PAPER *Special Section on Enriched Multimedia — Multimedia Security and Forensics —*

A Scheme of Reversible Data Hiding for the Encryption-Then-Compression System

Masaaki FUJIYOSHI[†a)], ***Senior Member***, **Ruifeng LI**[†b)], ***Nonmember***, ***and*** **Hitoshi KIYA**[†c)], ***Fellow***

SUMMARY This paper proposes an encryption-then-compression (EtC) system-friendly data hiding scheme for images, where an EtC system compresses images after they are encrypted. The EtC system divides an image into non-overlapping blocks and applies four block-based processes independently and randomly to the image for visual encryption of the image. The proposed scheme hides data to a plain, i.e., unencrypted image and the scheme can take hidden data out from the image encrypted by the EtC system. Furthermore, the scheme serves reversible data hiding, so it can perfectly recover the unmarked image from the marked image whereas the scheme once distorts unmarked image for hiding data to the image. The proposed scheme copes with the three of four processes in the EtC system, namely, block permutation, rotation/flipping of blocks, and inverting brightness in blocks, whereas the conventional schemes for the system do not cope with the last one. In addition, these conventional schemes have to identify the encrypted image so that image-dependent side information can be used to extract embedded data and to restore the unmarked image, but the proposed scheme does not need such identification. Moreover, whereas the data hiding process must know the block size of encryption in conventional schemes, the proposed scheme needs no prior knowledge of the block size for encryption. Experimental results show the effectiveness of the proposed scheme.

key words: *parameter memorization-free, asymmetry data hiding, perceptual encryption, lossless compression, pulse amplitude modulation*

1. Introduction

As cloud computing and various network services become popular nowadays, information media such as images take a much more important role for information transmission and retrieval over the Internet. In addition, popularization of high resolution image and video acquisition makes image compression techniques further important for high speed and efficiency transmitting/storing images. On the other hand, there is serious concern about privacy and copyright protection of image contents, so encryption of images before transmission becomes common.

Since existing image compression techniques are mainly developed for natural images, highly efficient compression of encrypted images is not easy. Thus, compression-then-encryption systems [1], [2] are widely used at this time where a system encrypts compressed images. However, new systems which serve efficient compression of encrypted images and/or compression-resilient encryption have been realized these days [3]–[9]. This paper focuses on the latter, i.e., encryption-then-compression (EtC) systems.

Regardless of whether images are encrypted, several applications require image-related information and/or image-accompanied information for image/information processing [10], [11]. Thus, data hiding schemes have been proposed [12]–[16] where each scheme imperceptibly hides data into a unmarked image and takes hidden data out from the marked image whereas the image is encrypted. For the EtC system which divides an image into blocks and visually encrypts the image based on blocks [9], data hiding schemes have been proposed [15], [16].

This EtC system [9] visually encrypts an image by independent and random applying block permutation, rotation/flipping blocks, inverting luminance in blocks, and so on to the image. Conventional data hiding schemes for this EtC system cope with block permutation and rotation/flipping blocks [15], [16] but not with inverting luminance in blocks, whereas luminance inversion is one of the essence of the difficulty in estimating the original image in the EtC system [9], [17]. Moreover, these schemes have to know the block size for encryption to hide data to the image. Furthermore, these schemes have to identify the encrypted image to extract hidden data and to recover the unmarked image from the image.

This paper proposes a new data hiding scheme which copes with the EtC system [9]. The proposed scheme is a reversible data hiding scheme as well as conventional schemes [15], [16] where a reversible data hiding scheme can recovers the unmarked image from a marked image [18], [19]. This scheme copes with inverting luminance in blocks as well as block permutation and rotation/flipping blocks, whereas conventional schemes does not cope with. In addition, the scheme does not have to know the block size for encryption and has a feature that no identification of the image is required for data extraction and image recovery [20], [21].

2. Preliminaries

The EtC system [9] and the EtC system-friendly conventional reversible data hiding schemes [15], [16] are mentioned in this section with the assumption that grayscale images are used for the fundamental and essential study hereafter.

Manuscript received March 16, 2020.
Manuscript revised July 31, 2020.
Manuscript publicized October 21, 2020.

[†]The authors are with Tokyo Metropolitan University, Hino-shi, 191–0065 Japan.
a) E-mail: mfujiyoshi@m.ieice.org (Corresponding author)
b) E-mail: li-ruifeng@tmu.ac.jp
c) E-mail: kiya@tmu.ac.jp

DOI: 10.1587/transinf.2020MUP0006

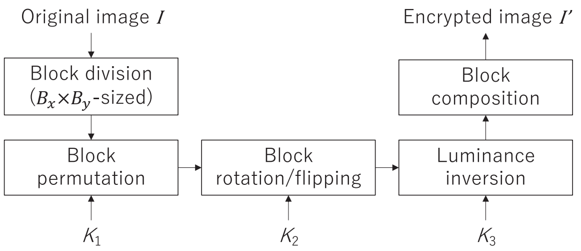


Fig. 1 The block-based EtC system [9].

1	4	7
2	5	8
3	6	9

(a) Before permutation.

6	3	7
4	9	5
1	8	2

(b) After permutation.

Fig. 2 An example of block permutation.

2.1 The EtC System

This section briefly describes the block-based EtC system [9] shown in Fig. 1.

Step 1. Divide X×Y-sized grayscale image I to B_x×B_y-sized non-overlapping blocks.

Step 2. Permute blocks randomly.

Step 3. Rotate and flip each block randomly.

Step 4. Invert luminance in each block randomly.

Step 5. Blocks form X×Y-sized grayscale encrypted image I'.

Subsequent sections explain Steps 2, 3, and 4.

2.1.1 Block Permutation

By using a pseudo random number generator (PRNG) with key K_1, blocks are permuted. Figure 2 shows an example of block permutation.

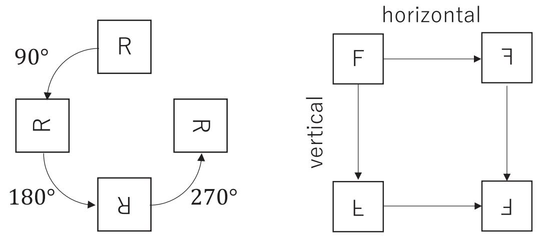
2.1.2 Block Rotation/Flipping

By using a PRNG with key K_2, each block is rotated and flipped. As shown in Fig. 3, a block can be rotated either 0°, 90°, 180°, or 270° under the condition $B_x = B_Y$ and four flipping patterns exist; no flipping, flipping horizontally, flipping vertically, and flipping horizontally and vertically.

2.1.3 Luminance Inversion

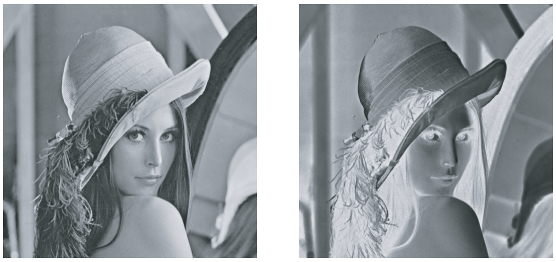
By using a PRNG with key K_3, luminance value of pixels are inverted in randomly chosen blocks. Luminance inversion is done by

$$p' = \begin{cases} p, & r(i) = 0 \\ A - p, & r(i) = 1 \end{cases}, \tag{1}$$



(a) Block rotation. (b) Block flipping.

Fig. 3 Block rotation and flipping in the EtC system.



(a) Original. (b) Luminance inverted.

Fig. 4 An example of luminance inversion (all pixels are inverted).

where p', p, $r(i)$, and A represent luminance value of a pixel in the i-th block of the image after Step 4, that before Step 4, pseudo randomly generated integer for the i-th block, and the dynamic range of luminance of image I and I' ($A = 2^8 - 1 = 255$ for 8-bit grayscale images), respectively. Figure 4 shows the image in which the luminance value is inverted in all pixels.

2.2 Conventional Reversible Data Hiding Schemes for the EtC System

Conventional schemes [15], [16] for the EtC System [9] are based on the histogram shifting-based reversible data hiding scheme [22]. Let $h(v)$ denote the frequency of occurrence for luminance value v in a grayscale image where $v \in \{0, 1, \ldots, A\}$. Histogram shifting-based schemes use pixel luminance values $v_{\min} = \arg\min h(v)$ and $v_{\max} = \arg\max h(v)$ for hiding data into the image. Schemes need these parameters to distinguish marked area from unmarked area in the image for taking hidden data out from the marked image and for recovering the unmarked image from the marked image, so exact parameters should be needed for correct data extraction and right image recovery.

These parameters, however, depend on the image, so schemes aiming to extract hidden data from a marked and encrypted image firstly need to identify the target image whereas the target image is encrypted. The larger the number of images encrypted by the EtC system, the higher identification costs, and identification of the unmarked and unencrypted image from the marked and encrypted image is quite difficult.

In addition, these schemes [15], [16] cope with block permutation and block rotation and flipping, but they do

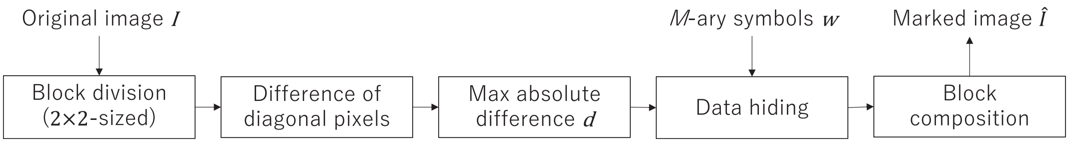


Fig. 5 Proposed data hiding algorithm.

not cope with luminance inversion of blocks. Furthermore, these schemes hide data to an image based on blocks whose size are the same as the block size for encryption. So, the next section proposes a new reversible data hiding scheme to overcome above mentioned problems in conventional schemes.

3. Proposed Scheme

This section proposes a reversible data hiding scheme which hides data into plain, i.e., unencrypted image and takes hidden data out from the image encrypted by the EtC system [9]. This scheme copes with block permutation and block rotation/flipping of the EtC system as well as conventional schemes do [15], [16], the scheme further copes with luminance inversion. Moreover, the proposed scheme does not need either the block size in the EtC system or identification of images for data extraction and image recovery whereas conventional schemes need.

3.1 Requirements and Strategies

The proposed scheme meets two requirements, namely,

Req. A coping with three visual encryption processes of the EtC system [9] including luminance inversion, and

Req. B extracting hidden data out and recovering the unmarked image without identification of the image.

For Requirement A, the scheme divides an image into non-overlapping blocks where the block size is much smaller than that for encryption. Moreover, the scheme hides data into the image based on small blocks independently from the block position. Furthermore, this scheme uses the difference between main diagonal elements of small blocks for hiding data into the image because hidden data are required to survive through block rotation and flipping by the EtC system.

For Requirement B, the scheme embeds a parameter to the image as well as data. There are two ways for realizing this feature; embedding the parameter by using one embedding mechanism and by employing another reversible data hiding scheme. The proposed scheme take the former way, so no other reversible data hiding scheme is employed.

Based on the above mentioned strategies, successive sections describes an implementation example of data hiding, data extraction, and image recovery. It is assumed that L of 2^M-ary data symbols, $\mathbf{w} = \left\{ w_l \middle| w_l \in \left\{0, \ldots, 2^M - 1\right\}\right\}$ where $M \geq 1$ and $l = 1, \ldots, L$, i.e., LM bits data, are hidden into grayscale image I whose luminance values are in $\{0, 1, \ldots, A\}$ and B_x and B_y in the EtC system are the same even numbers.

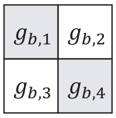


Fig. 6 The b-th 2×2-sized block in the proposed scheme. Gray main diagonal pixels are used for data hiding.

3.2 Data Hiding

The algorithm for data hiding shown in Fig. 5 is explained here.

Step 1. Divide grayscale image I into B of 2×2-sized blocks.

Step 2. Derive the difference between main diagonal elements and that between antidiagonal elements in each block, as

$$d_{b,1} = g_{b,1} - g_{b,4}, \text{ and} \tag{2}$$

$$d_{b,2} = g_{b,2} - g_{b,3}, \tag{3}$$

where $g_{b,1}$, $g_{b,2}$, $g_{b,3}$, and $g_{b,4}$ are luminance values in the b-block, c.f., Fig. 6, and $b = 1, 2, \ldots, B$.

Step 3. Find maximum absolute difference d as

$$d = \max_{a,b} \left| d_{b,a} \right|, \tag{4}$$

where $a \in \{1, 2\}$.

Step 4. Parameter M is firstly hidden to the image as 2^M; Randomly find 2^M of blocks which satisfy either

$$d_{b,1} = 1, \tag{5}$$

$$g_{b,1} \leq A - k, \text{ and} \tag{6}$$

$$g_{b,4} \geq k, \tag{7}$$

or

$$d_{b,1} = -1, \tag{8}$$

$$g_{b,1} \geq k, \text{ and} \tag{9}$$

$$g_{b,4} \leq A - k, \tag{10}$$

where $k = \left\lfloor \frac{A}{2} \right\rfloor$.

Step 5. Hide M into the image by applying following equations to selected 2^M blocks.

$$\hat{g}_{b,1} = g_{b,1} + d_{b,1}k, \text{ and} \tag{11}$$
$$\hat{g}_{b,4} = g_{b,1} - d_{b,1}k, \tag{12}$$

where $\hat{g}_{b,1}$ and $\hat{g}_{b,4}$ are marked version of $g_{b,1}$ and $g_{b,4}$, respectively.

Step 6. To hide L of 2^M-ary symbols $\mathbf{w}$ to the image where $L = A - d - 4$ (c.f., Fig. 7 and Sect. 3.5), repeat Step 7 to Step 9 unless $l > L$. Set $l := 1$.

Step 7. Continue to Step 9 if $w_l = 0$. If $w_l > 0$, set $k = \left\lfloor \frac{A-l}{2} \right\rfloor$. If $A - l$ is even, randomly find w_l of unmarked blocks which satisfy

$$d_{b,1} = 0, \tag{13}$$
$$g_{b,1} \leq A - k, \text{ and} \tag{14}$$
$$g_{b,4} \geq k. \tag{15}$$

If $A - l$ is odd, randomly find w_l of unmarked blocks which satisfy either Eqs. (5), (6), and (7), or Eqs. (8), (9), and (10).

Step 8. If $A - l$ is even, hide w_l into the image by applying following equations to selected w_l blocks.

$$\hat{g}_{b,1} = g_{b,1} + k, \text{ and} \tag{16}$$
$$\hat{g}_{b,4} = g_{b,1} - k. \tag{17}$$

If $A - l$ is odd, hide w_l into the image by applying Eqs. (11) and (12) to selected w_l blocks.

Step 9. Set $l := l + 1$. Back to Step 7 unless $l > L$.

Step 10. Randomly find 2^M of blocks by Step 7 and hide M into the image by Step 8 under the condition $k = d + 2$.

Step 11. All blocks form the marked image $\hat{I}$.

3.3 Data Extraction

This algorithm can take out embedded L of 2^M-ary symbols from the image encrypted by the EtC system [9].

Step 1. Divide marked grayscale image $\hat{I}$ into B of 2×2-sized blocks.

Step 2. Derive the difference between main diagonal elements and that between antidiagonal elements in each block, as

$$\hat{d}_{b,1} = \hat{g}_{b,1} - \hat{g}_{b,4}, \text{ and} \tag{18}$$
$$\hat{d}_{b,2} = \hat{g}_{b,2} - \hat{g}_{b,3}, \tag{19}$$

Step 3. From $\hat{d}_{b,a}$ where $a \in \{1, 2\}$, derive $\hat{h}(\upsilon)$, the frequency of occurrence for absolute difference $\upsilon = \left|\hat{d}_{b,a}\right|$, where $\upsilon \in \{0, 1, \ldots, A\}$.

Step 4. Extract parameter M from the image as $M = \log_2 \hat{h}(A)$.

Step 5. Find d as $d = \delta$ where $\hat{h}(\delta + 1) = 0$, $\hat{h}(\delta + 2) = 2^M$, and $\hat{h}(\delta + 3) = 0$. If multiple δs are found, choose the maximum one as δ.

Step 6. Extract L of 2^M-ary symbols $\mathbf{w}$. The l-th symbol w_l is extracted as $w_l = \hat{h}(A - l)$ for $l = 1, \ldots, L$ where $L = A - d - 4$.

3.4 Image Recovery

The algorithm for image recovery is described here.

Step 1. Do Steps 1, 2, 3, 4, and 5 of the above described data extraction algorithm.

Step 2. Find $\hat{h}(A)$ of blocks whose absolute difference of main diagonal or antidiagonal elements is A and identify the marked diagonal, i.e., main diagonal or antidiagonal, to recover the original state of blocks. If $\hat{d}_{b,1}$ given by Eq. (18) is equal to A, main diagonal elements are marked. Otherwise, antidiagonal elements are marked because of block rotation/flipping in the EtC system. To recover the unmarked blocks, apply

$$g_{b,1} = \hat{g}_{b,1} - \operatorname{sign}(\hat{g}_{b,1} - \hat{g}_{b,4})\,\kappa, \text{ and} \tag{20}$$
$$g_{b,4} = \hat{g}_{b,4} + \operatorname{sign}(\hat{g}_{b,1} - \hat{g}_{b,4})\,\kappa, \tag{21}$$

to blocks whose main diagonal elements are marked, or apply

$$g_{b,2} = \hat{g}_{b,2} - \operatorname{sign}(\hat{g}_{b,2} - \hat{g}_{b,3})\,\kappa, \text{ and} \tag{22}$$
$$g_{b,3} = \hat{g}_{b,3} + \operatorname{sign}(\hat{g}_{b,2} - \hat{g}_{b,3})\,\kappa, \tag{23}$$

to blocks whose antidiagonal elements are marked, where sign() returns the positive and negative sign of the input and $\kappa = \left\lfloor \frac{A}{2} \right\rfloor$.

Step 3. Recover the original state of blocks by applying Eqs. (20) and (21) to blocks whose absolute difference of main diagonal elements is $A - l$, or by applying Eqs. (22) and (23) to blocks whose absolute difference of antidiagonal elements is $A - l$, where $\kappa = \left\lfloor \frac{A-l}{2} \right\rfloor$ and $l = 1, \ldots, L$.

Step 4. Do Step 3, but absolute difference is $d + 2$ and $\kappa = \left\lfloor \frac{d+2}{2} \right\rfloor$.

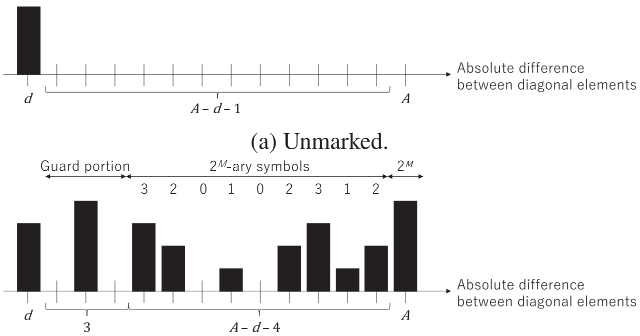
Step 5. Recovered blocks form unmarked image I.

3.5 Features

This section summarizes the features of the proposed scheme from the viewpoint of requirements described in Sect. 3.1.

3.5.1 Coping with the EtC System [9]

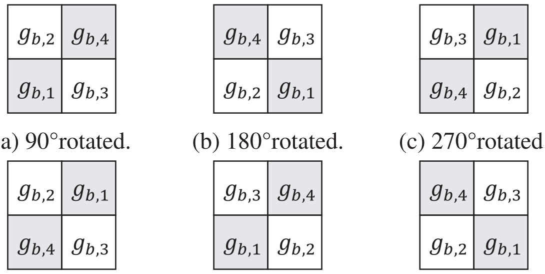
To cope with block permutation in the EtC system, the proposed scheme expands the difference between main diagonal elements of blocks as Eqs. (11), (12), (16), and (17)



(a) Unmarked.

(b) Marked. Parameter M represented as 2^M, data consisting of nine ($L = 9$) quaternary ($M = 2$) symbols '213201023,' and the guard portion with three symbols '02^M0' are hidden to the image (right to left).

Fig. 7 An example of histogram of absolute difference between main diagonal elements in blocks.



(a) 90°rotated. (b) 180°rotated. (c) 270°rotated.

(d) H flipped. (e) V flipped. (f) H & V flipped.

Fig. 8 Rotated/flipped blocks (H and V in (d), (e), and (f) are horizontally and vertically, respectively).

to map 2^M-ary symbols to the histogram of the image, c.f., Fig. 7. Different from ordinary difference expansion-based schemes [18], [19], [23] needing an image-dependent location map which indicates the location of marked/unmarked pairs in the image for data extraction and image recovery, the proposed scheme easily identifies marked blocks by the difference of diagonal elements of blocks as Steps 2, 3, and 4. Furthermore, the scheme does not have to identify marked blocks as Step 6 of the data extraction algorithm. So, it concludes the proposed scheme is invariant for block permutation.

Here, the absolute difference instead of the difference between main diagonal elements of blocks is used for data hiding, because the scheme copes with luminance inversion in the EtC system. For a non-inverted blocks, absolute difference is

$$\left|\hat{d}_{b,1}\right| = \left|\hat{g}_{b,1} - \hat{g}_{b,4}\right|, \tag{24}$$

and that for an inverted block is

$$\left|\hat{d}_{b,1}\right| = \left|(A - \hat{g}_{b,1}) - (A - \hat{g}_{b,4})\right| = \left|\hat{g}_{b,4} - \hat{g}_{b,1}\right|. \tag{25}$$

As they result in the same value, it is explicit that the scheme is invariant for luminance inversion.

In addition, the absolute difference of main diagonal and antidiagonal elements of blocks is used for data extraction and image recovery to cope with block rotation/flipping in the EtC system, as Step 3 of data extraction algorithm and Steps 1, 2, 3, and 4 of the image recovery algorithm. Figure 8 shows rotated/flipped version of the block shown in Fig. 6. It is shown that original main diagonal elements can become antidiagonal elements in transformed blocks, the scheme, however, can uniquely identify marked diagonal elements. Since the absolute difference between antidiagonal elements in an original block does not exceed d, c.f., Step 3 of data hiding algorithm, marked diagonal elements whose absolute difference is larger than d can be easily distinguished from unmarked diagonal elements. Thus, it is concluded that this scheme is invariant for block rotation/flipping.

It is noteworthy that the proposed scheme can hide data to the image encrypted by the EtC system [9] and can take hidden data from the decrypted image as well as conventional schemes [15], [16], whereas the detailed explanation is omitted.

3.5.2 Processing without Image Identification

The proposed scheme hides parameter M into the image twice as Steps 4, 5, and 10 of data embedding algorithm. Steps 4 and 5 of data embedding algorithm transmits parameter M itself from the data hiding part to the data extraction and image recovery part as Step 4 of data extraction algorithm and Step 1 of image recovery algorithm. Step 10 of data hiding algorithm inserts a guard portion between marked and unmarked blocks to distinguish marked blocks from unmarked blocks as Step 5 of data extraction algorithm and Step 1 of image recovery algorithm. Since all w_l's are less than 2^M and condition that $\hat{h}(d+1) = 0$, $\hat{h}(d+2) = 2^M$, and $\hat{h}(d+3) = 0$ rarely occurs, it is easily determine the guard portion. Consequently, it is confirmed that the scheme does not need image identification.

4. Experimental Results

By using 24 of 8-bits 512 × 512-sized grayscale images (or converted to grayscale images) [24], maximum absolute difference between diagonal elements, d's are listed in Table 1. There are images whose d is equal to A, and the proposed scheme does not hide data into these images.

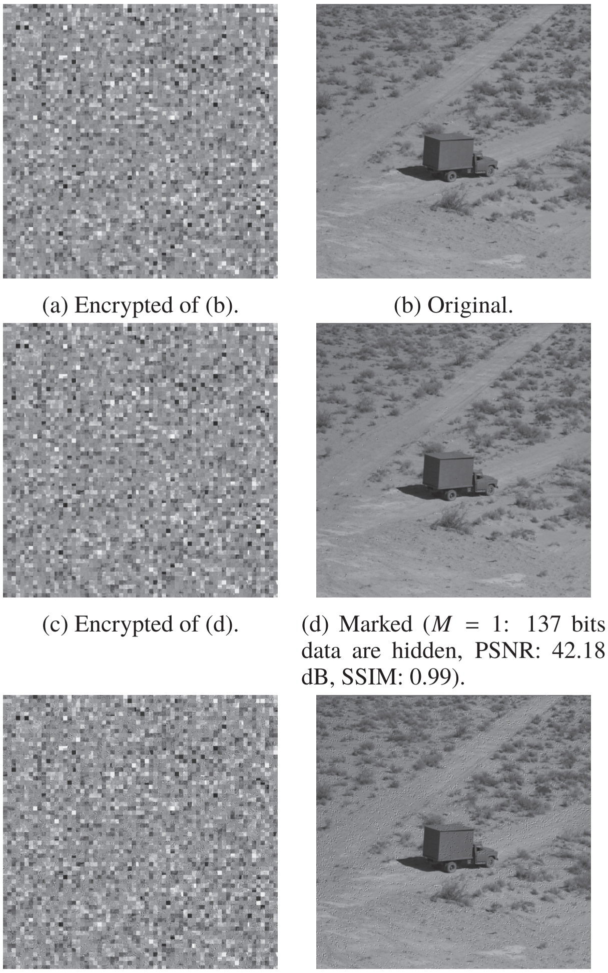
Table 2 shows the maximum embeddable payload size for images whose d is less than A. The payload size is not so large but it could be enough for some applications like labeling, tagging, and so on. It is noted that the proposed scheme find blocks for data hiding based on criteria given by Eqs. (5), (6), (7), (8), (9), (10), (13), (14), and (15), so no block satisfying the required condition can be found dependently on images, i.e., the maximum embeddable payload size results in zero bits, similarly to other reversible data hiding schemes [26], [27].

Table 1 Maximum absolute difference between diagonal elements in the image, d.

Image	d	Image	d	Image	d	Image	d
4.2.01	173	4.2.02	255	4.2.03	196	4.2.04	150
4.2.05	148	4.2.06	191	4.2.07	185	5.2.08	255
5.2.09	236	5.2.10	174	7.1.01	114	7.1.02	172
7.1.03	107	7.1.04	135	7.1.05	173	7.1.06	136
7.1.07	152	7.1.08	130	7.1.09	133	7.1.10	83
boat	218	house	204	gray21	164	ruler	255

Table 2 Maximum embeddable payload size [bits]. $M = 0$ for images without enough blocks satisfying the required condition for data hiding.

Image	M	Size	Image	M	Size	Image	M	Size
4.2.01	4	312	4.2.03	5	275	4.2.04	6	606
4.2.05	3	309	4.2.06	2	120	4.2.07	4	264
5.2.09	2	30	5.2.10	0	0	7.1.01	6	822
7.1.02	1	79	7.1.03	0	0	7.1.04	0	0
7.1.05	0	0	7.1.06	0	0	7.1.07	0	0
7.1.08	0	0	7.1.09	0	0	7.1.10	0	0
boat	5	165	house	4	188	gray21	0	0



(a) Encrypted of (b).

(b) Original.

(c) Encrypted of (d).

(d) Marked ($M = 1$: 137 bits data are hidden, PSNR: 42.18 dB, SSIM: 0.99).

(e) Encrypted of (f).

(f) Marked ($M = 6$: 822 bits data are hidden, PSNR: 31.60 dB, SSIM: 0.87).

Fig. 9 Image examples for image '7.1.01' where $B_x = B_y = 8$ for encryption and K_1's, K_2's, and K_3's are common for (a), (c), and (e).

This paper assumes that after an image is marked by the proposed scheme, the EtC system visually encrypts the marked image based on $B_x \times B_y$-sized blocks before transmitting the image. Figures 9 (a), (c), and (e) show encrypted image examples for '7.1.01' where Figs. 9 (b), (d), and (f) show those unencrypted version. Since the correlation coefficient in a block is not changed by encryption, to evaluate the randomness based on the correlation coefficient, the $1/B_x \times 1/B_y$-sized downsampled image is generated from an encrypted image where $B_x = B_y = 8$ here. From the downsampled image, 2000 pixels are randomly selected and those adjacent pixels in horizontal, vertical, and diagonal dimensions are used for evaluating correlation. From Tables 3 (a) and (b), it is found that the proposed scheme keeps the randomness of encrypted images, where 50 different 2^M-ary symbols that are converted from equiprobable binary sequences are hidden to 11 embeddable images. In addition, Table 4 lists compression ratios of JPEG 2000 [28] lossless compression for 11 images, where the compression ratio is given by the uncompressed file size over the compressed file size, so the better compression is achieved, the larger compression ratio becomes. It is found again the proposed scheme keeps the randomness of encrypted images from the fact that the compression ratios for marked and encrypted images are almost the same as those for encrypted images as shown in Tables 4 (a) and (b).

The performance of the proposed scheme itself is investigated for reference because the proposed scheme is independent from the EtC system. Averaged peak signal-to-noise ratios (PSNR's) and averaged structural similarities [25] (SSIM's) of marked image are listed in Table 5. Hiding binary data into the image ($M = 1$) serves the small embeddable payload size but better image quality, c.f., Fig. 9 (d). Since the scheme embeds 2^M-ary symbols by the pulse amplitude modulation-like manner, i.e., large differences could be given to images by data hiding, for achieving data extraction and image recovery without image identification as described in Sect. 3.5.2. Thus, under some conditions, the naturalness (Tables 3 (c) and (d)), compression ratios (Tables 4 (c) and (d)), and quality (Table 5) of marked images are much degraded. Further development/sophistication of the scheme is expected for making the better use of the scheme's independence from the EtC system.

5. Conclusions

This paper has proposed a reversible data hiding scheme for the EtC system. This scheme hides data to unencrypted image and takes hidden data out from the image encrypted by the system, as well as conventional schemes. In contrast with conventional schemes, the proposed scheme cope with luminance inversion in the EtC system as well as block permutation and block rotation/flipping. In addition, this scheme does not have to identify the target image to take hidden data out from the image, whereas conventional schemes need to do.

Table 3 Correlation coefficients between two horizontal (H), vertical (V), and diagonal (D) blocks for 11 embeddable images, c.f., Table 2, where marked images convey those maximum embeddable payloads.

(a) Average for encrypted.

	4.2.01	4.2.03	4.2.04	4.2.05	4.2.06	4.2.07	5.2.09	7.1.01	7.1.02	boat	house
H	0.01	-0.01	0.00	0.00	0.00	-0.00	-0.00	-0.00	-0.00	-0.00	0.00
V	-0.01	-0.00	-0.00	-0.01	-0.00	0.00	-0.00	-0.00	-0.01	0.01	-0.00
D	-0.00	0.01	0.01	0.00	0.00	0.00	0.00	0.00	0.00	0.01	0.01

(b) Average for marked and encrypted (the maximum embeddable payload is hidden to an image).

	4.2.01	4.2.03	4.2.04	4.2.05	4.2.06	4.2.07	5.2.09	7.1.01	7.1.02	boat	house
H	0.01	-0.01	0.00	-0.01	0.00	0.00	-0.01	0.00	-0.01	0.00	-0.01
V	-0.02	-0.00	-0.00	-0.00	0.00	-0.00	-0.01	-0.02	-0.01	0.02	-0.01
D	-0.01	-0.01	0.00	-0.01	0.00	0.01	-0.01	-0.01	-0.01	0.00	0.01

(c) Original.

	4.2.01	4.2.03	4.2.04	4.2.05	4.2.06	4.2.07	5.2.09	7.1.01	7.1.02	boat	house
H	0.80	0.54	0.70	0.68	0.79	0.74	0.34	0.73	0.54	0.75	0.71
V	0.89	0.55	0.84	0.68	0.79	0.82	0.23	0.57	0.62	0.72	0.74
D	0.77	0.49	0.64	0.54	0.70	0.63	0.21	0.54	0.44	0.59	0.58

(d) Average for marked (the maximum embeddable payload is hidden to an image).

	4.2.01	4.2.03	4.2.04	4.2.05	4.2.06	4.2.07	5.2.09	7.1.01	7.1.02	boat	house
H	0.78	0.50	0.58	0.66	0.78	0.72	0.35	0.42	0.56	0.72	0.66
V	0.86	0.54	0.69	0.66	0.78	0.79	0.23	0.34	0.60	0.66	0.70
D	0.74	0.47	0.54	0.53	0.71	0.62	0.20	0.31	0.47	0.56	0.55

Table 4 Compression ratios of JPEG 2000 [28] lossless compression for 11 embeddable images, c.f., Table 2.

(a) Average for encrypted.

Image	Ratio	Image	Ratio	Image	Ratio	Image	Ratio
4.2.01	1.56	4.2.03	1.19	4.2.04	1.48	4.2.05	1.47
4.2.06	1.29	4.2.07	1.40	5.2.09	1.29	7.1.01	1.49
7.1.02	1.61	boat	1.37	house	1.41		

(b) Average for embedded and encrypted (the maximum embeddable payload is hidden to an image).

Image	Ratio	Image	Ratio	Image	Ratio	Image	Ratio
4.2.01	1.53	4.2.03	1.18	4.2.04	1.41	4.2.05	1.45
4.2.06	1.29	4.2.07	1.38	5.2.09	1.29	7.1.01	1.40
7.1.02	1.61	boat	1.36	house	1.40		

(c) Original.

Image	Ratio	Image	Ratio	Image	Ratio	Image	Ratio
4.2.01	2.35	4.2.03	1.32	4.2.04	1.99	4.2.05	2.23
4.2.06	1.61	4.2.07	1.81	5.2.09	1.62	7.1.01	1.76
7.1.02	2.38	boat	1.72	house	2.08		

(d) Average for marked (the maximum embeddable payload is hidden to an image).

Image	Ratio	Image	Ratio	Image	Ratio	Image	Ratio
4.2.01	1.97	4.2.03	1.26	4.2.04	1.49	4.2.05	1.95
4.2.06	1.54	4.2.07	1.65	5.2.09	1.53	7.1.01	1.36
7.1.02	2.14	boat	1.57	house	1.82		

Further works include increasing the maximum embeddable payload size, improvement of the image quality of marked image, and security enhancement for other applications.

Table 5 Image quality of marked images for 11 embeddable images, c.f., Table 2, where the maximum embeddable payload is hidden to an image.

(a) Averaged peak signal-to-noise ratios (PSNR's) [dB].

Image	PSNR	Image	PSNR	Image	PSNR	Image	PSNR
4.2.01	36.23	4.2.03	35.50	4.2.04	32.17	4.2.05	37.67
4.2.06	41.14	4.2.07	36.70	5.2.09	45.09	7.1.01	31.60
7.1.02	42.61	boat	37.18	house	37.75		

(b) Averaged structural similarities (SSIM's) [25].

Image	SSIM	Image	SSIM	Image	SSIM	Image	SSIM
4.2.01	0.96	4.2.03	0.97	4.2.04	0.89	4.2.05	0.98
4.2.06	0.99	4.2.07	0.97	5.2.09	0.99	7.1.01	0.87
7.1.02	0.99	boat	0.97	house	0.98		

References

[1] A. Piva and S. Katzenbeisser, eds., "Editorial: signal processing in the encrypted domain," EURASIP J. Information Security, vol.2007, July 2007.

[2] M. Fujiyoshi, K. Kuroiwa, and H. Kiya, "A scrambling method for Motion JPEG videos enabling moving objects detection from scrambled videos," Proc. IEEE Int. Conf. Image Process., San Diego, CA, the U.S., pp.773–776, Oct. 2008.

[3] M. Johnson, P. Ishwar, V. Prabhakaran, D. Schonberg, and K. Ramchandran, "On compressing encrypted data," IEEE Trans. Signal Process., vol.52, no.10, pp.2992–3006, Oct. 2004.

[4] D. Schonberg, S.C. Draper, C. Yeo, and K. Ramchandran, "Toward compression of encrypted images and video sequences," IEEE Trans. Inf. Forensics Security, vol.3, no.4, pp.749–762, Dec. 2008.

[5] W. Liu, W. Zeng, L. Dong, and Q. Yao, "Efficient compression of encrypted grayscale images," IEEE Trans. Image Process., vol.19, no.4, pp.1097–1102, April 2010.

[6] X. Zhang, "Lossy compression and iterative reconstruction for en-

crypted image," IEEE Trans. Inf. Forensics Security, vol.6, no.1, pp.53–58, March 2011.
[7] X. Zhang, G. Feng, Y. Ren, and Z. Qian, "Scalable coding of encrypted images," IEEE Trans. Image Process., vol.21, no.6, pp.3108–3114, June 2012.
[8] 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. Inf. Forensics Security, vol.9, no.1, pp.39–50, Jan. 2014.
[9] 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.E98-A, no.11, pp.2238–2245, Nov. 2015.
[10] W. Sirichotedumrong, Y. Kinoshita, and H. Kiya, "Pixel-based image encryption without key management for privacy-preserving deep neural networks," IEEE Access, vol.7, pp.177844–177855, Dec. 2019.
[11] T. Nakachi, Y. Bandoh, and H. Kiya, "Secure overcomplete dictionary learning for sparse representation," IEICE Trans. Inf. & Syst., vol.E103-D, no.1, pp.50–58, Jan. 2020.
[12] X. Zhang, "Separable reversible data hiding in encrypted image," IEEE Trans. Inf. Forensics Security, vol.7, no.2, pp.826–832, April 2012.
[13] M. Fujiyoshi, "A separable lossless data embedding scheme in encrypted images considering hierarchical privilege," Proc. EURASIP European Signal Process. Conference, Tu-P3.13, Marrakech, Morocco, Sept. 2013.
[14] X. Zhang, "Commutative reversible data hiding and encryption," Security and Communication Networks, vol.6, no.11, pp.1396–1403, Nov. 2013.
[15] K. Wong and H. Kiya, "Reversible data hiding for compression-friendly image encryption method," Proc. APSIPA Annual Sumit and Conference, Kuala Lumpur, Malaysia, Dec. 2017.
[16] Y. Izawa, R. Hirasawa, S. Imaizumi, and H. Kiya, "A reversible data hiding method for both plain and encrypted images," IEICE Technical Report, vol.119, no.335, pp.29–34, Dec. 2019.
[17] T. Chuman, K. Kurihara, and H. Kiya, "On the security of block scrambling-based EtC systems against extended jigsaw puzzle solver attacks," IEICE Trans. Inf. & Syst., vol.E101-D, no.1, pp.37–44, Jan. 2018.
[18] R. Caldelli, F. Filippini, and R. Becarelli, "Reversible watermarking techniques: An overview and a classification," EURASIP J. Information Security, vol.2010, no.134546, 2010.
[19] Y.Q. Shi, X. Li, X. Zhang, H.T. Wu, and B. Ma, "Reversible data hiding: Advances in the past two decades," IEEE Access, vol.4, pp.3210–3237, May 2016.
[20] S. Han, M. Fujiyoshi, and H. Kiya, "A reversible image authentication method without memorization of hiding parameters," IEICE Trans. Fundamentals, vol.E92-A, no.10, pp.2572–2579, Oct. 2009.
[21] M. Fujiyoshi and H. Kiya, "A blind reversible data hiding method for high dynamic range images taking advantage of sparse histogram," LNCS, vol.10431, pp.347–361, Springer Berlin Heidelberg, Magdeburg, Germany, Aug. 2017.
[22] Z. Ni, Y.Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," IEEE Trans. Circuits Syst. Video Technol., vol.16, no.3, pp.354–362, March 2006.
[23] J. Tian, "Reversible data embedding using a difference expansion," IEEE Trans. Circuits Syst. Video Technol., vol.13, no.8, pp.890–896, Aug. 2003.
[24] Signal & Image Processing Institute, University of Southern California, "The USC-SIPI Image Database." http://sipi.usc.edu/database/
[25] Z. Wang, A.C. Bovik, H.R. Sheikh, and E.P. Simoncelli, "Image quality assessment: From error visibility to structural similarity," IEEE Trans. Image Process., vol.13, no.4, pp.600–612, April 2004.
[26] H.L. Jin, M. Fujiyoshi, and H. Kiya, "Lossless data hiding in the spatial domain for high quality images," IEICE Trans. Fundamentals, vol.E90, no.4, pp.771–777, April 2007.
[27] M. Fujiyoshi, S. Sato, H.L. Jin, and H. Kiya, "A location-map free reversible data hiding method using block-based single parameter," Proc. IEEE Int. Conf. Image Process., San Antonio, TX, the U.S., vol.III, pp.257–260, Sept. 2007.
[28] Information technology — JPEG 2000 image coding system – Part 1: Core coding system, Int. Std. ISO/IEC IS-15444-1, Dec. 2000. JPEG 2000.

Masaaki Fujiyoshi received his B.Arts, M.Eng., and Ph.D. degrees from Saitama University, Japan, in 1995, 1997, and 2001, respectively. In 2001, he joined Tokyo Metropolitan University, where he is currently a Full Professor. He is a Member of IEEE, EURASIP, APSIPA, ITE, and JSET. He currently serves as Director, General Affairs, IEICE Engineering Sciences Society and Vice Chair, IEICE Enriched Multimedia Technical Committee. He is/was Guest/Associate Editor of several Special Sections of IEICE Transactions. He has received best paper award from IEICE and ITE, respectively.

Ruifeng Li received his B.Eng. degree from Qingdao University, P.R.C., in 2017. He is currently a Research Student at Tokyo Metropolitan University, Japan.

Hitoshi Kiya received his B.Eng. and M.Eng. degrees from Nagaoka University of Technology, Japan, in 1980 and 1982, respectively, and his Dr.Eng. degree from Tokyo Metropolitan University, Japan 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 of APSIPA, and he served as Inaugural Vice President (Technical Activities) of APSIPA from 2009 to 2013, and as Regional Director-at-Large for Region 10 of IEEE Signal Processing Society from 2016 to 2017. He was also President of 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. Signal Processing, Image Processing, and Information Forensics and Security, Chair of two technical committees (TCs) and Member of nine TCs including APSIPA Image, Video, and Multimedia TC and IEEE Information Forensics and Security TC. He has organized many 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 nine best paper awards.