mathematics

MDPI

Article

Reversible Data Hiding in Encrypted Images Based on Two-Round Image Interpolation

Qing Zhang and Kaimeng Chen *

College of Computer Engineering, Jimei University, Xiamen 361021, China; 202111810029@jmu.edu.cn
* Correspondence: chenkaimeng@jmu.edu.cn

Abstract: The data embedding of vacating room after encryption reversible data hiding in encrypted images (VRAE RDHEI) is performed on an encrypted image without redundancy and spatial correlation. Data extraction and image recovery rely on a range of unique mechanisms that utilize spatial correlation in the decrypted domain. Of these mechanisms, pixel prediction is among the most frequently used, directly affecting the capacity and fidelity. In this paper, we propose a novel method that uses a two-round interpolation mechanism to enhance pixel prediction precision while preserving a large number of carrier pixels. In the proposed method, the content owner uses a stream cipher to encrypt the image as a carrier. The data hider flips specific LSBs of the encrypted image for data embedding. On the receiver side, the process of data extraction and image recovery is divided into two stages. In each stage, based on the varying distributions of the original or recovered pixels with the carrier pixels, the corresponding pixel interpolation schemes are used to accurately predict the pixels for data extraction and image recovery. The results demonstrate that the proposed method can efficiently improve the capacity and fidelity with full reversibility compared to existing VRAE RDHEI methods.

Keywords: reversible data hiding; encryption; interpolation

MSC: 68P27; 68U10

check for updates

Citation: Zhang, Q.; Chen, K. Reversible Data Hiding in Encrypted Images Based on Two-Round Image Interpolation. *Mathematics* **2024**, *12*, 32. https://doi.org/10.3390/math12010032

Academic Editors: Cheonshik Kim, Ki-Hyun Jung and Cheng-Chi Lee

Received: 16 October 2023
Revised: 15 December 2023
Accepted: 18 December 2023
Published: 22 December 2023

1. Introduction

Reversible data hiding in encrypted images (RDHEI) refers to embedding secret data into encrypted images in a reversible process without decryption. RDHEI has an important application value in some special scenarios such as cloud computing, healthcare and military applications. In these scenarios, the content owner encrypts the image to protect the contents, and the data manager must embed secret data into the encrypted images without accessing the contents to achieve source authentication, content integrity protection or other security requirements. The RDHEI technology involves three parties: the content owner, the data hider and the receiver. The content owner encrypts the plaintext image before transmitting it to the data hider. The data hider embeds secret data into the encrypted image without performing decryption or viewing the content of the image. The receiver then extracts the secret data and recovers the original image.

Based on the concept of reversibility, RDHEI can be classified into three categories [1]: (1) vacating room after encryption (VRAE), (2) reserving room before encryption (RRBE) and (3) creating room by encryption (CRBE). These three types of methods are not interchangeable due to their different image encryption requirements and the requirements of the content owner.

When using VRAE methods, the content owner generates an encrypted image without redundancy and spatial correlation as a carrier. The data hider embeds data into the encrypted image by encoding the ciphertext in a way that is not reversible in the encryption domain. After image decryption, the receiver uses specially designed spatial correlation-based image recovery mechanisms to recover the original image for reversibility. Based on the relationship between data extraction and image recovery, VRAE methods are further categorized into two subclasses: joint type and separated type. In existing joint methods, the data hider performs data embedding using different bit-flipping schemes, and the receiver jointly performs data extraction and image recovery using specially designed spatial correlation-based estimators to judge the bit flipping. In [2], Zhang proposed encrypting the image using a stream cipher through bitwise XOR operations. In their paper, the encrypted image was divided into non-overlapping blocks. Half of the pixels in each block were selected using the data-hiding key, and the three least significant bits (LSBs) of these selected pixels were flipped to embed one bit per block. After the image was decrypted, a smoothness estimation function was used to detect the LSB-flipped pixels within each block to extract the secret bit and recover the block. This method is described in further detail in [3–9]. Hong et al. [3] reduced the error rate during data extraction and image recovery by improving the estimation function and using a side-match strategy. Liao and Shu [4] defined the estimation function by applying different estimation functions to different positions within an image. Meanwhile, the authors of [5] proposed, a novel bit-flipping scheme and an image content adaptive estimation function to enhance reversibility and image quality. In [6], multiple estimation functions were used jointly to improve the accuracy. In [7], a two-class Support Vector Machine (SVM) classifier was employed to distinguish between the original block and the flipped block. In [8], an LSB swapping/shifting data embedding scheme was used to embed multiple bits. Meanwhile, in [9], the blocks were further subdivided into sub-blocks to carry additional secret bits. Some methods use pixel groups rather than blocks to embed data. Wu et al. [10] used the data-hiding key to pseudo-randomly select pixels to form pixel groups, and they flipped an LSB plane of all pixels within the group to embed data. A highly accurate pixel predictor was used to detect pixel flipping to extract the secret data and recover the image. This method was described in further detail in [11,12]. In [11], an improved pixel division scheme and its corresponding pixel predictor were proposed to turn more pixels into carrier pixels to increase their capacity. In [12], multiple predictors are used jointly to enhance the accuracy of data extraction and image recovery. In existing separable methods, some specific bits of the encrypted image are compressed to vacate additional bits for secret data. The data extraction process is separated from the image recovery process. Since there is no redundancy in the encrypted image, this compression is lossy and will result in multiple potential original states after decompression. To judge the correct original state of the lossy compressed bits, spatial correlation-based estimators are used after image decryption. In [13], a pseudo-random sparse matrix was generated to compress the LSBs of the selected pixels. After decrypting the image, the MSBs of the image were used to predict the original states of the compressed LSBs. In [14], a three-stage embedding strategy and a progressive recovery mechanism were proposed to compress more LSBs and allow more accurate image recovery. In [15], a Low-Density Parity-Check (LDPC) code check matrix was used to compress half of the LSBs in the fourth LSB plane to vacate additional bits. In [16], a Slepian–Wolf coding scheme was used to compress the MSBs of the encrypted image to vacate additional bits. The above two methods generate the log-likelihood ratios of the original states of the compressed bits after image decryption; after that, the compressed bits can be decoded correctly by the log-likelihood ratio-based belief propagation algorithm. The authors of [17] proposed an RDHEI method without any additional information transmission between the image owner and the data hider. In terms of security, embeddedness and reversibility, their method showed significant improvement. The embedding performance was not influenced by the image contents, and the algorithmic complexity decreased.

The VRAE methods are limited by the carriers' lack of redundancy and spatial correlation, which makes it very difficult to vacate room. To further improve capacity, the RRBE methods and CRBE methods, which utilize the redundancy of the plaintext images by preprocessing images, have been proposed.

When implementing RRBE methods, the content owner preprocesses the original image prior to encryption to vacate the room without loss. The room remains after image encryption and can be used directly by the data hider. Some methods divide the image into complex regions and smoothness regions and then use plaintext image-based RDH methods to embed the LSB of the complex regions into the smooth regions to vacate room [18,19]. Some methods use special lossless compression coding to compress a portion of the image to vacate room [20–27]. Other methods use special reversible integer transformation mechanisms to transform some pixels into special values with LSBs of 0 to vacate room [28]. In [29], the MED predictor is used to generate a predicted image from the original image. Then, the pixel differences are encoded to make additional room. In [26], the prediction errors are discarded and labeled to achieve higher data embedding capacity. In [30], a compression coding scheme based on multi-level blocking with quad-tree is used to make more room for secret data.

When using CRBE methods, the content owner generates a ciphertext image with redundancy using a specially designed image encryption scheme. The data hider can then use the variants of plaintext image-based RDH methods or lossless compression schemes to reversibly vacate room. Some methods encrypt the image at the block level rather than at the pixel level to preserve intra-block redundancy. Based on the block-level encryption, some methods then use variants of RDH methods, such as histogram shifting [31–36], prediction error expansion [37] and pixel value sorting [38], to embed secret data into the encrypted image. Some methods employ lossless compression coding schemes to vacate room [39–41]. Others design specific reversible image transformation schemes to convert a plaintext image into another image with a high degree of redundancy, directly using plaintext image-based RDH methods to embed secret data [42,43]. In [44], the image is divided into blocks, which are categorized into three different types, and then different encoding schemes are used on the blocks to vacate room. In [45], a block-level encryption algorithm based on a chaotic system is used, and an adaptive-layer MSB substitution scheme is used for reversible data hiding.

Although RRBE and CRBE methods can obtain larger embedding rates, both types of methods have additional costs, which limits their applicability. In RRBE methods, the main work of reversible data hiding is undertaken by the content owner rather than the data hider. Thus, RRBE is impractical if the content owner is unable to process the image or requires the data-hiding process to be transparent. CRBE methods demand that encryption strength be sacrificed to preserve redundancy, making them unsuitable for applications with high security requirements. Compared to these two methods, the VRAE method accepts very strong encryption algorithms and does not require the content owner to process the image, providing higher security and more applicable environments. Therefore, VRAE methods cannot be replaced with RRBE or CRBE methods, and further research on high-performance VRAE methods is still needed.

In this paper, we aim to design a novel high-capacity VRAE RDHEI method based on a highly accurate pixel prediction mechanism. Similar to previous works such as [10,11], our method uses pixel groups for data embedding and employs pixel prediction for data extraction and image recovery. The main challenge associated with these types of methods is the trade-off between the number of carrier pixels and the prediction precision. On the one hand, if too many pixels are used as carriers, the reduction in the original pixels will affect the prediction precision, leading to a higher error rate in data extraction and image recovery, and ultimately a loss of effective capacity. On the other hand, if too many original pixels are retained, the increase in pixel prediction precision will be unable to offset the loss of carrier pixels, which will also affect the effective capacity. Therefore, the carrier pixel segmentation and the pixel predictor must be designed to construct a good trade-off and ultimately improve the overall performance. Based on the above ideas, the proposed method divides three-quarters of the image pixels into two subsets of carrier pixels and employs a two-round image interpolation mechanism as the precise pixel predictor for data extraction and image recovery. The contributions of this paper are as follows:

1. We propose a novel VRAE RDHEI method that uses a parabolic interpolation algorithm and a variant bicubic interpolation algorithm for two rounds of data extraction and image recovery. This two-round interpolation mechanism can obtain both a high carrier pixel ratio and high prediction precision, improving the overall performance of RDHEI.
2. The results prove that our method achieves higher capacity and image fidelity than existing methods due to the effectiveness of the two-round interpolation mechanism.

The rest of this paper is organized as follows. In Section 2, we introduce the framework and details of the proposed method. In Section 3, the experimental results are provided and analyzed. The conclusion of this paper is provided in Section 4.

2. Proposed Method

In this section, we introduce the details of the proposed joint method. Figure 1 shows the framework of the proposed method. First, the content owner encrypts the image using a stream cipher with an image encryption key. Then, the carrier pixels are divided into two subsets, and the data hider uses the data-hiding key to embed secret data into the two subsets, respectively. Finally, the receiver uses the image encryption key to directly decrypt the image into a stego-image, which is highly approximate to the original image, and then uses the parabolic interpolation algorithm and the variant bicubic interpolation algorithm with the data-hiding key for two rounds of data extraction and image recovery on the decrypted image.

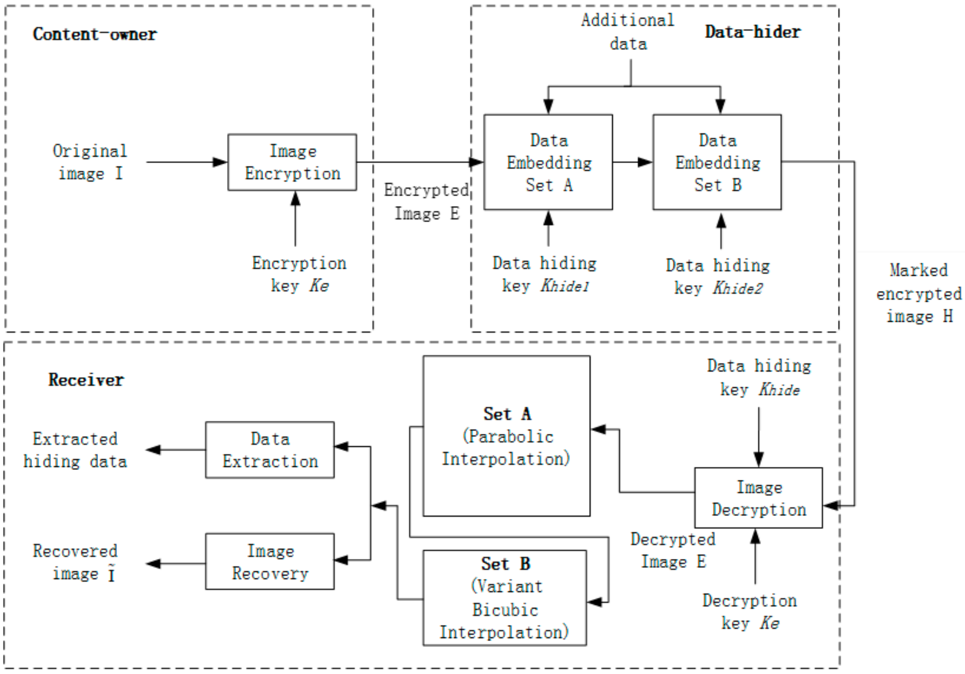


Figure 1. Framework of the proposed joint RDHEI method.

2.1. Content Owner's Work

First, the original image is encrypted by a stream cipher. Given the original grayscale image sized $H \times W$, we denote $b_{i,j,k}$ as the k-th LSB of the pixel $p_{i,j}$ with coordinates (i, j) in the image, where $1 \leq i \leq H, 1 \leq j \leq W$. $b_{i,j,k}$ can be derived as

$$b_{i,j,k} = p_{i,j}/2^{k-1} \text{mod} 2, \text{where } 1 \leq k \leq 8 \tag{1}$$

For each $b_{i,j,k}$, a pseudo-random bit $r_{i,j,k}$ is generated using the image encryption key and a standard stream cipher. The encrypted bit $e_{i,j,k}$ is generated as

$$e_{i,j,k} = b_{i,j,k} \oplus r_{i,j,k} \tag{2}$$

Finally, each plaintext pixel $p_{i,j}$ is encrypted into a ciphertext pixel $E_{i,j}$ as

$$E_{i,j} = \sum_{k=1}^{8} e_{i,j,k} \times 2^{k-1}, \text{ where } 1 \le i \le H,\ 1 \le j \le W \tag{3}$$

After encryption, the cipher image is sent to the data hider for data embedding.

2.2. Data Hider's Work

When an encrypted image is received, the data hider begins by dividing the encrypted image into carrier pixels and reference pixels. Carrier pixels are used for embedding secret data, while reference pixels are used for image recovery. As shown in Figure 2, the carrier pixels are divided into two subsets: Set A and Set B. Set A is denoted as

U	U	U	U	U	U	…
U	B	A	B	A	B	…
U	A	U	A	U	A	…
U	B	A	B	A	B	…
U	A	U	A	U	A	…
U	B	A	B	A	B	…
⋮	⋮	⋮	⋮	⋮	⋮	

Figure 2. Pixel distribution for the proposed method. The gray portion is the portion of the reference pixel that is not densely embedded and is used as a reference pixel for subsequent interpolation predictions.

$Set_A = \{C_{2i+1,2j}, C_{2i,2j+1} | 1 \le i \le \lfloor H/2 \rfloor - 1, 1 \le j \le \lfloor W/2 \rfloor - 1\}$, and Set B is denoted as $Set_B = \{C_{2i,2j} | 1 \le i \le \lfloor (H-1)/2 \rfloor, 1 \le j \le \lfloor (W-1)/2 \rfloor\}$. Pixels outside the carrier pixels are considered reference pixels and are denoted as U.

Data embedding is performed in two rounds. In the first round, the pixels of Set A are selected for embedding. The data hider uses the data-hiding key to randomly divide all the pixels from Set A into non-overlapping same-size pixel groups, and the number of pixels contained in each pixel group is denoted as L_A. By flipping the t-th least significant bit (LSB) (where $1 \le t \le 8$) of each pixel $E_{i,j}$ in a pixel group, the data hider embeds one secret bit b into the pixel group as follows:

$$E'_{i,j} = \begin{cases} E_{i,j}, \text{ if } b = 0 \\ E_{i,j} \oplus 2^{t-1}, \text{ if } b = 1 \end{cases} \tag{4}$$

If the pixels in Set A are not sufficient to embed all the secret data, the data embedding process enters the second round, which uses pixels from Set B. Similarly, the data hider uses the data-hiding key to randomly partition the pixels in Set B into the same-size pixel groups. The group size is denoted as L_B. L_B can be different from L_A for the purpose of performance optimization. The same LSB flipping scheme in Equation (4) is used to embed secret data into these pixel groups.

2.3. Receiver's Work

2.3.1. Basic Process of Data Extraction and Image Recovery

When the receiver obtains an encrypted image containing secret data from the data hider, if the receiver only holds the image encryption key, the bit stream $\left\{r_{i,j,k}\middle|1 \leq i \leq H, 1 \leq j \leq W, 1 \leq k \leq 8\right\}$ for encryption can be generated again and the image can be directly decrypted. The decrypted image will be very similar to the original image. When the receiver holds both the data-hiding key and the image encryption key, the secret data can be extracted and the original image can be retrieved jointly from the decrypted image.

The process of data extraction and image recovery is also divided into two rounds. In the first round, the secret data embedded in the carrier pixels of Set A are extracted, and the original values of the carrier pixels are recovered.

First, the receiver uses the data-hiding key to reconstruct each pixel group $G_{\mathrm{i}} = \{p_1^{(i)}, p_2^{(i)}, \ldots, p_{L_A}^{(i)}\}$ from Set A. Then, by flipping the t-th LSB of all pixels within the group, the flipped pixel group $FG_i = \{fp_1^{(i)}, fp_2^{(i)}, \ldots, fp_{L_A}^{(i)}\}$ is generated. According to Equation (4), one of G_i and FG_i is the original pixel group. To judge the true original pixel group, a highly accurate parabolic interpolation algorithm is used to predict the carrier pixels from Set A based on reference pixels, thus the predicted values $EG_i = \{ep_1^{(i)}, ep_2^{(i)}, \ldots, ep_{L_A}^{(i)}\}$ for all pixels in G_i are generated. The details of this parabolic interpolation algorithm will be introduced in Section 2.3.2. Based on FG_i and EG_i, the secret bit b embedded in G_i can be extracted as follows:

$$b = \begin{cases} 0, \text{ if} \sum_{k=1}^{L_A} \left|p_k^{(i)} - ep_k^{(i)}\right| \leq \sum_{k=1}^{L_A} \left|fp_k^{(i)} - ep_k^{(i)}\right| \\ 1, \text{ if} \sum_{k=1}^{L_A} \left|p_k^{(i)} - ep_k^{(i)}\right| > \sum_{k=1}^{L_A} \left|fp_k^{(i)} - ep_k^{(i)}\right| \end{cases} \tag{5}$$

According to Equation (4), if b = 0, the pixel value in G_i is the original pixel value. Conversely, the pixel value in FG_i is the original pixel value. Therefore, the carrier pixels in Set A can be recovered to the original state simultaneously when the secret bit is extracted.

After all the carrier pixels in Set A have been successfully recovered and the data extracted, the data hider proceeds to extract the data from and recover the original values of the carrier pixels in Set B. As in the first round, the data hider reconstructs each pixel group, $G_{\mathrm{i}} = \{p_1^{(i)}, p_2^{(i)}, \ldots, p_{L_{\mathrm{B}}}^{(i)}\}$, in Set B using the data-hiding key, and then the data hider extracts the secret data and recovers the original values of the carrier pixels following the same process as in the first round. However, unlike the first round, the pixel prediction for Set B is based on the reference pixels and the recovered carrier pixels in Set A, and a variant bicubic interpolation algorithm is used as the pixel predictor. The details of this interpolation algorithm will also be introduced in Section 2.3.2.

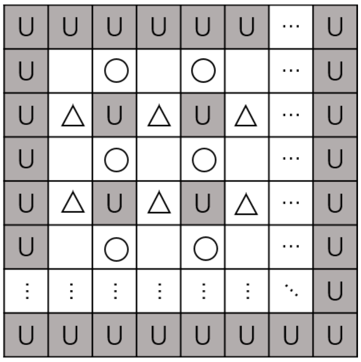
2.3.2. Prediction of Carrier Pixel Values Based on Pixel Interpolation Algorithm

The error rates of data extraction and image recovery are directly related to the pixel group size and the precision of the prediction algorithm. When the pixel prediction precision is improved, full reversibility can be achieved using smaller groups, which will improve the availability of groups of pixels and indicate that fewer image modifications are required when embedding the same bits. Thus, the capacity and the quality of the image containing secret data can be improved. Therefore, a highly precise pixel prediction algorithm is the key to the performance of RDHEI. To improve the prediction precision, based on the division of the carrier pixels, we make certain modifications to two existing pixel interpolation algorithms to predict the carrier pixels in Set A and Set B, respectively.

1. Carrier pixel prediction for Set A

To predict the carrier pixels in Set A, a parabolic interpolation algorithm in [46] is used based on the reference pixels. To predict pixels adjacent to the boundary, additional prediction formulas for these pixels are added to the original algorithm.

As shown in Figure 3, the pixels in Set A are reclassified into the circle set and the triangle set. The circle set can be denoted as $Circle\_Set = \{P(2m, 2n+1) | 1 \leq m \leq \lfloor H/2 \rfloor - 1, 1 \leq n \leq \lfloor W/2 \rfloor - 1\}$, and the triangle set can be denoted as $Triangle\_Set = \{P(2m+1, 2n) | 1 \leq m \leq \lfloor H/2 \rfloor - 1, 1 \leq n \leq \lfloor W/2 \rfloor - 1\}$ $(i = 2m, j = 2n+1)$.



U	U	U	U	U	U	⋯	U
U		○		○		⋯	U
U	△	U	△	U	△	⋯	U
U		○		○		⋯	U
U	△	U	△	U	△	⋯	U
U		○		○		⋯	U
⋮	⋮	⋮	⋮	⋮	⋮	⋱	U
U	U	U	U	U	U	U	U

Figure 3. Circle set and triangle set of Set A.

For the pixels in the circle set, supposing that the pixel value to be predicted is $p(i, j)$, the prediction is performed as follows. In the following equations, the parameter k can take any value from ten values [0.1, 0.2, 0.3, . . ., 1], and the receiver selects the best value according to the prediction results obtained after image decryption.

If $p(i, j)$ is located in the second row of the image, the predicted value of $p(i, j)$ is calculated as

$$\begin{aligned} p(i,j) = {} & kf_1 + (1-k)[p(i-1,j-2)/\sqrt{5} + p(i-1,j-1) + p(i-1,j+2)/\sqrt{5} \\ & + p(i+1,j-2)/\sqrt{5} + p(i+1,j) + p(i+1,j+2)/\sqrt{5}]/\left(4/\sqrt{5}+2\right)(0 \leq k \leq 1) \end{aligned} \tag{6}$$

where $f_1 = \begin{pmatrix} 2^2 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1/8 & -1/4 & 1/8 \\ -1 & 3/2 & -1/2 \\ 15/8 & -5/4 & 3/8 \end{pmatrix} \begin{pmatrix} p(i-1,j) \\ p(i+1,j) \\ p(i+3,j) \end{pmatrix}$.

If $p(i, j)$ is located in the $H - 2$ row of the image, the predicted value of $p(i, j)$ is calculated as

$$\begin{aligned} p(i,j) = {} & k((f_1+f_2)/2) + (1-k)[p(i-1,j-2)/\sqrt{5} + p(i-1,j) + p(i-1,j+2)/\sqrt{5} \\ & + p(i+1,j-2)/\sqrt{5} + p(i+1,j) + p(i+1,j+2)/\sqrt{5}]/\left(4/\sqrt{5}+2\right)(0 \leq k \leq 1) \end{aligned} \tag{7}$$

where $f_1 = \begin{pmatrix} 4^2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1/8 & -1/4 & 1/8 \\ -1 & 3/2 & -1/2 \\ 15/8 & -5/4 & 3/8 \end{pmatrix} \begin{pmatrix} p(i-3,j) \\ p(i-1,j) \\ p(i+1,j) \end{pmatrix}$ and $f_2 = \begin{pmatrix} 2^2 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1/6 & -1/2 & 1/3 \\ -7/6 & 5/2 & -4/3 \\ 2 & -2 & 1 \end{pmatrix} \begin{pmatrix} p(i-1,j) \\ p(i+1,j) \\ p(i+2,j) \end{pmatrix}$.

If $p(i, j)$ is located in the $W - 1$ column of the image, the predicted value of $p(i, j)$ is calculated as

$$\begin{aligned} p(i,j) = {} & k((f_1+f_2)/2) + (1-k)[p(i-1,j-2)/\sqrt{5} + p(i-1,j) + p(i-1,j+1)/\sqrt{2} + p(i,j+1) \\ & + p(i+1,j-2)/\sqrt{5} + p(i+1,j) + p(i+1,j+1)/\sqrt{2}]/(2/\sqrt{5} + 2/\sqrt{2} + 3)(0 \leq k \leq 1) \end{aligned} \tag{8}$$

where $f_1 = \begin{pmatrix} 4^2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1/8 & -1/4 & 1/8 \\ -1 & 3/2 & -1/2 \\ 15/8 & -5/4 & 3/8 \end{pmatrix} \begin{pmatrix} p(i-3,j) \\ p(i-1,j) \\ p(i+1,j) \end{pmatrix}$ and $f_2 = \begin{pmatrix} 2^2 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1/8 & -1/4 & 1/8 \\ -1 & 3/2 & -1/2 \\ 15/8 & -5/4 & 3/8 \end{pmatrix} \begin{pmatrix} p(i-1,j) \\ p(i+1,j) \\ p(i+2,j) \end{pmatrix}$.

Apart from the above, the predicted value of $p(i,j)$ is calculated as

$$\begin{aligned} p(i,j) = {} & k((f_1+f_2)/2) + (1-k)[p(i-1,j-2)/\sqrt{5} + p(i-1,j) + p(i-1,j+2)/\sqrt{5} \\ & + p(i+1,j-2)/\sqrt{5} + p(i+1,j) + p(i+1,j+2)/\sqrt{5}]/\left(4/\sqrt{5}+2\right)(0 \le k \le 1) \end{aligned} \tag{9}$$

where $f_1 = \begin{pmatrix} 4^2 & 4 & 1 \end{pmatrix} \begin{pmatrix} 1/8 & -1/4 & 1/8 \\ -1 & 3/2 & -1/2 \\ 15/8 & -5/4 & 3/8 \end{pmatrix} \begin{pmatrix} p(i-3,j) \\ p(i-1,j) \\ p(i+1,j) \end{pmatrix}$ and $f_2 = \begin{pmatrix} 2^2 & 2 & 1 \end{pmatrix} \begin{pmatrix} 1/8 & -1/4 & 1/8 \\ -1 & 3/2 & -1/2 \\ 15/8 & -5/4 & 3/8 \end{pmatrix} \begin{pmatrix} p(i-1,j) \\ p(i+1,j) \\ p(i+2,j) \end{pmatrix}$.

For the pixels in the triangle set, the pixels to be predicted can be regarded as the mirror pixels of the pixels in the circle set centered on the diagonal. Therefore, these pixels can also be predicted using Equations (6)–(9), simply by mapping each pixel $p(i+x, j+y)$ in the equation to $p(i+y, j+x)$.

2. Carrier pixel prediction for Set B

Based on the reference pixels and the recovered pixels in set A, a variant of the cubic-based bicubic interpolation algorithm [47] is used to predict the pixels in set B. Unlike the original interpolation algorithm, the variant algorithm in the proposed method uses pixels at different locations as the inputs.

The pixels in Set B are divided into two subcategories: pixels that are not adjacent to the boundaries and pixels that are adjacent to the boundaries (the second row and the second column). For the pixels that are not adjacent to the boundaries, the 16 previously identified known pixels around the pixel that is yet to be predicted are used as shown in Figure 4. The prediction value of $p(i,j)$ is calculated as

$$\begin{aligned} p(i,j) = {} & W(\tfrac{1}{2})W(\tfrac{1}{2})(p(i-1,j) + p(i,j-1) + p(i+1,j) + p(i,j+1)) \\ & + W(\tfrac{1}{2})W(\tfrac{3}{2})(p(i-2,j-1) + p(i-2,j-1) + p(i+1,j-2) + p(i+2,j-1) + p(i+2,j+1) + p(i+1,j+2) + p(i-1,j+2) + p(i-2,j+1)) \\ & + W(\tfrac{3}{2})W(\tfrac{3}{2})(p(i-1,j-1) + p(i+1,j-1) + p(i+1,j+1) + p(i-1,j+1)) \end{aligned} \tag{10}$$

where $W(x)$ is calculated as

$$W(x) = \begin{cases} 1.5|x|^3 - 2.5|x|^2 + 1 & |x| \le 1 \\ -0.5|x|^3 + 2.5|x|^2 - 4|x| + 2 & 1 < |x| < 2 \\ 0 & \mathit{otherwise} \end{cases} \tag{11}$$

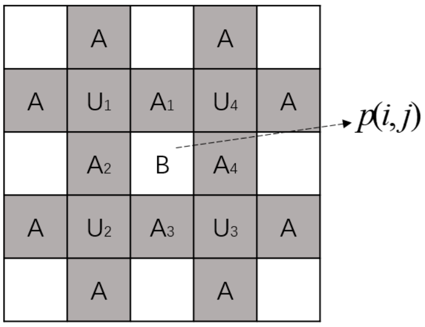


Figure 4. Prediction of pixels not adjacent to the boundaries in Set B.

Since the cubic-based bicubic algorithm uses the surrounding 16 pixels shown in (b) for interpolation prediction, the surrounding 16 pixels in (a) are shift-transformed into (b) before interpolation prediction is performed.

For the pixels adjacent to the boundaries, which cannot be predicted using the variant bicubic interpolation, the interpolation algorithm in [48] is used for prediction. As shown in Figure 5, where B denotes the pixel to be predicted in the second row and the second column, the prediction value of B is calculated as

$$B = [U_1 + U_2 + U_3 + U_4 + 2U_5)]/6 \tag{12}$$

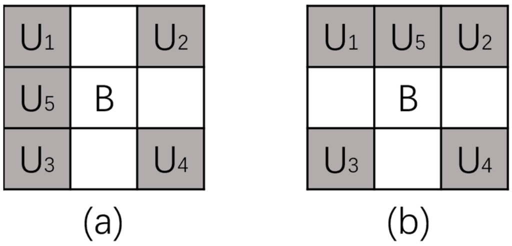


Figure 5. Prediction of pixels adjacent to the boundaries in Set B. (**a**) Pixels adjacent to the left boundary. (**b**) Pixels adjacent to the upper boundary.

3. Separable Proposed Method

Based on the joint RDHEI framework described above, in this section, we described a separable RDHEI method. The framework of this method is shown in Figure 6. Firstly, the content owner generates the location map using the interpolation algorithms. The location map is used to mark the MSBs which cannot be predicted correctly using the interpolation algorithms. Then, the original image is encrypted by using the encryption key. Second, the data hider embeds the location map and the secret data into the encrypted image with the data-hiding key using MSB substitution. Finally, by using the encryption key only, the receiver can recover an image that is similar to the original image. Meanwhile, using the data-hiding key only, the receiver can obtain the secret data from the encrypted image. If the receiver possesses both the encryption key and the data-hiding key, he can recover both the original image and the secret data without any errors.

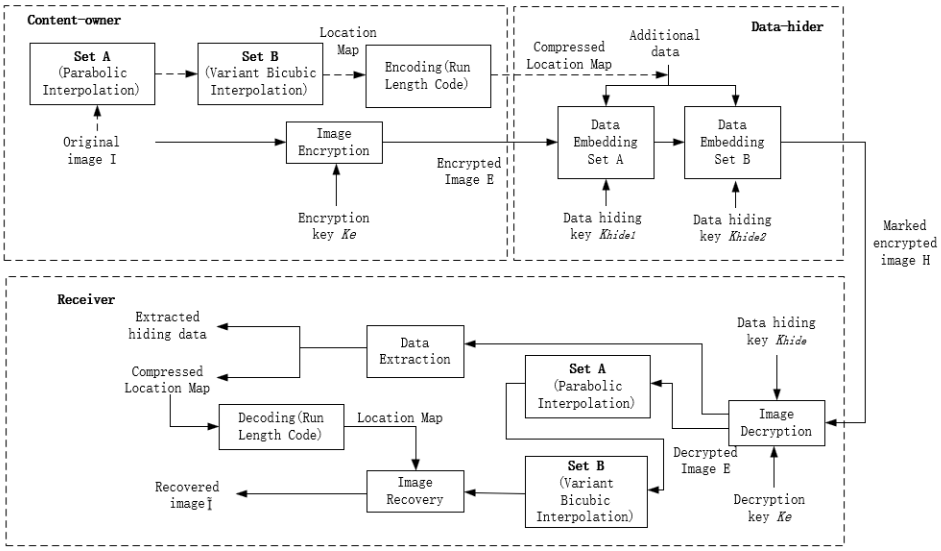


Figure 6. Framework of the proposed separable RDHEI method.

3.1. Content Owner's Work

To ensure full reversibility, in addition to encryption, the content owner must generate a location map of the original MSBs. First, the content owner uses the two interpolation algorithms to predict each pixel, as described in Section 2.3.2, and judges if the MSB of each pixel can be recovered correctly according to Equation (5). Then, a location map that marks the coordinates of the incorrectly predicted MSBs is generated and subsequently compressed by the run-length code.

After the location map has been generated, the content owner uses the image encryption key to encrypt the original image described in Equation (2), and then sends the encrypted image and the compressed location map to the data hider.

3.2. Data Hider's Work

The data hider embeds the secret data into the encrypted image along with the compressed location map, as follows. First, the data hider divides the encrypted image into two Set A and Set B as shown in Figure 2. Then, the data hider uses the data-hiding key to pseudo-randomly select the encrypted pixels in Set A, before the MSBs of the selected pixels are substituted with the bits of the compressed location map and the secret data for data embedding. When the pixels of Set A are exhausted, the pixels of Set B are selected for data embedding in the same way.

3.3. Receiver's Work

Data extraction. When the receiver has the data-hiding key, the secret data can be directly extracted from the encrypted image. First, the receiver divides the pixels into Set A and Set B. Then, the data-hiding key is used to retrieve all selected pixels which are used for data embedding. Finally, the secret data can be extracted directly from the MSBs of the pixels.

Image recovery. If the receiver only has the image encryption key, the receiver can retrieve an approximated image that is very similar to the original image. The receiver begins by decrypting the encrypted image directly using the image encryption key. Then, by using the two interpolation algorithms, respectively, on Set A and Set B, the MSBs of all pixels are predicted as described in Equation (2). Since the receiver does not have the data-hiding key, pixels embedded with a secret bit are not recognizable, so the MSBs of all carrier pixels are replaced by the predicted values to reconstruct the approximated image.

If the receiver has both the image encryption key and data-hiding key, the compressed location map can be retrieved from the encrypted image. After image decryption and approximated image generation, the receiver can use the location map to identify all of the MSBs that have been incorrectly predicted, and then recover the approximated image into the original image by correcting the MSB errors.

4. Experimental Results and Analysis

In this section, to evaluate the performance of the proposed method, we test the proposed method on six standard 512 × 512 grayscale images as shown in Figure 7. For the jointly proposed method, four existing VRAE RDHEI methods created by Liao and Shu [4], Bhardwaj and Aggarwal [9], Wu and Sun [10] and Dragoi et al. [11] are used as the competitors. To ensure a fair comparison, for the proposed method and for [4,9,11], we adjust the size of the pixel groups or image blocks to the minimum values to ensure error-free data extraction and image recovery. For the separable proposed method, two existing separable methods created by Qian and Zhang [16] and Yu et al. [17] are used as the competitors.

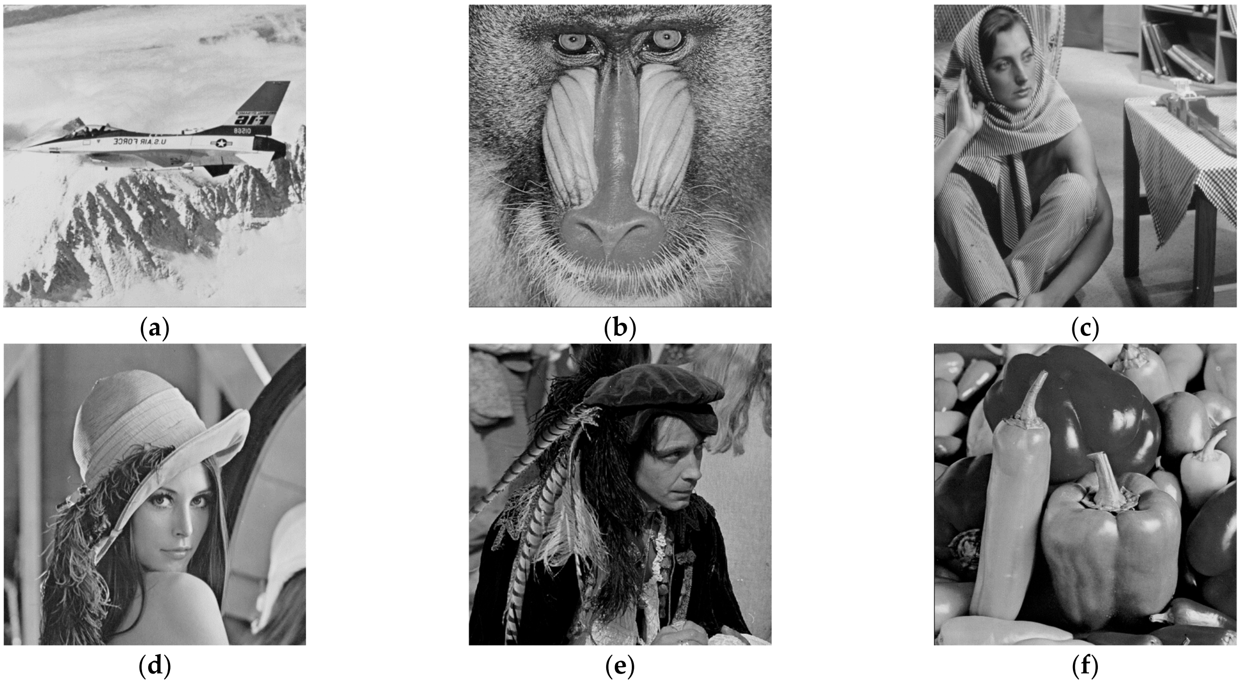


Figure 7. Six test images. (**a**) Airplane; (**b**) baboon; (**c**) Barbara; (**d**) Lena; (**e**) man; (**f**) peppers.

4.1. Experimental Results and Comparison of Joint Proposed Method

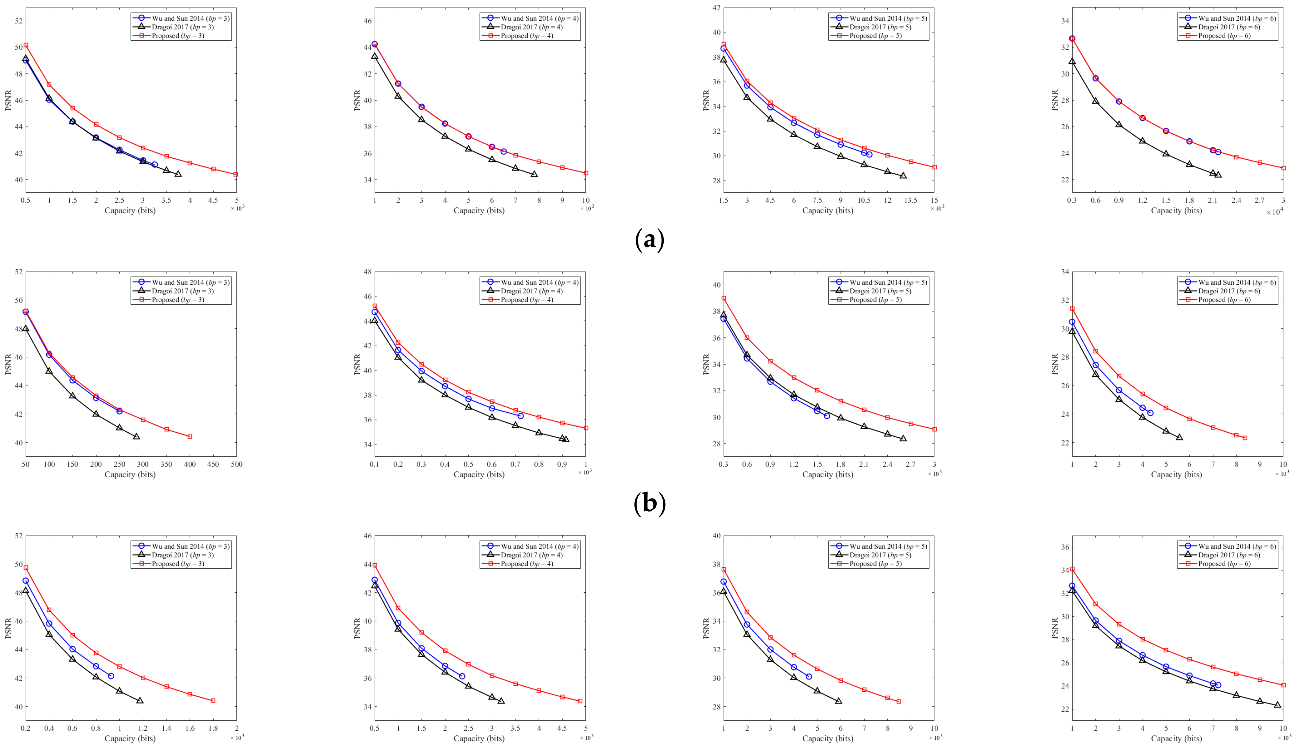
Table 1 shows the capacity of all of the described methods. In the jointly proposed method [10,11], different LSB planes can be chosen for data embedding to achieve the trade-off between capacity and image fidelity, and the experimental results for the third to sixth LSB plane are provided. In [4,9], only the least three LSB planes can be used for data embedding. As shown in the table, when the third LSB plane is used, the proposed method can achieve higher capacity than [4,9], which use the least three LSB planes. For each bit plane, the embedding rates of the proposed method are all higher than [10,11]. In conclusion, the proposed method can achieve better capacity.

Table 1. Embedding rates comparison between [4,9–11] and the proposed method based on different LSB planes.

Method	LSB Plane	Airplane	Baboon	Barbara	Lena	Man	Peppers
Proposed (joint)	3rd	0.0190	0.0015	0.0069	0.0112	0.0044	0.0063
	4th	0.0394	0.0048	0.0186	0.0354	0.0146	0.0218
	5th	0.0677	0.0137	0.0324	0.0700	0.0374	0.0607
	6th	0.1323	0.0319	0.0572	0.1322	0.0699	0.0974
Wu and Sun [10]	3rd	0.0113	0.0010	0.0042	0.0078	0.0030	0.0044
	4th	0.0237	0.0026	0.0102	0.0217	0.0094	0.0135
	5th	0.0415	0.0083	0.0199	0.0415	0.0226	0.0332
	6th	0.0711	0.0208	0.0332	0.0830	0.0415	0.0623
Dragoi et al. [11]	3rd	0.0143	0.0011	0.0045	0.0093	0.0034	0.0063
	4th	0.0298	0.0035	0.0114	0.0248	0.0090	0.0213
	5th	0.0496	0.0106	0.0213	0.0496	0.0114	0.0532
	6th	0.0827	0.0248	0.0372	0.0930	0.0677	0.0827
Liao and Shu [4]	1st~3rd	0.0044	0.0009	0.0008	0.0080	0.0030	0.0058
Bhardwaj and Aggarwal [9]	1st~3rd	0.0050	0.0011	0.0011	0.0066	0.0037	0.0050

The reversibility of the VRAE method is related to the size of the data-hiding unit (pixel group or image block); the larger the data-hiding unit, the stronger the spatial correlation inside it, and the lower the probability of error in the data extraction and image recovery. However, a larger data-hiding unit size will reduce the overall ability of the units, subsequently reducing the capacity. Improving the precision of the spatial correlation-based prediction/evaluation mechanism can effectively reduce the data-hiding unit size required for full reversibility. The two-round interpolation mechanism used in the proposed method provides as many carrier pixels as possible for the construction of data-hiding units on the one hand, and on the other hand, it reduces the size of the pixel group required for full reversibility through highly precise pixel prediction. Therefore, the proposed method can obtain a higher capacity compared to the related methods.

Figures 8 and 9 compare the image fidelity comparison between the proposed method and the competitors on different LSB planes and different embedding rates as measured by PSNR. As shown in Figure 8, the proposed method can achieve higher PSNR than the competitors on the six test images. Since the proposed method can achieve full reversibility using a smaller pixel group, compared to other methods, the proposed method can modify fewer pixels to embed the same secret bits and thus achieve higher fidelity. In particular, in the lower LSB plane of Man, Lena and peppers (e.g., the third LSB plane), the PSNR of the images from the proposed method is only slightly higher than [10,11], or even almost close. The reason is that in the third LSB plane of these images, there is no significant advantage in the prediction accuracy of the proposed method. Thus the group size required for the full reversibility of the proposed method is close to [10,11]. In this case, embedding the same bits leads to similar image distortion.

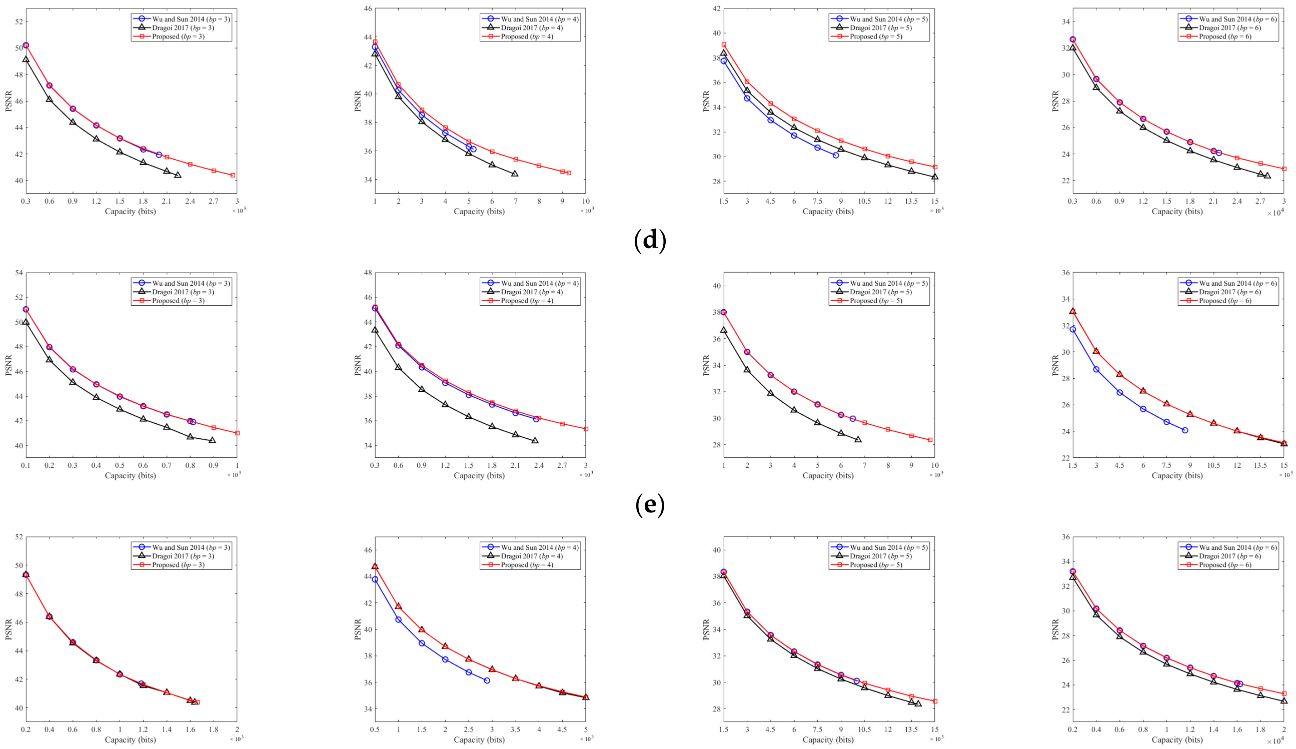


(**a**)

(**b**)

(**c**)

Figure 8. *Cont.*

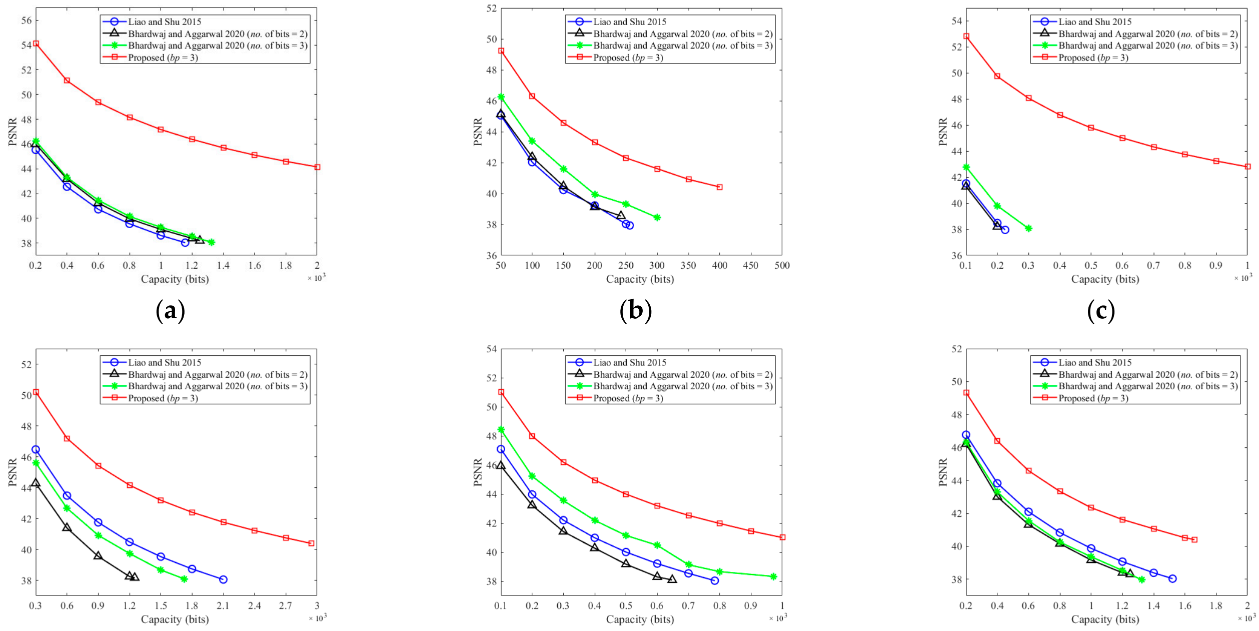


(**d**)

(**e**)

(**f**)

Figure 8. PSNR comparison between [10,11] and the proposed method using 3rd~6th LSB Planes. (**a**) Airplane; (**b**) baboon; (**c**) Barbara; (**d**) Lena; (**e**) man; (**f**) peppers.



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

(**d**) (**e**) (**f**)

Figure 9. Comparison of PSNR between [4,9] and the proposed method using the 3rd LSB plane. (**a**) Airplane; (**b**) baboon; (**c**) Barbara; (**d**) Lena; (**e**) man; (**f**) peppers.

4.2. Experimental Results and Comparison of Separable Proposed Method

Table 2 shows the capacity comparison between [16,17] and the separable proposed method based on the MSB plane. As shown in the table, the proposed separable method has a higher capacity than the other two separable methods. Compared with [16], the interpolation algorithms used in the proposed method can achieve better prediction accuracy, and the location map used in the proposed method can help reduce the capacity cost for correcting prediction errors. Compared with [17], the method in this paper allows more pixels to be used as carrier pixels.

Table 2. Comparison of the embedding rates between [16,17] and the proposed method based on the MSB plane.

Method	Airplane	Baboon	Barbara	Lena	Man	Peppers
Proposed	0.7171	0.5010	0.6231	0.7429	0.7041	0.7219
Qian and Zhang [16]	0.2952	0.2952	0.2952	0.2952	0.2952	0.2952
Yu and Yao [17]	0.2481	0.2476	0.2471	0.2481	0.2480	0.2481

Table 3 shows the image fidelity comparison between the proposed method and the competitors on the MSB plane measured by PSNR. Since all three methods use the MSB plane for data embedding, the approximated images of the three methods are generated by predicting and reconstructing all MSBs, so that the PSNR values of the approximated images are independent of the embedding rates. The PSNR of the proposed method is higher than [16] but lower than [17]. The reason is that the proposed method uses the same number of carrier pixels as [16], but the prediction accuracy is higher, and therefore the reconstructed image is of better quality. However, [17] uses a much lower number of carrier pixels than the proposed method so it requires less MSBs to be reconstructed and hence the distortion is lower, but this is at the expense of capacity.

Table 3. Comparison of PSNR between [16,17] and the proposed method using the MSB plane.

Method	Airplane	Baboon	Barbara	Lena	Man	Peppers
Proposed	36.2153	26.0855	27.0917	49.7581	33.7971	34.6697
Qian and Zhang [16]	29.8257	24.3856	25.7503	35.7316	31.6778	32.7684
Yu et al. [17]	$+\infty$	39.8784	36.2451	$+\infty$	45.7004	60.1720

5. Conclusions

In this paper, we proposed a novel RDHEI method with a two-round image interpolation mechanism as the pixel predictor for data extraction and image recovery. This mechanism uses a parabolic interpolation algorithm and a bicubic interpolation algorithm separately over two rounds to achieve high-precision pixel prediction, thereby improving the overall RDHEI performance. The experimental results show that the method proposed in this paper can effectively improve capacity and fidelity compared with existing VRAE RDHEI methods.

Author Contributions: Conceptualization, K.C.; methodology, Q.Z.; software, Q.Z.; validation, Q.Z. and K.C.; writing—original draft preparation, Q.Z.; writing—review and editing, K.C.; visualization, Q.Z.; supervision, K.C.; project administration, K.C.; funding acquisition, K.C. All authors have read and agreed to the published version of the manuscript.

Funding: This research and the APC were funded by the Natural Science Foundation of Fujian Province, China, grant number 2020J01698, and the Research Support Fund of Jimei University, grant number ZP2021014.

Data Availability Statement: Publicly available datasets were analyzed in this study. This data can be found here: http://decsai.ugr.es/cvg/dbimagenes/g512.php.

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

References

1. Yi, S.; Zhou, Y. Separable and Reversible Data Hiding in Encrypted Images Using Parametric Binary Tree Labeling. *IEEE Trans. Multimed.* **2019**, *21*, 51–64. [CrossRef]
2. Zhang, X. Reversible Data Hiding in Encrypted Image. *IEEE Signal Process. Lett.* **2011**, *18*, 255–258. [CrossRef]
3. Hong, W.; Chen, T.-S.; Wu, H.-Y. An improved reversible data hiding in encrypted images using side match. *IEEE Signal Process. Lett.* **2012**, *19*, 199–202. [CrossRef]
4. Liao, X.; Shu, C. Reversible data hiding in encrypted images based on absolute mean difference of multiple neighboring pixels. *J. Vis. Commun. Image Represent.* **2015**, *28*, 21–27. [CrossRef]
5. Qin, C.; Zhang, X. Effective reversible data hiding in encrypted image with privacy protection for image content. *J. Vis. Commun. Image Represent.* **2015**, *31*, 154–164. [CrossRef]
6. Pan, Z.; Wang, L.; Hu, S.; Ma, X. Reversible data hiding in encrypted image using new embedding pattern and multiple judgments. *Multimed. Tools Appl.* **2015**, *75*, 8595–8607. [CrossRef]
7. Zhou, J.; Sun, W.; Dong, L.; Liu, X.; Au, O.C.; Tang, Y.Y. Secure Reversible Image Data Hiding over Encrypted Domain via Key Modulation. *IEEE Trans. Circuits Syst. Video Technol.* **2016**, *26*, 441–452. [CrossRef]
8. Qian, Z.; Dai, S.; Jiang, F.; Zhang, X. Improved joint reversible data hiding in encrypted images. *J. Vis. Commun. Image Represent.* **2016**, *40*, 732–738. [CrossRef]
9. Bhardwaj, R.; Aggarwal, A. An improved block based joint reversible data hiding in encrypted images by symmetric cryptosystem. *Pattern Recognit. Lett.* **2020**, *139*, 60–68. [CrossRef]
10. Wu, X.; Sun, W. High-capacity reversible data hiding in encrypted images by prediction error. *Signal Process.* **2014**, *104*, 387–400. [CrossRef]
11. Dragoi, I.C.; Coanda, H.-G.; Coltuc, D. Improved reversible data hiding in encrypted images based on reserving room after encryption and pixel prediction. In Proceedings of the 2017 25th European Signal Processing Conference (EUSIPCO), Kos Island, Greece, 28 August–2 September 2017; pp. 2186–2190. [CrossRef]
12. Dragoi, I.C.; Coltuc, D. Reversible data hiding in encrypted images based on reserving room after encryption and multiple predictors. In Proceedings of the 2018 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP), Calgary, AB, Canada, 15–20 April 2018; pp. 2102–2105. [CrossRef]
13. Zhang, X. Separable Reversible Data Hiding in Encrypted Image. *IEEE Trans. Inf. Forensic Secur.* **2012**, *7*, 826–832. [CrossRef]
14. Qian, Z.; Zhang, X.; Feng, G. Reversible Data Hiding in Encrypted Images Based on Progressive Recovery. *IEEE Signal Process. Lett.* **2016**, *23*, 1672–1676. [CrossRef]
15. Zhang, X.; Qian, Z.; Feng, G.; Ren, Y. Efficient reversible data hiding in encrypted images. *J. Vis. Commun. Image Represent.* **2014**, *25*, 322–328. [CrossRef]
16. Qian, Z.; Zhang, X. Reversible Data Hiding in Encrypted Images with Distributed Source Encoding. *IEEE Trans. Circuits Syst. Video Technol.* **2016**, *26*, 636–646. [CrossRef]
17. Yu, M.; Yao, H.; Qin, C. Reversible data hiding in encrypted images without additional information transmission. *SPIC* **2022**, *105*, 116696. [CrossRef]
18. Ma, K.; Zhang, W.; Zhao, X.; Yu, N.; Li, F. Reversible Data Hiding in Encrypted Images by Reserving Room before Encryption. *IEEE Trans. Inf. Forensic Secur.* **2013**, *8*, 553–562. [CrossRef]
19. Xiang, S.; Luo, X. Reversible Data Hiding in Homomorphic Encrypted Domain by Mirroring Ciphertext Group. *IEEE Trans. Circuits Syst. Video Technol.* **2018**, *28*, 3099–3110. [CrossRef]
20. Puteaux, P.; Puech, W. An Efficient MSB Prediction-Based Method for High-Capacity Reversible Data Hiding in Encrypted Images. *IEEE Trans. Inf. Forensic Secur.* **2018**, *13*, 1670–1681. [CrossRef]
21. Yin, Z.; Xiang, Y.; Zhang, X. Reversible Data Hiding in Encrypted Images Based on Multi-MSB Prediction and Huffman Coding. *IEEE Trans. Multimed.* **2020**, *22*, 874–884. [CrossRef]
22. Mohammadi, A.; Nakhkash, M.; Akhaee, M.A. A High-Capacity Reversible Data Hiding in Encrypted Images Employing Local Difference Predictor. *IEEE Trans. Circuits Syst. Video Technol.* **2020**, *30*, 2366–2376. [CrossRef]
23. Yi, S.; Zhou, Y. Binary-block embedding for reversible data hiding in encrypted images. *Signal Process.* **2017**, *133*, 40–51. [CrossRef]
24. Chen, F.; Yuan, Y.; He, H.; Tian, M.; Tai, H.-M. Multi-MSB Compression Based Reversible Data Hiding Scheme in Encrypted Images. *IEEE Trans. Circuits Syst. Video Technol.* **2021**, *31*, 905–916. [CrossRef]
25. Wu, X.; Qiao, T.; Xu, M.; Zheng, N. Secure Reversible Data Hiding in Encrypted Images Based on Adaptive Prediction-error Labeling. *Signal Process.* **2021**, *188*, 108200. [CrossRef]
26. Yin, Z.; She, X.; Tang, J.; Luo, B. Reversible data hiding in encrypted images based on pixel prediction and multi-MSB planes rearrangement. *Signal Process.* **2021**, *187*, 108146. [CrossRef]
27. Puteaux, P.; Puech, W. A recursive reversible data hid-ing in encrypted images method with a very high payload. *IEEE Trans. Multimedia* **2021**, *23*, 636–650. [CrossRef]
28. Qiu, Y.; Qian, Z.; Zeng, H.; Lin, X.; Zhang, X. Reversible data hiding in encrypted images using adaptive reversible integer transformation. *Signal Process.* **2020**, *167*, 107288. [CrossRef]
29. Wu, F.; Zhou, X.; Chen, Z.; Yang, B. A reversible data hiding scheme for encrypted images with pixel difference encoding. *Knowl.-Based Syst.* **2021**, *234*, 107583. [CrossRef]

30. Kumar, R.; Sharma, A.K. Bit-Plane Based Reversible Data Hiding in Encrypted Images Using Multi-Level Blocking with Quad-Tree. *IEEE Trans. Multimed.* **2023**, 1–14. [CrossRef]
31. Xiao, D.; Xiang, Y.; Zheng, H.; Wang, Y. Separable reversible data hiding in encrypted image based on pixel value ordering and additive homomorphism. *J. Vis. Commun. Image Represent.* **2017**, *45*, 1–10. [CrossRef]
32. Ge, H.; Chen, Y.; Qian, Z.; Wang, J. A High Capacity Multi-Level Approach for Reversible Data Hiding in Encrypted Images. *IEEE Trans. Circuits Syst. Video Technol.* **2019**, *29*, 2285–2295. [CrossRef]
33. Xu, D.; Su, S. Reversible data hiding in encrypted images with separability and high embedding capacity. *Signal Process. Image* **2021**, *95*, 116274. [CrossRef]
34. Li, X.; Li, B.; Yang, B.; Zeng, T. General framework to histogram-shifting-based reversible data hiding. *IEEE Trans. Image Process.* **2013**, *22*, 2181–2191. [CrossRef] [PubMed]
35. Li, X.; Zhang, W.; Gui, X.; Yang, B. Efficient Reversible Data Hiding Based on Multiple Histograms Modification. *IEEE Trans. Inf. Forensic Secur.* **2015**, *10*, 2016–2027. [CrossRef]
36. Li, M.; Xiao, D.; Zhang, Y.; Nan, H. Reversible Data Hiding in Encrypted Images Using Cross Division and Additive Homomorphism. *Signal Process. Image* **2015**, *39*, 234–248. [CrossRef]
37. Yi, S.; Zhou, Y.; Hua, Z. Reversible data hiding in encrypted images using adaptive block-level prediction-error expansion. *Signal Process. Image* **2018**, *64*, 78–88. [CrossRef]
38. Long, M.; Zhao, Y.; Zhang, X.; Peng, F. A separable reversible data hiding scheme for encrypted images based on Tromino scrambling and adaptive pixel value ordering. *Signal Process.* **2020**, *176*, 107703. [CrossRef]
39. Qin, C.; He, Z.; Luo, X.; Dong, J. Reversible data hiding in encrypted image with separable capability and high embedding capacity. *Inf. Sci.* **2018**, *465*, 285–304. [CrossRef]
40. Liu, Z.-L.; Pun, C.-M. Reversible Data Hiding in Encrypted Images using Chunk Encryption and Redundancy Matrix Representation. *IEEE Trans. Depend. Secur.* **2020**, *19*, 1382–1394. [CrossRef]
41. Wang, Y.; He, W. High capacity reversible data hiding in encrypted image based on adaptive MSB prediction. *IEEE Trans. Multimedia* **2021**, *24*, 1288–1298. [CrossRef]
42. Huang, D.; Wang, J. High-capacity reversible data hiding in encrypted image based on specific encryption process. *Signal Process. Image* **2020**, *80*, 115632. [CrossRef]
43. Zhang, W.; Wang, H.; Hou, D.; Yu, N. Reversible Data Hiding in Encrypted Images by Reversible Image Transformation. *IEEE Trans. Multimed.* **2016**, *18*, 1469–1479. [CrossRef]
44. Gao, G.; Tong, S.; Xia, Z.; Shi, Y. A universal reversible data hiding method in encrypted image based on MSB prediction and error embedding. *IEEE Trans. Cloud Comput.* **2022**, *11*, 1692–1706. [CrossRef]
45. Chen, S.; Chang, C.-C. Reversible data hiding in encrypted images using block-based adaptive MSBs prediction. *J. Inf. Secur. Appl.* **2022**, *69*, 103297. [CrossRef]
46. Zhang, X.; Sun, Z.; Tang, Z.; Yu, C.; Wang, X. High capacity data hiding based on interpolated image. *Multimed. Tools Appl.* **2016**, *76*, 9195–9218. [CrossRef]
47. Hou, H.; Andrews, H. Cubic splines for image interpolation and digital filtering. *IEEE Trans. Acoust. Speech Signal Process.* **1978**, *26*, 508–517. [CrossRef]
48. Malik, A.; Sikka, G.; Verma, H.K. A Reversible Data Hiding Scheme for Interpolated Images Based on Pixel Intensity Range. *Multimed. Tools Appl.* **2020**, *79*, 18005–18031. [CrossRef]

Disclaimer/Publisher's Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.