applied sciences

MDPI

Article

A Reversible Data-Hiding Method with Prediction-Error Expansion in Compressible Encrypted Images

Ryota Motomura [1], Shoko Imaizumi [2,*] and Hitoshi Kiya [3,*]

[1] Graduate School of Science and Engineering, Chiba University, 1-33 Yayoicho, Chiba 263-8522, Japan
[2] Graduate School of Engineering, Chiba University, 1-33 Yayoicho, Chiba 263-8522, Japan
[3] Department of Computer Science, Tokyo Metropolitan University, 6-6 Asahigaoka, Tokyo 191-0065, Japan
* Correspondence: imaizumi@chiba-u.jp (S.I.); kiya@tmu.ac.jp (H.K.); Tel.: +81-43-290-3450 (S.I.); +81-42-585-8419 (H.K.)

Abstract: This paper proposes a novel reversible data-hiding method in encrypted images to achieve both a high hiding capacity and good compression performance. The proposed method can also decrypt marked encrypted images without data extraction, so marked images containing a payload can be derived from marked encrypted images. A perceptual encryption algorithm proposed for an encryption-then-compression framework is used to generate compressible encrypted images. In addition, a predictor with high accuracy and a prediction-error expansion and histogram shifting method are used for data hiding. Consequently, the proposed method can compress marked encrypted images without loss using image coding standards and achieve a high hiding rate. Experimental results show the effectiveness of the method in terms of hiding capacity or marked-image quality and lossless compression efficiency.

Keywords: encryption-then-compression system; hiding capacity; image encryption; lossless compression; reversible data hiding

Citation: Motomura, R.; Imaizumi, S.; Kiya, H. A Reversible Data-Hiding Method with Prediction-Error Expansion in Compressible Encrypted Images. *Appl. Sci.* **2022**, *12*, 9418. https://doi.org/10.3390/app12199418

Academic Editors: David Megías, Minoru Kuribayashi and Wojciech Mazurczyk

Received: 5 August 2022
Accepted: 16 September 2022
Published: 20 September 2022

1. Introduction

In recent years, with the development of cloud computing, an increasing number of users have been uploading images to external services or cloud servers. However, this leads to serious security problems where confidentiality and authentication are constantly threatened. To respond to this situation, data hiding and encryption have attracted attention as techniques for protecting the copyright and privacy of images. In particular, reversible data hiding (RDH) can perfectly retrieve original images from marked images [1–16]. It is practically effective, such as in medical, military, and evidential images. Numerous RDH methods have been proposed for plain images. Recently, RDH in encrypted images (RDH-EI) has been actively studied [17–33]. In RDH-EI methods, an image owner first encrypts a target image and sends it to a third party such as a service provider. The third party then embeds additional information, e.g., server information, access history, and annotation data. Hence, hiding capacity is one of the requirements in the field of RDH-EI methods.

Many RDH-EI methods have been proposed to attain a high hiding capacity [24–29]. Puteaux et al. [24] introduced MSB replacement instead of LSB replacement, which has been adopted in many conventional methods. Dragoi et al. [25] enhanced the security of [24]. The hiding capacity is quite high, 0.97 bpp on average, and the mathematical complexity is low. The method of Wu et al. [27] achieved a higher hiding capacity of 2.2 bpp on average by utilizing the method of Puteaux et al. [24]. Further, Puteaux et al. [29] proposed a new RDH-EI method with a higher capacity and full reversibility. This method attained a higher hiding capacity of 2.4 bpp on average by recursively conducting a hiding process. These methods, however, cannot compress their marked encrypted images at all.

The first method to attain effective compressibility for marked encrypted images is that of Imaizumi et al. [30]. This method uses an encryption-then-compression (EtC)

system [34–36] for encryption. Thus, it can compress marked encrypted images without loss using image coding standards, such as JPEG-LS [37] and JPEG 2000 [38], without losing reversibility. Further, we can flexibly embed and extract payloads in plain and/or encrypted domains by using an RDH method based on histogram shifting (RDH-HS) [30]. This method, however, has an extremely low hiding capacity, i.e., about 0.1 bpp.

RDH-EI methods can be classified into two types: reserving room before encryption (RRBE) and vacating room after encryption (VRAE). The former methods have a preprocessing step, so that the embeddable area can be ensured before encryption. A content owner encrypts the preprocessed image and sends the encrypted image to a third party. The third party hides some information into an embeddable area. In contrast, the latter methods do not have a preprocessing step. A content owner encrypts the original image directly and sends the encrypted image to a third party. The third party embeds the information into the encrypted image. Most of the state-of-the-art RDH-EI methods with high hiding capacity [29,31–33] are classified into RRBE. In RRBE, however, a content owner should assume that a data-hiding step would be conducted to the encrypted image and reserve the embeddable area. This can be a problem that limits the range of practical applications.

We propose a novel VRAE-based method to simultaneously achieve a high hiding capacity and high compression efficiency. The proposed method introduces the method of Chuman et al. [39] with which conventional EtC systems [34,35] are extended to enhance security. Consequently, the proposed method can produce marked encrypted images with high compression efficiency by using lossless image coding standards. The interpixel correlation in each block is not transformed before or after the EtC process; thus, we can obtain prediction values with high accuracy even after encryption. Accordingly, we achieved high hiding capacity using prediction-error expansion and histogram shifting. The proposed method can also derive marked images by decryption without data extraction. Through our experiments, we confirm the effectiveness of the proposed method in terms of data-hiding capacity, marked-image quality, and lossless compression performance using JPEG-LS and JPEG 2000.

2. Related Work

2.1. RDH Methods

Data-hiding techniques have attracted attention over the most recent decades in the image security field. The main purpose of data hiding is copyright protection by imperceptibly embedding information such as ownership information into a target image. In particular, RDH can perfectly retrieve the original image by extracting the embedded payload. Specifically, it is required to preserve the original data in practical images, e.g., medical, military, and evidential images. In response to such demand, numerous RDH techniques have been proposed [1–16]. RDH algorithms are mainly based on well-known techniques such as different expansion [2] and histogram shifting [3]. In recent years, the RDH research field has been expanded to HDR [13,14] and 3D [15,16] images.

2.2. RDH-EI Methods

In addition to RDH methods proposed for plain images, RDH in encrypted images has been actively studied in recent years [24–33]. RDH-EI methods are effective in embedding data in the encrypted domain without knowing the secret key used for encryption and disclosing the original-image content. They are mostly used for both copyright protection for image owners, and for the authentication and management purposes of third parties such as service providers. Therefore, a high hiding capacity is required in the field of RDH-EI methods.

Puteaux et al. [24] introduced MSB prediction and replacement instead of using LSB replacement to greatly extend the capacity. This method does not require any complex processes. Dragoi et al. [25] enhanced the security of [24], and Puteaux et al. [26] further improved the capacity of [24]. Wu et al. [27] introduced the method of Puteaux et al. [24] to an RDH-EI scheme based on bit-plane partition. Since redundancy is still preserved in images after the self-embedding process, this method [27] attained a hiding capacity of

2.2 bpp on average by utilizing the method in [24]. Nonetheless, there still exist multiple cases where reversibility is not fully ensured. Hirasawa et al. [28] extended the method of Puteaux et al. [24] to guarantee full reversibility by defining precise conditions.

Puteaux et al. [29] proposed a new RDH-EI method called RDH-MSB with a higher capacity that guaranteed full reversibility and high capacity. Figure 1 illustrates the framework of the RDH-MSB method. This method uses bit planes of a target image from MSB to LSB until the iterative process becomes invalid. The first step is prediction-error (PE) detection to identify pixels that are not correctly predicted from their neighbor ones. Pixel values are updated in accordance with PE values, so that the original image can be perfectly reconstructed through the restoration process. The whole current bit plane is encrypted, and PE values are then embedded from a top-left pixel in the bit plane. Some marker bits are embedded ahead of the PE values. Consequently, regions not containing marker bits and PE values become an embeddable area for an arbitrary payload. The same steps are repeated for the latter bit planes. When a PE value cannot be embedded, the process is stopped, and only current and all latter bit planes are encrypted. The hiding capacity of the RDH-MSB method is 2.4 bpp on average. These high-capacity RDH-EI methods, however, cannot compress their marked encrypted images because a bitwise exclusive-or operation is used for encryption. Additionally, previous RDH-EI methods cannot decrypt marked encrypted images without data extraction.

Imaizumi et al. [30] proposed RDH-EI method RDH-EtC with effective compressibility for marked encrypted images. An outline of the RDH-EtC method is shown in Figure 2. This method uses two of four processes in block-scrambling-based encryption for EtC systems [34,35]: position scrambling and block rotation or flip. Since an image histogram is not transformed before or after the encryption processes, we can embed a payload in plain and/or encrypted domains by using RDH-HS [3]. Additionally, this method can flexibly extract payloads from either domain. Thus, a marked encrypted image can be decrypted without extracting a payload. Further, this method can compress marked encrypted images with loss using image coding standards, such as JPEG-LS [37] and JPEG 2000 [38]. This method, however, has an extremely low hiding capacity, i.e., about 0.1 bpp.

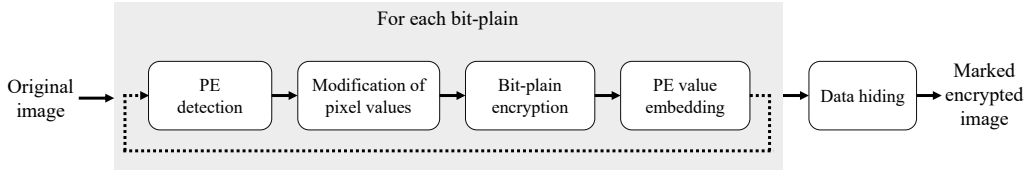


Figure 1. Block diagram of RDH-MSB method [29].

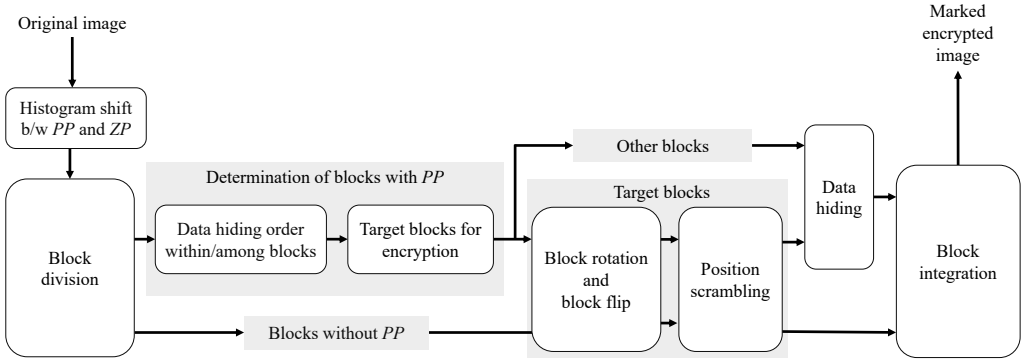


Figure 2. Block diagram of RDH-EtC method [30]. *PP* and *ZP* are bins with the highest and lowest frequency, respectively, in original-image histogram.

The proposed method simultaneously achieves high compression efficiency and high hiding capacity. We compare our method with the related work in Table 1. The method has the advantages of both the RDH-MSB and RDH-EtC methods.

Table 1. Feature comparison of the proposed method with related work.

	Hiding Capacity	Lossless Compression Performance	Flexible Restoration
Proposed Method	✓	✓	✓
RDH-EtC [30]	×	✓	✓
RDH-MSB [29]	✓	×	×

2.3. Encryption-then-Compression Images

EtC systems have been proposed for secure image transmission. Most studies on EtC systems are based on the premise that a proprietary scheme is used for compression. Meanwhile, block-scrambling-based encryption methods [34,35], which are compatible with image coding standards, have been proposed for EtC systems. Chuman et al. [39] extended these methods to enhance security. Their method transforms an original image from RGB into YCbCr and combines each component to derive a grayscale-based image. Block-scrambling-based encryption is conducted on the grayscale image. Since the encrypted image is three times as large as the original image, the key space of the encrypted image is thereby larger than that of conventional methods [34,35]. This contributes to enhancing robustness against brute-force (BF) attacks. Further, this method is more resistant to jigsaw-puzzle solver (JPS) attacks because it uses grayscale images with less color information. We refer to this method as G-EtC. G-EtC is used for encryption in our proposed method. Figure 3 shows the procedure of the G-EtC method.

Step 1: Transform an original image I from RGB into YCbCr.
Step 2: Combine YCbCr channels into a single grayscale image I_G.
Step 3: Divide I_G into a certain size of blocks.
Step 4: Conduct position scrambling, block rotation or flip, and negative–positive transformation on each block.
Step 5: Integrate all blocks and derive an encrypted image $I_{G_{enc}}$.

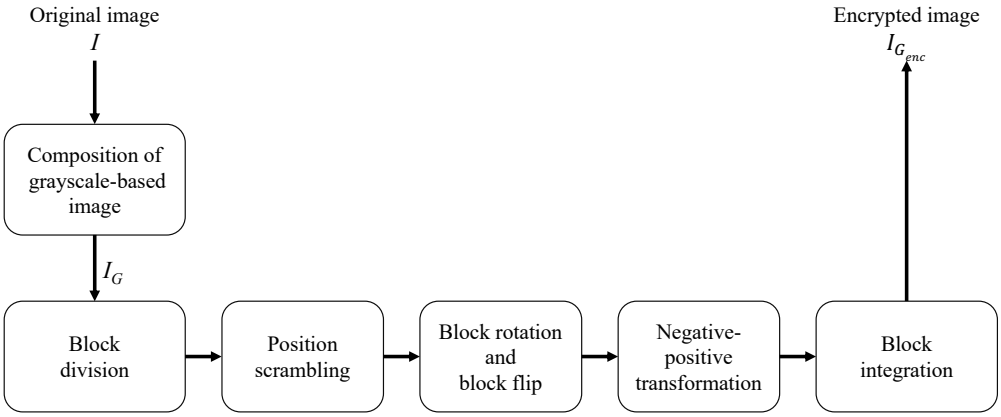


Figure 3. Block diagram of G-EtC method [39].

3. Proposed Method

In this section, we propose a high-capacity RDH method for encrypted images. The proposed method can compress marked encrypted images without loss owing to the use of the G-EtC method [39]. Since a prediction-error expansion and histogram-shifting process were effectively adopted, our method attained a high hiding capacity. We first overview the method and describe its procedure in detail. Then, the effectiveness of the method is described.

3.1. Framework of Proposed Method

The proposed method simultaneously achieves high hiding capacity and high compression efficiency. An outline of the method is illustrated in Figure 4. We used the G-EtC

method [39] for encryption. Therefore, this method could compress marked encrypted images using image coding standards because the interpixel correlation in each block is retained even after encryption and data hiding. In our method, reversibility is an essential condition for perfectly retrieving an original image. Thus, we had to use lossless compression algorithms such as JPEG-LS [37] and JPEG 2000 [38].

Figure 4. Outline of proposed method.

A payload is then embedded using prediction-error expansion and histogram shifting (PEE-HS) [16] for each block used in encryption. Here, the prediction values are highly accurate due to the introduction of the median edge detection (MED) predictor, so high hiding capacity could be attained. However, the superior performance shown in Section 4 could not be obtained by simply using the PEE-HS algorithm. Thus, we modified the original algorithm so as to preserve the high prediction accuracy even after encryption using the EtC system. Consequently, the proposed method had significant advantages, i.e., the compatibility between high hiding capacity and good compression performance.

The proposed method must conduct decryption after data extraction in order to restore an original image. Nevertheless, we could also decrypt a marked encrypted image without data extraction, thus obtaining a marked image containing a payload.

3.2. Procedure of Encryption and Data hiding

Here, we explain data-hiding and encryption processes in reference to Figure 5. We assumed that the size of an original image I was $M \times N$ pixels.

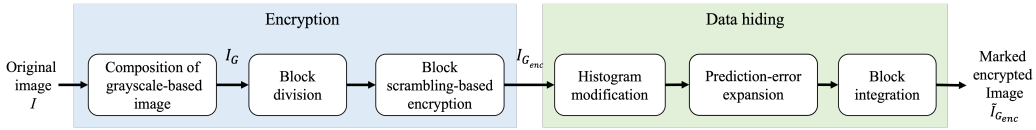


Figure 5. Encryption and data-hiding procedure of proposed method.

3.2.1. Image Encryption

The proposed method uses the G-EtC method [39] in the encryption process. We omitted the color transformation process in the G-EtC method to guarantee full reversibility and alternatively combine RGB color components to derive a grayscale image.

Step1-1: Combine R, G, and B components of an original image I, and a grayscale-based image I_G is derived.
Step1-2: Divide I_G into multiple blocks with $B_x \times B_y$ pixels.
Step1-3: Conduct position scrambling, block rotation or flip, and negative–positive transformation on each block, and obtain an encrypted image $I_{G_{enc}}$.

3.2.2. Data Hiding

The data-hiding process is divided into three parts: histogram modification, PEE-HS, and block integration. We describe each part below.

- Histogram modification: Since PEE-HS is used for data hiding, overflow (OF) or underflow (UF) may be caused in the value of each pixel. With the following steps, our method preliminarily modifies an image histogram in order to prevent OFs and UFs in pixel values.

  Step2-1: Explore a zero point (ZP) that is a bin with no pixels in an encrypted image histogram.
  Step2-2: To prevent UFs, add 1 to pixels with a value lower than ZP.

Step2-3: Repeat Steps 2-1 and 2-2 $L+1$ times. Here, L is a threshold used in data hiding.
Step2-4: Explore a ZP in the image histogram.
Step2-5: To prevent OFs, subtract 1 from pixels with a value higher than ZP.
Step2-6: Repeat Steps 2-4 and 2-5 $L+1$ times.

We needed to exclude eight pixels from the top-left corner of encrypted images from the above steps and the following data-hiding process. An 8-bit value of threshold L was embedded into these pixels. Additionally, if there was no ZP in the histogram, we focused on two neighboring bins with the lowest sum of frequencies. These bins were integrated into a single bin, and another bin was emptied (LP). We built a location map where the original pixel values with the two neighboring bins were recorded in order to identify their original pixel values in the restoration process. It is necessary to embed the value of ZP or LP with an arbitrary payload to perfectly retrieve the original image. In the case of LP, the location map should be stored along with LP.

- Prediction-error expansion and histogram shifting: We extended an RDH method on the basis of PEE-HS for stereoimages [16] and incorporated it into the proposed method. Our method embeds payload bits into each block, which is the same block as that in the encryption process. We describe the data-hiding procedure as follows.

Step3-1: For pixels $p_{i,j}$ in each block, where $0 \leq i < B_x$ and $0 \leq j < B_y$, predicted values $\hat{p}_{i,j}$ are derived from

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

Here, prediction values $\hat{p}_{0,j}$ and $\hat{p}_{i,0}$ cannot be obtained with (1). Thus, we define

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

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

The top-left pixel $p_{0,0}$ in each block was excluded from data hiding for reversibility.

Step3-2: Derive prediction errors $e_{i,j}$:

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

Step3-3: in the prediction-error histogram, empty bins are derived in the range of $[-2L-1, -L-1]$ and $[L+1, 2L+1]$ in accordance with the following equation.

$$e'_{i,j} = \begin{cases} e_{i,j} + (L+1), & \text{if } e_{i,j} \geq L+1 \\ e_{i,j} - (L+1), & \text{if } e_{i,j} \leq -(L+1) \\ e_{i,j}, & \text{otherwise,} \end{cases} \tag{5}$$

where $e'_{i,j}$ denotes the prediction error after shifting. Figure 6a shows an example of a histogram shift in the case of $L = 2$.

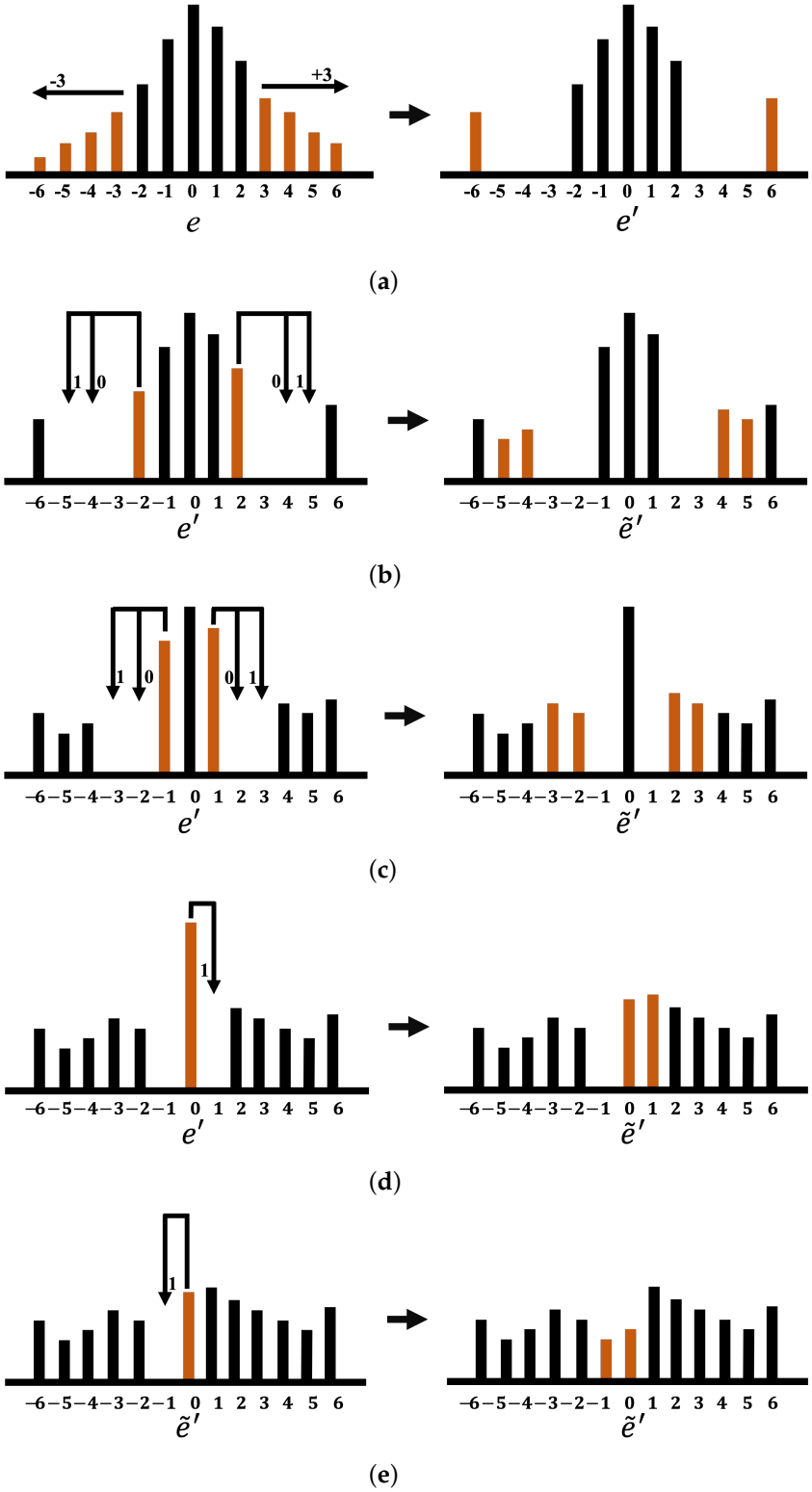


Figure 6. Procedure of data hiding ($L = 2$). (**a**) Derivation of empty bins, (**b**) data hiding for pixels with $|e'_{i,j}| = 2$, (**c**) data hiding for pixels with $|e'_{i,j}| = 1$, (**d**) data hiding for pixels with $e'_{i,j} = 0$, (**e**) data hiding for pixels with $\tilde{e}'_{i,j} = 0$.

Step3-4: Here, configure $\alpha = L$. Embed a payload w into pixels with $e'_{i,j} = \pm\alpha$:

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

where $\tilde{e}'_{i,j}$ and w_k denote the prediction error after data hiding and the k-th bit of w, respectively. Then, decrease α by 1, i.e., $\alpha = \alpha - 1$, and repeat (6) until $\alpha = 1$, as shown in Figure 6b,c.

Step3-5: in the case of $e'_{i,j} = 0$, embed the payload bits w_k as follows (see Figure 6d).

$$\tilde{e}'_{i,j} = \begin{cases} e'_{i,j} + 1, & \text{if } e'_{i,j} = 0 \text{ and } w_k = 1 \\ e'_{i,j}, & \text{if } e'_{i,j} = 0 \text{ and } w_k = 0. \end{cases} \tag{7}$$

Step3-6: as shown in Figure 6e, recursively embed w into pixels with $\tilde{e}'_{i,j} = 0$:

$$\tilde{e}'_{i,j} = \begin{cases} \tilde{e}'_{i,j} - 1, & \text{if } \tilde{e}'_{i,j} = 0 \text{ and } w_k = 1 \\ \tilde{e}'_{i,j}, & \text{if } \tilde{e}'_{i,j} = 0 \text{ and } w_k = 0. \end{cases} \tag{8}$$

In this case, $\tilde{e}'_{i,j}$ is updated by (8).

Step3-7: Marked pixel values $\tilde{p}_{i,j}$ are given by

$$\tilde{p}_{i,j} = \hat{p}_{i,j} - \tilde{e}'_{i,j}. \tag{9}$$

- Block integration: lastly, we integrate all the blocks into a marked encrypted image $\tilde{I}_{G_{enc}}$.

The LSBs of eight pixels from the top-left pixels in marked encrypted images are replaced with the value of L. Those LSBs before replacement should be embedded with a pure payload.

3.3. Procedure of Restoration

The proposed method has two options for restoration as shown in Figure 7. First, it can perfectly retrieve an original image by using a normal restoration process consisting of data extraction and decryption (see Figure 7a). With this option, we first extracted the threshold L from a marked encrypted image. The image is divided into blocks, and the payload is extracted from them using L. We turned back the histogram of the encrypted image, and then decrypted and integrated the blocks. Lastly, the RGB color components were restructured, and the original image was obtained.

Our method has another model for omitting data extraction as shown in Figure 7b. With this option, we could obtain a marked image $\tilde{I}$ that still contains a payload after decryption. This means that the proposed method could decrypt a marked encrypted image without revealing the payload to other users.

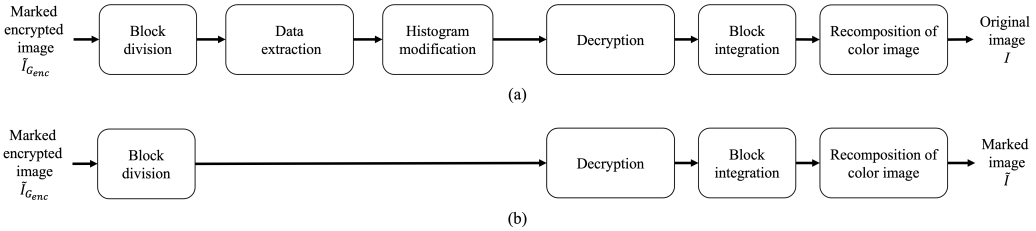


Figure 7. Options for restoration in proposed method. (**a**) Data extraction and decryption;(**b**) decryption without data extraction.

3.4. Threat Models and Security Evaluation

In this paper, we use EtC images as compressible encrypted images. EtC images are not only compressible, but also robust against various ciphertext-only attacks (COAs) [40,41]. As we focus on the privacy of datasets in an image classification scenario, the goal of an adversary is to recover visual information on encrypted images. We assumed that an adversary had access to encrypted images and knew the encryption algorithm, but not the secret key. In other words, we assumed that the adversary could carry out a COA only from encrypted images. In addition, we assumed that the adversary knew the distribution of the dataset; thus, the adversary may prepare synthetic examples in conducting an attack.

EtC images were evaluated under COAs. The robustness of EtC images against BF and JPS attacks as COAs was evaluated in [40]. An EtC image had almost the same correlation among pixels in each block as that of the original image, and this property allows for it to efficiently compress images. Therefore, an attacker can utilize this correlation to decrypt the image in some way, so the security of the encryption against JPS attacks was discussed in [40], in addition to BF attacks. In contrast, recently, novel attack methods for restoring visual information have been proposed that use deep neural networks [42,43]. The feature reconstruction attack (FR-Attack) [42] exploits the local properties of an encrypted image to reconstruct visual information from encrypted images. Furthermore, with a synthetic dataset and encrypted images, the adversary may carry out a GAN-based attack (GAN-Attack) [43]. EtC images were confirmed to be robust against these attacks [41].

In addition, regarding the security for the content of a payload, we assume that the payload is encrypted before embedding. Thus, if the encryption scheme is secure, the encrypted payload should be robust against unauthorized disclosure.

3.5. Advantages of Proposed Method

The proposed method has three main advantages that are summarized in Table 1 and precisely described as follows.

- ***High hiding capacity***
  The proposed method encrypts a target image in units of blocks, so interpixel correlation in each block can be stable before or after encryption. Since we could obtain prediction values with high accuracy in the encrypted domain, the hiding capacity of our method was around 1 bpp using PEE-HS. The proposed method has high hiding capacity, so we could embed not only copyright information and time stamps, but also information on image content, e.g., categorical and annotation data. With such information, we could determine the type of target images in the encrypted domain.
- ***Effective compression performance***
  The proposed method preserves the interpixel correlation in each block after encryption and data hiding. Thus, international standards for lossless image compression, such as JPEG-LS and JPEG 2000, can be effectively utilized for the marked encrypted images produced by our method. Consequently, the proposed method alleviates the constraint on transmission and storage.

- ***Flexible restoration***
  While the conventional method [29] has to extract the payload before decryption, our method could omit the data extraction process and decrypt only marked encrypted images in common with the conventional method [30]. The flexible restoration process provides a user with any one of the following three types of privilege: data extraction and decryption, data extraction only, and decryption only. This advantage allows for us to expand the range of applications.

Conventional methods [29,30] are deficient in at least one of the above three advantages. In contrast, the proposed method has all three in the RDH-EI field. These advantages are necessary to more widely apply RDH-EI techniques. As a practical application, for example, the proposed method could provide privacy preservation with flexible access control for Internet services such as image storage or sharing.

4. Experimental Results

We confirmed the effectiveness of the proposed method in terms of hiding capacity, marked-image quality, and lossless compression performance using JPEG-LS [37] and JPEG 2000 [38]. In the experiments, we used three databases: Kodak [44], SIPI [45], and IHC [46]. The Kodak database consists of 24 color images with 512×768 or 768×512 pixels, while the SIPI database consists of 6 color images with 512×512 pixels. The IHC database contains 6 color images with 4680×3456 pixels. To explore the influence of image size, we used two different sizes for the IHC test images: he original size and 1/16 of the original. Figure 8 shows example images from each database.

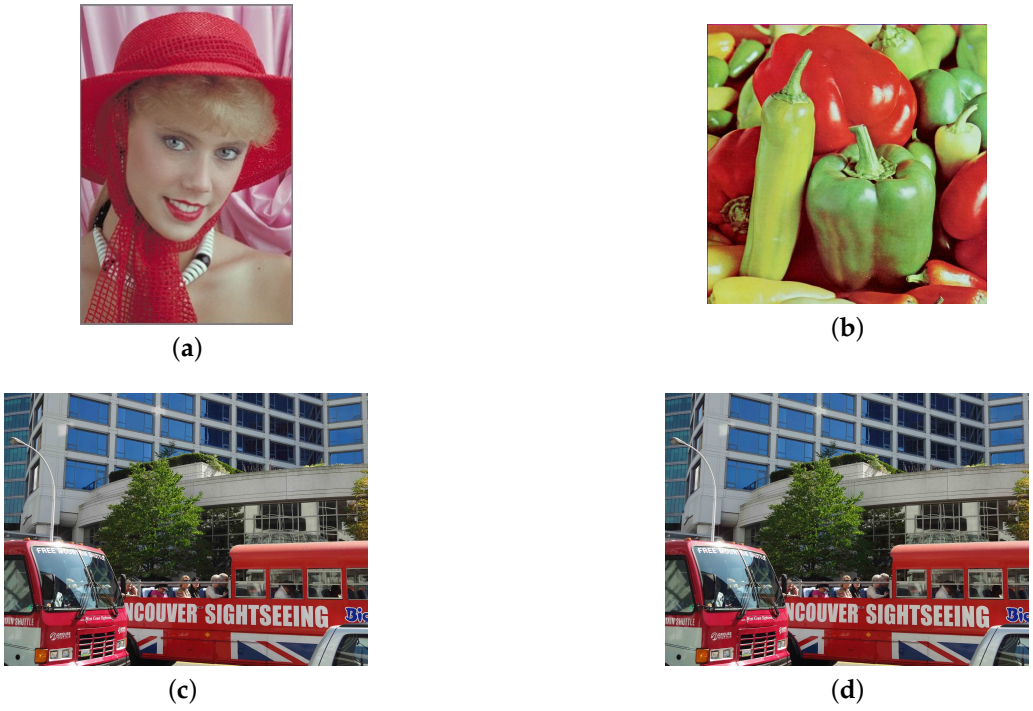


Figure 8. Examples of test images. (**a**) Kodim4 from Kodak [44]; (**b**) peppar from SIPI [45]; (**c**) ihc5 with 1/16 of original size from IHC [46]; (**d**) ihc5 with original size from IHC.

We horizontally concatenated three color components in the order of R, G, and B, as shown in Figures 9a, 10a, 11a and 12a. The block size for encryption was 8×8 pixels. Since the RDH-MSB method [29] was designed for grayscale images, the algorithm of [29] was independently applied to each color component. For data hiding, threshold L, which controls the hiding capacity, was defined as 1, 3, and 10. Figures 9–12 exhibit marked encrypted images derived with the proposed method.

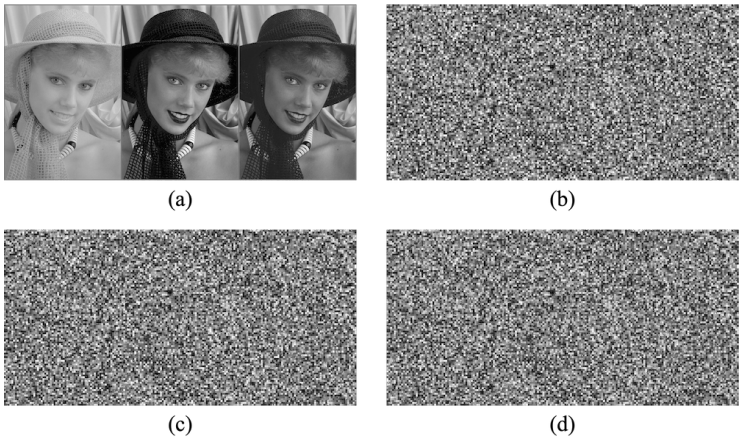


Figure 9. Marked encrypted images (Kodim4). (**a**) Grayscale-based image; (**b**) $L = 1$, (**c**) $L = 3$; (**d**) $L = 10$.

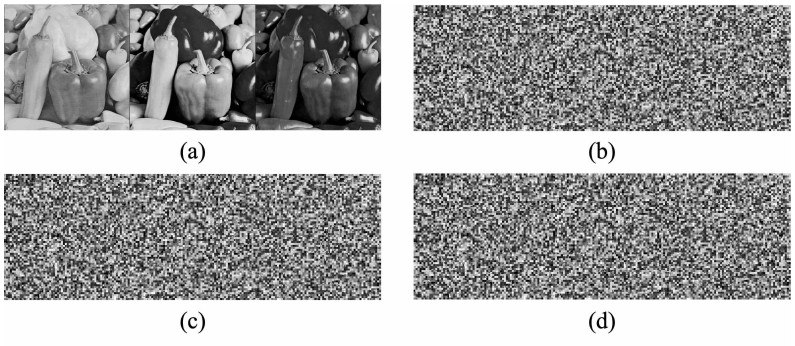


Figure 10. Marked encrypted images (peppar). (**a**) Grayscale-based image; (**b**) $L = 1$, (**c**) $L = 3$; (**d**) $L = 10$.

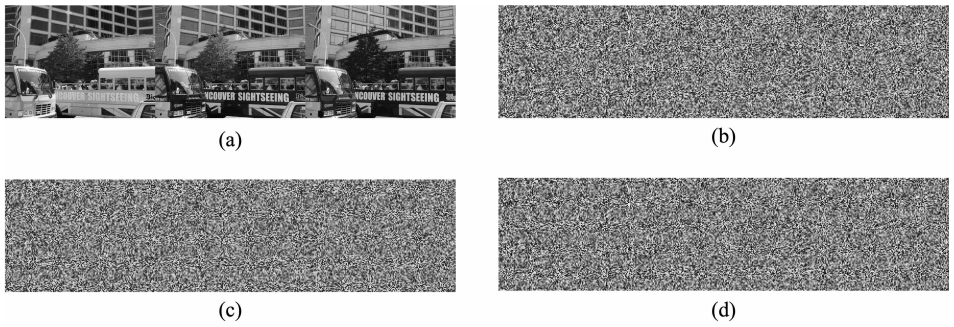


Figure 11. Marked encrypted images (ihc5 (1/16)). (**a**) Grayscale-based image; (**b**) $L = 1$, (**c**) $L = 3$; (**d**) $L = 10$.

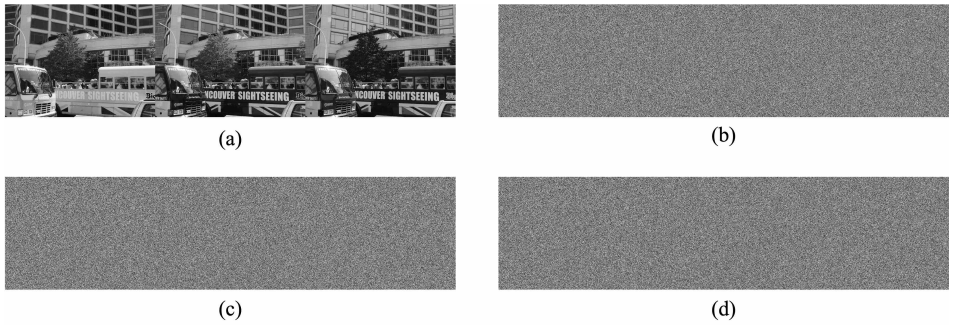


Figure 12. Marked encrypted images (ihc5 (original)). (**a**) Grayscale-based image; (**b**) $L = 1$; (**c**) $L = 3$; (**d**) $L = 10$.

4.1. Data-Hiding Capacity and Marked-Image Quality

The data-hiding capacity and marked-image quality of the proposed method were compared with those of the RDH-EtC [30] and RDH-MSB [29] methods. The RDH-MSB method could conduct decryption only after data extraction, so it did not derive the marked images.

Figure 13 illustrate the hiding capacity for all the test images of each database. With the proposed method, higher hiding capacity could be attained as the value of L increased. In all databases, the proposed method achieved a high hiding capacity of around 1 bpp in the case of $L = 10$. With respect to the Kodak database, the hiding capacity of our method was around 0.82 bpp on average ($L = 10$). In contrast, the hiding capacity of the RDH-EtC method was 0.04 bpp on average. The RDH-MSB method achieved a hiding capacity of 1.64 bpp on average, which was much higher than that of the proposed method. However, despite the high capacity, the compression performance of marked encrypted images is not considered in this method, and the order of restoration is completely fixed without any flexibility. Figure 13c,d show that the proposed method further achieved higher hiding capacity in the case of using a larger image.

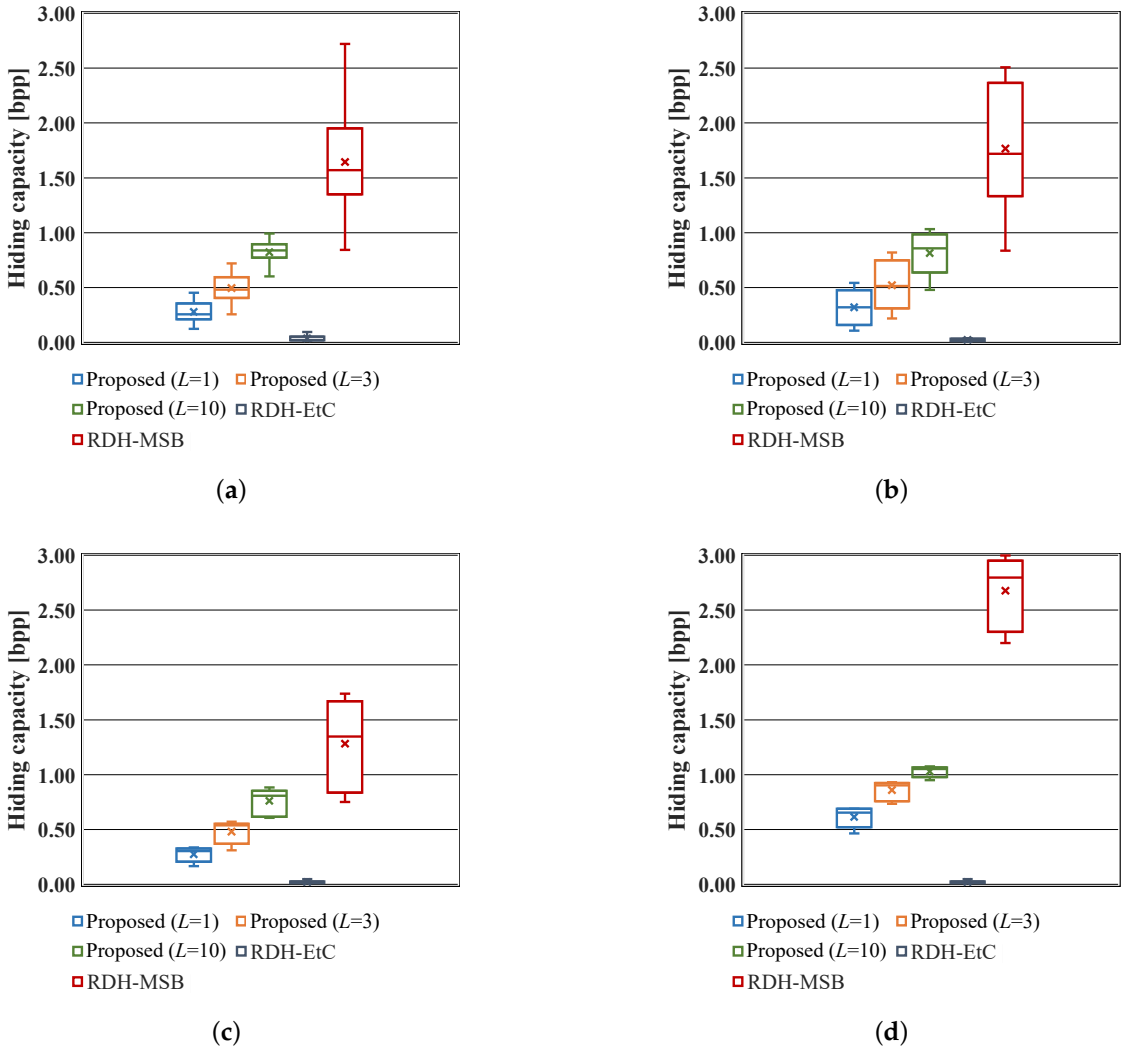
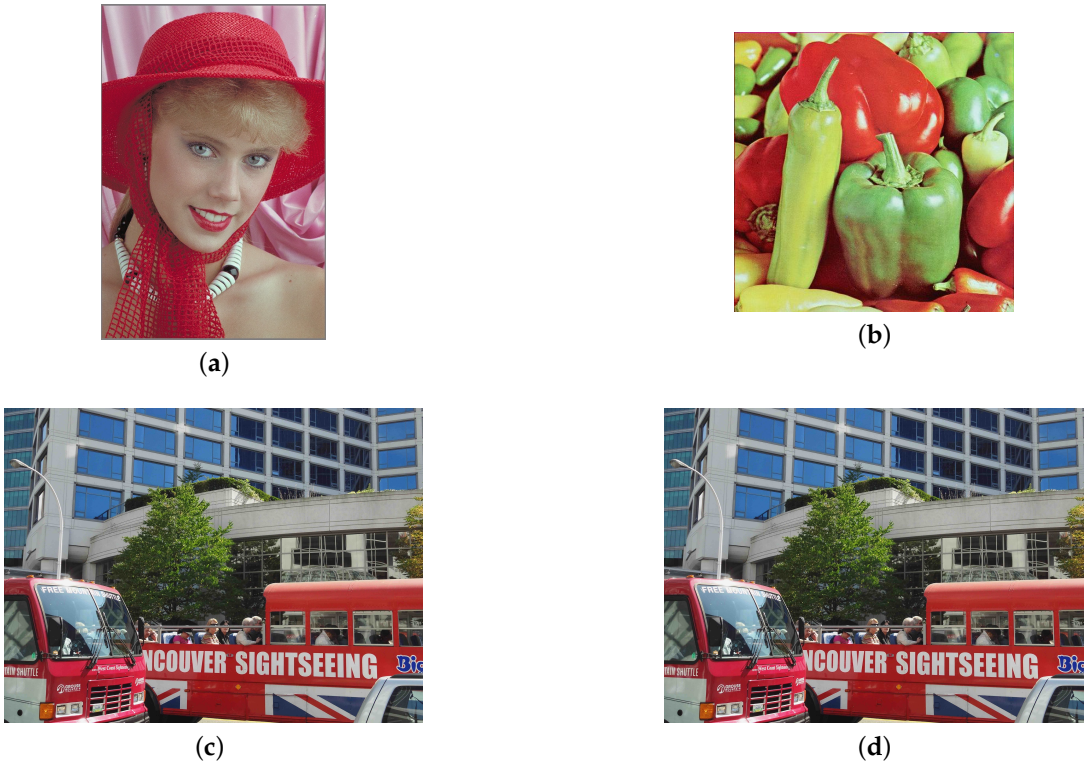


Figure 13. Data hiding capacity of proposed, RDH-EtC [30] and RDH-MSB [29] methods. (**a**) Kodim4; (**b**) peppar; (**c**) ihc5 (1/16); (**d**) ihc5 (original).

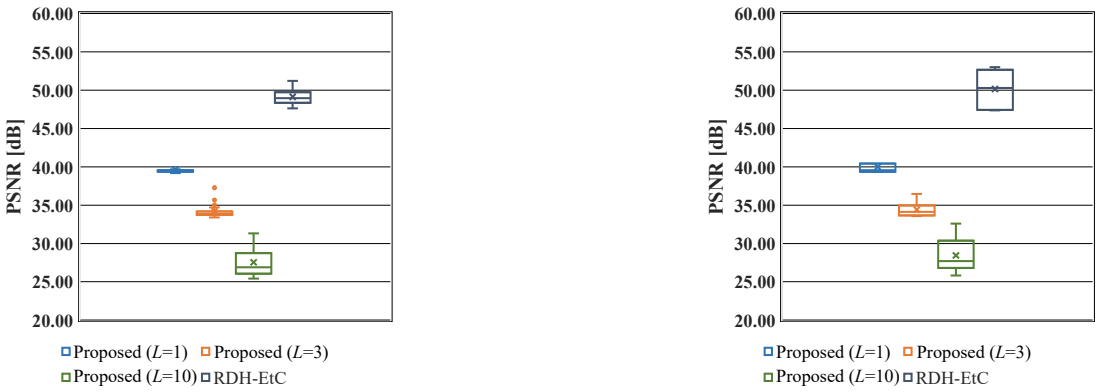
Figure 14 shows examples of marked images obtained with the proposed method with $L = 10$. The RDH-MSB method could not conduct decryption before data extraction; thus, marked images could not be obtained as described above. Figures 15 and 16 exhibit the marked-image quality of the proposed and RDH-EtC methods, respectively. It is clear that

both the PSNR and SSIM values of the proposed method decreased as the value of L, i.e., the hiding capacity, increased. In addition, the values of the proposed method were lower than those of the RDH-EtC method because there was a trade-off between hiding capacity and marked-image quality. In the Kodak database, the proposed method achieved a PSNR of 27.54 dB and SSIM of 0.8960 with a hiding capacity of 0.82 bpp on average (L = 10). In contrast, the PSNR and SSIM values of the RDH-EtC method were 49.14 dB and 0.9989, respectively, with a hiding capacity of 0.04 bpp. As shown in Figures 15c,d and 16c,d, the marked-image quality was affected by image size. The influence on SSIM was particularly large; the SSIM for the images with the original size was much higher than that for the 1/16 images.



(**a**) (**b**) (**c**) (**d**)

Figure 14. Marked images (L = 10). (**a**) Kodim4; (**b**) peppar; (**c**) ihc5 (1/16); (**d**) ihc5 (original).



(**a**) (**b**)

Figure 15. *Cont.*

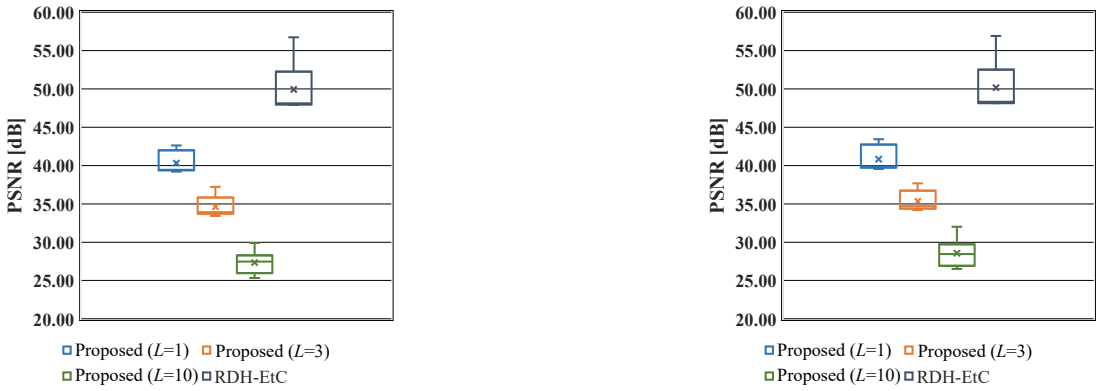


Figure 15. Marked-image quality of proposed and RDH-EtC [30] methods (PSNR). (**a**) Kodim4; (**b**) peppar; (**c**) ihc5 (1/16); (**d**) ihc5 (original).

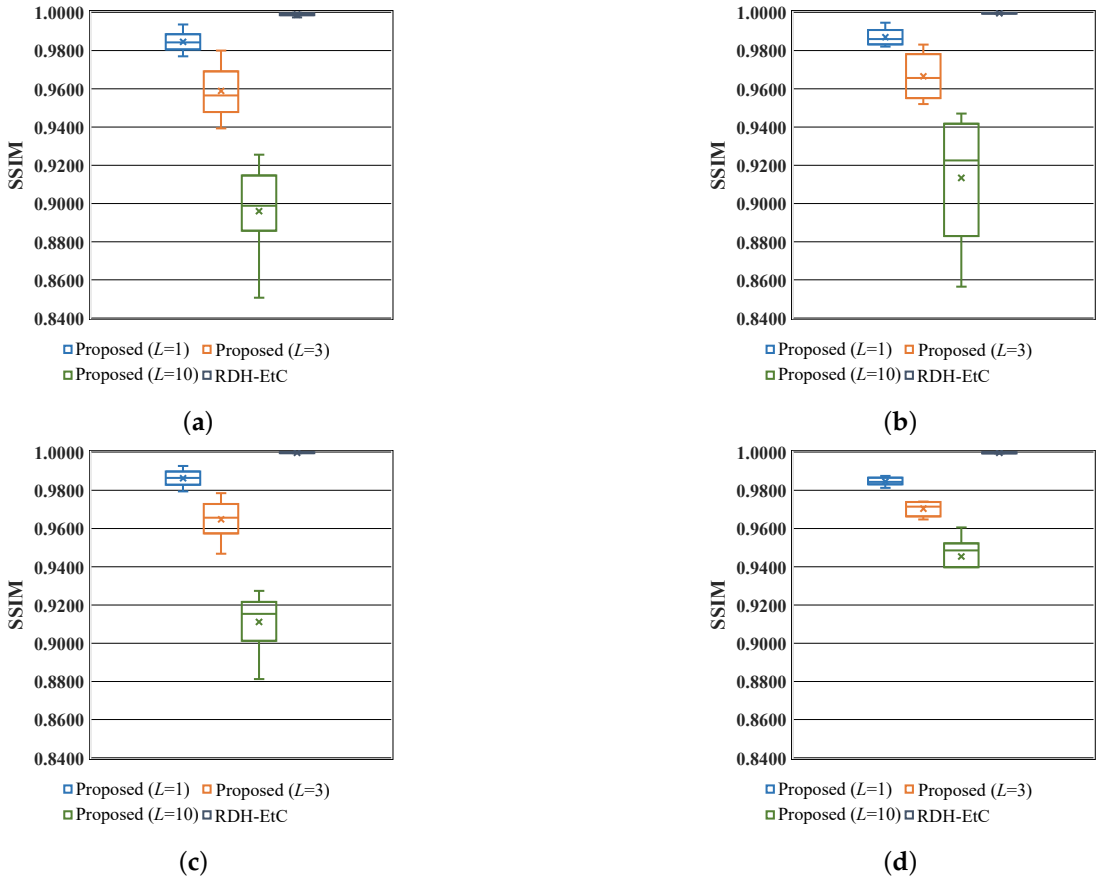


Figure 16. Marked-image quality of proposed and RDH-EtC [30] methods (SSIM). (**a**) Kodim4; (**b**) peppar; (**c**) ihc5 (1/16); (**d**) ihc5 (original).

4.2. Lossless Compression Performance

We evaluated the lossless compression performance using JPEG-LS and JPEG 2000. Figures 17 and 18 show the bitrates of encrypted, marked, and compressed images. While the bitrates of the original images were 8 bpp, those of the encrypted, marked, and compressed images for the proposed method were lower than 7 bpp with any of the three values of *L* for all databases. The RDH-EtC method [30] further attained bitrates lower than those of the proposed method due to a significantly low hiding capacity. Meanwhile, the bitrates of the encrypted, marked, and compressed images for the RDH-MSB method [29]

were expanded compared with those before compression. This was caused by the encryption algorithm using a bitwise exclusive-or operation. Consequently, our method could compress marked encrypted images without loss while enhancing the hiding capacity. Additionally, a larger image contributed to further enhancing performance.

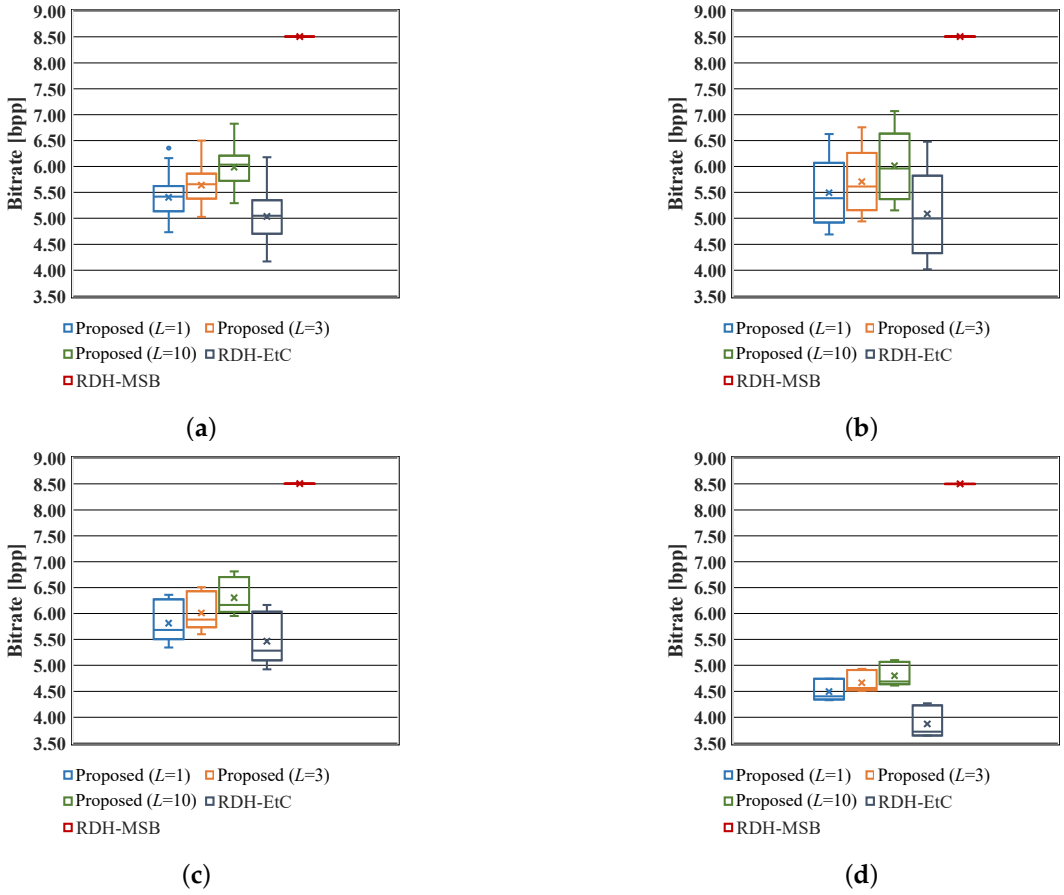


Figure 17. JPEG-LS compression performance of proposed, RDH-EtC [30] and RDH-MSB [29] methods. (**a**) Kodim4; (**b**) peppar; (**c**) ihc5 (1/16); (**d**) ihc5 (original).

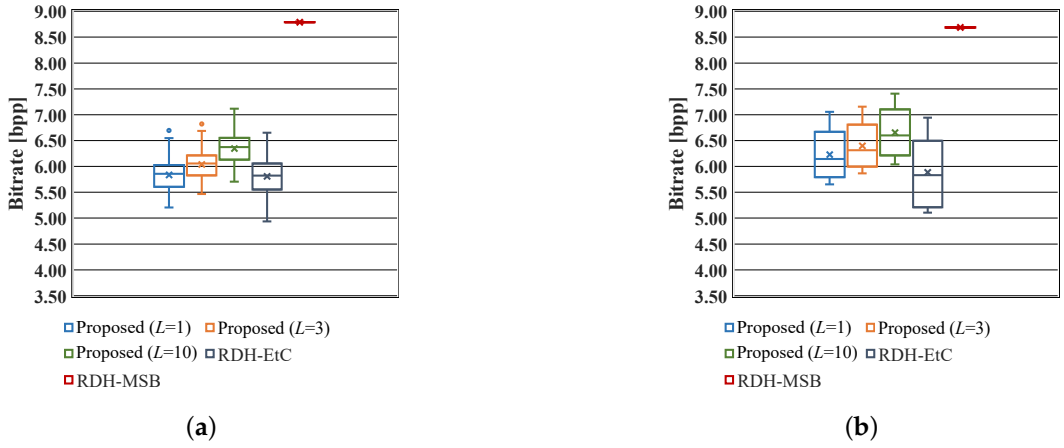


Figure 18. *Cont.*

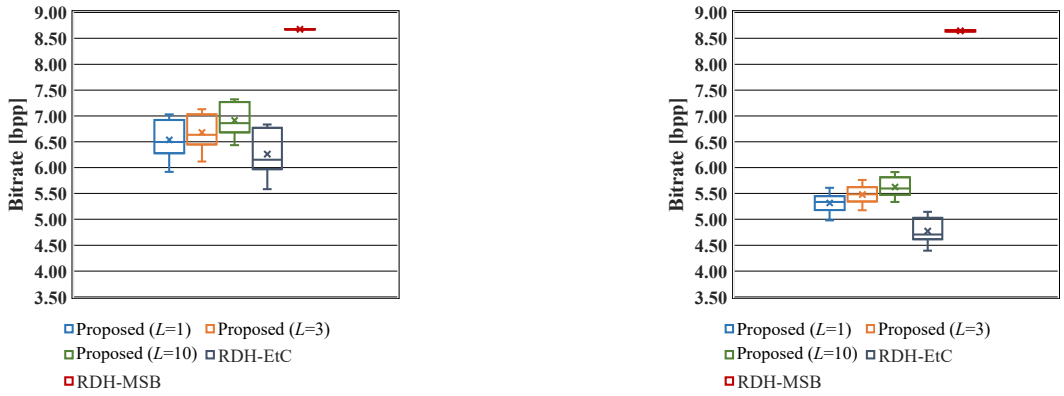


Figure 18. JPEG 2000 compression performance of proposed, RDH-EtC [30] and RDH-MSB [29] methods. (**a**) Kodim4; (**b**) peppar; (**c**) ihc5 (1/16); (**d**) ihc5 (original image).

5. Conclusions

We proposed a new algorithm for reversible data hiding in encrypted images that simultaneously accomplishes both high hiding capacity and high compression performance. Our method has three main advantages. First, a compressible encryption method WAS used to attain high compression performance using international standards JPEG-LS and JPEG 2000. Second, our method achieveD high hiding capacity of around 1 bpp. For this purpose, we introduced an MED predictor for pixel prediction and a PEE-HS method for data hiding. Lastly, we could decrypt marked encrypted images without data extraction; marked images containing a payload could accordingly be obtained.

The proposed method was evaluated in terms of data-hiding capacity, marked-image quality, and lossless compression performance with JPEG-LS and JPEG 2000. We discussed the experimental results with $L = 10$ using the Kodak database, and we confirmed a similar trend in the other databases. The hiding capacity of our method was 0.82 bpp on average. This capacity was approximately 20 times higher than that of a conventional compressible RDH-EI method. In terms of marked-image quality, our method achieved a PSNR of 27.54 dB and SSIM of 0.8960 under hiding capacity of 0.82 bpp. Lastly, we proved that the marked encrypted images could be effectively compressed by using JPEG-LS and JPEG 2000. Regarding the influence of image size, we confirmed that our method further enhanced performance with a larger image. Through our experiments, it was clear that our method was the only technique that possessed all three advantages.

The method still has a constraint on flexibility. When we first decrypted a marked encrypted image before data extraction, a marked image was derived. However, it is difficult to retrieve the original image and extract a payload from the marked image. To alleviate the constraint, we will properly define the embedding order within and among blocks in the data-hiding algorithm. This would further expand the range of applications.

Author Contributions: Conceptualization, R.M., S.I. and H.K.; methodology, R.M. and S.I.; validation, R.M. and S.I.; investigation, R.M.; writing—original draft preparation, R.M.; writing—review and editing, S.I. and H.K.; supervision, S.I. and H.K.; project administration, S.I. and H.K. All authors have read and agreed to the published version of the manuscript.

Funding: This work was partially supported by JSPS KAKENHI, grant number JP21H01327, and the Yutaka Kojima Research Fund of Society of Photography and Imaging of Japan.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Shi, Y.Q.; Li, X.; Zhang, X.; Wu, H.T.; Ma, B. Reversible data hiding: advances in the past two decades. *IEEE Access* **2016**, *4*, 3210–3237.
2. Tian, J. Wavelet-Based Reversible Watermarking for Authentication. *Secur. Watermarking Multimed. Contents IV* **2002**, *4675*, 679–690.
3. Ni, Z.; Shi, Y.Q.; Ansari, N.; Su, W. Reversible data hiding. *IEEE Trans. Circuits Syst. Video Technol.* **2006**, *16*, 354–362.
4. Fujiyoshi, M.; Sato, S.; Jin, H.L.; Kiya, H. A Location-Map Free Reversible Data Hiding Method using Block-Based Single Parameter. In Proceedings of the IEEE International Conference on Image Processing, San Antonio, TX, USA, 16 September–19 October 2007; pp. 257–260.
5. Weng, S.; Shi, Y.Q.; Hong, W.; Yao, Y. Dynamic improved pixel value ordering reversible data hiding. *Inf. Sci.* **2019**, *489*, 136–154.
6. Wang, J.; Chen, X.; Ni, J.; Mao, N.; Shi, Y. Multiple histograms-based reversible data hiding: Framework and realization. *IEEE Trans. Circuits Syst. Video Technol.* **2020**, *30*, 2313–2328.
7. He, W.; Xiong, G.; Wang, Y. Reversible Data Hiding Based on Adaptive Multiple Histograms Modification. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3000–3012.
8. Kim, S.; Qu, X.; Sachnev, V.; Kim, H.J. Skewed Histogram Shifting for Reversible Data Hiding Using a Pair of Extreme Predictions. *IEEE Trans. Circuits Syst. Video Technol.* **2019**, *29*, 3236–3246.
9. Zhang, T.; Li, W.; Qi, W.; Guo, Z. Location-Based PVO and Adaptive Pairwise Modification for Efficient Reversible Data Hiding. *IEEE Trans. Inf. Forensics Secur.* **2020**, *15*, 2306–2319.
10. Qu, B.; Li, X.; Zhang, W.; Zhao, Y. Improving Pairwise PEE via Hybrid-Dimensional Histogram Generation and Adaptive Mapping Selection. *IEEE Trans. Circuits Syst. Video Technol.* **2019**, *29*, 2176–2190.
11. Hassan, F.S.; Gutub, A. Efficient Image Reversible Data Hiding Technique Based on Interpolation Optimization. *Arab. J. Sci. Eng.* **2021**, *46*, 8441–8456.
12. Hassan, F.S.; Gutub, A. Novel embedding secrecy within images utilizing an improved interpolation-based reversible data hiding scheme. *J. King Saud Univ. Comput. Inf. Sci.***2022**, *34*, 2017–2030.
13. Gao, X.; Pan, Z.; Gao, E.; Fan, F. Reversible data hiding for high dynamic range images using two-dimensional prediction-error histogram of the second time prediction. *Signal Process.* **2020**, *173*, 107579.
14. He, X.; Zhang, W.; Zhang, H.; Ma, L.; Li, Y. Reversible data hiding for high dynamic range images using edge information. *Multimedia Tools Appl.* **2019**, *78*, 29137–29160.
15. Bhardwaj, R. Efficient separable reversible data hiding algorithm for compressed 3D mesh models. *Biomed. Signal Process. Control.* **2022**, *73*, 103265.
16. Lue, T.; Jiang, G.; Shao, F.; Peng, Z. Disparity based stereo image reversible data hiding. In Proceedings of the IEEE International Conference on Image Processing, Paris, France, 27–30 October 2014; pp. 5492–5496.
17. Puteaux, P.; Ong, S.Y.; Wong, K.S.; Puech, W. A survey of reversible data hiding in encrypted images—The first 12 years. *J. Vis. Commun. Image Represent.* **2021**, *77*, 103085.
18. Zhang, X. Reversible data hiding in encrypted image. *IEEE Signal Process. Lett.* **2011**, *18*, 255–258.
19. Hong, W.; Chen, T.; Wu, H. An Improved Reversible Data Hiding in Encrypted Images Using Side Match. *IEEE Signal Process. Lett.* **2012**, *19*, 199–202.
20. Zhang, X. Separable reversible data hiding in encrypted image. *IEEE Trans. Inf. Forensics Secur.* **2012**, *7*, 826–832.
21. Ma, K.; Zhang, W.; Zhao, X.; Yu, N.; Li, F. Reversible data hiding in encrypted images by reserving room before encryption. *IEEE Trans. Inf. Forensics Secur.* **2013**, *8*, 553–562.
22. Qian, Z.; Zhang, X.; Wang, S. Reversible Data Hiding in Encrypted JPEG Bitstream. *IEEE Trans. Multimedia.* **2014**, *16*, 1486–1491.
23. Qian, Z.; Zhang, X.; Wang, S. Reversible data hiding in encrypted image with distributed source encoding. *IEEE Trans. Circuits Syst. Video Technol.* **2016**, *26*, 636–646.
24. Puteaux, P.; Puech, W. An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images. *IEEE Trans. Inf. Forensics Secur.* **2018**, *13*, 1670–1681.
25. Dragoi, I.C.; Coltuc, D. On the Security of Reversible Data Hiding in Encrypted Images by MSB Prediction. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 187–189.
26. Puteaux, P.; Puech, W. EPE-based huge-capacity reversible data hiding in encrypted images. In Proceedings of the IEEE International Workshop on Information Forensics and Security (WIFS), Hong Kong, China, 11–13 December 2018; pp. 1–7.
27. Wu, H.T.; Yang, Z.; Cheung, Y.M.; Xu, L.; Tang, S. High-capacity reversible data Hiding in encrypted images by bit plane partition and MSB prediction. *IEEE Access* **2019**, *7*, 62361–62371.
28. Hirasawa, R.; Imaizumi, S.; Kiya, H. An MSB Prediction-Based Method with Marker Bits for Reversible Data Hiding in Encrypted Images. In Proceedings of the IEEE 3rd Global Conference on Life Sciences and Technologies, Nara, Japan, 9–11 March 2021; pp. 48–50.
29. Puteaux, P.; Puech, W. A recursive reversible data hiding in encrypted images method with a very high payload. *IEEE Trans. Multimed.* **2021**, *23*, 636–650.
30. Imaizumi, S.; Izawa, Y.; Hirasawa, R.; Kiya, H. A Reversible Data Hiding Method in Compressible Encrypted Images. *IEICE Trans. Fundam.* **2020**, *E103-A*, 1579–1588.

31. Zhang, Y.; Luo, W. Vector-based Efficient Data Hiding in Encrypted Images via Multi-MSB Replacement. *IEEE Trans. Circuits Syst. Video Technol.* **2022**. http://doi.org/10.1109/TCSVT.2022.3183391.
32. Yu, C.; Zhang, X.; Zhang, X.; Li, G.; Tang, Z. Reversible Data Hiding With Hierarchical Embedding for Encrypted Images. *IEEE Trans. Circuits Syst. Video Technol.* **2022**, *32*, 451–466.
33. Arai, E.; Imaizumi, S. High-Capacity Reversible Data Hiding in Encrypted Images with Flexible Restoration. *J. Imaging* **2022**, *8*, 176.
34. Kurihara, K.; Kikuchi, M.; Imaizumi, S.; Shiota, S.; Kiya, H. An encryption-then-compression system for JPEG/Motion JPEG standard. *IEICE Trans. Fundam.* **2015**, *E98-A*, 2238–2245.
35. Imaizumi, S.; Kiya, H. A block-permutation-based encryption scheme with independent processing of RGB components. *IEICE Trans. Inf. Syst.* **2018**, *E101-D*, 3150–3157.
36. Kiya, H.; Maung, A.P.M.; Kinoshita, Y.; Imaizumi, S.; Shiota, S. An Overview of Compressible and Learnable Image Transformation with Secret Key and Its Applications. *APSIPA Trans. Signal Inf. Process.* **2022**, *11*, e11.
37. Weinberger, M.J.; Seroussi, G.; Sapiro, G. The LOCO-I lossless image compression algorithm: principles and standardization into JPEG-LS. *IEEE Trans. Image Process.* **2000**, *9*, 1309–1324.
38. *ISO/IEC IS–15444–1 Information Technology—JPEG 2000 Image Coding System—Part 1: Core Coding System*; International Organization for Standardization: Geneva, Switzerland, 2019.
39. Chuman, T.; Sirichotedumrong, W.; Kiya, H. Encryption-Then-Compression Systems Using Grayscale-Based Image Encryption for JPEG Images. *IEEE Trans. Inf. Forensics Secur.* **2019**, *14*, 1515–1525.
40. 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.* **2018**, *E101-D*, 37–44.
41. Maungmaung, A.; Kiya, H. Privacy-Preserving Image Classification Using an Isotropic Network. *IEEE Multimed.* **2022**, *29*, 23–33.
42. Chang, A.H.; Case, B.M. Attacks on Image Encryption Schemes for Privacy-Preserving Deep Neural Networks. *arXiv* **2020**, arXiv:2004.13263.
43. Madono, K.; Tanaka, M.; Onishi, M., Ogawa, T. SIA-GAN: Scrambling Inversion Attack Using Generative Adversarial Network. *IEEE Access* **2021**, *9*, 129385–129393.
44. Kodak Lossless True Color Image Suite. Available online: http://www.r0k.us/graphics/kodak/ (accessed on 6 December 2021).
45. The USC-SIPI Image Database. Available online: https://sipi.usc.edu/database/ (accessed on 6 August 2022).
46. IHC Evaluation Resources. Available online: https://www.ieice.org/iss/emm/ihc/ (accessed on 6 August 2022).