Multimed Tools Appl (2014) 72:417–435
DOI 10.1007/s11042-013-1369-0

High capacity reversible hiding scheme based on interpolation, difference expansion, and histogram shifting

Tzu-Chuen Lu · Chin-Chen Chang · Ying-Hsuan Huang

Published online: 7 February 2013

Abstract Difference expansion and histogram shifting methods are two popular hiding strategies that have been widely used in many researches. For example, Hong and Chen developed a reversible hiding method based on interpolation and histogram shifting. The image quality of their scheme is exceptional; however, their scheme needs to keep and transmit two peak points for secret data extraction and pixel recovering. Moreover, the reference pixels in their scheme cannot be used to embed secret data that will decrease the hiding capacity. Therefore, this paper shall propose a reversible hiding method to enhance their scheme. The proposed method applies the difference expansion, histogram shifting and interpolation strategies to conceal secret data in the reference pixels for increasing the hiding payload. Experimental results indicate that the proposed method performs better in terms of hiding capacity than recently developed methods.

Keywords Reversible hiding · Difference expansion · Histogram shifting · Interpolation

T.-C. Lu
Department of Information Management, Chaoyang University of Technology, Taichung 41349, Taiwan, Republic of China
e-mail: tclu@cyut.edu.tw

C.-C. Chang
Department of Information Engineering and Computer Science, Feng Chia University, Taichung 40724, Taiwan, Republic of China

C.-C. Chang (✉)
Department of Computer Science and Information Engineering, Asia University, Taichung 41354, Taiwan, Republic of China
e-mail: alan3c@gmail.com

Y.-H. Huang
Department of Computer Science and Engineering, National Chung Hsing University, Taichung 40227, Taiwan, Republic of China
e-mail: phd9807@cs.nchu.edu.tw

1 Introduction

Internet is a convenient and speedy way to share and transmit digital data. In order to ensure the confidentiality of the transmitted data, many people use cryptographic techniques to encrypt the data to generate the meaningless ciphertext [3, 8, 9]. However, the ciphertext might be attacked by illegal hackers. To overcome this problem, many information hiding methods have been developed [1, 4–7, 10–18, 20–26, 28–31]. A hiding method embeds secret data into a cover image to generate a stego image. Because the cover image and stego image are similar, hackers cannot detect that the secret information is concealed in the stego image.

Information hiding schemes can be further divided into two categories, reversible [1, 4, 5, 7, 10, 11, 13, 14, 16, 17, 20–25, 28, 31] and irreversible [6, 12, 15, 18, 29, 30]. An irreversible hiding scheme can extract the secret information but can not recover the original image from the stego image. On the contrary, a reversible hiding scheme not only can extract the secret information but also recover the original image from the stego image.

In the past decade, many reversible hiding methods have been developed. Most of them are based on compression [4, 5], difference expansion [1, 16, 21, 23] and histogram shifting techniques [10, 11, 14, 17, 22, 24, 28, 31]. For example, Celik et al. developed a compression-based reversible hiding method in 2005 [4]. In the scheme, a cover image is quantified to produce an image. Next, the differences between the cover pixels and quantification pixels are calculated and compressed by a lossless compression method. The compressed results, along with the secret data, were embedded into the cover image to generate the stego image. The scheme is simple. However, the amount of the compression results is massive, thereby seriously influencing the image quality and reducing the hiding capacity.

Hence, Chan et al. applied Haar digital wavelet transform (HDWT) and Huffman coding to improve Celik et al.'s scheme [5]. In their scheme, a spatial-domain cover image is transformed into the frequency-domain image, which consists of four sub-bands: low-low (LL), high-low (HL), low-high (LH) and high-high (HH). The coefficients in the HH sub-band are compressed by Huffman coding. The compression results and secret data are embedded into HH sub-bands.

Chan et al.'s scheme is great for smooth images but not good for complex images. Because the size of the compressed codes for a complex image is huge, the scheme cannot spare more space for hiding secret data.

Tian developed a difference expansion (DE) method for embedding secret data in 2003 [23]. In Tian's scheme, the average value and the difference between two adjacent pixels are calculated. The difference is then doubled to generate an even value. Then, the secret bit is added into the even value to produce an expansion difference. The expansion difference is then equally shared with the adjacent pixels. The hiding capacity of Tian's scheme is lower than 0.5 bpp.

To increase the hiding capacity of Tian's scheme, Alattar developed an integer transform method in 2004 [1]. In the scheme, four cover pixels can be used to embed three secret bits. Therefore, the ideal hiding capacity of this method is 0.75 bpp. In the same year, Thodi and Rodriguez designed a reversible hiding method based on the inherent primitive edge detector [21]. The edge detector is used to generate a prediction value. The difference between the current embedding pixel and the prediction value is calculated. The scheme doubles the difference and embeds the secret bit in the expansion difference. The image quality of this method is satisfactory and its hiding capacity is close to 1 bpp.

In 2009, Tseng and Hsieh developed a prediction-based reversible hiding method [25], in which the scheme first computes a prediction value for the current embedding pixel. The prediction value is the average value of the upper pixel and the left pixel. Then, the scheme

calculates the difference between the current pixel and the average value. If the difference is smaller than a predefined threshold, the difference can be used to embed secret data. Although image quality with this method is high, its hiding capacity can be enhanced further. Furthermore, the hiding capacity of this method is related to a pre-determined threshold. However, setting an appropriate threshold is difficult for users.

Liu et al., in 2011, proposed a reversible data hiding method based on DE and bilinear interpolation. In their scheme, two secret bits can be embedded into one cover pixel [16]. This approach divides the cover image into several blocks, sized 2×2. Next, the prediction value is produced by the bilinear interpolation method, and the difference between the current embedding pixel and the prediction value is calculated for each block. The maximum absolute difference for each block is extracted to determine whether the pixel in a block can embed two secret bits or not. If the maximum absolute difference is smaller than the pre-determined threshold, then the pixel can embed two secret bits. Therefore, the ideal hiding capacity of this method is better than that of the other four methods [1, 21, 23, 25].

The hiding methods based on DE [1, 21, 23] have excellent hiding capacity. However, this kind of method may have overflow and underflow problems. To overcome such problems, DE-based methods [1, 21, 23] usually use a location map to record the pixel having an overflow or underflow problem. In addition, a location map is concealed into the cover image along with the secret message for the receiver to restore the original image. The location map and extra restoration information may seriously distort the image and reduce the hiding capacity.

Histogram is another popular technique used in information hiding [10, 11, 14, 17, 22, 24, 28, 31]. In 2006, Ni et al. developed a histogram-based hiding method [17]. In this scheme, the pixel in the cover image is compiled to generate a histogram. The most frequently occurring cover pixel in the histogram is called the peak point and the least frequently occurring cover pixel is called the zero point. The pixels ranging from the right one of the peak point to the zero point are increased by 1 to create a concealing space, while the pixels of the peak point are used to embed secret data. Therefore, the maximum modification of a pixel with this method is 1. Although the stego image quality produced by this method is great, the hiding capacity is poor.

In 2007, Thodi and Rodriguez combined the inherent primitive edge detector and histogram techniques to improve the image quality and hiding capacity of Tian's method and Thodi and Rodriguez's method [22]. Although the hiding capacity and image quality of this method are satisfactory, the approach requires an overflow location map to record whether a pixel can embed a secret message or not. To reduce the size of the overflow location map, Hu et al. designed a payload-dependent overflow location map [11]. Their scheme divides the histogram into two regions; one is an embeddable region and the other is a shifting region. The pixels having the overflow problem of the shifting region is fewer than those of the embeddable region. Therefore, the size of the overflow location map of Hu's scheme is smaller than that of Thodi and Rodriguez's scheme.

Besides, Tsai et al. proposed a linear prediction reversible data hiding method [24]. In their scheme, the cover image is divided into several non-overlapping blocks, sized 3×3. Differences between the center pixel and its eight adjacent pixels are calculated for each block. Tsai et al. generated a difference histogram for hiding secret message. Because the center pixel is similar to its adjacent pixel, most of differences are close to 0. They concealed the secret message in the adjacent pixels, whose difference is equal to 0. In their scheme, the center pixel is a prediction value that cannot be used to embed secret data.

In 2009, Yang et al. proposed a reversible data hiding method based on interleaving a max-min difference histogram [28]. Different from Tsai et al.'s method [24], Yang et al.'s scheme uses the maximum or minimum pixel to generate the prediction value for each block. Consequently, the prediction result and hiding capacity of Yang et al.'s scheme are good.

Li et al. also proposed a histogram-based reversible hiding method in 2009 [14]. Two neighboring pixels are subtracted to compute the difference. The differences are then compiled to generate a histogram. They then choose one peak point to embed secret data. The image quality and hiding capacity of their method are good; however, the scheme needs to keep one peak point to extract secret data and recover the original image. In order to remove the extra information, Zhao et al. proposed the multilevel histogram modification method based on Li et al.'s scheme [31]. They used an integer pointer to determine whether the difference in the histogram is embeddable or not. The method does not maintain the extra information such as peak point or zero point.

Hong and Chen utilized the interpolation method, histogram method and detection technique of smooth and complex blocks to embed secret data [10]. In their scheme, the cover image is divided into several blocks, and these blocks are classified into smooth block or complex block. If the block is complex, the pixel remains unchanged. Otherwise, the interpolation method and pre-determined reference pixel are used to produce the interpolation pixel. The difference between the interpolation pixel and embeddable pixel is calculated to compile a histogram. They also use two peak points to embed secret data. Similar with Li et al.'s scheme, Hong and Chen's scheme also needs to maintain the extra information. Moreover, in their scheme, the reference pixel cannot be used to conceal secret data. In Hong and Chen's method, if the number of secret data is higher than the frequency of peak point, then the algorithm is reapplied to embed the remaining secret data that will increase computational burden and time cost.

Therefore, this paper shall propose an enhanced hiding scheme to improve Hong and Chen's scheme. The proposed scheme applies DE, histogram and bilinear interpolation strategies to embed a secret message. In the proposed scheme, the reference pixel also can be used to embed the message. Hence, the hiding capacity of the proposed scheme is high and its stego image quality is satisfactory.

2 Related work

Hong and Chen's algorithm is expressed as follows [10].

Step 1: Classify cover pixel $P_{i,j}$ as the reference pixel and the embeddable pixel by using the equation:

$$I_{i,j} = \begin{cases} 0, \text{ if } \mathrm{mod}\,(\mathrm{i},\ \Delta) = 0 \text{ and } \mathrm{mod}\,(\mathrm{j},\ \Delta) = 0, \\ 1, \text{ otherwise,} \end{cases}$$

where $I_{i,j}$ represents the pixel and is the reference pixel or the embeddable pixel. i and j represent the position of the pixel in the cover image and Δ refers to a threshold used to control the number of reference pixels.

Step 2: If $I_{i,j} = 0$, $\mathrm{mod}\left(\frac{i}{\Delta} + \frac{j}{\Delta}\right) = 0$, and $\mathrm{Range}\left(\mathrm{P_{i-\Delta,j}}, \mathrm{P_{i,j-\Delta}}, \mathrm{P_{i+\Delta,j}}, \mathrm{P_{i,j+\Delta}}\right) < \mathrm{T_1}$, then modify $I_{i,j}$ as 1. In other words, the reference pixel is changed as the embeddable pixel. Notably, T_1 is the second threshold used to reduce the number of reference pixels.

Step 3: If the four indices $\left\{I_{i,j}, I_{i+\Delta,j}, I_{i,j+\Delta}, I_{i+\Delta,j+\Delta}\right\}$ are equal to 0 and $\mathrm{Range}\left(\mathrm{I}_{i,j}, \mathrm{I}_{i+\Delta,j}, I_{i,j+\Delta}, I_{i+\Delta,j+\Delta}\right) > T_2$, modify $I_{i',j'}$ as 0, where $i \le i' \le i + \Delta, j \le j' \le i + \Delta$ and T_2 refers to the third threshold, which increases the number of reference pixels to reduce image distortion.

Step 4: To avoid underflow/overflow problems, if the cover pixel $P_{i,j}$ is equal to 0, then change the cover pixel $P_{i,j}$ to be 1 and record its position information (i.e., i and j). If the cover pixel $P_{i,j}$ equals 255, then change the cover pixel $P_{i,j}$ to be 254 and record its position information.

Step 5: Compress the position information in *Step* 4 by using the run-length compression method.

Step 6: Obtain interpolation pixel $\widehat{P}_{i,j}$ by using all reference pixels (i.e., $I_{i,j}$=0) and the interpolation method.

Step 7: Calculate the prediction error $e_{i,j}$ between the embeddable pixel (i.e., $I_{i,j}$=1) and interpolation pixel $\widehat{P}_{i,j}$.

Step 8: Compile the occurrence number of prediction error $e_{i,j}$ to produce a prediction error histogram. In the histogram, M_1 denotes the prediction error with most occurrence frequency. M_2 refers to the prediction error with the second largest occurrence frequency.

Step 9: Embed secret data and the compressed results into prediction error $e_{i,j}$ by using the following equation:

$$e'_{i,j} = \begin{cases} e_{i,j} + w, & \text{if } e_{i,j} = M_1, \\ e_{i,j} - w, & \text{if } e_{i,j} = M_2, \\ e_{i,j} + 1, & \text{if } e_{i,j} > M_1, \\ e_{i,j} - 1, & \text{if } e_{i,j} < M_2, \end{cases}$$

where w represents secret data and compressed results.

Step 10: The modified prediction error $e'_{i,j}$ is increased by interpolation pixel $\widehat{P}_{i,j}$, i.e., $P'_{i,j} = e'_{i,j} + \widehat{P}_{i,j}$, where $P'_{i,j}$ denotes the stego pixel.

3 Proposed scheme

The proposed method has two phases—the data embedding phase and the extraction and recovering phase. Both of them are introduced in Subsection 3.1 and Subsection 3.2, respectively. Subsection 3.3 examines the overflow and underflow problems and applies a mechanism to resolve them.

3.1 Data embedding phase

Figure 1 shows our flowchart of the embedding phase, with its details described as follows. The pixels in a cover image sized $W \times H$ are classified into two types: the reference pixels, $R_k (k = 1, 2, \ldots, \lceil \frac{W}{2} \rceil \times \lceil \frac{H}{2} \rceil)$, and the embeddable pixels, $E_l (l = 1, 2, \ldots, W \times H - \lceil \frac{W}{2} \rceil \times \lceil \frac{H}{2} \rceil)$, where k and l represent the location of the reference pixel and that of the embeddable pixel. The diagram is shown in Fig. 2. After reference pixel R_k and embeddable pixel E_l are determined, the interpolation pixels $I_l (l = 1, 2, \ldots, W \times H - \lceil \frac{W}{2} \rceil \times \lceil \frac{H}{2} \rceil)$ are obtained by using the equation

$$I_l = avg\left(\sum_{z=1}^{n} neg_z^l \right), \quad n \in \{2, 4\}. \tag{1}$$

Equation (1) is equivalent to the traditional bi-linear interpolation method. The equation is used to compute the average value of the reference pixels which around the embeddable

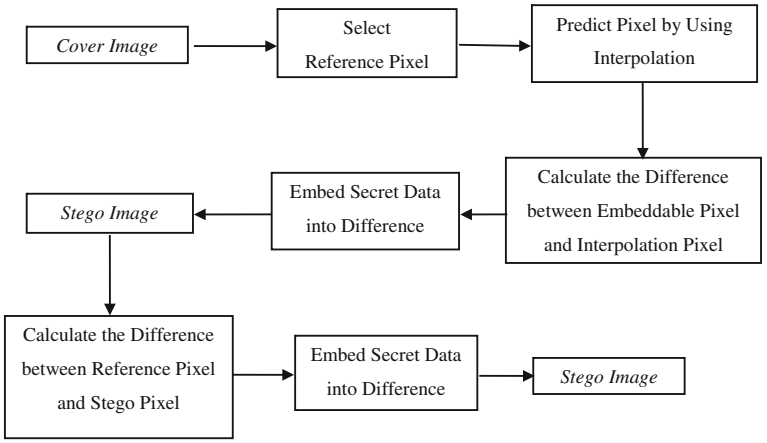


Fig. 1 Flowchart of our embedding phase

pixel E_l. In this equation, n denotes the number of neighboring reference pixels of pixel E_l, and neg_z^l represents the z^{th} neighboring reference pixel of the pixel E_l; for example, the reference pixels of E_4 are R_1, R_2, R_3 and R_4. Hence, I_4 is the average value of these four pixels.

Next, the scheme computes the difference d_l between the embeddable pixel E_l and interpolation pixel I_l, i.e., $d_l=E_l-I_l$. If the absolute difference $|d_l|$ is larger than the pre-determined threshold T, then the pixel is non-embeddable. The scheme applies the histogram shifting equation to shift the pixel. The shifting equation is

$$E_l^{'} = \begin{cases} E_l + (T+1), & \text{if } |d_1| > T \text{ and } d_1 \geq 0, \\ E_l - (T+1), & \text{if } |d_1| > T \text{ and } d_1 < 0. \end{cases} \tag{2}$$

Otherwise, if the absolute difference $|d_l|$ is smaller than the pre-determined threshold T, then the scheme embed a secret message s by using the equation

$$E_l^{'} = I_l + 2 \times d_l + s, \tag{3}$$

where $s \in \{0,1\}$ and $E_l^{'}$ is the stego pixel.

In order to increase the hiding capacity, the scheme also embeds a secret message into the reference pixels R_k. The embedding process of R_k is similar to that of E_l, and it is listed below:

- Compute the difference d_k between the reference pixel R_k and its right pixel $E_k^{'}$, i.e., $d_k = R_k - E_k^{'}$.

Fig. 2 Cover image

R_1	E_1	R_2	E_2
E_3	E_4	E_5	E_6
R_3	E_7	R_4	E_8
E_9	E_{10}	E_{11}	E_{12}

- Determine if the reference pixel is embeddable or not. If the absolute difference $|d_k|$ is larger than the pre-determined threshold T, the reference pixel R_k is shifted by using the shifting equation

$$R_k^{'} = \begin{cases} R_k + (T+1), & \text{if } |d_k| > T \text{ and } d_k \geq 0, \\ R_k - (T+1), & \text{if } |d_k| > T \text{ and } d_k < 0. \end{cases} \quad (4)$$

Otherwise, if the absolute difference $|d_k|$ is smaller than the pre-determined threshold T, the scheme embeds the secret message by using the equation

$$R_k^{'} = E_k^{'} + 2 \times d_k + s. \quad (5)$$

The proposed setting threshold method is the same as that of Chang et al.'s method [7]. The number of the difference d ranged in $[-T, T]$ is counted. If the hiding capacity is smaller than the number of secret messages, threshold T is then increased by one. Otherwise, the current threshold T is an appropriate threshold, capable of improving stego image quality more than other thresholds.

An example is presented to illustrate the embedding procedure. Figure 3(a) shows an example cover image, sized 4×4. Suppose that the secret bits are {0, 1, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1} and the threshold T is four. First, the four reference pixels are {160, 160, 150, 150}. Then, the interpolation pixels I_l= {160, 160, 155, 155, 155, 155, 150, 150, 150, 150, 150, 150} are obtained by using Eq. (1). The differences d_l between the embeddable pixels E_l and the interpolation pixels I_l are calculated: $d_1=E_1-I_1=160-160=0$, $d_2=E_2-I_2=160-160=0$, and so on. The first and second differences ($d_1=0$ and $d_2=0$) are less than the threshold, hence Eq. (3) is used to embed the secret data {0, 1}. The results of embedding are $E_1^{'} = I_1 + 2 \times d_1 + s = 160 + 2 \times 0 + 0 = 160$ and $E_2^{'} = I_2 + 2 \times d_2 + s = 160+2\times0+1=161$.

Next, the third and fourth differences ($d_3=-5$ and $d_4=-5$) are larger than the threshold T, hence they are shifted using Eq. (2): $E_3^{'} = E_3 - (T+1) = 150 - (4+1) = 145$ and $E_4^{'} = E_4 - (T+1) = 150 - (4+1) = 145$. The differences ($d_5=0$, $d_6=0$, $d_7=0$, $d_8=0$, $d_9=0$, $d_{10}=0$, $d_{11}=0$, and $d_{12}=0$) are smaller than the threshold T, so the secret data {1, 0, 0, 0, 0, 0, 0, 0} are embedded into the embeddable pixels. Figure 3(b) presents the stego image.

To increase the hiding capacity, the reference pixels are used to embed secret data. First, the differences d_k between the reference pixels R_k and the pixels $E_k^{'}$ on the right hand side of R_k are calculated: $d_1 = R_1 - E_1^{'} = 160 - 160 = 0$, $d_2 = R_2 - E_2^{'} = 160 - 161 = -1$, and so on. These four differences are less than the threshold T, so Eq. (5) is utilized to embed secret bits {0, 0, 0, 1}. The results are $R_1^{'} = E_1^{'} + 2 \times d_1 + s = 160 + 2 \times 0 + 0 = 160$, $R_2^{'} = E_2^{'} + 2 \times d_2 + s = 161 + 2 \times (-1) + 0 = 159$, and so on. Figure 3(c) displays the stego image with high hiding capacity.

160	160	160	160
150	150	155	155
150	150	150	150
150	150	150	150

(a) Cover image

160	160	160	161
145	145	156	155
150	150	150	150
150	150	150	150

(b) Stego image

160	160	159	161
145	145	156	155
150	150	151	150
150	150	150	150

(c) Stego image with high hiding capacity

Fig. 3 Example of embedding data procedure

3.2 Extraction and recovery phase

Figure 4 shows our flowchart of the extraction and recovery phase, with its details described as follows. When a receiver obtains the stego image and the threshold T, the stego pixel will be classified as the reference pixel, $R_k^{'}\left(k = 1,\ 2, \ldots,\ \left\lceil \frac{W}{2} \right\rceil \times \left\lceil \frac{H}{2} \right\rceil \right)$, and embedded pixel, $E_l^{'}\left(l = 1,\ 2, \ldots,\ W \times H - \left\lceil \frac{W}{2} \right\rceil \times \left\lceil \frac{H}{2} \right\rceil \right)$, in the same way as in data embedding phase. The scheme first extracts the concealed message from the reference pixels. The difference $d_k^{'}$ between the stego reference pixel $R_k^{'}$ and its right pixel $E_k^{'}$ is derived by $d_k^{'} = R_k^{'} - E_k^{'}$. If $\left|d_k^{'}\right| \le 2 \times T + 1$, the reference pixel $R_k^{'}$ has a secret message in it. The scheme extracts the secret bit s by using the equation

$$s = \mathrm{mod}\left(d_k^{'}, 2\right) \tag{6}$$

and recovers the original reference pixel R_k by using the equation

$$R_k = \begin{cases} E_k^{'} + \left\lfloor \frac{\left|d_k^{'}\right|}{2} \right\rfloor, & \text{if } \mathrm{R_k^{'}} \ge \mathrm{E_k^{'}}, \\ E_k^{'} - \left\lfloor \frac{\left|d_k^{'}\right|}{2} \right\rfloor, & \text{otherwise.} \end{cases} \tag{7}$$

Otherwise, if $\left|d_k^{'}\right| > 2 \times T + 1$, the reference pixel does not have a secret message in it. The original reference pixel R_k can be recovered by using the equation

$$R_k = \begin{cases} R_k^{'} - (T+1), & \text{if } \mathrm{R_k^{'}} \ge \mathrm{E_k^{'}}, \\ R_k^{'} + (T+1), & \text{otherwise.} \end{cases} \tag{8}$$

Next, the scheme extracts the message from $E_l^{'}$. First, the interpolation pixel, $I_l^{'} \times \left(l = 1,\ 2, \ldots,\ W \times H - \left\lceil \frac{W}{2} \right\rceil \times \left\lceil \frac{H}{2} \right\rceil \right)$, is generated by Eq. (1). Then, the scheme calculates

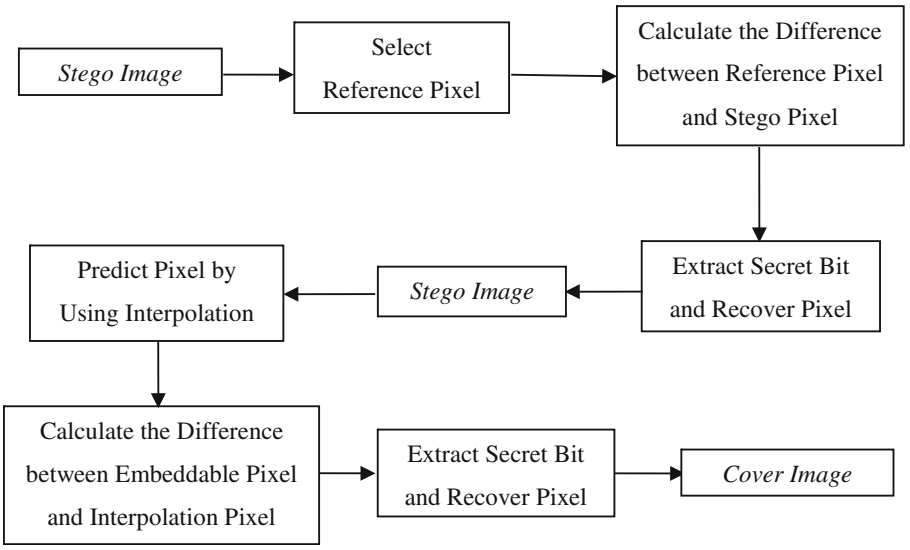


Fig. 4 Flowchart of our extraction and recovery phase

the difference $d_l^{'}$ between the embedded pixel $E_l^{'}$ and interpolation pixel $I_l^{'}$ by $d_l = E_l^{'} - I_l^{'}$. If $\left|d_l^{'}\right| \le 2 \times T + 1$, then the secret message is embedded in $E_l^{'}$ and can be extracted by using the equation

$$s = \mathrm{mod}\left(d_l^{'}, 2\right). \tag{9}$$

The original pixel is recovered by using the equation

$$E_l = \begin{cases} I_l^{'} + \left\lfloor \frac{\left|d_l^{'}\right|}{2} \right\rfloor, & \text{if } \mathrm{E}_1^{'} \ge \mathrm{I}_1^{'}, \\ I_l^{'} - \left\lfloor \frac{\left|d_l^{'}\right|}{2} \right\rfloor, & \text{otherwise.} \end{cases} \tag{10}$$

Otherwise, if $\left|d_l^{'}\right| > 2 \times T + 1$, $E_l^{'}$ does not have a secret message in it. The original pixel is recovered by using the equation

$$E_l = \begin{cases} E_l^{'} - (T+1), & \text{if } E_1^{'} \ge I_1^{'}, \\ E_l^{'} + (T+1), & \text{otherwise.} \end{cases} \tag{11}$$

An extraction and recovery example is introduced as follows. Figure 3(c) shows a stego image and the threshold T is four. After reference pixels $\left(R_1^{'} = 160,\ R_2^{'} = 159,\ R_3^{'} = 150,\ \text{and}\ R_4^{'} = 151\right)$ are determined, the differences $d_k^{'}$ between the reference pixels $R_k^{'}$ and its right pixel $E_k^{'}$ are calculated by $d_1^{'} = R_1^{'} - E_1^{'} = 160 - 160 = 0$, $d_2^{'} = R_2^{'} - E_2^{'} = 159 - 161 = -2$, and so on. Since these four differences $\left(d_1^{'} = 0,\ d_2^{'} = -2,\ d_3^{'} = 0, \text{and } \mathrm{d}_4^{'} = 0\right)$ are less than $2 \times T + 1$, four embedded bits {0, 0, 0, 1} can be extracted using Eq. (6). Meanwhile, the original reference pixels can be recovered using Eq. (7). The recovered pixels are $R_1 = E_1^{'} + \left\lfloor \frac{\left|d_1^{'}\right|}{2} \right\rfloor = 160 + \left\lfloor \frac{0}{2} \right\rfloor = 160$, $R_2 = E_2^{'} - \left\lfloor \frac{\left|d_2^{'}\right|}{2} \right\rfloor = 161 - \left\lfloor \frac{|-2|}{2} \right\rfloor = 160$, and so on.

After the reference pixels have been recovered, Eq. (1) is adopted to generate interpolation pixels $I_l^{'} = \{160,\ 160,\ 155,\ 155,\ 155,\ 155,\ 150,\ 150,\ 150,\ 150,\ 150,\ 150\}$. Then, the differences $d_l^{'}$ between the embedded pixels $E_l^{'}$ and interpolation pixels $I_l^{'}$ are calculated by $d_1^{'} = E_1^{'} - I_1^{'} = 160 - 160 = 0$, $d_2^{'} = E_2^{'} - I_2^{'} = 161 - 160 = 1$, and so forth. Since $\left|d_1^{'}\right| = 0$ and $\left|d_2^{'}\right| = 1$ two secret bits {0, 1} are extracted using Eq. (9). Additionally, the original pixel can be restored using Eq. (10). The restored pixels are $E_1 = I_1^{'} + \left\lfloor \frac{\left|d_1^{'}\right|}{2} \right\rfloor = 160 + \left\lfloor \frac{0}{2} \right\rfloor = 160$ and $E_2 = I_2^{'} + \left\lfloor \frac{\left|d_2^{'}\right|}{2} \right\rfloor = 160 + \left\lfloor \frac{1}{2} \right\rfloor = 160$. Since $\left|d_3^{'}\right| = 10 > 2 \times T + 1$ and $\left|d_4^{'}\right| = 10 > 2 \times T + 1$, no secret message is embedded. These two pixels can be recovered using Eq. (11), i.e., $E_3 = E_3^{'} + (T+1) = 145 + (T+1) = 150$ and $E_4 = E_4^{'} + (T+1) = 145 + (T+1) = 150$. Since $\left|d_5^{'}\right| = 1 < 2 \times T + 1$, the secret message can be extracted by applying Eq. (9). Further, the original pixel can be recovered using Eq. (10), i.e., $E_5 = I_5^{'} + \left\lfloor \frac{\left|d_5^{'}\right|}{2} \right\rfloor = 155 + \left\lfloor \frac{1}{2} \right\rfloor = 155$. The extraction and recovery process of the embedded pixels $\left(E_6^{'}\ E_7^{'}\ E_8^{'}\ E_9^{'}\ E_{10}^{'}\ E_{11}^{'}\ \text{and}\ \mathrm{E}_{12}^{'}\right)$ is similar to that of $E_5^{'}$. Figure 5 shows the recovered image.

Fig. 5 Recovered image

160	160	160	160
150	150	155	155
150	150	150	150
150	150	150	150

3.3 Overflow and underflow problems

The extreme pixel may generate an overflow or underflow problem when secret messages are embedded. The maximum modification of pixels is $T+1$ according to Eqs. (2)–(5). Therefore, the original pixel, ranged in [0, T] and [255−T, 255], may have an overflow or underflow problem. Inspired by the method [25], our scheme modifies the pixels as $T+1$, when the original pixel is smaller than $T+1$, to avoid an underflow problem. Moreover, if the original pixel is larger than $255-(T+1)$, then the pixel will be modified as $255-(T+1)$. Additionally, these modified pixels must be identified and recovered by recording their location information and the last $\lceil \log_2 T + 1 + 1 \rceil$ bits of the original pixel.

Suppose that the cover pixels are {1, 2, 0, 1, 2}, and threshold T is 0. Therefore, maximum modification of the pixel is 1, and the third pixel "0" may incur an underflow problem. To avoid this problem, the third pixel "0" is modified as "1". Moreover, its location information "3" and its last bit "0" are recorded and embedded into the cover image. When users extract the location information "3" and the last bit "0" by using the extraction and recovery algorithm, the third pixel "1" is modified as "0".

4 Experimental results

To compare the performance of the proposed method and that of recently developed methods, ten test images, sized 512×512, are used, as shown in Fig. 6. The peak signal-to-noise ratio (PSNR) is applied to determine the similarity between the original image and the stego image. The equation of PSNR is

$$\mathrm{PSNR} = 10 \times \log_{10} \frac{255^2}{\mathrm{MSE}}, \tag{12}$$

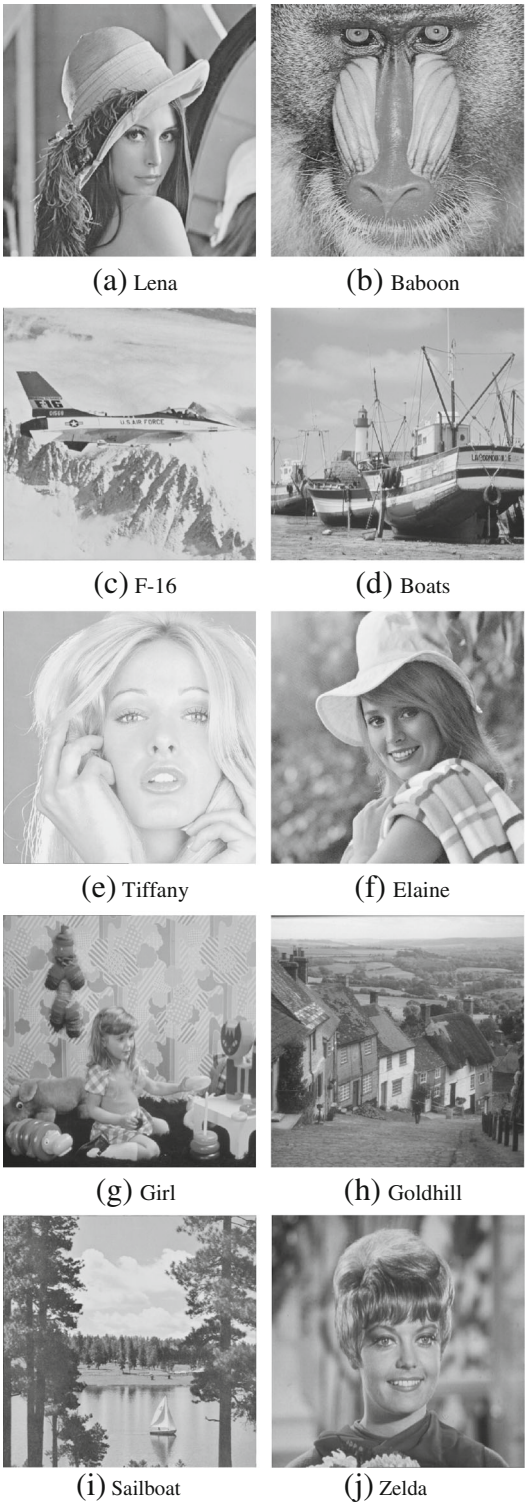
where MSE is obtained by using the equation

$$\mathrm{MSE} = \frac{1}{\mathrm{H} \times \mathrm{W}} \sum_{i=1}^{\mathrm{H}} \sum_{j=1}^{\mathrm{W}} \left[P(i,j) - P'(i,j) \right]^2. \tag{13}$$

MSE is mean square error between the cover image and the stego image; H and W are the height and width of the test image, respectively; and $P(i,j)$ and $P'(i,j)$ represent the $(i,j)^{\mathrm{th}}$ pixel of the cover image and that of the stego image, respectively.

Figure 7(a) and (b) show the hiding capacity and image quality obtained by the proposed method with different thresholds. We can see that the hiding capacities of all stego images except Baboon are more than 185,940 bits. There are too many edges in Baboon, such that the differences between the reference pixel and the embeddable pixel are too large to be

Fig. 6 Test images



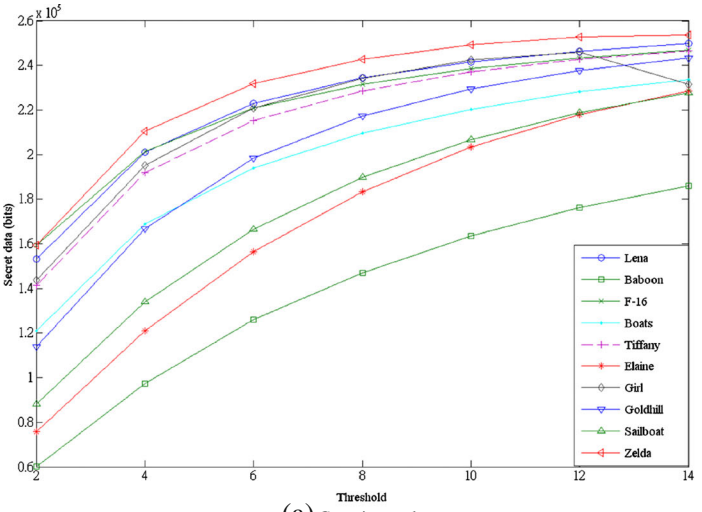
(a) Lena (b) Baboon

(c) F-16 (d) Boats

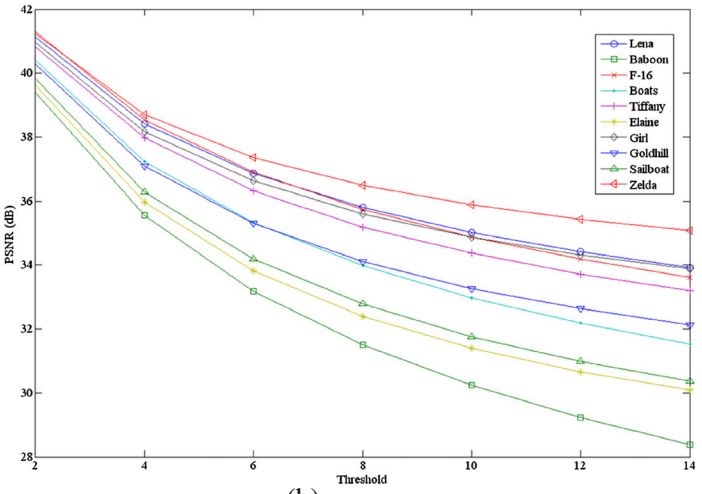
(e) Tiffany (f) Elaine

(g) Girl (h) Goldhill

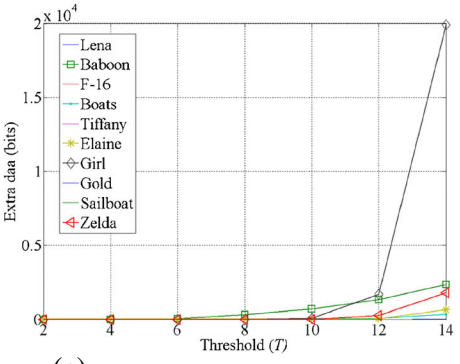
(i) Sailboat (j) Zelda



(a) Capacity results



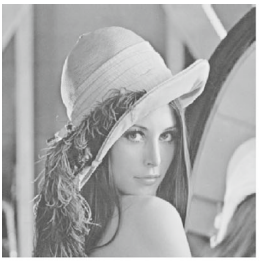
(b) Image quality



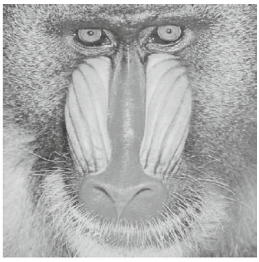
(c) Extra data for the underflow/overflow problem

Fig. 7 Ten test images with different thresholds

Fig. 8 stego images



(a) 249,763 bits, 33.923 dB, and $T = 14$



(b) 185,940 bits, 28.392 dB, and $T = 14$

(c) 246,811 bits, 33.614 dB, and $T = 14$

(d) 233,479 bits, 31.534 dB, and $T = 14$

(e) 246,459 bits, 33.194 dB, and $T = 14$

(f) 228,528 bits, 30.106 dB, and $T = 14$

(g) 231,382 bits, 33.893 dB, and $T = 14$

(h) 243,259 bits, 32.132 dB, and $T = 14$

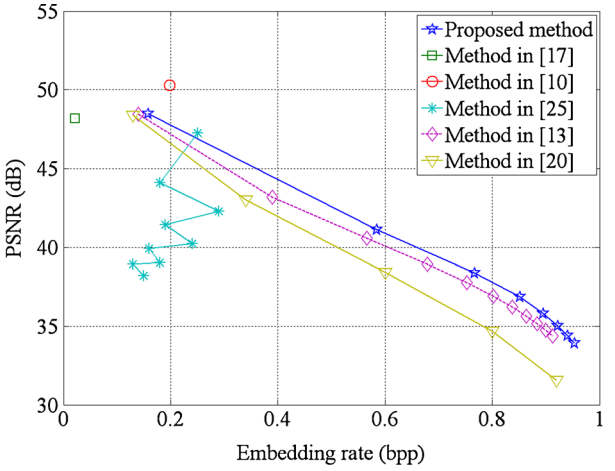
(i) 227,687 bits, 30.373 dB, and $T = 14$

(j) 253,662 bits, 35.089 dB, and $T = 14$

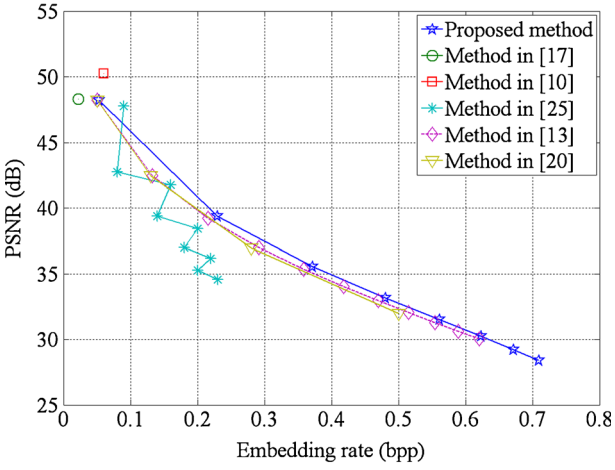
embedded. Figure 7(c) shows the size of our extra data. When threshold T is equal to 14, the extra data is significantly increased. Therefore, the range of our threshold T is [0, 14].

The proposed method still has high image quality and hiding capacity in other images, especially for a smooth image. Figure 8 shows the stego images produced by the proposed method; the stego image qualities of all images are higher than 28 dB.

Figure 9(a)–(b) show the comparison results among the proposed method with some recently developed methods by Ni et al. [17], Hong and Chen [10], Tseng and Hsieh [25], Lee and Chen [13] and Tai et al. [20]. Experimental results indicate that the stego image quality and embedding rate of the proposed method are higher than that of Tseng and Hsieh, Lee and Chen, and Tai et al.'s proposed methods. This advantage is due to the number of reference pixels in the proposed method being more than that of the other methods. In



(a) Lena



(b) Baboon

Fig. 9 Comparison results among the proposed method and recently developed methods [10, 13, 17, 20, 25]

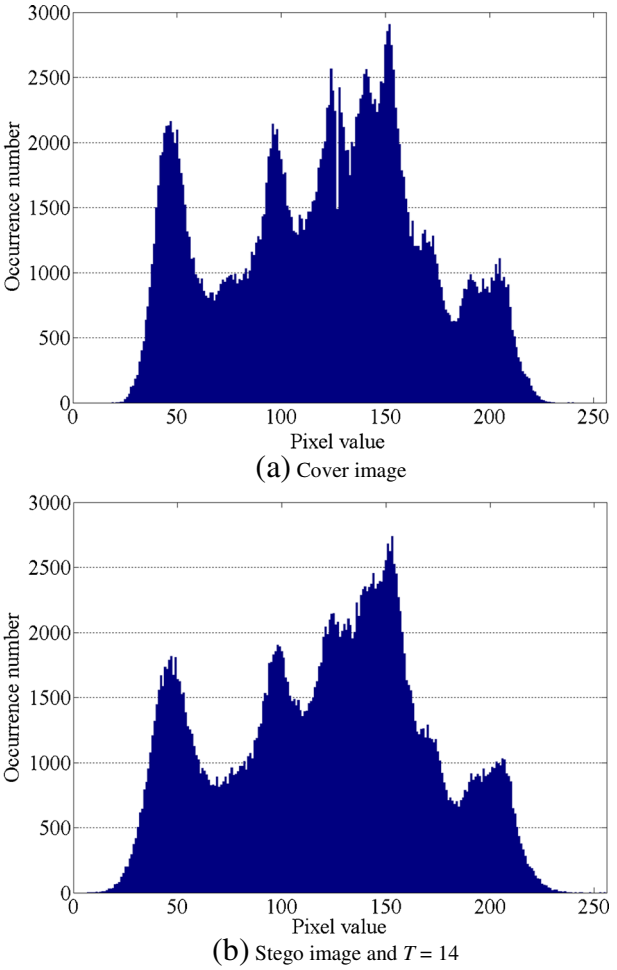


Fig. 10 Pixel histogram of Lena

addition, the large reference pixels can help to raise the accuracy of prediction. With high prediction accuracy, the number of embeddable pixels is high and the number of shifting pixels is low; that is why the proposed method can embed a large amount of secret data and produce an excellent stego image.

Table 1 The lowest requirements of our method and that of the other methods

Requirements	Our method	[25]	[10]	[17]
Threshold	One threshold	One threshold	Two thresholds	No
Peak point	No	No	Two peak points	One peak point
Zero point	No	No	No	One zero point
Compression technique	No	No	Yes	No

Although the stego image quality of the proposed method is lower than that of Hong and Chen's method, maximum hiding capacity of the proposed method is higher than that of Hong and Chen's method [10]. In Hong and Chen's method, the pixel in a complex block remains constant. However, these pixels cannot embed secret data, thus limiting the maximum hiding capacity. The proposed method can thus embed more secret data than Hong and Chen's method. The hiding capacity of the proposed scheme is superior to that of Ni et al.'s method [17], with the same stego image quality.

Figure 10 indicates that the pixel histogram of the stego image closely resembles that of the cover image. Additionally, before embedding, the secret data can be encrypted by a reliable cryptographic algorithm (i.e., RSA or Elgamal). Only persons granted legal access with the correct key can extract and decode the secret information. Therefore, the proposed scheme is secure.

Table 1 compares the lowest requirements of the proposed method with other methods. The threshold and peak point are extra information that must be transmitted over a secure channel. According to the comparison results, the amount of extra information of the proposed method is less than that of the methods developed by Hong and Chen [10] and Ni et al. [17]. Further, Hong and Chen's scheme requires a compression technique to compress side messages. The proposed method does not require a compression technique.

5 Conclusions

This paper proposes a reversible hiding method based on the DE, histogram and bilinear interpolation. The proposed method does not need to search for the peak points, nor does extra data need to be compressed. Therefore, our implementation costs are lower than Hong and Chen's method. In the proposed method, the pixel (except for the reference pixel) in a smooth or complex region can embed secret data. After some secret data are embedded, the remaining secret data are embedded into the reference pixel. Consequently, the proposed method can embed a large amount of secret data.

Since the number of our reference pixels is more than that of recently developed methods, the prediction results are accurate and our performances (i.e., embedding rate and image quality) are satisfactory. Experimental results demonstrate that the proposed method performs better than recently developed methods. In the future, the authors will attempt to adopt the recently developed interpolation methods [19, 26] to yield a better prediction. A precise prediction can greatly improve the hiding capacity and stego image quality. Additionally, the human visual system (HVS) model in [2] will be added into the proposed scheme to enhance imperceptibility for the stego image. On the other hand, the proposed scheme will attempt to use the minimum/maximum preserved overflow/underflow avoidance (MMPOUA) algorithm [27], which can avoid overflow/underflow problems and enhance embedding rate and stego image quality.

References

1. Alattar AM (2004) Reversible watermark using the difference expansion of a generalized integer transform. IEEE Trans Image Process 13(8):1147–1156

2. Awrangjeb M, Kankanhalli MS (2005) Reversible watermarking using a perceptual model. J Electron Imaging 14(1):1–8
3. Berson TA (1993) Differential cryptanalysis mod 2^{32} with applications to MD5. Advances in Cryptology — EUROCRYPT' 92 658:71–80
4. Celik MU, Sharma G, Tekalp AM, Saber E (2005) Lossless generalized-LSB data embedding. IEEE Trans Image Process 14(2):253–266
5. Chan YK, Chen WT, Yu SS, Ho YA, Tsai CS, Chu YP (2009) A HDWT-based reversible data hiding method. J Syst Softw 82(3):411–421
6. Chan CK, Cheng LM (2004) Hiding data in images by simple LSB substitution. Pattern Recogn 37 (3):469–474
7. Chang CC, Huang YH, Tsai HY, Qin C (2012) Prediction-based reversible data hiding using the difference of neighboring pixels. Int J Electron Commun (AEÜ) 66(9):758–766
8. Chu YH, Chang S (1999) Dynamical cryptography based on synchronized chaotic systems. IEE Electron Lett 35(12):974–975
9. Highland HJ (1997) Data encryption: a non-mathematical approach. Comput Secur 16(5):369–386
10. Hong W, Chen TS (2011) Reversible data embedding for high quality images using interpolation and reference pixel distribution mechanism. J Vis Commun Image Represent 22(2):131–140
11. Hu Y, Lee HK, Li J (2009) DE-based reversible data hiding with improved overflow location map. IEEE Trans Circ Syst Video Technol 19(2):250–260
12. Kieu TD, Chang CC (2011) A steganographic scheme by fully exploiting modification directions. Expert Syst Appl 38:10648–10657
13. 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
14. Li YC, Yeh CM, Chang CC (2009) Data hiding based on the similarity between neighboring pixels with reversibility. Digit Signal Proc 20(4):1116–1128
15. Lin CC (2011) An information hiding scheme with minimal image distortion. Comput Stand Interfaces 33 (5):477–484
16. Liu YC, Wu HC, Yu SS (2011) Adaptive DE-based reversible steganographic technique using bilinear interpolation and simplified location map. Multimed Tools Appl 52(2–3):263–276
17. Ni Z, Shi YQ, Ansari N, Su W (2006) Reversible data hiding. IEEE Trans Circ Syst Video Technol 16 (3):354–362
18. Petitcolas FAP, Anderson RJ, Kuhn MG (1999) Information hiding - a survey. Proc IEEE 87(7):1062–1078
19. Qin C, Wang S, Zhang X (2012) Simultaneous inpainting for image structure and texture using anisotropic heat transfer model. Multimed Tools Appl 56(3):469–483
20. Tai WL, Yeh CM, Chang CC (2009) Reversible data hiding based on histogram modification of pixel differences. IEEE Trans Circ Syst Video Technol 19(6):906–910
21. Thodi DM, Rodriguez JJ (2004) Prediction-error based reversible watermarking. Proc 2004 Int Conf Image Process 3:1549–1552
22. Thodi DM, Rodriguez JJ (2007) Expansion embedding techniques for reversible watermarking. IEEE Trans Image Process 16(3):721–730
23. Tian J (2011) Reversible data embedding using a difference expansion. IEEE Trans Circ Syst Video Technol 13(8):890–896
24. Tsai P, Hu YC, Yeh HL (2009) Reversible image hiding scheme using predictive coding and histogram shifting. Signal Process 89(6):1129–1143
25. Tseng HW, Hsieh CP (2009) Prediction-based reversible data hiding. Inform Sci 179(14):2460–2469
26. Wu HT, Huang J (2012) Reversible image watermarking on prediction errors by efficient histogram modification. Signal Process 92(12):3000–3009
27. Yang CY, Hu WC (2011) High-performance reversible data hiding with overflow/underflow avoidance. ETRI J 33(4):580–588
28. Yang HW, Hwang KF, Liao IE (2009) Reversible data hiding based on interleaving max-min difference histogram. Proceedings of the 2009 Joint Conferences on Pervasive Computing 823–828. doi: 10.1109/JCPC.2009.5420071
29. Yang CH, Weng CY, Tso HK, Wang SJ (2011) A data hiding scheme using the varieties of pixel-value differencing in multimedia images. J Syst Softw 84(4):669–678
30. Zhang X, Wang S (2006) Efficient steganographic embedding by exploiting modification direction. IEEE Commun Lett 10(11):781–783
31. Zhao ZF, Luo H, Lu ZM, Pan JS (2011) Reversible data hiding based on multilevel histogram modification and sequential recovery. Int J Electron Commun (AEÜ) 65(10):814–826

Tzu-Chuen Lu received the B.M. degree (1999) and MSIM degree (2001) in Information Management from Chaoyang University of Technology, Taiwan. She received her Ph.D. degree (2006) in Computer Science and Information Engineering from National Chung Cheng University, Taiwan. Her current title is Associate Professor with the Department of Information Management at Chaoyang University of Technology.

Chin-Chen Chang received his Ph.D. degree in computer engineering from National Chiao Tung University. His first degree is Bachelor of Science in Applied Mathematics and master degree is Master of Science in computer and decision sciences. Both were awarded in National Tsing Hua University. Dr. Chang served in National Chung Cheng University from 1989 to 2005. His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. Prior to joining Feng Chia University, Professor Chang was an associate professor in Chiao Tung University, professor in National Chung Hsing University, chair professor in National Chung Cheng University. He had also been Visiting Researcher and Visiting Scientist to Tokyo University and Kyoto University, Japan. During his service in Chung Cheng, Professor Chang served as Chairman of the Institute of Computer Science and Information Engineering, Dean of College of Engineering, Provost and then Acting President of Chung Cheng University and Director of Advisory Office in Ministry of Education, Taiwan. Professor Chang has won many research awards and honorary positions by and in prestigious organizations both nationally and internationally. He is currently a Fellow of IEEE and a Fellow of IEE, UK. And since his early years of career development, he consecutively won Outstanding Talent in Information Sciences of the R. O. C., AceR Dragon Award of the Ten Most Outstanding Talents, Outstanding Scholar Award of the R. O. C., Outstanding Engineering Professor Award of the R. O. C., Distinguished Research Awards of National Science Council of the R. O. C., Top Fifteen Scholars in Systems and Software Engineering of the Journal of Systems and Software, and so on. On numerous occasions, he was invited to serve as Visiting Professor, Chair Professor, Honorary Professor, Honorary Director, Honorary Chairman, Distinguished Alumnus, Distinguished Researcher, Research Fellow by universities and research institutes. His current research interests include database design, computer cryptography, image compression and data structures.

Ying-Hsuan Huang received the MS degree in Information Management from Chaoyang University of Technology, Taiwan. He is currently pursuing the Ph.D. degree in Computer Science and Engineering from National Chung Hsing University. His research interests include data hiding, secret sharing and image processing.