*APSIPA Transactions on Signal and Information Processing, 2023, 12, e31*


**Original Paper**

# Reversible Data Hiding in Compressible Encrypted Images with Capacity Enhancement

Ryota Motomura[1], Shoko Imaizumi[1*] and Hitoshi Kiya[2]

[1] *Chiba University, Chiba, Japan*
[2] *Tokyo Metropolitan University, Tokyo, Japan*

ABSTRACT

In this paper, we propose a method for high-capacity reversible data hiding in compressible encrypted images. While reversible data hiding in encrypted images (RDH-EI) has been actively studied, most previous research in this field has focused on the hiding capacity. We previously proposed an RDH-EI method that achieves both a high hiding capacity and high compression performance simultaneously. The method can effectively compress marked encrypted images using lossless image coding standards with a hiding capacity of up to about 1 bpp. In addition, there is an option to decrypt marked encrypted images without data extraction, so marked images can be obtained, still containing the embedded data, i.e., payload. Without losing the advantages of the previous method, we propose an extended method, in which the highest frequency bin is constantly used for data hiding. Consequently, the hiding capacity is further enhanced up to 2.45 bpp for each color component in the proposed method. Through our experiments, we prove the superiority of the proposed method.

*Keywords:* Reversible data hiding in encrypted images, hiding capacity, compressible image encryption, encryption-then-compression system, lossless compression.

*Corresponding author: Shoko Imaizumi, imaizumi@chiba-u.jp.

Received 07 February 2023; Revised 23 May 2023
ISSN 2048-7703; DOI 10.1561/116.00000014

## 1 Introduction

With the rapid development of cloud services, we currently have more and more opportunities to store and share images through external servers and services. In addition, the data amount of each image is increasing due to higher resolutions; it is thus desirable to compress images. As a result, data hiding has been attracting attention as a technique for protecting copyright. In particular, reversible data hiding (RDH) has been actively studied since it can completely restore an original image by extracting embedded data (hereafter, a payload) [2, 6, 14, 17, 22, 24]. RDH methods could be particularly useful in fields where the preservation of the original state is required, such as for medical, satellite, and military images.

More recently, methods for reversible data hiding in encrypted images (RDH-EI) have also been studied [1, 3, 5, 7, 15, 16, 18–21, 25, 27–29]. For these methods, we assume that an image owner first encrypts a target image, and a third party such as a service provider (hereafter, a data hider) then embeds arbitrary data in the encrypted domain. This allows the image owner and data hider to perform independent processing without disclosing the image content to the data hider. We can suppose multiple applications, e.g., cloud storage, photo sale services, and medical image management [18]. For instance, in cloud storage, an image owner would first encrypt his/her images to protect privacy and then upload the encrypted images to a cloud. On the cloud provider side, administrative data such as server information and annotation data is embedded into the images for management purposes. A high hiding capacity is one of the common requirements in the field of data hiding techniques. In RDH-EI, it is particularly desirable to embed image information, e.g., categorical data and annotation data, to obtain an outline of an image in the encrypted domain.

Puteaux *et al.* proposed a high-capacity RDH-EI method for gray-scale images by using most-significant-bit substitution instead of the commonly used least-significant-bit substitution [19]. Applied to color images, that method achieved a high hiding capacity of 1.64 bpp on average for each color component. However, since the encryption process uses the pixel-by-pixel XOR operation, compression of marked encrypted images is ineffective. In a previous work, the authors proposed an effective method in terms of both compression efficiency and hiding capacity [16]. In the method, a grayscale-based encryption-then-compression (EtC) system [4] was introduced for the encryption process, which enabled lossless compression of marked encrypted images using international standards. For the data hiding process, a prediction error expansion with histogram shifting (PEE-HS) method [14] was adopted to achieve a high hiding capacity of up to about 1 bpp for each color component. Note that the PEE-HS method was modified from the original [14] to be effectively applied to

EtC images. Furthermore, by decrypting a marked encrypted image without extracting the payload, we can obtain a marked image in which the payload is still contained.

In this paper, we extended the data hiding process of our previous method so as to significantly improve the hiding capacity without losing the advantages. Our previous method never uses bins repeatedly that have been once used for data hiding in the prediction error histogram. Thus, even when a bin that has already been used still has the highest frequency, we could not use the bin again. We focused on capacity enhancement by constantly using the highest frequency bin without any constraints in this paper. The proposed method achieves a higher hiding capacity of 2.45 bpp for each color component by selecting two bins for data hiding from all bins each time, including bins that have already been used. Experimental results demonstrate the effectiveness of the proposed method in terms of the hiding capacity, compression performance of marked encrypted images, and marked image quality.

## 2 Related Work

### *2.1 RDH-EI Methods*

RDH methods have been generally studied in the plane domain, but recently, those in the encrypted domain have also been attractive for researchers in terms of security enhancement [1, 3, 5, 7, 15, 16, 18–21, 25, 27–29]. RDH-EI can clearly separate the roles of image owner and data hider. The image owner first encrypts target images; the data hider embeds arbitrary payloads into the encrypted images without knowing the image content. The data hider may embed payloads for authentication or management, so a high hiding capacity is required. Additionally, from the aspect of storage equipment for the service provider, a high compression performance for marked encrypted images would be desirable.

RDH-EI methods can be divided into two types: reserving room before encryption (RRBE) and vacating room after encryption (VRAE). In the former, an original image is pre-processed by an image owner before encryption so as to ensure an embeddable area. The image owner encrypts the pre-processed image and then sends the encrypted image to a data hider. The data hider embeds an arbitrary payload into the reserved area. In comparison, the pre-processing step is not required in the latter methods. An image owner encrypts an original image directly and then sends the encrypted image to a data hider. The data hider then embeds the information into the encrypted image. A data hider vacates the embeddable area in the encrypted image and hides the desired payload into the area.

#### 2.1.1 Reserving Room Before Encryption (RRBE)

Many RRBE methods have been proposed to pursue a high hiding capacity [1, 5, 7, 19–21, 27]. For example, Puteaux *et al.* [20] boldly introduced most significant bits (MSBs) for prediction and replacement instead of using least significant bits (LSBs). Several methods were proposed by extending this method [20] to enhance the hiding capacity or security [5, 21, 27]. Nevertheless, these extended methods cannot fully retrieve the original image in multiple cases, so Hirasawa *et al.* [7] modified some conditions of the original method [20] and attained full reversibility. Later, Puteaux *et al.* [19] proposed a more efficient method for grayscale images, in which full reversibility was guaranteed, and the hiding capacity was drastically enhanced. In the method, all bit-planes of a target image are processed recursively from the MSBs to the LSBs to the maximum extent. When the method was applied to color images, the hiding capacity was 1.64 bpp on average for each color component. That method, however, has a constraint in the restoration process; data extraction should be conducted before decryption no matter the case. Arai *et al.* [1] proposed another method that independently conducts encryption and data hiding by using bit-plane partitions. Thus, decryption and data extraction can be performed without restriction on their order. This method was originally proposed for grayscale images. When we simply extended the method for color images, the hiding capacity was 1.99 bpp for each color component. These high-capacity methods [1, 5, 7, 19–21, 27], however, can never compress marked encrypted images that were bit-wise encrypted using an exclusive-or operation. Further, in RRBE, an image owner should preliminarily reserve the embeddable area before encryption. This would limit the range of practical applications.

#### 2.1.2 Vacating Room After Encryption (VRAE)

In recent years, VRAE methods have also attracted attention in this field [3, 16, 25]. In VRAE, a data hider vacates an embeddable area in an encrypted image. Thus, pre-processing is not required on the image owner side, and the embeddable area consequently can be concealed from the image owner. It is apparent that VRAE is more suitable for practical use than RRBE. Wang *et al.* [25] proposed a method using pixel value ordering (PVO). An original image is divided into blocks with $2 \times 2$ pixels and then encrypted by not only block shuffling but also pixel shuffling within each block. Data hiding is conducted by PVO. Accordingly, the method attained a hiding capacity of up to 0.5 bpp. Chen and Chang [3] proposed another method, in which the hiding capacity surpassed Wang *et al.*'s method [25]. The method divides an original image into blocks with $3 \times 3$ pixels and performs block-by-block encryption. Multiple upper bit-planes in each block are then replaced with a payload. In light of the compression capability, however, it is difficult for these two methods to

compress marked encrypted images. Further, these methods should extract the payload before decryption. For instance, Figure 1(b) shows a decrypted image obtained by Chen *et al.*'s method [3]. It is hard to recognize the image content. Additionally, this image still contains a payload, but the payload cannot be extracted from the decrypted image. Thus, decryption without data extraction is meaningless in these methods. The image content cannot be confirmed because the pixel values have been significantly varied by the data-hiding process. In contrast, the proposed method discloses the image content by decryption only without data extraction.

(a) (b)

Figure 1: Decrypted image without data extraction by previous method [3] (kodim5). (a) Original image, (b) decrypted image.

#### *2.1.3 Our Goal*

To tackle the above issue, we previously proposed a novel VRAE method that achieved both a high hiding capacity and high compression performance simultaneously [16]. This method introduced an EtC system [4], which is a block-wise encryption, so the inter-pixel correlation in each block is stable before/after encryption. Since we could obtain prediction values with high accuracy in the encrypted domain, the hiding capacity was 0.94 bpp on average for each color component when using PEE-HS [14]. Further, this method can compress marked encrypted images using lossless image coding standards such as JPEG-LS [26] and JPEG 2000 [10]. It can omit the data extraction process and decrypt only marked encrypted images. This leads to the derivation of marked images with a payload, in which the image content is disclosed. Preserving the advantages of the method [16], this paper proposes an extended VRAE method, where the hiding capacity is over 2.5 times more.

### *2.2 Existing Compressible RDH-EI Method*

We previously proposed an RDH-EI method that simultaneously had both a high hiding capacity and high compression performance [16]. Figure 2 shows an outline of the method. In the encryption process, that method uses Chuman

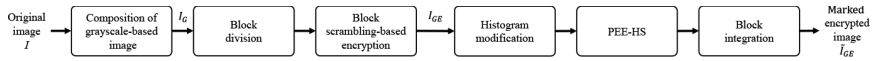



Figure 2: Block diagram of proposed method and previous method [16].

*et al.*'s method [4], where the security has been enhanced compared with the conventional EtC systems [9, 11, 13]. The inter-pixel correlation within each block is consistent before/after the EtC process; thus, we can obtain accurate prediction results for the target pixels by using the median edge detection (MED) predictor even in the encrypted domain. Accordingly, our previous method achieved a high hiding capacity of 0.94 bpp on average through the extension of a PEE-HS method [14]. PEE-HS methods have been widely researched, and many of them achieved a high hiding capacity. These methods were, however, designed for plain images with inter-pixel correlation, so it is not straightforward to apply them to encrypted images. In the previous method, we extended the PEE-HS method enough for application to EtC images.

Furthermore, marked encrypted images can be efficiently compressed using lossless image coding standards, such as JPEG-LS [26] and JPEG 2000 [10]. This is because the inter-pixel correlation within each block is retained even after encryption and data hiding. This method can not only perfectly retrieve an original image and payload but also decrypt a marked encrypted image without data extraction. In this case, a receiver obtains a marked image containing a payload. Obviously, the method can only extract the payload from the marked encrypted image. Thus, we can give a selectable privilege for each receiver.

In the previous method, PEE-HS utilizes multiple bins with high frequencies in a prediction error histogram to embed a payload. The number of bins to be used for data hiding is determined depending on the threshold $L$. A higher hiding capacity can be attained as the value of $L$ becomes larger. However, general PEE-HS methods including the method [14] have prohibited each bin from being used multiple times. Thus, even when a bin that has been once used still has the highest frequency, the bin is never used again. Alternatively, bins with lower frequencies need to be used as $L$ becomes larger.

In the next section, we significantly enhance the hiding capacity by redefining the conditions of the bins to be used for data hiding without losing the advantages of our previous method [16]. Specifically, we focused on constantly using the highest frequency bin without any constraints in the PEE-HS process. The main contribution of this paper is that we designed an extended PEE-HS method that can be effectively used for EtC images.

## 3 Proposed Method

In this section, we propose an extended RDH-EI method with a high hiding capacity and almost the same compression performance compared with our

previous RDH-EI method [16]. The maximum hiding capacity has been intensely extended. Since the proposed method retains the advantages of the previous method [16], marked encrypted images can be efficiently compressed using lossless image coding standards and also be decrypted without data extraction. The outline of the proposed method is analogous to that of the previous method [16]. We describe the detailed procedures in accordance with Figure 2.

### *3.1 Image Encryption*

The proposed method adopts Chuman *et al.*'s method [4] for the encryption process. Note that we omit the color transformation process in the method [4] to guarantee full reversibility and alternatively combine R, G, and B components into a single component on the xy plane in order to form an 8-bit image. This 8-bit image is called a grayscale-based image hereafter.

**Step 1-1:** Combine R, G, and B components of an original image $I$, and single grayscale-based image $I_G$ is derived.

**Step 1-2:** Divide $I_G$ into multiple blocks with $B \times B$ pixels.

**Step 1-3:** Execute position scrambling, block rotation/flip, and negative-positive transformation on each block, and obtain an encrypted image $I_{GE}$.

### *3.2 Data Hiding*

In the proposed method, a payload is embedded based on PEE-HS [14]. We preliminarily perform preprocessing on $I_{GE}$ so as to prevent overflows (OFs) and underflows (UFs) in the pixel values. Note that we should exclude the top-left pixels in each block defined in Section 3.1 from the entire process of data hiding. We explain each part below.

#### *3.2.1 Histogram Modification*

Data hiding using PEE-HS may cause an OF and UF in the value of each pixel. With the following steps, our method preliminarily modifies an image histogram to prevent OFs and UFs in the pixel values. Here, we define $L$ as a parameter to control the hiding capacity; $L$ denotes the number of times a series of the data hiding process is executed.

**Step 2-1:** Explore the smallest bin (hereafter, $ZP_1$) among bins with no pixel in an encrypted image histogram.

**Step 2-2:** To prevent UFs, add 1 to pixels with a value lower than $ZP_1$.

**Step 2-3:** Repeat Steps 2-1 and 2-2 $L-1$ times.

**Step 2-4:** Explore the largest bin (hereafter, $ZP_2$) among bins with no pixel in the encrypted image histogram.

**Step 2-5:** To prevent OFs, subtract 1 from pixels with a value higher than $ZP_2$.

**Step 2-6:** Repeat Steps 2-4 and 2-5 $L-1$ times.

If there is no $ZP_1$ or/and $ZP_2$ in the histogram, we instead use two bins next to each other with the lowest sum of their frequencies. These bins are integrated into one bin, and another bin becomes empty ($LP_1$ or $LP_2$). In such a case, we need to build a location map to identify their original pixel values in the restoration process. The values of $ZP$s/$LP$s and the location map are embedded with a pure payload.

### *3.2.2 PEE-HS*

We extended the original PEE-HS [14] to enhance the hiding capacity. Consequently, the proposed method achieves a hiding capacity of 2.45 bpp, which is more than twice the previous capacity [16]. We describe the data-hiding procedure in reference to Figure 3.

**Step 3-1:** For pixels $p_{i,j}$ in each block, where $0 \leq i < B$ and $0 \leq j < B$, derive predicted values $\hat{p}_{i,j}$ by

$$\hat{p}_{i,j} = \begin{cases} \min(p_{i-1,j},\ p_{i,j-1}), & \text{if } p_{i-1,j-1} \geq \max(p_{i-1,j},\ p_{i,j-1}) \\ \max(p_{i-1,j},\ p_{i,j-1}), & \text{if } p_{i-1,j-1} \leq \min(p_{i-1,j},\ p_{i,j-1}) \\ p_{i-1,j} + p_{i,j-1} - p_{i-1,j-1}, & \text{otherwise.} \end{cases} \tag{1}$$

In respect to $p_{0,j}$ and $p_{i,0}$, obtain $\hat{p}_{0,j}$ and $\hat{p}_{i,0}$ with

$$\hat{p}_{0,j} = p_{0,j-1}, 1 \leq j < B, \tag{2}$$

$$\hat{p}_{i,0} = p_{i-1,0}, 1 \leq i < B, \tag{3}$$

respectively.

**Step 3-2:** Calculate prediction errors $e_{i,j}$ as follows:

$$e_{i,j} = \hat{p}_{i,j} - p_{i,j}. \tag{4}$$

**Step 3-3:** Explore two bins $E_s$ and $E_l$ ($E_s < E_l$), which are next to each other with the highest sum of frequency, from a prediction error histogram (see Figures 3a and 3d).

**Step 3-4:** In the prediction error histogram, vacate the neighboring bins to $E_s$ and $E_l$ (see Figures 3b and 3e):

$$e'_{i,j} = \begin{cases} e_{i,j} + 1, & \text{if } e_{i,j} > E_l \\ e_{i,j} - 1, & \text{if } e_{i,j} < E_s \\ e_{i,j}, & \text{otherwise,} \end{cases} \tag{5}$$

where $e'_{i,j}$ denotes the prediction error after the vacating process.

**Step 3-5:** Embed a payload $w$ into pixels with $e'_{i,j} = E_s$ or $e'_{i,j} = E_l$ (see Figures 3c and 3f):

$$\tilde{e}'_{i,j} = \begin{cases} e'_{i,j} + 1, & \text{if } e'_{i,j} = E_l \text{ and } w_k = 1 \\ e'_{i,j}, & \text{if } e'_{i,j} = E_l \text{ and } w_k = 0 \\ e'_{i,j} - 1, & \text{if } e'_{i,j} = E_s \text{ and } w_k = 1 \\ e'_{i,j}, & \text{if } e'_{i,j} = E_s \text{ and } w_k = 0, \end{cases} \tag{6}$$

where $\tilde{e}'_{i,j}$ and $w_k$ denote the prediction error with a payload bit and the $k$-th bit of $w$, respectively.

**Step 3-6:** Repeat Steps 3-3, 3-4, and 3-5 $L - 1$ times.

**Step 3-7:** Marked pixel values $\tilde{p}_{i,j}$ are given by

$$\tilde{p}_{i,j} = \hat{p}_{i,j} - \tilde{e}'_{i,j}. \tag{7}$$

**Step 3-8:** Integrate all the blocks into a marked encrypted image $\tilde{I}_{GE}$.

The value of $L$ and $L$ pairs of $E_s$ and $E_l$ should be stored as additional information to extract a payload. They are replaced with the LSBs of the pixels excluded from the above process. The LSBs before replacement are embedded with a pure payload.

### *3.3 Image Restoration*

Here, we elaborate the image decryption and data extraction processes. The proposed method has two types of restoration options as shown in Figure 4. First, our method can perfectly retrieve an original image with the normal restoration process consisting of data extraction and image decryption (see Figure 4a). With this option, we first extract the threshold $L$ and $L$ pairs of $E_s$ and $E_l$ from a marked encrypted image. The image is divided into blocks, and the payload is extracted from them using $L$, $E_s$, and $E_l$. We retrieve the histogram of the encrypted image and then decrypt and integrate the blocks.

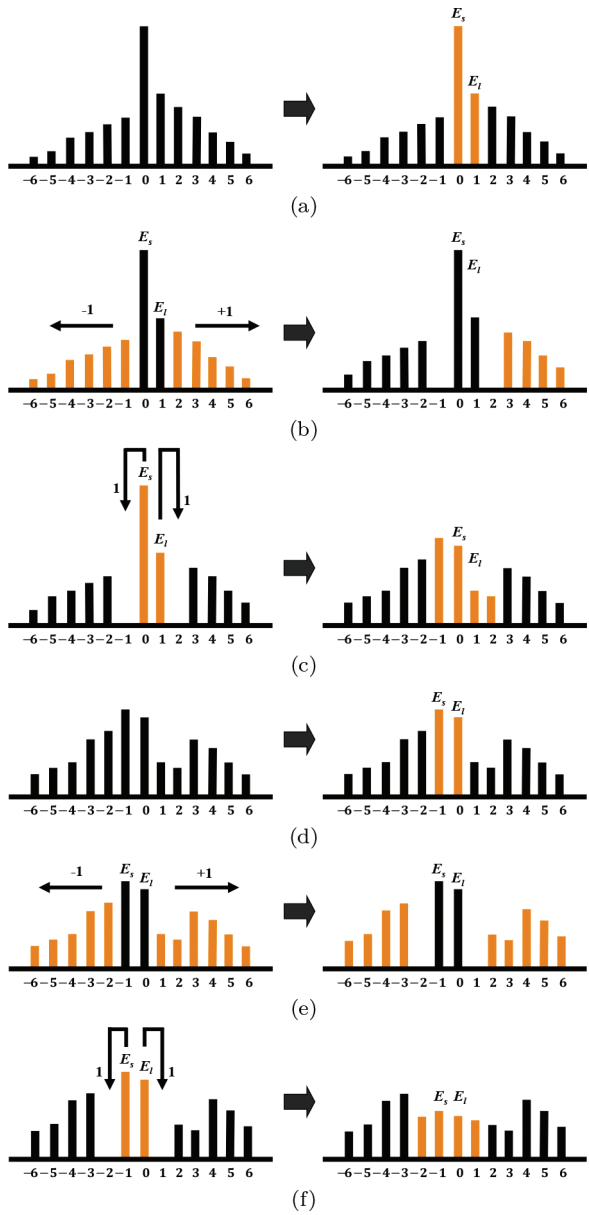



Figure 3: Procedure of data hiding using prediction error histogram (first and second times). (a) Exploration of $E_s$ and $E_L$ (first time), (b) derivation of empty bins (first time), (c) data hiding for pixels with $e_{i,j} = E_s$ and $E_l$ (first time), (d) exploration of $E_s$ and $E_L$ (second time), (e) derivation of empty bins (second time), (f) data hiding for pixels with $e_{i,j} = E_s$ and $E_l$ (second time).

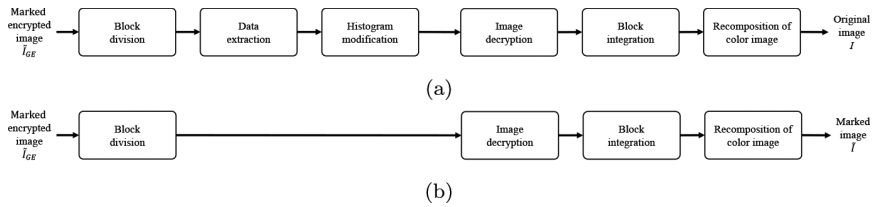



Figure 4: Restoration options. (a) Data extraction and image decryption, (b) image decryption without data extraction.

Finally, the RGB color components are restructured, and the original image is obtained.

With the other option, we can omit the data extraction as shown in Figure 4b. In this case, we can directly decrypt a marked encrypted image without data extraction and obtain a marked image. This means that the proposed method can perform image decryption without revealing the payload.

In Step 3-3, the original PEE-HS excludes any pairs that have been once used for data hiding. However, in our experiments, such pairs still had the highest sum of frequency even after embedding payload bits in many cases. Thus, in the proposed method, we constantly explore a pair with the highest sum of frequency in all pairs of adjacent bins without exclusion. Further, the amount of additional information can be reduced by composing a pair of adjacent bins instead of non-adjacent bins. These modifications lead to the notable enhancement of the hiding capacity.

## 4 Experimental Results

In comparison with another VRAE method with high capacity [16], we evaluated the effectiveness of the proposed method from three aspects: hiding capacity, lossless compression performance using JPEG-LS [26] and JPEG 2000 [10], and marked-image quality. In addition, to confirm the influences of encryption, we also generated marked images using the data hiding algorithm of the proposed method and evaluated the performance. As shown in Table 1, we used test images from three different datasets [8, 12, 23]. Figure 5 shows two examples of the test images. We concatenated three color components

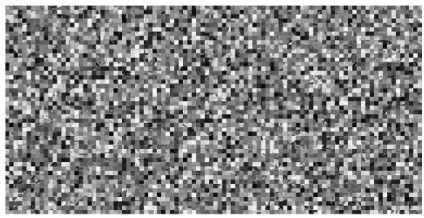
Table 1: Image datasets.

| Database | Kodak [12] | USC-SIPI [23] | IHC [8] |
|---|---|---|---|
| # of images | 24 | 6 | 6 |
| Image size [pixels] | $512 \times 768$ | $512 \times 512$ | $864 \times 1152$ |

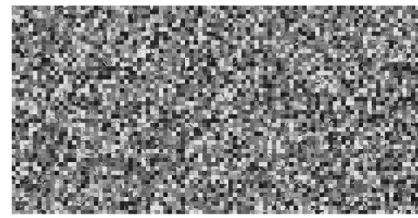
(a)

(b)

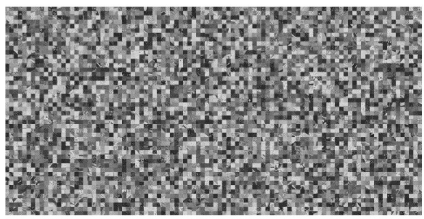
Figure 5: Examples of test images. (a) kodim4, (b) kodim18.



(a)



(b)



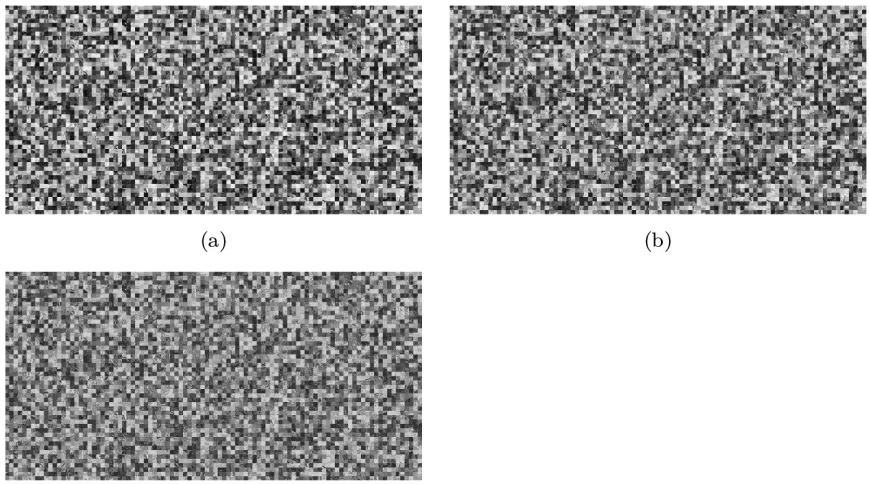
(c)

Figure 6: Marked encrypted images (kodim4). (a) $L = 10$, (b) $L = 25$, (c) $L = 45$.

horizontally in the order of R, G, and B. The fundamental block size for encryption was $16 \times 16$ pixels. In this experiment, threshold $L$, which is the number of times a series of the data hiding process is performed, was ranged from 1 to 45. Figures 6 and 7 depict the marked encrypted images obtained by the proposed method. It can be clearly seen that the encrypted images included more noise as the payload amount increased.

### *4.1 Hiding Capacity and Compression Performance*

We first compared the hiding capacity between the proposed method and the previous method [16]. Figure 8 shows the capacity of each method. Focusing

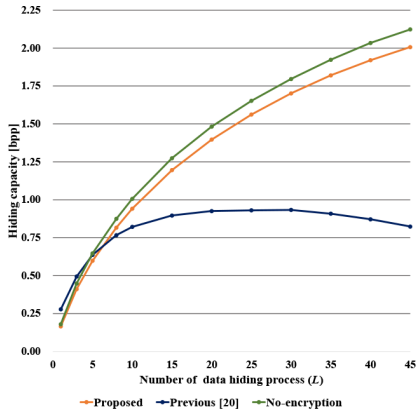


(a) (b) (c)

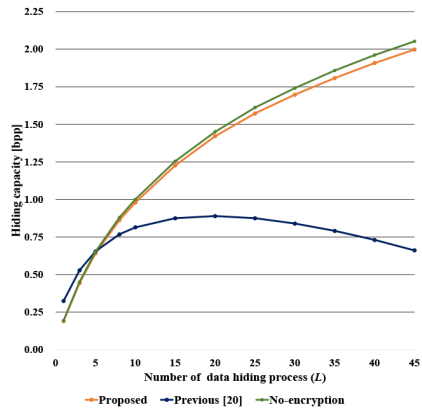
Figure 7: Marked encrypted images (kodim18). (a) $L = 10$, (b) $L = 25$, (c) $L = 45$.

on Figure 8a, the previous method had a maximum capacity of 0.94 bpp for each color component in the case of $L = 30$ and thereafter decreased in capacity as the value of $L$ increased. This is because the increment of additional information exceeded the increment of the hiding capacity. Consequently, the total capacity for the pure payload got smaller. In contrast, the proposed method attained a much higher capacity than the previous method after the value of $L$ exceeded 8. The hiding capacity of the proposed method was 0.94 bpp on average with $L = 10$ and 2.01 bpp with $L = 45$. Eventually, the proposed method achieved a maximum hiding capacity of 2.45 bpp on average for each color component, while the value of $L$ for the maximum capacity was different among the test images. As is obvious, the hiding capacity in the case of data hiding only was higher than the others. Figures 8b and 8c show trends analogous to Figure 8a. Figure 9 shows the hiding capacity when using different block sizes, i.e., 8×8 and 32×32 pixels. By using a larger block size, the hiding capacity becomes higher.

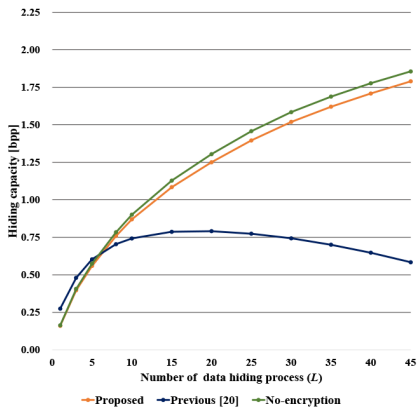
We evaluated the lossless compression performance using JPEG-LS [26] and JPEG 2000 [10]. Figure 10 shows the mean bitrates of images, which were encrypted, marked, and then compressed. The bitrate of the proposed method linearly varied depending on the hiding capacity. When the capacity was less than 1 bpp, the compression performance of the proposed method was analogous to that of the previous method [16]. Even in the case of around 2 bpp, JPEG-LS and JPEG 2000 compression for the images was still effective with the proposed method. The proposed method can enhance the hiding




(a) Kodak




(b) USC-SIPI

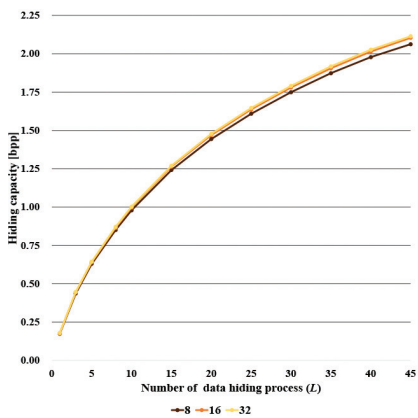



(c) IHC

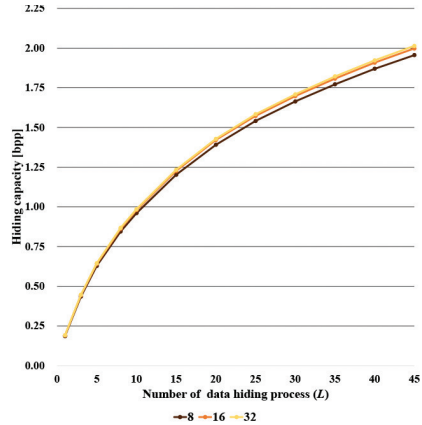
Figure 8: Hiding capacity.

capacity up to 2.45 bpp. In this case, however, it would be difficult to effectively compress the marked encrypted images. For comparison, Figure 10 also shows the mean bitrate of images that were marked only and then compressed. The encryption process was omitted for the images, so the compression performance naturally increased. Figure 11 illustrates the compression performance using different block sizes. The inner-pixel correlation degraded as the block size became smaller, and thus, the compression performance also declined.

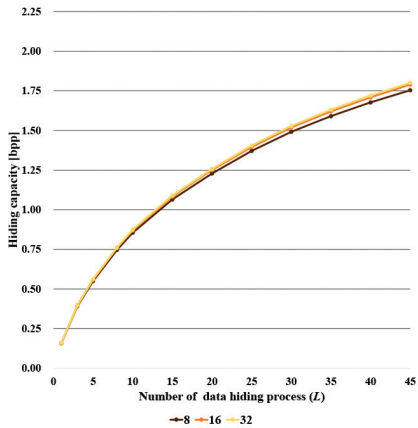
We used an Intel(R) Core i9-9900K CPU operating at 3.60 GHz with $16 \times 2$ GB of RAM. The program was implemented using MATLAB R2022a. Figure 12 shows the computational cost of our new data hiding algorithm. The cost is nearly equal to that of the previous data hiding algorithm.




(a) Kodak




(b) USC-SIPI

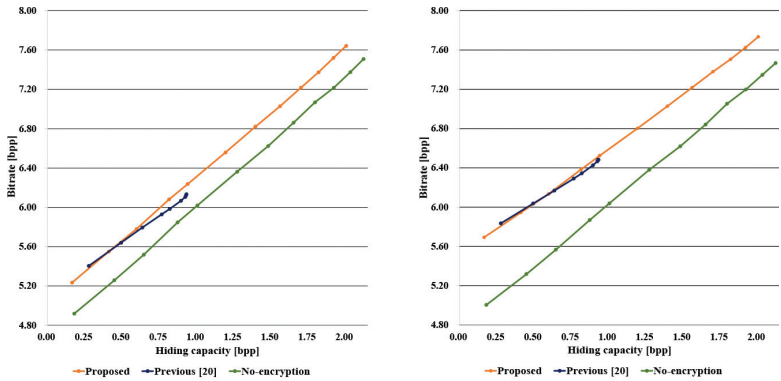



(c) IHC

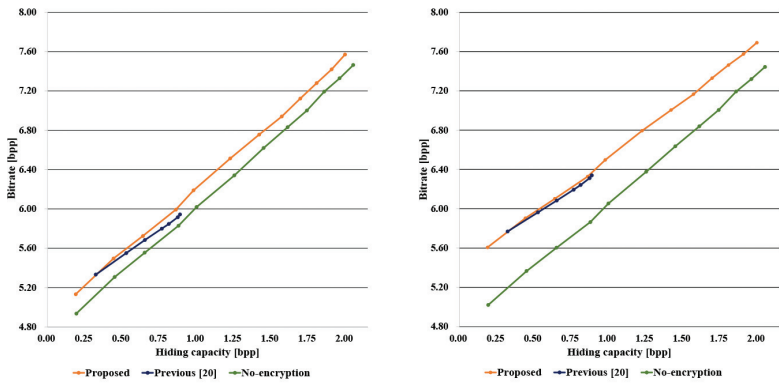
Figure 9: Hiding capacity using different block sizes (Kodak).

### *4.2 Decryption without Data Extraction*

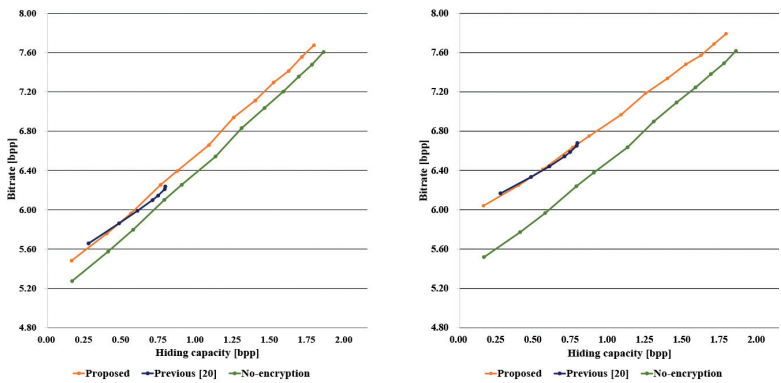
Generally, decryption should be conducted after data extraction in the restoration process. As shown in Figure 1(b), if the marked encrypted image obtained by the previous method [3] is directly decrypted without data extraction, the image content is kept confidential. On the other hand, the proposed and previous [16] methods have another option to obtain a marked image with high quality by decrypting the marked encrypted image without data extraction. The marked image still contains a payload while disclosing the image content.




(a) Kodak, JPEG-LS (b) Kodak, JPEG2000

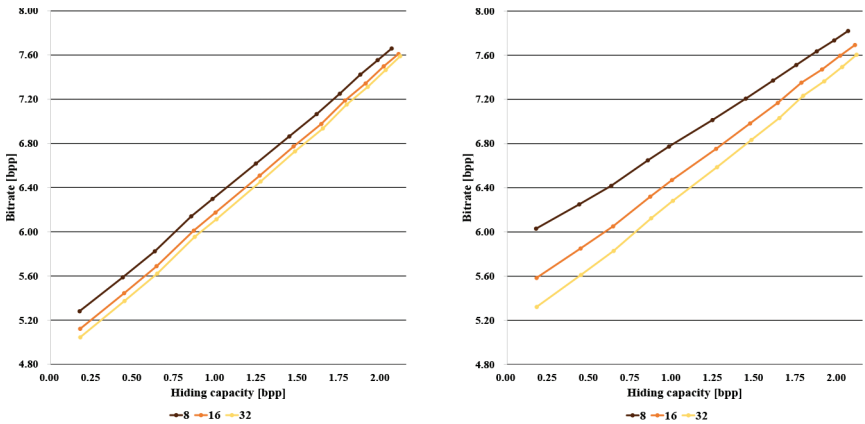



(c) USC-SIPI, JPEG-LS (d) USC-SIPI, JPEG2000




(e) IHC, JPEG-LS (f) IHC, JPEG2000

Figure 10: Lossless compression performance using JPEG-LS and JPEG2000.




(a) JPEG-LS (b) JPEG2000

Figure 11: Lossless compression performance using different block sizes (Kodak).

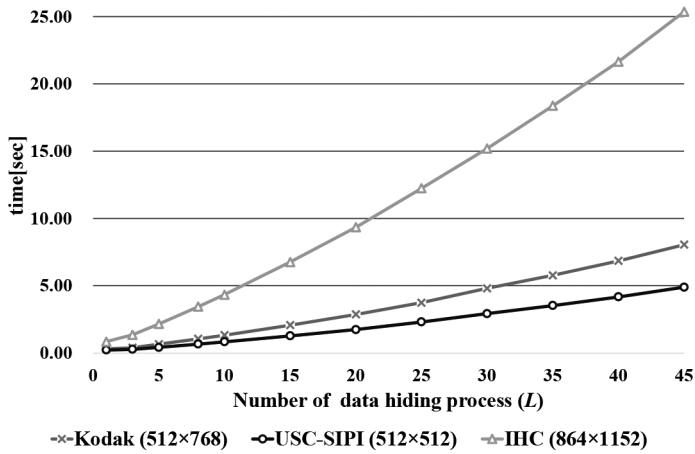
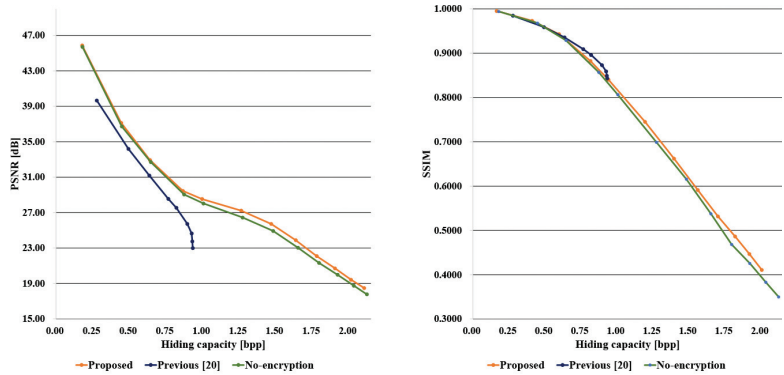



Figure 12: Processing time.

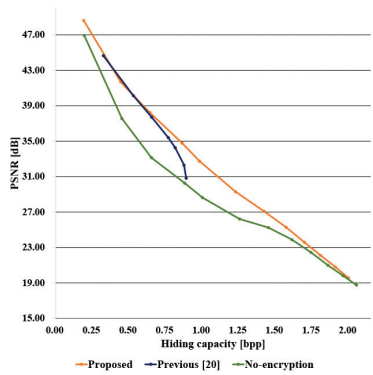
We then evaluated the marked-image quality using PSNR and SSIM in terms of the hiding capacity. The PSNR and SSIM values were calculated using the luminance component. Figure 13 shows the marked-image quality of the proposed, proposed without encryption, and previous methods. It is clear that there is a trade-off between the hiding capacity and marked-image quality. From the aspect of PSNR, the proposed method was superior to the previous method in most cases. The SSIM values of the proposed method were analogous to those of the previous method with a hiding capacity of less



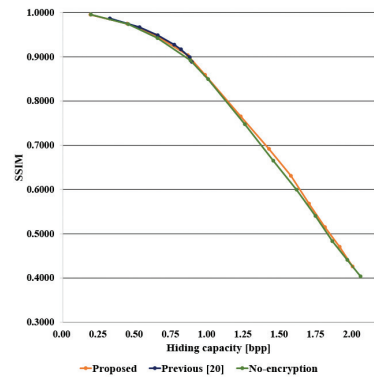

(a) Kodak, PSNR



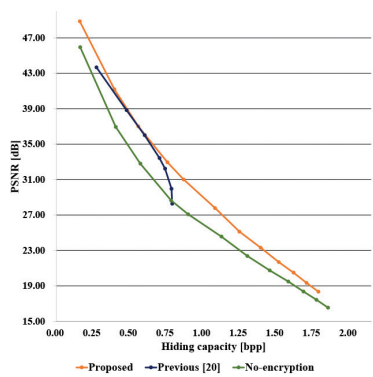

(b) Kodak, SSIM



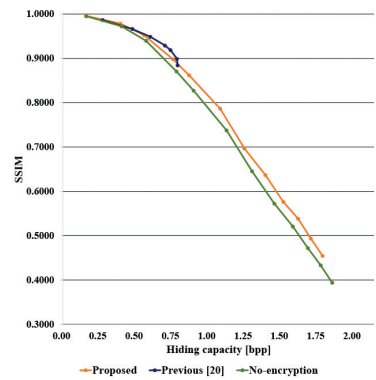

(c) USC-SIPI, PSNR




(d) USC-SIPI, SSIM

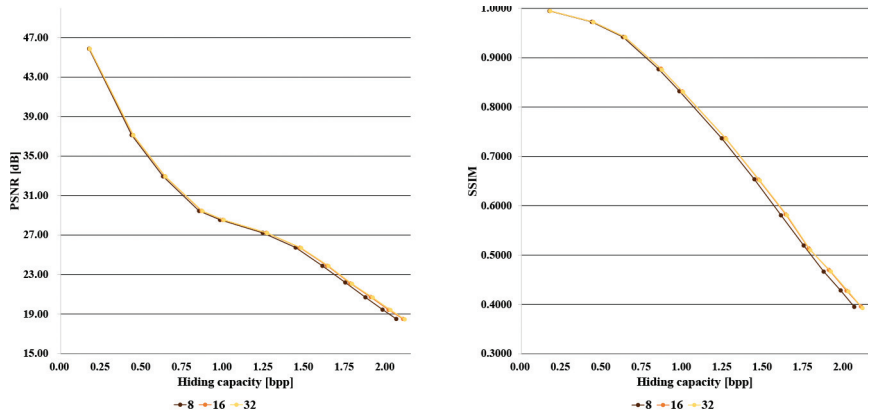



(e) IHC, PSNR




(f) IHC, SSIM

Figure 13: Marked-image quality using PSNR and SSIM.




(a) PSNR (b) SSIM

Figure 14: Marked-image quality using different block sizes (Kodak).

(a) (b) (c)

Figure 15: Marked images (kodim4, block size = 16). (a) $L = 10$ (PSNR = 26.05 dB/SSIM = 0.8219), (b) $L = 25$ (PSNR = 18.19 dB/SSIM = 0.5372), (c) $L = 45$ (PSNR = 17.04 dB/SSIM = 0.3683).

than 1 bpp. Compared with the method without encryption, the proposed method achieved higher quality. This is because the distortion caused by the preprocessing of data hiding was alleviated through the EtC process. Figure 14 exhibits the marked-image quality using different block sizes. Both the PSNR and SSIM values became slightly higher as the block size got larger.

Figures 15 and 16 exhibit examples of marked images obtained by the proposed method under different $L$ values. We could sufficiently identify the image context from the marked image with any value of $L$. However, it is clear that the marked image quality got worse as the hiding capacity increased. We are aware that this is a limitation of this paper and part of our future work.

(a) (b) (c)

Figure 16: Marked encrypted images (kodim18, block size = 16). (a) $L = 10$ (PSNR = 26.06 dB/SSIM = 0.8957), (b) $L = 25$ (PSNR = 18.50 dB/SSIM = 0.6628), (c) $L = 45$ (PSNR = 13.94 dB/SSIM = 0.4716).

## 5 Conclusion

We proposed an extended RDH-EI method to significantly enhance the hiding capacity. In this method, the data-hiding algorithm has been refined on the basis of our previous method. In PEE-HS, which was a data hiding algorithm in the previous method, each bin could be selected as an embeddable field only once even when the bin still had the highest frequency in the prediction error histogram. We modified such a condition so that the bins with the highest frequency would be constantly selected. Consequently, the maximum hiding capacity in the proposed method has been extended up to 2.45 bpp for each color component, while that in the previous method was 0.94 bpp at most. Through experiments, we confirmed that the proposed method enhanced the hiding capacity without losing the advantages of our previous method. Even when the hiding capacity was about 2 bpp, JPEG-LS and JPEG 2000 compression of the marked encrypted images was still effective.

## Acknowlegment

The authors would like to thank K. Abe for collaborating in the experimental stages. This work was partially supported by JSPS KAKENHI Grant Number JP21H01327.

## Biographies

**Ryota Motomura** received his B.Eng. degree from Chiba University, Japan in 2021. Since 2021, he has been a Master course student at Chiba University. His research interests include image processing and security.

**Shoko Imaizumi** received her B. Eng., M. Eng., and Ph.D. degrees from Tokyo Metropolitan University, Japan in 2002, 2005, and 2011. In 2011, she joined Chiba University, where she is currently an Associate Professor of the Graduate School of Engineering. From 2003 to 2004, she was with the Ministry of Education, Culture, Sports, Science and Technology of Japan. She was a Researcher at the Industrial Research Institute of Niigata Prefecture from 2005 to 2011. Her research interests include image processing and multimedia security. She is currently a Director for SPIJ (Society of Photography and Imaging of Japan) and a Topical Advisory Panel member for MDPI J. Imaging. She is a member of IEEE, APSIPA, IEICE, ITE, IEEJ, and SPIJ.

**Hitoshi Kiya** received B.E. and M.E. degrees from the Nagaoka University of Technology, Japan, in 1980 and 1982, respectively, and a 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 life fellow of IEEE, and a fellow of IEICE and ITE. He served as the President of APSIPA from 2019 to 2020 and the Regional Director-at-Large for Region 10 of the IEEE Signal Processing Society from 2016 to 2017. He was also the President of the IEICE Engineering Sciences Society from 2011 to 2012. He has been an editorial board member of eight journals, including IEEE TIP, IEEE TSP, and IEEE TIFS. He has organized a lot of international conferences in such roles as the TPC Chair of IEEE ICASSP 2012 and as the General Co-Chair of IEEE ISCAS 2019.

## References

[1] E. Arai and S. Imaizumi, "High-Capacity Reversible Data Hiding in Encrypted Images with Flexible Restoration," *Journal of Imaging*, 8(7), 2022, 176.

[2] R. Bhardwaj, "Efficient separable reversible data hiding algorithm for compressed 3D mesh models," *Biomedical Signal Processing and Control*, 73, 2022, 103265.

[3] S. Chen and C.-C. Chang, "Reversible data hiding in encrypted images using block-based adaptive MSBs prediction," *Journal of Information Security and Applications*, 69, 2022, 103297.

[4] T. Chuman, W. Sirichotedumrong, and H. Kiya, "Encryption-then-compression systems using grayscale-based image encryption for JPEG images," *IEEE Transactions on Information Forensics and security*, 14(6), 2018, 1515–25.

[5] I. C. Dragoi and D. Coltuc, "On the security of reversible data hiding in encrypted images by MSB prediction," *IEEE Transactions on Information Forensics and Security*, 16, 2020, 187–9.

[6] X. Gao, Z. Pan, E. Gao, and G. Fan, "Reversible data hiding for high dynamic range images using two-dimensional prediction-error histogram of the second time prediction," *Signal Processing*, 173, 2020, 107579.

[7] R. Hirasawa, S. Imaizumi, and H. Kiya, "An MSB prediction-based method with marker bits for reversible data hiding in encrypted images," in *2021 IEEE 3rd Global Conference on Life Sciences and Technologies (LifeTech)*, IEEE, 2021, 48–50.

[8] "IHC Standard Images," https://www.ieice.org/iss/emm/ihc/en/image/image.php.

[9] S. Imaizumi and H. Kiya, "A block-permutation-based encryption scheme with independent processing of RGB components," *IEICE Transactions on Information and Systems*, 101(12), 2018, 3150–7.

[10] "Information Technology-JPEG2000 image coding system-Part 1 : Core coding sytem," *ISO/IEC IS 15444-1*, 2019.

[11] H. Kiya, A. P. M. Maung, Y. Kinoshita, S. Imaizumi, and S. Shiota, "An Overview of Compressible and Learnable Image Transformation with Secret Key and its Applications," *APSIPA Transactions on Signal and Information Processing*, 11(1), 2022, DOI: 10.1561/116.00000048.

[12] "Kodak Lossless True Color Image Suite," http://www.r0k.us/graphics/kodak/.

[13] K. Kurihara, M. Kikuchi, S. Imaizumi, S. Shiota, and H. Kiya, "An encryption-then-compression system for jpeg/motion jpeg standard," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, 98(11), 2015, 2238–45.

[14] T. Luo, G. Jiang, M. Yu, F. Shao, and Z. Peng, "Disparity based stereo image reversible data hiding," in *2014 IEEE International Conference on Image Processing (ICIP)*, IEEE, 2014, 5492–6.

[15] K. Ma, W. Zhang, X. Zhao, N. Yu, and F. Li, "Reversible data hiding in encrypted images by reserving room before encryption," *IEEE Transactions on information forensics and security*, 8(3), 2013, 553–62.

[16] R. Motomura, S. Imaizumi, and H. Kiya, "A Reversible Data-Hiding Method with Prediction-Error Expansion in Compressible Encrypted Images," *Applied Sciences*, 12(19), 2022, 9418.

[17] Z. Ni, Y.-Q. Shi, N. Ansari, and W. Su, "Reversible data hiding," *IEEE Transactions on circuits and systems for video technology*, 16(3), 2006, 354–62.

[18] P. Puteaux, S. Ong, K. Wong, and W. Puech, "A survey of reversible data hiding in encrypted images–The first 12 years," *Journal of Visual Communication and Image Representation*, 77, 2021, 103085.

[19] P. Puteaux and W. Puech, "A recursive reversible data hiding in encrypted images method with a very high payload," *IEEE Transactions on Multimedia*, 23, 2020, 636–50.

[20] P. Puteaux and W. Puech, "An efficient MSB prediction-based method for high-capacity reversible data hiding in encrypted images," *IEEE transactions on information forensics and security*, 13(7), 2018, 1670–81.

[21] P. Puteaux and W. Puech, "EPE-based huge-capacity reversible data hiding in encrypted images," in *2018 IEEE International Workshop on Information Forensics and Security (WIFS)*, IEEE, 2018, 1–7.

[22] Y.-Q. Shi, X. Li, X. Zhang, H.-T. Wu, and B. Ma, "Reversible data hiding: advances in the past two decades," *IEEE access*, 4, 2016, 3210–37.

[23] "The USC-SIPI Image Database," https://sipi.usc.edu/database/.

[24] J. Tian, "Wavelet-based reversible watermarking for authentication," in *Security and watermarking of multimedia contents IV*, Vol. 4675, SPIE, 2002, 679–90.

[25] Y. Wang, G. Xiong, and W. He, "High-capacity reversible data hiding in encrypted images based on pixel-value-ordering and histogram shifting," *Expert Systems with Applications*, 211, 2023, 118600.

[26] M. J. Weinberger, G. Seroussi, and G. Sapiro, "The LOCO-I lossless image compression algorithm: Principles and standardization into JPEG-LS," *IEEE Transactions on Image processing*, 9(8), 2000, 1309–24.

[27] H.-T. Wu, Z. Yang, Y.-M. Cheung, L. Xu, and S. Tang, "High-capacity reversible data hiding in encrypted images by bit plane partition and MSB prediction," *IEEE Access*, 7, 2019, 62361–71.

[28] X. Zhang, "Reversible data hiding in encrypted image," *IEEE signal processing letters*, 18(4), 2011, 255–8.

[29] X. Zhang, "Separable reversible data hiding in encrypted image," *IEEE transactions on information forensics and security*, 7(2), 2011, 826–32.