A Reversible Steganography Suitable for Embedding Small Amounts of Data

Qian Mao[1, 2], Chin-Chen Chang[2, 3], and Ting-Feng Chung[3]
(Corresponding author: Chin-Chen Chang)

School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology[1]
516, Jungong Road, Yangpu, Shanghai 200093, P. R. China
Department of Computer Science and Information Engineering, Asia University[2]
500, Lioufeng Road, Wufeng, Taichung 41354, Taiwan
Department of Information Engineering and Computer Science, Feng Chia University[3]
100, Wenhwa Road, Seatwen, Taichung 40724, Taiwan
(Email: alan3c@gmail.com)

(Received Apr. 16, 2013; revised and accepted June 5, 2013)

Abstract

A reversible information hiding scheme that is suitable for embedding small amounts of data is proposed in this paper. The secret data are transformed to base-*k* data stream, and each number is embedded into a pixel pair if the pixels' difference is within a certain range. Referring a pre-determined table, the gray values of the pixel pair are modified so as to carry the secret number. In order to distinguish the secret-carry pairs from no-secret-carry pairs, the differences of the pixel pairs without secret data embedded are expanded by modification of the difference histogram. The proposed information hiding scheme has flexible embedding capacity and low overhead. The peak signal-to-noise ratio (PSNR) is greater than those of existing methods that are based on histogram modification when the embedding capacity is low. Experimental results showed that the proposed scheme provides good embedding performances for small amounts of embedded data.

Keywords: Histogram modification, reference table, reversible, steganography

1 Introduction

Image hiding techniques embed imperceptible secret messages into cover images, allowing the secret messages to be transmitted without being perceived. In order to hide such an imperceptible secret message in the cover image, the embedding algorithm modifies the pixels' gray values, thereby producing a stego image. The modification of the cover image decreases its quality, but, due to the video redundancy, it is difficult for anyone to perceive the presence of the embedded information. At the receiver side, an extraction algorithm reads the stego image and extracts the embedded message. The security of an image hiding technique lies in the imperceptibility of the existence of the embedded message. Therefore, when embedding a secret message, the effectiveness of the embedding algorithm is determined by its ability to minimize the distortion to the cover image.

Information hiding can be processed either in the frequency domain or in the spatial domain. Usually, for hiding schemes based on the frequency transform [13, 20], either the discrete cosine transform (DCT) or the discrete wavelet transform (DWT) is performed to the cover image. The secret message is embedded into the frequency coefficients. Hiding in the frequency domain can provide a better quality to the stego image, but the frequency transform decreases the quality of the image, and the damage is permanent.

In addition to hiding in the frequency domain, there are other schemes that hide messages in the spatial domain of the cover image, such as least significant bit (LSB) replacement [12], dynamic running code [21], wet paper code [5], and the matrix embedding method [3]. A common goal of all these methods is high embedding efficiency, i.e., the quantity of embedded bits per modification to the cover image. High embedding efficiency leads to high security of the steganographic scheme. In 2006, Zhang and Wang proposed an exploiting modification direction (EMD) method for hiding information in images [22]. In this scheme, a reference table with elements that vary from 0 to $k-1$ is required, and the secret message is transformed to a base-k data sequence. When embedding, first, a pair of gray values of two consecutive pixels in the cover image is located on a point in the reference table. By searching the next-to-embed secret number around the point in the table, the minimum modification to the pixel pair that is required to carry the secret number can be found. This method improves the peak signal-to-noise ratio (PSNR) of the stego image to a large extent. Chang et al. proposed a hiding scheme that uses a Sudoku table as the reference table [2]. This scheme finds the modification to the pixel pair in a Sudoku table to embed a base-9 secret number. Subsequently, many studies have focused on the optimization of table-based hiding methods, and many novel approaches that enhance the PSNR of the stego image have been proposed [7, 8, 9].

The embedding schemes mentioned above provide high-quality images with large embedding capacity, but the cover image cannot be restored after the secret has been extracted. In 2002, Fridrich proposed a lossless data hiding scheme that can restore the cover image after the secret has been extracted [6]. As a result, lossless data hiding, which is also referred to as reversible data hiding, has attracted the attention of many researchers. Generally speaking, reversible data hiding can be classified into the following three classes, according to the embedding algorithms that are used:

1 Difference expansion (DE) schemes [1, 18]: By expanding the difference of two consecutive pixels, one secret bit can be embedded into the expanded difference. The embedding capacity of DE methods can be changed in a large range by varying the embedding threshold, but the pixel pairs that carry embedded secret bits must be recorded in order to restore the cover image. Therefore, the overhead information of DE methods includes a location map and the original LSBs of some pixels in the cover image; this is a huge amount of information, and it must be compressed by complicated computations.

2 Prediction-based schemes [11, 19]: Using the relevance of neighboring pixels, the pixel's gray value can be predicted by its neighbors. Using the difference between the predicted value and the actual value of a pixel, a secret bit can be embedded. The embedding capacity of a prediction-based scheme is dynamic. Since the prediction expansion may cause overflow and underflow for some pixels, overhead information is required to mark these pixels.

3 Histogram modification schemes [4, 10, 14]: By changing the histogram distribution of a cover image, the secret bits can be embedded into the pixels that occur most often in the image. Histogram modification schemes usually require less overhead, which includes the peak points, the zero points, overflow pixels, and underflow pixels. But the embedding capacity usually is low and depends on the histogram distribution of the cover image. If there are insufficient zero points in the histogram, the embedding capacity will be low. In 2009, Tai et al. proposed an embedding scheme based on modification of the difference histogram, which improved the embedding capacity significantly [17].

In this paper, a reversible embedding scheme based on modification of the difference histogram and the reference table is proposed. The proposed scheme provides extremely high quality to the stego image with a low capacity, which is suitable for the applications of small amounts of secret data with a high-quality stego image, such as copyright protection [16] and image authentication [15]. The remaining paper is organized as follows. The novel scheme is proposed in Section 2. The experimental results and comparisons with existing schemes based on histogram modification are provided in Section 3. Conclusions are given in Section 4.

2 Proposed Scheme

In this section, a reversible steganographic scheme that has low overhead is proposed. The proposed scheme uses a reference table to embed a secret number into two consecutive pixels in the cover image.

2.1 Reference Table

The reference table is used to decide the modification to the pixel pair of the cover image, according to the secret number. Assuming that the base of the steganographic system is k, the reference table, T, can be constructed as follows:

$$T=\begin{bmatrix} B & B & \cdots \\ B & B & \cdots \\ \vdots & \vdots & \ddots \end{bmatrix}_{256\times 256}, \tag{1}$$

where B is the sub-block of the reference table, which is a $k\times k$ matrix, as shown below:

$$B=\begin{bmatrix} 0 & 1 & \cdots & k-1 \\ k-1 & 0 & \cdots & k-2 \\ \vdots & \vdots & & \vdots \\ 1 & \cdots & k-1 & 0 \end{bmatrix}, \tag{2}$$

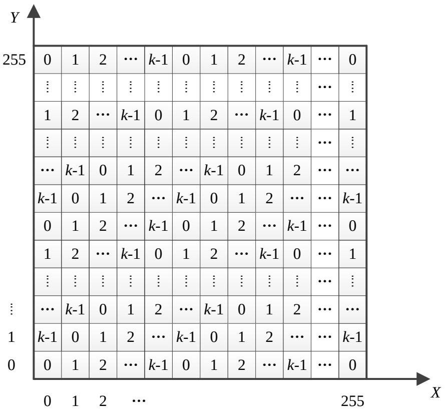
Equation (1) shows that the reference table is constructed by circulating B in both horizontal and vertical directions. The size of T is 256×256, which is the dynamic range of the pixels' gray values.

Using Equations (1) and (2), the reference table can be constructed as shown in Figure 1.

The lookup-table function, T, is:

$$z=\mathrm{T}(x,y),\ x,y\in[0,255], \tag{3}$$

where x and y are the x - and y - coordinates in Figure 1, z is the value with coordinates (x, y) in the table, and $z\in[0,k-1]$.



255	0	1	2	⋯	k-1	0	1	2	⋯	k-1	⋯	0
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋯	⋮
	1	2	⋯	k-1	0	1	2	⋯	k-1	0	⋯	1
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋯	⋮
	⋯	k-1	0	1	2	⋯	k-1	0	1	2	⋯	⋯
	k-1	0	1	2	⋯	k-1	0	1	2	⋯	⋯	k-1
	0	1	2	⋯	k-1	0	1	2	⋯	k-1	⋯	0
	1	2	⋯	k-1	0	1	2	⋯	k-1	0	⋯	1
	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋮	⋯	⋮
⋮	⋯	k-1	0	1	2	⋯	k-1	0	1	2	⋯	⋯
1	k-1	0	1	2	⋯	k-1	0	1	2	⋯	⋯	k-1
0	0	1	2	⋯	k-1	0	1	2	⋯	k-1	⋯	0
	0	1	2	⋯								255

Figure 1: Reference table

2.2 Difference Histogram Shift

The proposed steganography embeds a secret number *s* into two adjacent pixels, (p_1^c, p_2^c), where p_1^c and p_2^c are the gray values of the two pixels, and $s \in [0, k-1]$. A pixel pair is looked as embeddable if their difference, *d*, satisfies that $d_{\min} \le d \le d_{\max}$. After embedding, the secret-carry pairs may be confused with the pairs that have no secret embedded. In order to avoid this confusion, all of the pixel pairs with differences that satisfy $d < d_{\min}$ or $d > d_{\max}$ are expanded by the difference histogram shift operation.

First, the differences of all the pixel pairs in the cover image are computed in order to obtain the difference matrix, *D*. The dynamic range of the elements in *D* is $[-255, 255]$. Then, the histogram of *D* is constructed, which is the difference histogram of the original cover image. In the difference histogram, the location at which the frequency is 0 is called the 'zero point', and the location at which the difference is 0 is called the 'center' in this paper. In order to embed the secret message, a series of zero points near the center are needed. To obtain these zero points, we will first find gl zero points that are nearest to the center on the left side of the difference histogram, and gl is:

$$gl = |d_{\min} k| + \left\lfloor \frac{k-1}{2} \right\rfloor, \qquad (4)$$

where $|x|$ denotes the absolute value of *x* and $\lfloor x \rfloor$ denotes the largest integer smaller than *x*. The difference values of the gl zero points are denoted as zp_1^l, zp_2^l,…, zp_{gl}^l ($zp_1^l < zp_2^l < \cdots < zp_{gl}^l$). After that, we shift the values on the left side of the difference histogram to these gl zero points. For the pixel pair with a difference *d* satisfying $zp_i^l < d < zp_{i+1}^l$ ($i = 1, 2, \cdots, gl-1$), the gray value of the second pixel is subtracted by *i*. For the pixel pair that has a difference smaller than 0 and larger than zp_{gl}^l, subtract gl from the second pixel's gray value. For the pixel pair that has a difference smaller than zp_1^l, do not make any modification of the pixels.

On the right side of the difference histogram, find the gr zero points that are nearest to the center, and gr is:

$$gr = |d_{\max} k| + \left\lceil \frac{k-1}{2} \right\rceil, \qquad (5)$$

where $\lceil x \rceil$ denotes the smallest integer larger than *x*. The difference values of the gr zero points are denoted as zp_1^r, zp_2^r,…, zp_{gr}^r ($zp_1^r < zp_2^r < \cdots < zp_{gr}^r$). We shift the values on the right side of the difference histogram to these gr zero points. For the pixel pair with a difference *d* satisfying $zp_i^r < d < zp_{i+1}^r$ ($i = 1, 2, \cdots, gr-1$), the gray value of the second pixel is added by $gr - i$. For the pixel pair that has a difference larger than 0 and smaller than zp_1^r, add gl to the second pixel's gray value. For the pixel pair that has a difference larger than zp_{gr}^r, do not modify the pixels in any way. By this means, the differences of all the confused pairs are expanded, leaving the locations that satisfy $d_{\min} k - \lfloor (k-1)/2 \rfloor \le d < 0$ and $0 < d \le d_{\max} k + \lceil (k-1)/2 \rceil$ empty in the difference histogram. Figure 2 shows an example of difference histogram shift with $d_{\min} = d_{\max} = 0$ and $k = 4$.

Notice that during the process of difference histogram shift, if the pixel pair's difference satisfies that $zp_i^l < d < zp_{i+1}^l$ ($i = 1, 2, \cdots, gl-1$) and $p_2^c < i$, the phenomenon of underflow will occur. If the pixel pair's difference satisfies that $zp_i^r < d < zp_{i+1}^r$ ($i = 1, 2, \cdots, gr-1$) and $p_2^c > 255 - i$, the phenomenon of overflow will occur. The coordinates of both the underflow and overflow pixels should be recorded for the use of restoring the cover image.

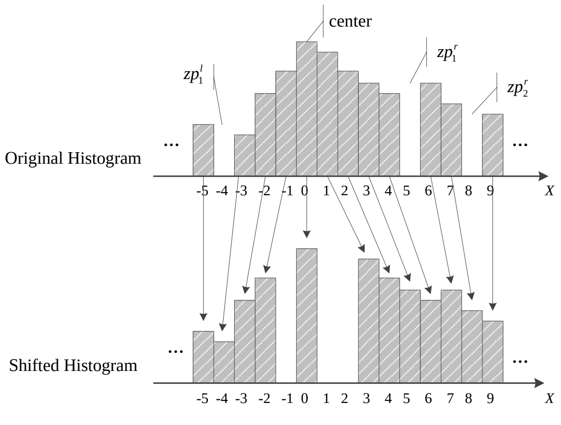


Figure 2: Example of difference histogram shift

2.3 Embedding Algorithm

The proposed steganography embeds a secret number into two adjacent pixels, (p_1^c, p_2^c), if the difference between the two pixels' gray values, $d = p_2^c - p_1^c$, satisfies that $d_{\min} \le d \le d_{\max}$, where $d_{\min}$ and $d_{\max}$ are pre-determined parameters. The embeddable pixel pair can be composed of two adjacent pixels that are located in the horizontal direction or the vertical direction. Therefore, first, the entire cover image will be scanned, and the direction that provides the most embeddable pairs will be chosen for embedding.

Assume that the embeddable pixel pair (p_1^c, p_2^c) is modified to (p_1^s, p_2^s) by the embedding algorithm. In the proposed embedding scheme, the first pixel in a pair is always unchanged, therefore, $p_1^s = p_1^c$, and the second pixel is modified to p_2^s so as to satisfy $s = \mathrm{T}(p_1^s, p_2^s)$, with the restriction that:

$$dk - \left\lfloor \frac{k-1}{2} \right\rfloor \le p_2^s - p_1^s \le dk + \left\lceil \frac{k-1}{2} \right\rceil, \qquad (6)$$

where $d = p_2^c - p_1^c$.

Equation (6) actually divides the modification to the pixel pair's difference into $d_{\max} - d_{\min}$ intervals in the reference table, as shown in Figure 3. Each interval includes k numbers, varying from 0 to $k-1$. For the pixel pair, (p_1^c, p_2^c), with difference d, the second pixel, p_2^c, is modified to p_2^s by the following rules (noting that $p_1^s = p_1^c$):

1 If $d = 0$ and $d_{\min} \le d \le d_{\max}$, the second pixel, p_2^c, is modified to p_2^s, which satisfies $s = \mathrm{T}(p_1^s, p_2^s)$ and $p_2^s - p_1^s \in \left[-\lfloor (k-1)/2 \rfloor, \lceil (k-1)/2 \rceil\right]$. The interval $\left[-\lfloor (k-1)/2 \rfloor, \lceil (k-1)/2 \rceil\right]$ is defined as the center modification interval, denoted as MI_C.

2 If $d < 0$ and $d_{\min} \le d \le d_{\max}$, the second pixel, p_2^c, is modified to p_2^s, which satisfies $s = \mathrm{T}(p_1^s, p_2^s)$ and $p_2^s - p_1^s \in \left[dk - \lfloor (k-1)/2 \rfloor, dk + \lceil (k-1)/2 \rceil\right]$. These intervals, $\left[dk - \lfloor (k-1)/2 \rfloor, dk + \lceil (k-1)/2 \rceil\right]$, are defined as left modification intervals, denoted as $\mathrm{MI\_L}_1$, $\mathrm{MI\_L}_2$, …, $\mathrm{MI\_L}_{gl}$.

3 If $d > 0$ and $d_{\min} \le d \le d_{\max}$, the second pixel, p_2^c, is modified to p_2^s, which satisfies $s = \mathrm{T}(p_1^s, p_2^s)$ and $p_2^s - p_1^s \in \left[dk - \lfloor (k-1)/2 \rfloor, dk + \lceil (k-1)/2 \rceil\right]$. These intervals, $\left[dk - \lfloor (k-1)/2 \rfloor, dk + \lceil (k-1)/2 \rceil\right]$, are defined as right modification intervals, denoted as $\mathrm{MI\_R}_1$, $\mathrm{MI\_R}_2$, …, $\mathrm{MI\_R}_{gr}$.

Notice that for an embeddable pair with difference of d, if $d < 0$ and $p_1^c < |dk| + \lfloor (k-1)/2 \rfloor$, the situation of underflow may occur; if $d > 0$ and $p_1^c > 255 - \left(|dk| + \lceil (k-1)/2 \rceil\right)$, the situation of overflow may occur. Therefore, these two kinds of pixel pairs are not embeddable.

The overhead information of the proposed scheme is shown in Table 1. The embedding direction is embedded into the first pixel of the cover image. Since the possible direction is either horizontal or vertical, one bit is required to indicate the embedding direction. Then, the length of the overhead is attached. The third part is the difference values of the zero points in the difference histogram. Since the pixel pairs that have differences that satisfy $d_{\min} \le d \le d_{\max}$ are embeddable, and each value of d requires a difference interval with the width of k for embedding, $k(d_{\max} - d_{\min} + 1) - 1$ continuous zero points round the center in the difference histogram are required for histogram shift. The last two parts of the overhead are the coordinates of the overflow and underflow pixels, which depend on the histogram distribution of the cover image. Table 1 shows that the length of the overhead of the proposed scheme is short.

The detailed procedures of secret embedding of the proposed scheme are listed below:

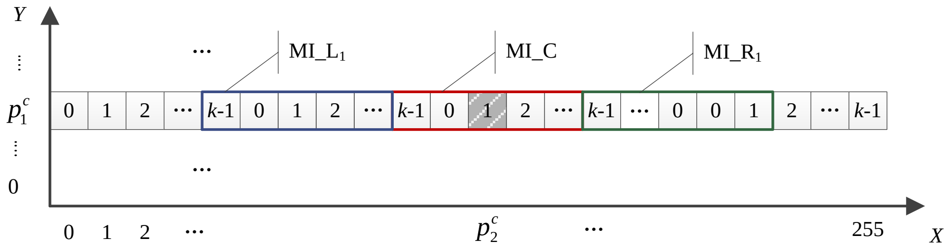


Figure 3: Modification intervals for different differences

Table 1: Overhead information

Content	Length (bit)
Scan Direction	1
Length of Overhead	variable
Zero Points in the Difference Histogram	$8(k(d_{\max} - d_{\min} + 1) - 1)$
Coordinates of the Overflow Pixels	variable
Coordinates of the Underflow Pixels	variable

1 Choose the base of the steganographic system, k. Transform the secret message into base-*k* numbers. Construct the reference table according to k.

2 Choose the parameters $d_{\min}$ and $d_{\max}$. Scan the cover image in horizontal and vertical directions to find the embeddable pixel pair for which the difference satisfies $d_{\min} \le d \le d_{\max}$. The direction that provides the most embeddable pairs is chosen as the embedding direction, in which the number of embeddable pairs is q.

3 Compute the differences of all the pixel pairs in the embedding direction. Make the histogram of the difference matrix. Find the zero points, zp_1^l, zp_2^l,…, zp_{gl}^l and zp_1^r, zp_2^r,…, zp_{gr}^r, in the difference histogram, where gl and gr are computed by Equations (4) and (5), respectively.

4 Set the initial value $i = 1$ and scan the cover image from the second row (or column) in the embedding direction. For the pixel pair (p_1^c, p_2^c) that has a difference d satisfying $zp_i^l < d < zp_{i+1}^l$ ($i = 1, 2, \cdots, gl - 1$), the gray value of the second pixel, p_2^c, is subtracted by i. If $p_2^c - i < 0$, the second pixel is marked as an underflow pixel. After all the pixel pairs are scanned, let $i = i + 1$. Repeat Step 4 until $i = gl$ (assuming that $zp_{gl+1}^l = 0$).

5 Set the initial value $i = gr - 1$ and scan the cover image from the second row (or column) in the embedding direction. For the pixel pair (p_1^c, p_2^c) that has a difference d satisfying $zp_i^r < d < zp_{i+1}^r$ ($i = 1, 2, \cdots, gr - 1$), the gray value of the second pixel is added by $gr - i$. If $p_2^c + gr - i > 255$, the second pixel is marked as an overflow pixel. After all the pixel pairs are scanned, let $i = i - 1$. Repeat Step 5 until $i = 0$ (assuming that $zp_0^r = 0$).

6 Embed the overhead information into the first row or column of the cover image by LSB replacement.

7 Scan the cover image from the second row (or column) along with the embedding direction. If the pixel pair (p_1^c, p_2^c) satisfies that $d_{\min} \le p_2^c - p_1^c \le d_{\max}$, take the next-to-embed secret number, s, and modify (p_1^c, p_2^c) to (p_1^s, p_2^s) so that it satisfies $s = \mathrm{T}(p_1^s, p_2^s)$, $p_1^c = p_1^s$, and Equation (6). Scan the entire cover image and implement the embedding operation for all of the embeddable pairs.

2.4 Extracting and Restoring Algorithm

At the receiver side, a pixel pair that has a secret number embedded can be recognized by checking the pixels' difference. A pixel pair, (p_1^s, p_2^s), is considered as a secret-carry pair if it satisfies the following requirement:

$$d_{\min} k - \left\lfloor \frac{k-1}{2} \right\rfloor \le p_2^s - p_1^s \le d_{\max} k + \left\lceil \frac{k-1}{2} \right\rceil. \quad (7)$$

For a secret-carry pair, the secret number can be extracted by Equation (3).

In order to restore the secret-carry pair, first it must be determined which interval the pair's difference belongs to so that the pair's difference, d, in the original image can be deduced. Assuming that the restored pixel pair is (p_1^r, p_2^r), it is apparent that $p_1^r = p_1^s$ and $p_2^r = p_1^s + d$. The restoration function for the secret-carry pair is:

$$p_1^r = p_1^s, p_2^r = p_1^s + d, \text{ where}$$
$$d = \begin{cases} \left\lfloor \dfrac{p_2^s - p_1^s + \lfloor \frac{k-1}{2} \rfloor}{k} \right\rfloor, & \text{if } p_2^s \ge p_1^s \\ \left\lfloor \dfrac{p_2^s - p_1^s - \lfloor \frac{k-1}{2} \rfloor}{k} \right\rfloor, & \text{if } p_2^s < p_1^s \end{cases}. \quad (8)$$

After all of the secret numbers are extracted and all the secret-carry pairs are restored, the no-secret-carry pairs will be restored by the reverse operation of the difference histogram shift in the embedding process. The overall extraction and restoration procedures of the proposed steganography are shown below:

1 Read the LSB of the first pixel of the stego image to determine the scan direction. Extract the information about the zero points, underflow pixels, and overflow pixels by reading the LSBs of the pixels in the first row or column.

2 Scan the stego image from the second row (or column) along with the embedding direction. For a pixel pair (p_1^s, p_2^s), if the pixels' difference satisfies Equation (7), extract the secret number by Equation (3) and modify (p_1^s, p_2^s) to (p_1^r, p_2^r) by Equation (8).

3 Set the initial value $i = gl$ and scan the stego image from the second row (or column) in the embedding direction. For the pixel pair (p_1^s, p_2^s), add i to p_2^s if the pair satisfies that $zp_i^l - i + 1 \le p_2^s - p_1^s < zp_{i+1}^l$ (assuming that $zp_{gl+1}^l = 0$). After all the pixel pairs are scanned, let $i = i - 1$. Repeat Step 3 until $i = 1$.

Table 2: bpp vs. PSNR when $d_{\max} = d_{\min} = 0$

	***k* = 2**		***k* = 3**		***k* = 4**		***k* = 5**		***k* = 7**	
	bpp	***PSNR***	***bpp***	***PSNR***	***bpp***	***PSNR***	***bpp***	***PSNR***	***bpp***	***PSNR***
lena	0.064	53.65	0.10	50.81	0.13	46.88	0.15	44.89	0.18	41.40
airplane	0.091	52.59	0.14	49.93	0.18	45.96	0.21	44.06	0.25	40.58
baboon	0.025	53.27	0.04	50.29	0.05	46.35	0.06	44.30	0.07	40.79
barbara	0.038	53.88	0.06	50.95	0.08	47.01	0.09	44.99	0.11	41.49
boat	0.057	53.73	0.09	50.83	0.11	46.92	0.13	44.89	0.16	41.40
girl	0.060	53.90	0.09	50.20	0.12	46.79	0.14	44.28	0.17	40.79
pepper	0.064	52.78	0.10	50.13	0.13	46.08	0.15	44.20	0.18	40.72
sailboat	0.035	52.92	0.06	50.01	0.07	46.06	0.08	44.04	0.10	40.54
tiffany	0.070	53.49	0.11	50.66	0.14	46.75	0.16	44.75	0.20	41.26

4. Set the initial value $i = gr$ and scan the stego image from the second row (or column) in the embedding direction. For the pixel pair (p_1^s, p_2^s), subtract i from p_2^s if the pair satisfies $zp_{gr-i}^r < p_2^s - p_1^s \le zp_{gr-i+1}^r + i - 1$ (assuming that $zp_0^r = 0$). After all the pixel pairs are scanned, let $i = i - 1$. Repeat Step 4 until $i = 1$.

3 Experimental Results

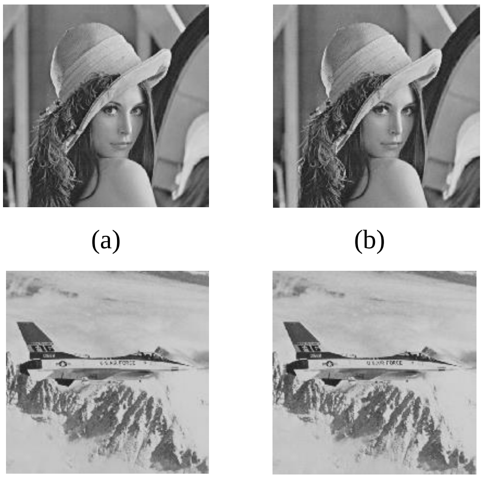
The embedding capacity of image hiding can be measured by the parameter of bpp (bit per pixel), which depends on three factors, i.e., the base (k), $d_{\min}$, and $d_{\max}$, for the proposed steganographic scheme. In the following, three scenarios with different parameters are simulated.

Scenario 1: Let $d_{\max} = d_{\min} = 0$. That is to say, only the pixel pair (p_1^c, p_2^c) that satisfies $p_1^c = p_2^c$ is used for embedding. Varying the base of the secret numbers, k, different embedding capacity can be obtained. The experimental results of embedding capacity vs. PSNR of this scenario are shown in Table 2. Some original images and the stego images with $k = 4$ are shown in Figure 4.

Scenario 2: Let $d_{\max} = 1$ and $d_{\min} = -1$. That is to say, the pixel pair (p_1^c, p_2^c) that satisfies $-1 \le p_2^c - p_1^c \le 1$ is used for embedding. The experimental results of embedding capacity vs. PSNR of this scenario are shown in Table 3. Some original images and the stego images with $k = 5$ are shown in Figure 5.

Scenario 3: Let $d_{\max} = 2$ and $d_{\min} = -2$. That is to say, the pixel pair (p_1^c, p_2^c) that satisfies $-2 \le p_2^c - p_1^c \le 2$ is used for embedding. The experimental results of embedding capacity vs. PSNR of this scenario are shown in Table 4. Some original images and the stego images with $k = 5$ are shown in Figure 6.

The lengths of overhead information of the above three scenarios are listed in Table 5, where the numbers are denoted in decimal form. Table 5 shows that the overhead of the proposed scheme is quite low.



(a) (b)

(c) (d)

Figure 4: Experimental results with $k = 4$ and $d_{\max} = d_{\min} = 0$

(a) original image --- Lena (b) stego image --- Lena

(c) original image --- airplane (d) stego image --- airplane

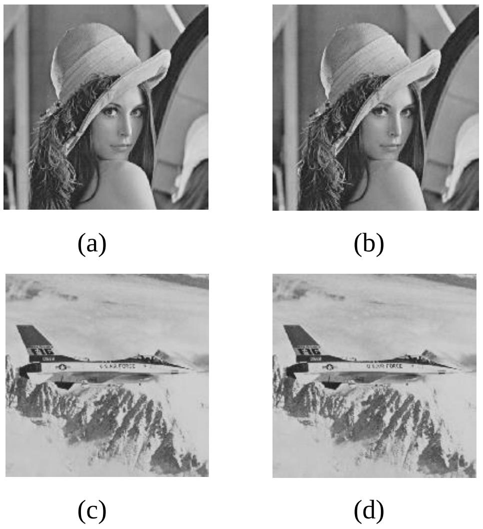
Hiding schemes based on histogram modification usually have low overhead and low embedding capacity. Figure 7 compares the results of the proposed scheme with existing hiding schemes based on histogram modification, i.e., Ni's scheme, Fallahpour et al.'s scheme, and Tai et al.'s scheme. In the experiments, the parameters of k, $d_{\max}$ and $d_{\min}$ of the proposed scheme that provide the highest PSNR were chosen for each embedding capacity. Ni's scheme and Fallahpour et al.'s scheme are based on histogram modification, the embedding capacities of which depend on the histogram distribution, therefore, the capacity cannot be changed flexibly. The proposed scheme has better PSNR performance than the two other schemes. Tai et al.'s scheme is based on difference histogram modification, which has flexible embedding capacity but cannot embed with low capacity even with the smallest threshold. The experimental results showed that the proposed scheme has a better performance than Tai et al.'s scheme when the embedding capacity is lower than approximately 0.12.

Table 3: bpp vs. PSNR when $d_{\max} = 1$ and $d_{\min} = -1$

	***k* = 3**		***k* = 5**		***k* = 7**		***k* = 9**		***k* = 11**	
	bpp	***PSNR***	***bpp***	***PSNR***	***bpp***	***PSNR***	***bpp***	***PSNR***	***bpp***	***PSNR***
lena	0.27	40.00	0.40	35.03	0.48	31.89	0.55	29.59	0.60	27.77
airplane	0.34	39.50	0.50	34.51	0.60	31.36	0.68	29.06	0.74	27.24
baboon	0.10	38.66	0.15	33.77	0.18	30.66	0.21	28.37	0.23	26.57
barbara	0.17	39.63	0.25	34.71	0.30	31.59	0.34	29.30	0.37	27.49
boat	0.26	39.92	0.38	35.00	0.46	31.83	0.51	29.53	0.56	27.71
pepper	0.27	39.30	0.40	34.37	0.48	31.25	0.54	28.97	0.59	27.18
sailboat	0.16	38.61	0.23	33.70	0.28	30.58	0.31	28.29	0.34	26.48
tiffany	0.29	39.92	0.42	34.95	0.51	31.81	0.58	29.51	0.63	27.69

Table 4: bpp vs. PSNR when $d_{\max} = 2$ and $d_{\min} = -2$

	***k* = 3**		***k* = 5**		***k* = 7**		***k* = 9**		***k* = 11**	
	bpp	***PSNR***	***bpp***	***PSNR***	***bpp***	***PSNR***	***bpp***	***PSNR***	***bpp***	***PSNR***
lena	0.41	36.20	0.60	31.32	0.72	28.21	0.82	25.92	0.89	24.11
airplane	0.47	35.87	0.68	30.95	0.83	27.83	0.94	25.53	1.02	23.72
baboon	0.17	34.15	0.24	29.41	0.29	26.35	0.33	24.10	0.36	22.32
barbara	0.27	35.40	0.39	30.59	0.48	27.52	0.54	25.27	0.58	23.52
boat	0.39	36.07	0.57	31.20	0.69	28.10	0.78	25.82	0.85	24.04
pepper	0.41	35.57	0.60	30.71	0.72	27.64	0.81	25.39	0.88	23.61
sailboat	0.24	34.30	0.36	29.52	0.43	26.46	0.49	24.19	0.53	22.39
tiffany	0.43	36.21	0.63	31.31	0.76	28.19	0.86	25.91	0.93	24.15

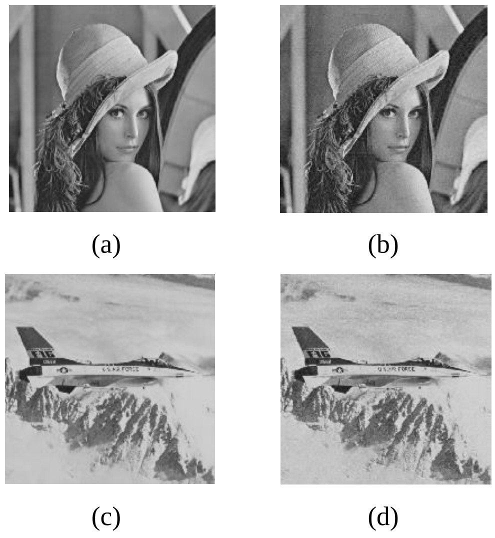


(a) (b)

(c) (d)

Figure 5: Experimental results with $k = 5$, $d_{\max} = 1$ and $d_{\min} = -1$

(a) original image --- Lena (b) stego image --- Lena
(c) original image --- airplane (d) stego image --- airplane



(a) (b)

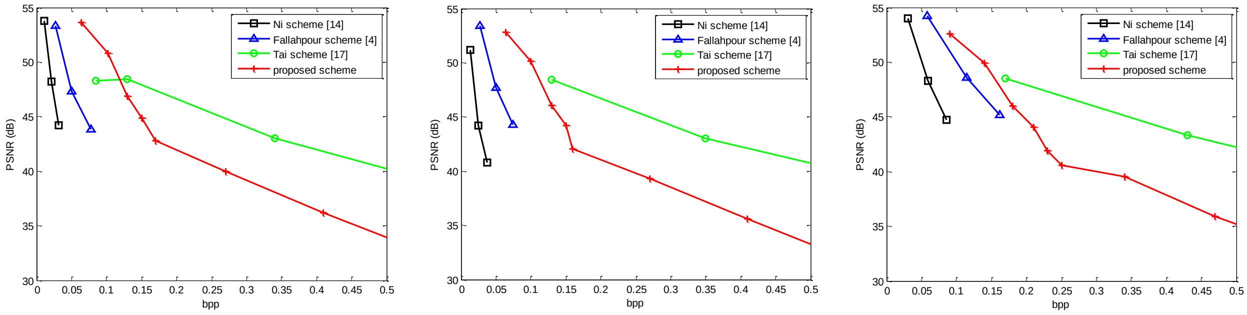
(c) (d)

Figure 6: Experimental results with $k = 5$, $d_{\max} = 2$ and $d_{\min} = -2$

(a) original image --- Lena (b) stego image --- Lena
(c) original image --- airplane (d) stego image --- airplane

Table 5: Overhead information

		lena	airplane	baboon	pepper	sailboat
$k=2$ $d_{\max}=0$ $d_{\min}=0$	Scan direction	vertical	vertical	horizontal	horizontal	horizontal
	Quantity of Left zero points	0	0	0	0	0
	Quantity of Right zero points	1	1	1	1	1
	Quantity of overflow pixels	0	0	0	0	0
	Quantity of underflow pixels	0	0	0	0	0
$k=3$ $d_{\max}=1$ $d_{\min}=-1$	Scan direction	vertical	horizontal	horizontal	horizontal	horizontal
	Quantity of Left zero points	4	4	4	4	4
	Quantity of Right zero points	4	4	4	4	4
	Quantity of overflow pixels	0	0	0	0	0
	Quantity of underflow pixels	0	0	0	60	0
$k=5$ $d_{\max}=2$ $d_{\min}=-2$	Scan direction	vertical	horizontal	horizontal	horizontal	horizontal
	Quantity of Left zero points	12	12	12	12	12
	Quantity of Right zero points	12	12	12	12	12
	Quantity of overflow pixels	0	0	0	0	0
	Quantity of underflow pixels	0	0	15	1476	0



(a) (b) (c)

Figure 7: Experimental results of PSNR performances

(a) Lena (b) Pepper (c) Airplane

4 Conclusions

A reversible information hiding scheme based on a reference table and difference histogram modification is proposed in this paper. The base- k secret numbers are embedded into the pixel pairs that have differences that are within a certain range. The proposed reversible hiding scheme has the following advantages: (1) low overhead, (2) the ability to change the embedding capacity arbitrarily by varying the base and the thresholds, and (3) higher PSNR than existing schemes when the embedding capacity is low. Therefore, the proposed scheme is very suitable for embedding small amounts of data.

References

[1] O. M. Al-Qershi and B. E. Khoo, "Two-dimensional difference expansion (2D-DE) scheme with a characteristics-based threshold," *Signal Processing*, vol. 93, no. 1, pp.154-162, 2013.

[2] C. C. Chang, Y. C. Chou and T. D. Kieu, "An information hiding scheme using sudoku," in *Proceedings of the 3^rd International Conference on Innovative Computing Information and Control (ICICIC'08)*, pp. 17, 2008.

[3] R. Crandall, "Some notes on steganography," *Steganography Mailing List*, 1998.

[4] M. Fallahpour and M. H. Sedaaghi, "High capacity lossless data hiding based on histogram modification," *IEICE Electronics Express*, vol. 4, no. 7, pp. 205-210, 2007.

[5] J. Fridrich, "Wet paper codes with improved embedding efficiency," *IEEE Transactions on Information Forensics and Security*, vol. 1, no. 1, pp. 102-110, 2006.

[6] J. Fridrich, M. Goljan and R. Du, "Lossless data embedding for all image formats," in *Proceedings of the SPIE, Security Watermarking of Multimedia Contents IV*, vol. 4675, pp. 572-583, 2002.

[7] W. Hong, "Adaptive image data hiding in edges using patched reference table and pair-wise embedding technique," *Information Sciences*, vol. 221, no. 1, pp. 473-489, 2013.

[8] W. Hong, T. S. Chen and C. W. Shiu, "Steganography using sudoku revisited," in *Proceedings of the 2nd*

International Symposium on Intelligent Information Technology Application (IITA'08), vol. 2, pp. 935-939, 2008.

[9] W. Hong, T. S. Chen and C. W. Shiu, "A minimal euclidean distance searching technique for sudoku steganography," in *Proceedings of the International Symposium on Information Science and Engineering (ISISE'08)*, vol. 1, pp. 515-518, 2008.

[10] L. C. Huang, L. Y. Tseng, M. S. Hwang, "The Study of Data Hiding in Medical Images," *International Journal of Network Security*, vol. 14, no. 6, pp. 301-309, 2012.

[11] X. Li, B. Yang and T. Zeng, "Efficient reversible watermarking based on adaptive prediction-error expansion and pixel selection," *IEEE Transactions on Image Processing*, vol. 20, no. 12, pp. 3524-3533, 2011.

[12] J. Mielikainen, "LSB matching revisited," *IEEE Signal Processing Letters*, vol. 13, no. 5, pp. 285-287, 2006.

[13] K. MohammadReza and B. FarnooshMerrikh, "Blind image watermarking method based on chaotic key and dynamic coefficient quantization in the DWT domain," *Mathematical and Computer Modelling*, In Press, Accepted Manuscript, Available online: http://www.sciencedirect.com/science/article/pii/S089571771200177X, 2012.

[14] Z. C. Ni, "Reversible data hiding," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 16, no. 3, pp. 354-362, 2006.

[15] S. S. Sujatha and M. M. Sathik "A Novel DWT Based Blind Watermarking for Image Authentication," *International Journal of Network Security*, vol. 14, no. 4, pp. 223-228, 2012.

[16] B. Surekha and G. N. Swamy, "Sensitive Digital Image Watermarking for Copyright Protection," *International Journal of Network Security*, vol. 15, no. 2, pp. 113-121, 2013.

[17] W. L. Tai, C. M. Yeh and C. C. Chang. "Reversible data hiding based on histogram modification of pixel differences," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 19, no. 6, pp. 906-910, 2009.

[18] J. Tian, "Reversible data embedding using a difference expansion," *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 13, no. 8, pp. 890-896, 2003.

[19] H. W. Tseng and C. P. Hsieh, "Prediction-based reversible data hiding," *Information Sciences*, vol. 179, no. 14, pp. 2460-2469, 2009.

[20] A. Westfeld, "F5: A steganographic algorithm," in *Proceedings of the 4th International Workshop Information Hiding 2001, Lecture Notes in Computer Science*, vol. 2137, pp. 289-302, 2011.

[21] X. Zhang, "Dynamical running coding in digital steganography," *IEEE Signal Processing Letters*, vol. 13, no. 3, pp. 165-168, 2006.

[22] X. Zhang and W. Shuozhong, "Efficient steganographic embedding by exploiting modification direction," *IEEE Communications Letters*, vol. 10, no. 11, pp. 781-783, 2006.

Qian Mao was born in Shanxi Province, China, in 1978. She received the B.S. degree in Mechanical Engineering and Automation Science from Nanjing University of Aeronautics and Astronautics, Jiangsu, China, in 2000, and M.E. degrees in Traffic Information Engineering and Control from Shanghai Ship and Shipping Research Institute, Shanghai, China, in 2003, and the Ph.D. degree in Traffic Information Engineering and Control from Tongji University, Shanghai, China, in 2006.

Since 2006, she has been with the faculty of the School of Optical-Electrical and Computer Engineering, University of Shanghai for Science and Technology, Shanghai, China, where she is currently a Lecturer. She is also a post-doctoral researcher of Asia University, Taiwan. Her research interests include communication security, image processing, and information theory and coding.

Chin-Chen Chang received the B.S. degrees in Science in Applied Mathematics and M.S. degree in Science in computer and decision sciences. Both were awarded in National Tsing Hua University, Taiwan. He received his Ph.D. degree in computer engineering from National Chiao Tung University, Taiwan.

His current title is Chair Professor in Department of Information Engineering and Computer Science, Feng Chia University, from Feb. 2005. He is currently a Fellow of IEEE and a Fellow of IEE, UK. His current research interests include database design, computer cryptography, image compression and data structures.

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.

Ting-Feng Chung was born in Kaohsiung, Taiwan, in 1990. He received the B.S. degree in Applied Informatics and Multimedia from Asia University, Taichung, Taiwan, in 2012. He is currently working toward the M.S. degree in Information Engineering and Computer Science from Feng Chia University, Taichung, Taiwan. His research interests include Steganography and image processing.