_y = 8$), and the proposed one ($B_x = B_y = 8$). The jigsaw puzzle solver was implemented in MATLAB2017a on a PC with a 3.6 GHz processor and a main memory 16Gbytes (Processor:Intel Core i7-7700 3.6 GHz, OS:Ubuntu 16.04 LTS).

As shown in Fig. 19, although the images encrypted by using the proposed method ($B_x = B_y = 8$) with 4:2:0 sub-sampling were solved in 10.33 min, the scores of assembled images were very low as $L_c = 0.002$ (see Table 4). It obviously takes more time to assemble encrypted images than that of images encrypted by the color-based scheme. The reason is that the proposed scheme can offer a smaller block size, the larger number of blocks and less color information. Moreover, the images encrypted by the proposed method without any sub-sampling were solved in 45.84 min


(a) Original image (b) Encrypted image (c) Encrypted image

(d) Encrypted image (e) Encrypted image

(f) Encrypted image (Conventional scheme, $B_x = B_y = 8, n = 1728$)

(g) Assembled image (h) Assembled image

(i) Assembled image (Proposed (j) Assembled image (Proposed (k) Assembled image

Fig. 18. Assembled images by using the extended jigsaw puzzle solver [27–29]. a) Original image ($X \times Y = 256 \times 144$), (b) encrypted image (color-based scheme, $B_x = B_y = 16, n = 144$), (c) encrypted image (color-based scheme, $B_x = B_y = 8, n = 576$), (d) encrypted image (proposed scheme without sub-sampling, $B_x = B_y = 8, n = 1728$), (e) encrypted image (proposed scheme with 4:2:0 sub-sampling, $B_x = B_y = 8, n = 864$), (f) encrypted image (conventional scheme, $B_x = B_y = 8, n = 1728$), (g) assembled image (color-based scheme, $B_x = B_y = 16, L_c = 0.208$), (h) assembled image (color-based scheme, $B_x = B_y = 8, L_c = 0.012$), (i) assembled image (proposed scheme without sub-sampling, $B_x = B_y = 8, L_c = 0.002$), (j) assembled image (proposed scheme with 4:2:0 sub-sampling, $B_x = B_y = 8, L_c = 0.002$), (k) assembled image (conventional scheme, $B_x = B_y = 8, L_c = 0.002$).

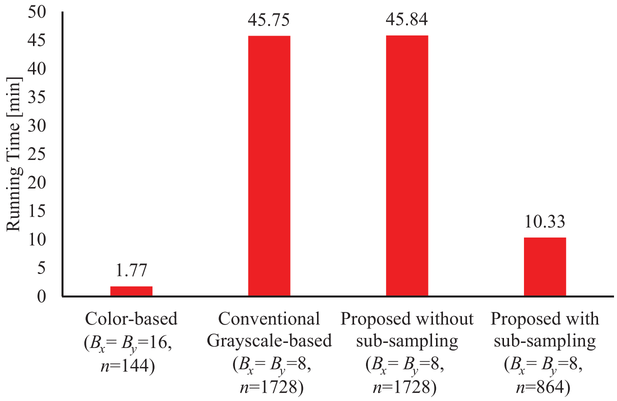


Fig. 19. Running time of assembling encrypted images from resized ultra-eye dataset (256 × 144).

Table 5. Key space of the color-based, conventional, and proposed scheme (N_p = 256 × 144)

Encryption type	Number of pixels	$B_x \times B_y$	Key space	Rank
Color-based scheme [16, 17]	N_p	16 × 16	$144! \cdot 2^{720} \cdot 3^{144}$	3
Conventional Grayscale-based scheme [20]	$3N_p$	8 × 8	$1728! \cdot 2^{6912}$	1
Proposed scheme without sub-sampling	$3N_p$	8 × 8	$1728! \cdot 2^{6912}$	1
Proposed scheme with sub-sampling	$\frac{3}{2}N_p$	8 × 8	$864! \cdot 2^{3456}$	2

which is almost the same as that of conventional one. As a result, the proposed scheme can enhance security against ciphertext-only attacks in terms of both computational complexity and the accuracy of assembled results.

D) Discussions on key space

Moreover, we evaluate robustness against brute-force attack in terms of the key space of encrypted images [39] where the number of pixels of the original images (N_p) is 256 × 144. The key space of the color-based scheme and the conventional scheme were calculated using equations (6) and (8), respectively. On the other hand, the key space of the proposed scheme without sub-sampling and with sub-sampling were calculated by using equations (8) and (12), respectively. As shown in Table 5, the key space of the proposed scheme without color sub-sampling is equal to that of the conventional one and greatly higher than the color-based scheme. Even if the key space of the proposed scheme with color sub-sampling is less than the conventional one due to the lower number of blocks, it is greatly higher than that of the color-based scheme.

V. CONCLUSION

We presented a new grayscale-based block scrambling image encryption scheme which enhances the security of EtC systems for JPEG images. Although $B_x = B_y = 8$ can be used as a block size in the conventional grayscale-based image encryption scheme, the compression performance is degraded, and the color sub-sampling cannot be considered. The proposed scheme allows us not only to enhance the compression performance of the EtC systems by using YCbCr color space, but also to preserve the security level at the same level as the conventional one. In addition, the proposed scheme allows us to consider the color sub-sampling operation which can improve the compression performance, although the encrypted images have no color information. As a result, the proposed scheme has better performance than the conventional one in terms of the compression performance. Experimental results showed that images encrypted by using the proposed scheme had a higher compression performance than those encrypted by the conventional grayscale-based scheme. Moreover, the proposed scheme was confirmed to have almost the same robustness against ciphertext-only attacks as the conventional grayscale-based encryption.

FINANCIAL SUPPORT

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

STATEMENT OF INTEREST

None.

REFERENCES

[1] Huang, C.T. *et al.*: Survey on securing data storage in the cloud. *APSIPA Trans. Signal Inf. Process.*, **3** (e7) (2014).

[2] Lagendijk, R.; Erkin, Z.; Barni, M.: Encrypted signal processing for privacy protection: conveying the utility of homomorphic encryption and multiparty computation. *IEEE Signal. Process. Mag.*, **30** (1) (2013), 82–105.

[3] Zhou, J.; Liu, X.; Au, O.C.; Tang, Y.Y.: Designing an efficient image encryption-then-compression system via prediction error clustering and random permutation. *IEEE Trans. Inf. Forensics Security*, **9** (1) (2014), 39–50.

[4] Ra, M.-R.; Govindan, R.; Ortega, A.: P3: toward privacy-preserving photo sharing, in *Proc. of the 10th USENIX Conf. on Networked Systems Design and Implementation*, 2013, 515–528.

[5] Zeng, W.; Lei, S.: Efficient frequency domain selective scrambling of digital video. *IEEE Trans. Multimedia*, **5** (1) (2003), 118–129.

[6] Ito, I.; Kiya, H.: A new class of image registration for guaranteeing secure data management, in *IEEE Int. Conf. on Image Processing (ICIP)*, 2008, 269–272.

[7] Kiya, H.; Ito, I.: Image matching between scrambled images for secure data management, in *16th European Signal Processing Conf. (EUSIPCO)*, 2008, 1–5.

[8] Ito, I.; Kiya, H.: One-time key based phase scrambling for phaseonly correlation between visually protected images. *EURASIP J. Inf. Security*, **2009** (841045) (2010), 1–11.

[9] Tang, Z.; Zhang, X.; Lan, W.: Efficient image encryption with block shuffling and chaotic map. *Multimedia Tools Appl.*, **74** (15) (2015), 5429–5448.

[10] Li, C.; Lin, D.; Lü, J.: Cryptanalyzing an image-scrambling encryption algorithm of pixel bits. *IEEE Trans. Multimedia*, **24** (3) (2017), 64–71.

[11] Zhang, Y.; Xu, B.; Zhou, N.: A novel image compression-encryption hybrid algorithm based on the analysis sparse representation. *Optical Commun.*, **392** (2017), 223–233.

[12] Erkin, Z. *et al.*: Protection and retrieval of encrypted multimedia content: when cryptography meets signal processing. *EURASIP J. Inf. Security*, **2007** (78943) (2007), 1–20.

[13] Nimbokar, K.G.; Sarode, M.V.; Ghonge, M.M.: A survey based on designing an efficient image encryption-then-compression system, in *IJCA Proc. on National Level Technical Conf. X-PLORE 2014*, vol, XPLORE2014, 2014, 6–8.

[14] Liu, T.Y.; Lin, K.J.; Wu, H.C.: Ecg data encryption then compression using singular value decomposition. *IEEE J. Biomed. Health Inform.*, **22** (3) (2018), 707–713.

[15] Watanabe, O.; Uchida, A.; Fukuhara, T.; Kiya, H.: An encryption-then-compression system for jpeg 2000 standard, in *IEEE Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP)*, 2015, 1226–1230.

[16] Kurihara, K.; Shiota, S.; Kiya, H.: An encryption-then-compression system for jpeg standard, in *Picture Coding Symp. (PCS)*, 2015, 119–123.

[17] Kurihara, K.; Kikuchi, M.; Imaizumi, S.; Shiota, S.; Kiya, H.: An encryption-then-compression system for jpeg/motion jpeg standard. *IEICE Trans. Fund. Electron. Comm. Comput. Sci.*, **98** (11) (2015), 2238–2245.

[18] Kurihara, K.; Watanabe, O.; Kiya, H.: An encryption-then-compression system for jpeg xr standard, in *IEEE Int. Symp. Broadband Multimedia Systems and Broadcast (BMSB)*, 2016, 1–5.

[19] Kurihara, K.; Imaizumi, S.; Shiota, S.; Kiya, H.: An encryption-then-compression system for lossless image compression standards. *IEICE Trans. Inf. Syst.*, **E100-D** (1) (2017), 52–56.

[20] Sirichotedumrong, W.; Chuman, T.; Imaizumi, S.; Kiya, H.: Grayscale-based block scrambling image encryption for social network services, in *IEEE Int. Conf. on Multimedia and Expo (ICME)*, 2018, 1–6.

[21] Chuman, T.; Sirichotedumrong, W.; Kiya, H.: Encryption-then-compression systems using grayscale-based image encryption for jpeg images, *IEEE Trans. Inf. Forensics Security*, https://doi.org/10.1109/TIFS.2018.2881677.

[22] Liu, W.; Zeng, W.; Dong, L.; Yao, Q.: Efficient compression of encrypted grayscale images. *IEEE Trans. Image Process.*, **19** (4) (2010), 1097–1102.

[23] Hu, R.; Li, X.; Yang, B.: A new lossy compression scheme for encrypted gray-scale images, in *IEEE Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP)*, 2014, 7387–7390.

[24] Johnson, M.; Ishwar, P.; Prabhakaran, V.; Schonberg, D.; Ramchandran, K.: On compressing encrypted data. *IEEE Trans. Signal Process.*, **52** (10) (2004), 2992–3006.

[25] Gaata, M.T.; Hantoosh, F.F.: An efficient image encryption technique using chaotic logistic map and rc4 stream cipher. *Int. J. Mod. Trends Eng. Res.*, **3** (9) (2016), 213–218.

[26] Wu, Y.; Noonan, J.P.; Yang, G.; Jin, H.: Image encryption using the two-dimensional logistic chaotic map. *J. Electron. Imaging.*, **21** (1) (2012), 013014.

[27] Chuman, T.; Kurihara, K.; Kiya, H.: On the security of block scrambling-based etc systems against jigsaw puzzle solver attacks, in *IEEE Int. Conf. on Acoustics, Speech, and Signal Processing (ICASSP)*, 2017, 2157–2161.

[28] Chuman, T.; Kurihara, K.; Kiya, H.: Security evaluation for block scrambling-based etc systems against extended jigsaw puzzle solver attacks, in *IEEE Int. Conf. on Multimedia and Expo (ICME)*, 2017, 229–234.

[29] Chuman, T.; Kurihara, K.; Kiya, H.: On the security of block scrambling-based etc systems against extended jigsaw puzzle solver attacks. *IEICE Trans. Inf. Syst.*, **E101-D** (1) (2018), 37–44.

[30] Chuman, T.; Kiya, H.: On the security of block scrambling-based image encryption including jpeg distorsion against jigsaw puzzle solver attacks, in *IEEE Int. Workshop on Signal Design and its Applications in Communications (IWSDA)*, 2017, 64–68.

[31] Information technology - digital compression and coding of continuous-tone still images: JPEG file interchange format (JFIF), Recommendation ITU-T T.871, 2012.

[32] Independent jpeg group, http://www.ijg.org/.

[33] Yang, E.H.; Wang, L.: Joint optimization of run-length coding, huffman coding, and quantization table with complete baseline jpeg decoder compatibility. *IEEE Trans. Image Process.*, **18** (1) (2009), 63–74.

[34] Schaefer, G.; Stich, M.: UCID: An uncompressed color image database, in *Storage and Retrieval Methods and Applications for Multimedia 2004*, 2004, 472–480.

[35] Chuman, T.; Iida, K.; Kiya, H.: Image manipulation on social media for encryption-then-compression systems, in *2017 Asia-Pacific Signal and Information Processing Association Annual Summit and Conf. (APSIPA ASC)*, 2017, 858–863.

[36] Larson, E.C.; Chandler, D.M.: Most apparent distortion: full reference image quality assessment and the role of strategy. *J. Electron. Imaging.*, **19** (2010), 011006-1–011006-21.

[37] Gallagher, A.: Jigsaw puzzles with pieces of unknown orientation, in *IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2012, 382–389.

[38] Cho, T.; Avidan, S.; Freeman, W.: A probabilistic image jigsaw puzzle solver, in *IEEE Conf. on Computer Vision and Pattern Recognition (CVPR)*, 2010, 183–190.

[39] Nemoto, H.; Hanhart, P.; Korshunov, P.; Ebrahimi, T.: Ultra-eye: Uhd and hd images eye tracking dataset, in *Sixth Int. Workshop on Quality of Multimedia Experience (QoMEX)*, 2014, 39–40.

Warit Sirichotedumrong received his B.Eng. and M.Eng. degrees from King Mongkut's University of Technology Thonburi, Thailand in 2014 and 2017, respectively. He has been a Doctor course student at Tokyo Metropolitan University since 2017. His research interests are in the area of image processing and information security.

Hitoshi Kiya received his B.E and M.E. degrees from Nagaoka University of Technology, in 1980 and 1982, respectively, and his Dr. Eng. degree from Tokyo Metropolitan University in 1987. In 1982, he joined Tokyo Metropolitan University, where he became a Full Professor in 2000. From 1995 to 1996, he attended the University of Sydney, Australia as a Visiting Fellow. He is a Fellow of IEEE, IEICE, and ITE. He currently serves as President-Elect of APSIPA, and he served as Regional Directorat-Large for Region 10 of the IEEE Signal Processing Society from 2016 to 2017. He was also President of the IEICE Engineering Sciences Society from 2011 to 2012, and he served there as a Vice President and Editor-in-Chief for IEICE Society Magazine and Society Publications. He was Editorial Board Member of eight journals, including IEEE Trans. on Signal Processing, Image Processing, and Information Forensics and Security, Chair of two technical committees and Member of nine technical committees including APSIPA Image, Video, and Multimedia Technical Committee (TC), and IEEE Information Forensics and Security TC. He has organized a lot of international conferences, in such roles as TPC Chair of IEEE ICASSP 2012 and as General Co-Chair of IEEE ISCAS 2019. He has received numerous awards, including six best paper awards.