

Reversible data hiding scheme based on exploiting modification direction with two steganographic images

Chuan Qin · Chin-Chen Chang · Tai-Jung Hsu

Published online: 9 February 2014
© Springer Science+Business Media New York 2014

Abstract In this paper, we propose a novel data hiding scheme with reversibility based on exploiting modification direction (EMD). One cover image is first chosen and prepared to generate two visually similar steganographic images. During the secret embedding, the pixels in the first steganographic image are modified by no more than one gray level to embed secret data using the traditional EMD method, while the pixels in the second steganographic image are adaptively modified through referring to the first steganographic image without any confusions in image recovery process. On the receiver side, secret data can be extracted easily and the original cover image can also be recovered from the two steganographic images correctly. Experimental results demonstrate that our scheme can achieve high hiding capacity and satisfactory visual quality.

Keywords Reversible data hiding · Exploiting modification direction · Hiding capacity · Image quality

1 Introduction

Due to the prevalence of Internet, a large amount of user data may be transmitted in the insecure channels. To protect the content of user data, data encryption techniques have been

C. Qin
School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai 200093, China
e-mail: qin@usst.edu.cn

C.-C. Chang (✉)
Department of Information Engineering and Computer Science, Feng Chia University, 100 Wenhwa Road, Taichung 40724, Taiwan
e-mail: alan3c@gmail.com

C.-C. Chang
Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan

T.-J. Hsu
Department of Computer Science and Information Engineering, National Chung Cheng University, Chiayi 62102, Taiwan
e-mail: andyblack77@gmail.com

applied [4, 11]. However, since the ciphertext after encryption is meaningless, it may arouse the attention of the interceptors. Therefore, in order to overcome this problem, data hiding techniques have been proposed in recent years, which can embed the secret data into the meaningful cover media imperceptibly, especially for digital images [1, 2, 5, 8, 9, 12, 13, 16]. The stego images after embedding can be utilized for data transmission with lower risks, and the receiver can extract the hidden secret data easily. According to whether the original cover image pixels can be recovered or not after data extraction, current data hiding schemes can be classified into two categories, i.e., reversible data hiding [1, 9, 12, 13] and irreversible data hiding [2, 5, 8, 16]. Earlier schemes of reversible data hiding usually exploited the techniques of difference expansion [1, 13] and histogram shifting [9] to achieve the reversibility. In the recent reported works of reversible data hiding [3, 6, 7, 10, 14, 15, 17], many researchers integrated the prediction mechanism and conducted data embedding on the prediction errors in order to improve the performances [6, 10, 14, 17]. Compared with reversible data hiding schemes, irreversible data hiding schemes often have greater hiding capacities. But, for irreversible schemes, the modifications on cover images caused by data embedding are not invertible.

Least significant bit (LSB) method is a well-known irreversible data hiding technique, which directly replaces the bits in the LSB planes of cover image with the secret bits for embedding. The distortions imposed on cover images depend on the hiding capacity. Later on, many studies have been conducted to improve the traditional LSB method. A LSB matching revisited method was proposed by Mielikainen [8], in which the secret bits were embedded by using the binary function and four embedding rules. In order to fully take advantage of the direction modifications for cover pixel values, Zhang and Wang proposed an efficient steganographic data embedding method based on the mechanism of exploiting modification direction (EMD) [16], which reduced the distortions caused by embedding and achieved greater hiding capacity than the traditional LSB method. The detailed descriptions of the EMD method [16] are given in the next section. Although the method in [16] based on EMD has higher embedding efficiency, it cannot achieve the reversibility of stego image. In other words, after secret data extraction, the EMD method [16] cannot recover the cover image reversibly. However, nowadays, in many application scenarios, such as military images and medical images, the images cannot be allowed with any alterations due to the risk of misinterpretations, thus, the reversibility under these scenarios is necessary.

In this work, to solve the irreversibility of the EMD method in [16], we propose a novel data hiding scheme based on EMD with reversibility by using two steganographic images, which can also achieve satisfactory performances of the hiding capacity and the stego image quality. In the proposed scheme, one cover image is chosen initially, and it produces two visually similar steganographic images after embedding. During the embedding, the first steganographic image has the property that all the pixels in this image are modified no more than one gray level based on [16]. According to the modification direction of each stego pixel pair in the first steganographic image, the modification direction of each pixel pair in the second steganographic image can be adaptively determined, which can guarantee no confusions in the image recovery procedure. On the receiver side, the embedded secret data can be easily extracted from these two steganographic images, and the cover image can be recovered correctly according to the corresponding direction relationships of the pixel pairs in the two steganographic images.

The rest of this paper is organized as follows. In Section 2, the EMD method in [16] is briefly reviewed. The procedures of embedding, extraction and recovery for the proposed scheme are presented detailedly in Section 3. Experimental results and comparisons are given in Section 4. Finally, conclusions are drawn in Section 5.

2 Related work

Zhang and Wang proposed an effective data hiding method that embeds secret data by modifying cover pixel groups with different directions [16]. In their method, the binary secret bits were first represented in $(2n+1)$ -ary notation system, i.e., the value of each secret digit for embedding was located in the range of $[0, 2n]$. The n different cover pixels chosen in one group were denoted as (g_1, g_2, \dots, g_n) , and each pixel group can obtain one f value by the defined function F , see Eq. (1).

$$f = F(g_1, g_2, \dots, g_n) = \left[\sum_{i=1}^n (g_i \times i) \right] \bmod(2n + 1). \quad (1)$$

If the current secret digit d for embedding in the pixel group (g_1, g_2, \dots, g_n) was equal to f , no modifications were required in this pixel group. If d was not equal to f , the value of s is calculated, see Eq. (2).

$$s = (d-f) \bmod(2n + 1). \quad (2)$$

If s was not greater than n , the pixel g_s was increased by one. Otherwise, g_{2n+1-s} was decreased by one. By this method, one secret digit d can be embedded into the pixel group (g_1, g_2, \dots, g_n) .

For example, suppose that n is equal to 2, and the current secret digit d for embedding is 1. Two pixels (g_1, g_2) in a group are given as $(4, 2)$. After calculating using Eq. (1), f is equal to 3, which is not equal to the secret digit 1. Then, the value of s is computed: $s=(1-3) \bmod 5=3$. Since s is greater than n , the pixel group is modified from $(4, 2)$ to $(4, 1)$, i.e., g_2 is decreased by one. The embedded secret digit d can be easily extracted from the modified pixel group using Eq. (1), i.e., $d=F(4, 1)=6 \bmod 5=1$. However, the original cover pixel group cannot be recovered by this method.

3 Proposed scheme

In this section, a data hiding scheme with reversibility based on the EMD mechanism is proposed. After a cover image C is chosen and pre-processed, secret data are embedded into the pixel pairs of C to generate the first steganographic image $S^{(1)}$, and then, according to $S^{(1)}$, the second steganographic image $S^{(2)}$ can be generated by adaptively modifying the corresponding pixel pairs of C for embedding. By using $S^{(1)}$ and $S^{(2)}$, the receiver can extract secret data and recover the original cover image C after the post-processing. The detailed embedding and extracting procedures are described below.

3.1 Embedding procedure

In the proposed scheme, every two pixels in the cover image C construct a pixel group, i.e., $n=2$. Thus, the secret data for embedding are represented in the quinary notation system. Initially, two steganographic images, i.e., $S^{(1)}$ and $S^{(2)}$, for data embedding are generated according to the pre-processed cover image C . Then, all pixel groups, i.e., pixel pairs, in C are traversed and the corresponding pixel pairs in $S^{(1)}$ and $S^{(2)}$ are sequentially modified to embed secret data. The flowchart of the data embedding procedure for each pixel pair is illustrated in Fig. 1.

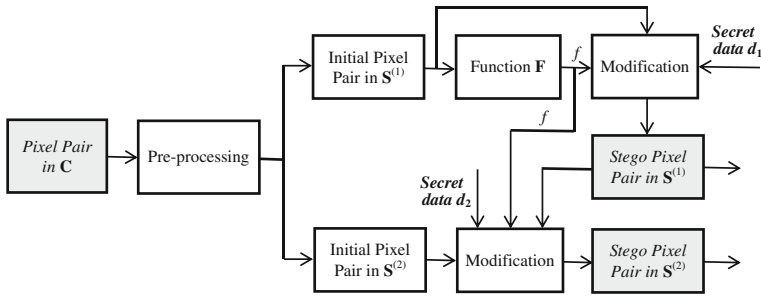


Fig. 1 Flowchart of the embedding procedure

Because the pixel values of the two steganographic images may be modified during the embedding, the pre-processing operation is required to overcome the overflow and underflow problems of pixels. In other words, the pre-processing operation is used to guarantee that all pixel values after embedding are kept in the range of $[0, 255]$. Due to the data embedding, compared with the pixels in the cover image C , the pixels in the steganographic image $S^{(1)}$ may be modified by no more than one gray level and the pixels in the steganographic image $S^{(2)}$ may be modified by no more than $(2n+1)$ gray levels. Thus, during the pre-processing, in order to avoid the overflow and underflow problems, the pixels in the original cover image C belonging to $[0, 2n]$ or $[255-2n, 255]$ are set to the values of $2n+1$ or $255-2n-1$, respectively. Note that the original values and coordinates of these changed pixels should be recorded for reversibility and then be compressed by arithmetic coding to form the extra information, which can be embedded together with the secret message. After the pre-processing, the two initial steganographic images, i.e., $S^{(1)}$ and $S^{(2)}$, are both set the same as the pre-processed cover image C . The following embedding procedure can be described detailedly in two phases as follows:

Phase 1 Embedding in the pixel pair of steganographic image $S^{(1)}$

For simplicity, the current pixel pair $(C_{i,j}, C_{i+1,j})$ for traversing in C is denoted as (g_1, g_2) , where $C_{i,j}$ is the pixel value with the coordinate (i, j) of the image C . By using the EMD method in Eq. (1), we can calculate the f value of the current pixel pair (g_1, g_2) . If the current secret digit d_1 in quinary notation system for embedding in the current pixel pair $(S^{(1)}_{i,j}, S^{(1)}_{i+1,j})$ of $S^{(1)}$ is equal to f , $(S^{(1)}_{i,j}, S^{(1)}_{i+1,j})$ is just made equal to $(C_{i,j}, C_{i+1,j})$, where $S^{(1)}_{i,j}$ denotes the pixel value with the coordinate (i, j) of $S^{(1)}$. If d_1 is not equal to f , the s_1 value is computed: $s_1 = (d_1 - f) \bmod (2n+1)$. If s_1 is not greater than n , i.e., $s_1 = 1$ or 2 , the pixel pair $(S^{(1)}_{i,j}, S^{(1)}_{i+1,j})$ is assigned according to Eq. (3).

$$\begin{cases} S^{(1)}_{i+s_1-1,j} = C_{i+s_1-1,j} + 1, \\ S^{(1)}_{i+n-s_1,j} = C_{i+n-s_1,j}. \end{cases} \tag{3}$$

Explicitly, when $s_1 = 1$, Eq. (3) denotes that $S^{(1)}_{i,j} = C_{i,j} + 1$ and $S^{(1)}_{i+1,j} = C_{i+1,j}$; when $s_1 = 2$, Eq. (3) denotes that $S^{(1)}_{i+1,j} = C_{i+1,j} + 1$ and $S^{(1)}_{i,j} = C_{i,j}$. Otherwise, if s_1 is greater than n , i.e., $s_1 = 3$ or 4 , the pixel pair $(S^{(1)}_{i,j}, S^{(1)}_{i+1,j})$ is assigned according to Eq. (4).

$$\begin{cases} S^{(1)}_{i+2n-s_1,j} = C_{i+2n-s_1,j} - 1, \\ S^{(1)}_{i+s_1-n-1,j} = C_{i+s_1-n-1,j}. \end{cases} \tag{4}$$

Explicitly, when $s_1 = 3$, Eq. (3) denotes that $S^{(1)}_{i+1,j} = C_{i+1,j} - 1$ and $S^{(1)}_{i,j} = C_{i,j}$; when $s_1 = 4$, Eq. (3) denotes that $S^{(1)}_{i,j} = C_{i,j} - 1$ and $S^{(1)}_{i+1,j} = C_{i+1,j}$.

Phase 2 Embedding in the pixel pair of steganographic image $S^{(2)}$

We can find from *Phase 1* that, after embedding the secret digit d_1 in the pixel pair $(S^{(1)}_{i,j}, S^{(1)}_{i+1,j})$ of $S^{(1)}$, there are totally three cases between $(C_{i,j}, C_{i+1,j})$ and $(S^{(1)}_{i,j}, S^{(1)}_{i+1,j})$, see Eq. (5). How to embed the secret digit d_2 in the corresponding pixel pair $(S^{(2)}_{i,j}, S^{(2)}_{i+1,j})$ of $S^{(2)}$ depends on which case in Eq. (5) is satisfied.

$$\begin{aligned}
 \text{Case 1 : } & C_{i,j} = S^{(1)}_{i,j} \text{ and } C_{i+1,j} = S^{(1)}_{i+1,j}, \\
 \text{Case 2 : } & C_{i,j} = S^{(1)}_{i,j} \text{ and } C_{i+1,j} \neq S^{(1)}_{i+1,j}, \\
 \text{Case 3 : } & C_{i,j} \neq S^{(1)}_{i,j} \text{ and } C_{i+1,j} = S^{(1)}_{i+1,j}.
 \end{aligned}
 \tag{5}$$

If Case 1 is satisfied and the secret digit d_2 in quinary notation system for embedding in the current pixel pair $(S^{(2)}_{i,j}, S^{(2)}_{i+1,j})$ of $S^{(2)}$ is equal to f , $(S^{(2)}_{i,j}, S^{(2)}_{i+1,j})$ is just made equal to $(C_{i,j}, C_{i+1,j})$, where $S^{(2)}_{i,j}$ denotes the pixel value with the coordinate (i, j) of $S^{(2)}$. If d_2 is not equal to f , the s_2 value is computed: $s_2 = (d_2 - f) \bmod (2n + 1)$. If s_2 is not greater than n , i.e., $s_2 = 1$ or 2 , the pixel pair $(S^{(2)}_{i,j}, S^{(2)}_{i+1,j})$ is assigned according to Eq. (6).

$$\begin{cases}
 S^{(2)}_{i+s_2-1,j} = C_{i+s_2-1,j} + 1, \\
 S^{(2)}_{i+n-s_2,j} = C_{i+n-s_2,j}.
 \end{cases}
 \tag{6}$$

Otherwise, if s_2 is greater than n , i.e., $s_2 = 3$ or 4 , the pixel pair $(S^{(2)}_{i,j}, S^{(2)}_{i+1,j})$ is assigned according to Eq. (7).

$$\begin{cases}
 S^{(2)}_{i+2n-s_2,j} = C_{i+2n-s_2,j} - 1, \\
 S^{(2)}_{i+s_2-n-1,j} = C_{i+s_2-n-1,j}.
 \end{cases}
 \tag{7}$$

If Case 2 is satisfied, a proper integer $k \in \{1, 2, \dots, 5\}$ should be first found to meet the relationship in Eq. (8).

$$d_2 = \mathbf{F} \left[C_{i,j}, C_{i+1,j} - k \times \text{sign} \left(S^{(1)}_{i+1,j} - C_{i+1,j} \right) \right],
 \tag{8}$$

where $\text{sign}(\cdot)$ is a sign function that returns 1 and -1 for the positive and the negative numbers, respectively. Then, the pixel pair $(S^{(2)}_{i,j}, S^{(2)}_{i+1,j})$ is assigned according to Eq. (9).

$$\begin{cases}
 S^{(2)}_{i,j} = C_{i,j}, \\
 S^{(2)}_{i+1,j} = C_{i+1,j} - k \times \text{sign} \left(S^{(1)}_{i+1,j} - C_{i+1,j} \right).
 \end{cases}
 \tag{9}$$

If Case 3 is satisfied, a proper integer $k \in \{1, 2, \dots, 5\}$ also should be first found to meet the relationship in Eq. (10).

$$d_2 = \mathbf{F} \left[C_{i,j} - k \times \text{sign} \left(S^{(1)}_{i,j} - C_{i,j} \right), C_{i+1,j} \right],
 \tag{10}$$

Then, the pixel pair $(S^{(2)}_{i,j}, S^{(2)}_{i+1,j})$ is assigned according to Eq. (11).

$$\begin{cases} S_{i,j}^{(2)} = C_{i,j-k} \times \text{sign}(S_{i,j}^{(1)} - C_{i,j}), \\ S_{i+1,j}^{(2)} = C_{i+1,j}. \end{cases} \tag{11}$$

Two examples in Fig. 2a and b are utilized to illustrate the embedding procedure, and the two current pixel pairs (g_1, g_2) of cover images in these two examples are both (3, 3). For the example in Fig. 2a, the secret digits d_1 and d_2 for embedding in the two pixel pairs of $S^{(1)}$ and $S^{(2)}$ are assumed to be 4 and 3, respectively. Because the f value of (3, 3), i.e., $F(3, 3)$, is equal to d_1 , the pixel pair in $S^{(1)}$ is not modified. Correspondingly, the pixel pair in $S^{(2)}$ is modified from (3, 3) to (2, 3). The other example is shown in Fig. 2b, and the secret digits d_1 and d_2 for embedding in $S^{(1)}$ and $S^{(2)}$ are assumed to be 3 and 1, respectively. Since the pixel pair in $S^{(1)}$ is modified to (2, 3), which is located on the left side of the original pixel pair (3, 3), thus, the pixel pair in $S^{(2)}$ is modified from (3, 3) to (5, 3).

After all pixel pairs in the cover image C are traversed and all corresponding pixel pairs in the two steganographic images $S^{(1)}$ and $S^{(2)}$ finish the above two phases, the secret embedding procedure is completed, and each pixel pair of $S^{(1)}$ and $S^{(2)}$ is embedded with one secret digit in quinary notation system. Additionally, during the embedding procedure, since the modifications to the two initial steganographic images are slight, thus, the appearances of $S^{(1)}$ and $S^{(2)}$ after embedding are both visually similar to the cover image C .

3.2 Extraction and recovery procedures

On the receiver side, after the two steganographic images $S^{(1)}$ and $S^{(2)}$ are received, the embedded secret digits can easily be extracted from all pixel pairs in $S^{(1)}$ and $S^{(2)}$ by using Eq. (1). In other words, all the pixel pairs in $S^{(1)}$ and $S^{(2)}$ are traversed and fed into the function F sequentially, and each return value of F is just the secret digit extracted from the fed pixel pair. Besides the secret extraction, for every two corresponding pixel pairs in $S^{(1)}$ and $S^{(2)}$, i.e.,

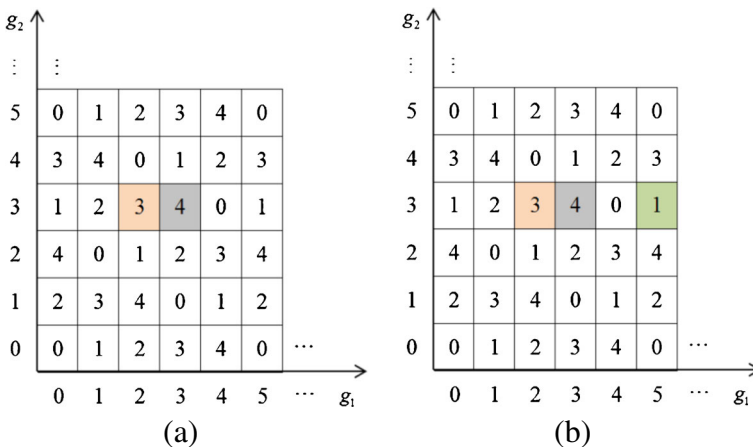


Fig. 2 Two examples of the embedding procedure

$(S^{(1)}_{i,j}, S^{(1)}_{i+1,j})$ and $(S^{(2)}_{i,j}, S^{(2)}_{i+1,j})$, their common cover pixel pair $(R_{i,j}, R_{i+1,j})$ before embedding can also be recovered correctly. The flowchart of the data extraction and image recovery procedures for each pixel pair is illustrated in Fig. 3, and the detailed recovery procedure for $(R_{i,j}, R_{i+1,j})$ is described as follows.

For every two corresponding pixel pairs in $S^{(1)}$ and $S^{(2)}$, the value of η is first calculated using Eq. (12).

$$\eta = \left| \left(S^{(1)}_{i,j} - S^{(2)}_{i,j} \right) + \left(S^{(1)}_{i+1,j} - S^{(2)}_{i+1,j} \right) \right|, \tag{12}$$

where $||$ represents the function of absolute value. If η is equal to 0 or 1, the recovered pixel pair is just made equal to the pixel pair in $S^{(1)}$, i.e., $(R_{i,j}, R_{i+1,j}) = (S^{(1)}_{i,j}, S^{(1)}_{i+1,j})$. Under the condition that $\eta > 1$, if $S^{(1)}_{i,j} \neq S^{(2)}_{i,j}$ and $S^{(1)}_{i+1,j} = S^{(2)}_{i+1,j}$, the recovered pixel pair $(R_{i,j}, R_{i+1,j})$ is assigned according to Eq. (13).

$$\begin{cases} R_{i,j} = S^{(1)}_{i,j} - \text{sign} \left[S^{(1)}_{i,j} - S^{(2)}_{i,j} \right], \\ R_{i+1,j} = S^{(1)}_{i+1,j}. \end{cases} \tag{13}$$

If $S^{(1)}_{i,j} = S^{(2)}_{i,j}$ and $S^{(1)}_{i+1,j} \neq S^{(2)}_{i+1,j}$, the recovered pixel pair $(R_{i,j}, R_{i+1,j})$ is assigned according to Eq. (14).

$$\begin{cases} R_{i,j} = S^{(1)}_{i,j}, \\ R_{i+1,j} = S^{(1)}_{i+1,j} - \text{sign} \left[S^{(1)}_{i+1,j} - S^{(2)}_{i+1,j} \right]. \end{cases} \tag{14}$$

For example, in Fig. 2a, the pixel pairs in the two embedded steganographic images $S^{(1)}$ and $S^{(2)}$ are (3, 3) and (2, 3), respectively. Since η is equal to 1, $(R_{i,j}, R_{i+1,j})$ is recovered to (3, 3). In Fig. 2b, the pixel pairs in $S^{(1)}$ and $S^{(2)}$ are (2, 3) and (5, 3), respectively, and η is equal to 3, thus, $(R_{i,j}, R_{i+1,j})$ is recovered to (3, 3) by Eq. (13).

After all the two corresponding pixel pairs in the received steganographic images $S^{(1)}$ and $S^{(2)}$ are conducted above procedure, all cover pixel pairs can be recovered to their pre-processed versions, and then, according to the extra information retrieved from the extracted data, the whole original cover image C can be easily reversed with no error after post-processing.

4 Experimental results and comparisons

In this section, experimental results and comparisons are presented. The eight standard test images, i.e., *Lena*, *Baboon*, *Sailboat*, *Lake*, *Tiffany*, *Jet*, *Goldhill*, and *Barbara*, with sizes of

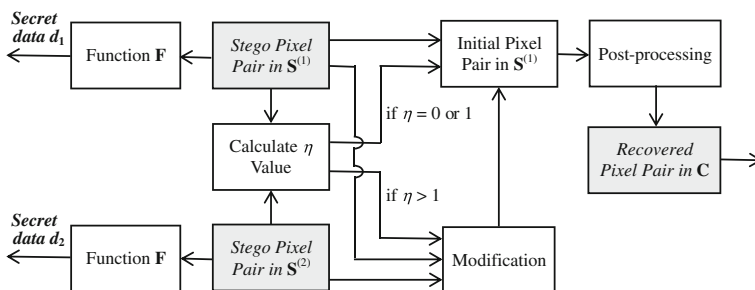


Fig. 3 Flowchart of the data extraction and image recovery procedures

512×512 shown in Fig. 4 were used as the cover images, and the two standard images, i.e., *Peppers* and *Zelda*, with sizes of 256×256 shown in Fig. 5 were used as the secret images for embedding. All images in the experiments are gray-scale images. As described in Section 3, each pixel value of the secret image in our scheme was represented in the quinary notation system by four digits. For example, the pixel value 70 was converted to (0240)₅.

To evaluate the image quality after secret embedding, the peak signal-to-noise ratio (PSNR) value was utilized, see Eq. (15).

$$\text{PSNR} = 10 \cdot \log_{10} \frac{255^2}{\text{MSE}}, \quad (15)$$

where the mean squared error (MSE) between the cover image **C** and the steganographic image **S** with the sizes of $H \times W$ is calculated by Eq. (16).

$$\text{MSE} = \frac{1}{H \times W} \sum_{i=1}^H \sum_{j=1}^W [C(i, j) - S(i, j)]^2. \quad (16)$$

In the proposed scheme, from the statistical viewpoint, three-fifth of the pixels in the first steganographic images $\mathbf{S}^{(1)}$ are not modified after embedding, while two-fifths of the pixels in $\mathbf{S}^{(1)}$ are modified by one gray level after embedding. On the other hand, after embedding, the 13 twenty-fifths of the pixels in the second steganographic images $\mathbf{S}^{(2)}$ are not modified, the two twenty-fifths of the pixels in $\mathbf{S}^{(2)}$ are modified by one gray level, and the remaining two-fifths of the pixels in $\mathbf{S}^{(2)}$ are modified by one, two, three, four, or five gray levels with the equal probabilities. Therefore, we can calculate two theoretical PSNR values, i.e., $\text{PSNR}^{(1)}$ and $\text{PSNR}^{(2)}$, for the two steganographic images $\mathbf{S}^{(1)}$ and $\mathbf{S}^{(2)}$ after embedding according to Eqs. (17–18).

$$\text{PSNR}^{(1)} = 10 \cdot \log_{10} \frac{255^2}{2/5} \approx 52.11 \text{ dB}, \quad (17)$$

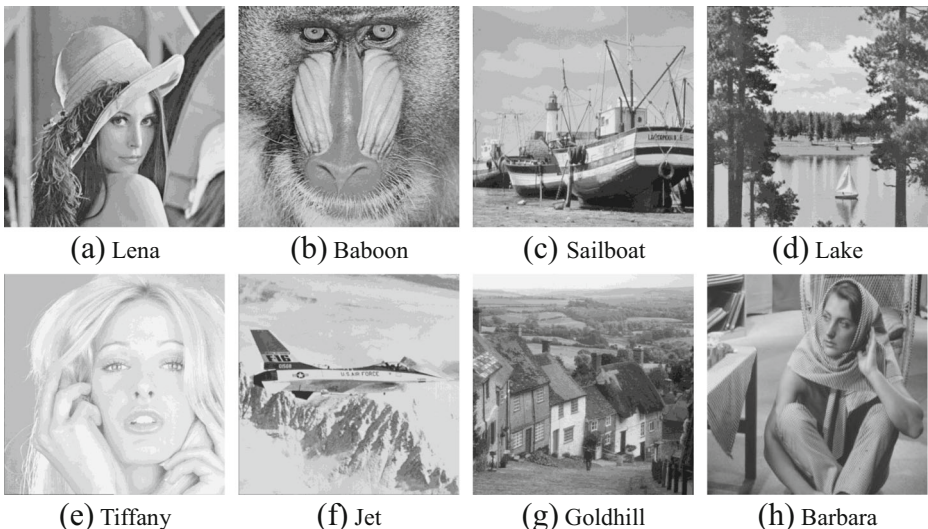


Fig. 4 Eight test images sized 512 × 512

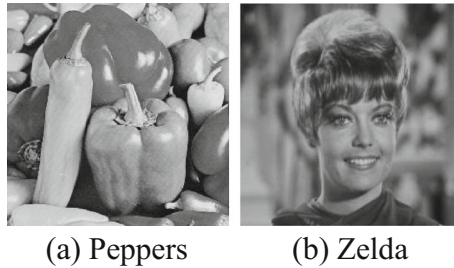


Fig. 5 Two secret images sized 256×256

$$\text{PSNR}^{(2)} = 10 \cdot \log_{10} \frac{255^2}{\frac{2}{25} + \frac{2}{5} \times \sum_{i=1}^5 \frac{i^2}{5}} \approx 41.62 \text{ dB}, \quad (18)$$

Note that, due to the pre-processing, the actual PSNR values of $S^{(1)}$ and $S^{(2)}$ after embedding may be slightly lower than the two theoretical values in Eqs. (17–18).

Figures 6a and b show the two steganographic images $S^{(1)}$ and $S^{(2)}$ that were generated by embedding the secret image *Peppers* into the cover image *Lena*, and the PSNR values for these two steganographic images are 52.11 dB and 41.34 dB, respectively. Because each pixel pair in one steganographic images can carry one secret digit in the quinary notation system, hence, the total hiding capacity of the proposed scheme is 608680 bits, i.e., $512 \times 512 \times \log_2 5$, and the embedding rate is 1.16 bits per pixel (bpp), i.e., $0.5 \times \log_2 5$.

We also compared the performance of our scheme with that of Lee et al.'s [6] and Zeng et al.'s [14] methods. Lee et al.'s method was based on histogram shifting and set a pre-defined threshold T to control the distortions of steganographic images. Here, T was set to 10. Zeng et al.'s method was also based on histogram shifting, in which the secret bits were embedded into multi-layers. When the secret bits were embedded into different layers, cover image blocks were divided with difference sizes. Here, the experimental results of [14] were for 10-



Fig. 6 Results of two steganographic images for *Lena* after embedding secret image *Peppers*

Table 1 Comparison results between the proposed scheme and [6, 14]

Test images		Lena	Baboon	Sailboat	Lake	Tiffany	Jet	Goldhill	Barbara
Scheme in [6]	PSNR	34.38	30.03	33.12	34.52	34.73	34.76	32.08	31.31
	Payload	0.91	0.62	0.86	0.94	0.92	0.91	0.84	0.73
Scheme in [14]	PSNR	32.74	30.97	32.96	33.16	33.32	33.94	31.82	31.96
	Payload	1.04	0.51	1.04	1.05	1.18	1.16	0.80	0.78
Proposed scheme	PSNR ₁ ⁽¹⁾	52.11	52.12	52.11	52.10	52.11	52.11	52.11	52.12
	PSNR ₁ ⁽²⁾	41.34	41.34	41.35	41.32	41.33	41.33	41.34	41.34
	Payload	1.16	1.16	1.16	1.16	1.16	1.16	1.16	1.16
	PSNR ₂ ⁽¹⁾	52.12	52.11	52.12	52.11	52.12	52.11	52.11	52.12
	PSNR ₂ ⁿ	41.27	41.26	41.27	41.25	41.27	41.26	41.24	41.27
	Payload	1.16	1.16	1.16	1.16	1.16	1.16	1.16	1.16

layer embedding, and the block sizes were set to 4×2 and 3×3 for layers 1–5 and layers 6–10, respectively. Table 1 shows the comparison results of PSNR values and pure embedding payloads among Lee et al.'s method [6], Zeng et al.'s method [14], and the proposed scheme for the eight cover images in Fig. 4. For the proposed scheme, PSNR₁⁽¹⁾ and PSNR₁⁽²⁾ correspond to the two steganographic images $S^{(1)}$ and $S^{(2)}$ after embedding the secret image *Peppers*, while PSNR₂⁽¹⁾ and PSNR₂⁽²⁾ correspond to the steganographic images $S^{(1)}$ and $S^{(2)}$ after embedding the secret image *Zelda*. It can be observed from Table 1 that, in our scheme, the PSNR values of the two steganographic images $S^{(1)}$ and $S^{(2)}$ exceed 52 dB and 41 dB, respectively. Irrespective of whether the cover images are smooth or complex, the image quality of our scheme is visually satisfactory, and the payload, i.e., embedding rate, of our scheme is 1.16 bpp, which outperforms that of Lee et al.'s and Zeng et al.'s methods.

5 Conclusions

In this paper, we proposed a novel reversible data hiding scheme based on the EMD method. The chosen cover image produces two steganographic images after embedding the secret data, which have visually similar appearances with the cover image. During the embedding procedure, the corresponding pixel pairs in the first and the second initial steganographic images are modified, and the modification directions for the pixel pairs in the second steganographic image are adaptively changed according to those in the first steganographic image, which can guarantee the correct image recovery on the receiver side. Experimental results show that the two steganographic images can carry high embedding payload and keep satisfactory image quality for both smooth and complex images.

Acknowledgments This work was supported by the Natural Science Foundation of China (61303203), the Natural Science Foundation of Shanghai, China (13ZR1428400), and the Innovation Program of Shanghai Municipal Education Commission (14YZ087).

References

1. Alattar AM (2004) Reversible watermarking using the difference expansion of a generalized integer transform. *IEEE Trans Image Process* 13(8):1147–1156
2. Chan CK, Cheng LM (2004) Hiding data in images by simple LSB substitution. *Pattern Recogn* 37(3):469–474
3. Coltuc D (2012) Low distortion transform for reversible watermarking. *IEEE Trans Image Process* 21(1): 412–417
4. Highland HJ (1997) Data encryption: a non-mathematical approach. *Comput Secur* 16(5):369–386
5. Ker A (2004) Improved detection of LSB steganography in grayscale images. In: *Proc Information Hiding Workshop*, vol. 3200. Springer LNCS, pp. 97–115
6. Lee CF, Chen HL, Tso HK (2010) Embedding capacity raising in reversible data hiding based on prediction of difference expansion. *J Syst Softw* 83(10):1864–1872
7. Li XL, Li B, Yang B, Zeng TY (2013) General framework to histogram-shifting-based reversible data hiding. *IEEE Trans Image Process* 22(6):2181–2191
8. Mielikainen J (2006) LSB matching revisited. *IEEE Signal Proc Lett* 13(5):285–287
9. Ni Z, Shi YQ, Ansari N, Su W (2006) Reversible data hiding. *IEEE Trans Circ Syst Video Technol* 16(3): 354–362
10. Qin C, Chang CC, Huang YH, Liao LT (2013) An inpainting-assisted reversible steganographic scheme using a histogram shifting mechanism. *IEEE Trans Circ Syst Video Technol* 23(7):1109–1118
11. Rivest RL, Shamir A, Adleman L (1978) A method for obtaining digital signatures and public-key cryptosystem. *Commun ACM* 21(2):120–126
12. Thodi DM, Rodriguez JJ (2007) Expansion embedding techniques for reversible watermarking. *IEEE Trans Image Process* 16(3):721–730
13. Tian J (2003) Reversible data embedding using a difference expansion. *IEEE Trans Circ Syst Video Technol* 13(8):890–896
14. Zeng XT, Li Z, Ping LD (2012) Reversible data hiding scheme using reference pixel and multi-layer embedding. *AEU Int J Electron Commun* 66(7):532–539
15. Zhang X (2013) Reversible data hiding with optimal value transfer. *IEEE Trans Multimed* 15(2):316–325
16. Zhang X, Wang S (2006) Efficient steganographic embedding by exploiting modification direction. *IEEE Commun Lett* 10(11):781–783
17. Zhou J, Au OC (2012) Determining the capacity parameters in PEE-based reversible image watermarking. *IEEE Signal Proc Lett* 19(5):287–290



Chuan Qin received the B.S. and M.S. degrees in electronic engineering from Hefei University of Technology, Anhui, China, in 2002 and 2005, respectively, and the Ph.D. degree in signal and information processing from Shanghai University, Shanghai, China, in 2008. Since 2008, he has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology. He also has been with Feng Chia University at Taiwan as a Postdoctoral Researcher and Adjunct Assistant Professor from July 2010 to June 2012. His research interests include digital image processing and multimedia security.



Chin-Chen Chang received his B.S. degree in applied mathematics in 1977 and the M.S. degree in computer and decision sciences in 1979, both from the National Tsing Hua University, Hsinchu, Taiwan. He received his Ph.D in computer engineering in 1982 from the National Chiao Tung University, Hsinchu, Taiwan. During the academic years of 1980–1983, he was on the faculty of the Department of Computer Engineering at the National Chiao Tung University. From 1983 to 1989, he was on the faculty of the Institute of Applied Mathematics, National Chung Hsing University, Taichung, Taiwan. From August 1989 to July 1992, he was the head of, and a professor in, the Institute of Computer Science and Information Engineering at the National Chung Cheng University, Chiayi, Taiwan. From August 1992 to July 1995, he was the dean of the college of Engineering at the same university. From August 1995 to October 1997, he was the provost at the National Chung Cheng University. From September 1996 to October 1997, Dr. Chang was the Acting President at the National Chung Cheng University. From July 1998 to June 2000, he was the director of Advisory Office of the Ministry of Education of Taiwan. From 2002 to 2005, he was a Chair Professor of National Chung Cheng University. Since February 2005, he has been a Chair Professor of Feng Chia University. In addition, he has served as a consultant to several research institutes and government departments. His current research interests include database design, data structures, computer cryptography and image processing. He is a fellow of the IEEE.



Tai-Jung Hsu received the B.S. degree in computer science and engineering from National University of Tainan, Taiwan, in 2011. He is currently pursuing the M.S. degree in computer science and engineering from National Chung Cheng University, Taiwan. His research interests include data hiding and watermarking.