Adjustment Hiding Method Based on Exploiting Modification Direction

Chin-Feng Lee[1], Chin-Chen Chang[2,3], Pei-Yan Pai[2], and Chia-Ming Liu[3]
(Corresponding author: Chin-Chen Chang)

Department of Information Management, Chaoyang University of Technology[1]
168, Jifeng E. Rd., Wufeng District, Taichung, 41349 Taiwan, R.O.C.
Department of Computer Science, National Tsing Hua University[2]
101, Section 2, Kuang-Fu Rd., Hsinchu, 30013, Taiwan, R.O.C.
Department of Information Engineering and Computer Science, Feng Chia University[3]
100, Wenhwa Rd., Seatwen, Taichung 40724, Taiwan, R.O.C
(Email: alan3c@gmail.com)

(Received Mar. 21, 2013; revised and accepted Nov. 6, 2013)

Abstract

In the exploiting modification direction (EMD) method, a secret digit in $(2\boldsymbol{n}+1)$-ary notational system is embedded into a group that is consisted of $\boldsymbol{n}$ pixels. Only one pixel in a group at most is being modified by either increasing or decreasing one. Therefore, the maximum embedding rate of EMD method is $(\log_2(2\boldsymbol{n}+1))/n$ when $\boldsymbol{n} \geqq 2$. In order to increase the embedding capacity of EMD method, a new adjustment data hiding method based on $\boldsymbol{c}^{\boldsymbol{n}}$-ary notational system is proposed in this paper. In the proposed method, at most $\boldsymbol{n}$ pixels in a group can be modified and each pixel has $\boldsymbol{c}$ different ways of modification. As the result, the maximal embedding rate of the proposed method is $\log_2 \boldsymbol{c}$. The experimental results demonstrated that the proposed method provides a higher embedding capacity than the compared methods and a satisfied image quality of stego-image. The proposed method provides an average 1~4.75 bits per pixel (bpp) and an average peak signal-to-noise rate (***PSNR***) of 51.14~30.30 dB with different $\boldsymbol{c}$. In addition, the proposed method also inherits the advantageous properties of EMD method: the computation efficiency and the ability to resist steganographic attack.

Keywords: Embedding capacity, embedding rate, image hiding, steganographic attack

1 Introduction

As the Internet has developed rapidly and became more and more popular, it is quite common for people to transmit the data to others via Internet. However, the illegal attackers can easily steal the data through the public Internet. Image hiding is one of the data security technologies to protect the secret data from illegal interception [1-2, 4-8, 10-12]. In the image hiding, the secret data is embedded into an image called cover image. Once the secret data are embedded, the cover image becomes a so-called "stego-image", and then the data becomes invisible for the illegal attacker. That is, illegal attackers should not be able to notice the existence of the embedded data, even though they have carefully analyzed the stego-image. Two important issues of image hiding are preserving good image quality and increasing the embedding capacity at the same time [4-5]. However, this is a trade-off problem. If we want to improve the image quality, we would have to sacrifice the embedding capacity, and vice versa.

In recent years, many image hiding methods have been proposed. Turner [9] presented a simple hiding method called least significant bit (LSB) replacement method. In the LSB replacement method, the binary secret bits are embedded into the LSBs of pixels in the cover image by replacement operation. The maximum embedding capacity is quite limited. However, the LSB replacement method cannot resist against the statistical analysis [3, 11]. Milikainen [7] proposed the LSB matching revisited method based on pixel pair to improve the security of LSB replacement method. The LSB matching revisited method can resist the statistical analysis, since it does not possess the asymmetric property of LSB replacement method [7]. However, maximum embedding capacity of the LSB matching revisited method is not raised same with the LSB replacement method. Chang *et al.* [2] introduced a new image hiding method based on discrete cosine transform (DCT). In Chang *et al.*'s method, the cover image is first converted into frequency domain. After that, the secret data are embedded into the coefficients of the medium frequency. The embedding capacity of Chang *et al.*'s method is low since only a few coefficients can carry the secret data. In addition, Chang *et al.*'s method needs complicated computations to transform the cover image into the frequency domain and the stego-image into its spatial domain.

Zhang *et al.* [12] proposed a new data hiding method based on exploiting modification direction (EMD) method, called EMD method. The binary secret bits are converted

into a sequence of secret digits in a (2n+1)-ary notational system and a group with n pixels used to carry one secret digit. In the EMD method, only one pixel at most in a group is increased or decreased by one. Accordingly, the EMD method provides a high image quality but the theoretical maximum embedding rate of EMD method is only about 1.16 bits per pixel (bpp) when n=2. In practical experiment, the embedding rate for the EMD method reaches only 1 bpp at the base 5 of numerical system. Moreover, the embedding rate of the EMD method decreases along with an increase of n. Lee *et al*. [5] improved the EMD method based on pixel segmentation strategy. Lee *et al.*'s method can produce an embedding capacity 1.7 times more than that of EMD method, but the average peak signal-to-noise rate (***PSNR***) of Lee *et al.*'s method decreased 8 dB more than EMD method. The EMD-2 method is proposed to improve the EMD method by Kim *et al*. [4]. The EMD-2 method allows only two pixels at most in a group of n pixels are modified by increasing one or decreasing one. The EMD-2 method can provide 1.58 bpp and similar image quality of EMD method when n=2.

In this paper, an adjustable image hiding method for improving the EMD-based methods is proposed. In this method, the binary secret bits are firstly converted into a sequence of secret digits in c^n-ary notational system. After that, a group with n pixels is used to embed a secret digit, and n pixels are modified at most with c different ways of modification. With various c values, the proposed method can provide an average of 1~4.75 bpp and an average ***PSNR*** of 51.14~30.3 dB, which means the embedding capacity can be adjusted depending on the requirements of application. In addition, the proposed method also inherits the advantages of EMD method: the computation efficiency and the ability to resist steganographic attack [4-5]. The experimental results have demonstrated that the proposed method provides a higher embedding capacity while satisfying image quality of stego-image than the compared methods.

The rest of this paper is organized as follows. In Section 2, we review the EMD method. Then, in Section 3, we introduce the proposed method including embedding and extracting procedures for gray-level images. In Section 4, we make comparisons of embedding rate R and stego-image quality between the proposed method and other related methods. Finally, we will provide a conclusion of our work in Section 5.

2 The EMD Embedding Method

Zhang *et al.* [12] presented a new image hiding method, which is called exploiting modification direction (EMD) method. In this method, the secret message is converted into a sequence of binary bit streams. The secret bits are divided into N pieces with L bits, and each secret piece is presented as a decimal value by D digital numbers in a (2n+1)-ary notational system, where

$$\begin{aligned} L &= \lfloor D \times \log_2(2n+1) \rfloor, \\ N &= \left\lceil \frac{\text{Secret bits length}}{L} \right\rceil, \end{aligned} \tag{1}$$

n is a parameter to determine how many pixels of cover image are used to hide one secret digit.

In the embedding phase, EMD method firstly uses pseudo-random generator to permute all pixels of cover image according to a secret key. After that, EMD method partitions the permuted pixels into a series of groups. The group is denoted as a vector G_n=(g_1, g_2, …, g_n), which is consisted of n cover pixels. A weight vector W_n=(w_1, w_2, …, w_n)=(1, 2, …, n) is defined. Therefore, the EMD method defines an embedding function f as weighted sum function modulo (2n+1) for each group, a secret digit d can be carried by the n cover pixels, and at most one pixel is increased or decreased by one. f can be expressed as Equation (2):

$$f(g_1, g_2, \ldots, g_n) = \left[\sum_{i=1}^{n} (g_i \times w_i) \right] \bmod (2n+1) \tag{2}$$

After embedding a secret digit d in the group G_n, G_n is modified into $G_n' = (g_1', g_2', \ldots, g_n')$, which is defined according to following conditions:

1. $G_n' = (g_1', g_2', \ldots, g_n') = (g_1, g_2, \ldots, g_n)$, if d=f.
2. When $d \neq f$, computes s=d-f mod (2n+1) and $g_i' = \begin{cases} g_i, & \text{if } i \neq s \\ g_i + 1, & \text{if } i = s \end{cases}$, and $s \leq n$, for $i = 1, 2, ..., n$.
3. Otherwise, $g_i' = \begin{cases} g_i, & \text{if } i \neq 2n+1-s \\ g_i - 1, & \text{if } i = 2n+1-s \end{cases}$, and $s > n$, for $i = 1, 2, ..., n$

From the above properties, the EMD method allows only one pixel value to be modified in a group, or none of the pixel values in the group to be modified. That means, one pixel is either increased or decreased by one; otherwise, all the pixels in the group get no modification at all. Thus, we can generate a corresponding table by the above embedding strategy to modify the pixel value while the secret digit is embedded in the G_n. Table 1 demonstrates the corresponding table with n=3 in EMD.

For example, let a secret digit d be 2, n be 3, G_n=(3, 1, 5), so that the f is computed as (3×1+1×2+5×3) mod 7=6 and s=(2-6) mod 7=3. Since s=3 is less than n=3, g_3 is increased by one, and it is corresponded to Case 2 (see Table 1). Therefore, G_3' is calculated as (3+0, 1+0, 5+1)=(3, 1, 6) with the secret digit d=2 embedded.

In the extracting phase, the secret digit can be extracted from stego-group $G_n' = (g_1', g_2', \ldots, g_n')$ by the following extraction function shown as Equation (3).

$$f(g_1', g_2', \ldots, g_n') = \left[\sum_{i=1}^{n} (g_i' \times w_i) \right] \bmod (2n+1). \tag{3}$$

Table 1: The corresponding table with n=3 in the EMD method

i / W_3 / Case	1	2	3
	1	2	3
Case 1	0	0	0
Case 2	0	0	+1
Case 3	0	0	-1
Case 4	0	+1	0
Case 5	0	-1	0
Case 6	+1	0	0
Case 7	-1	0	0

Table 2: A mapping corresponding to the minimum modification vector with n=3, c=2 and k in the proposed method ($W_{3,2}$={2^0, 2^1, 2^2})

$W_{3,2}$ / MV / Case	$w_1=2^0$	$w_2=2^1$	$w_3=2^2$	k
	mv_1	mv_2	mv_3	
Case 1	0	0	0	0
Case 2	0	0	+1	4
Case 3	0	+1	0	2
Case 4	0	+1	+1	6
Case 5	+1	0	0	1
Case 6	+1	0	+1	5
Case 7	+1	+1	0	3
Case 8	+1	+1	+1	7

Table 3: The corresponding mapping with n=2, c=4 in the proposed method ($W_{2,4}$={4^0, 4^1})

$W_{2,4}$ / MV / Case	$w_1=4^0$	$w_2=4^1$	k
	mv_1	mv_2	
Case 1	0	0	0
Case 2	0	+1	4
Case 3	0	-1	12
Case 4	0	+2	8
Case 5	+1	0	1
Case 6	+1	+1	5
Case 7	+1	-1	13
Case 8	+1	+2	9
Case 9	-1	0	15
Case 10	-1	+1	3
Case 11	-1	-1	11
Case 12	-1	+2	7
Case 13	+2	0	2
Case 14	+2	+1	6
Case 15	+2	-1	14
Case 16	+2	+2	10

The EMD method provides a good quality of stego-image with an average ***PSNR*** value of more than 51 dB, and the theoretical maximal embedded rate $R=\frac{\log_2(2n+1)}{n}$ of EMD method is 1.16 bpp for the best case n=2.

3 Proposed Method

In this section, the proposed data hiding method is introduced in detail. The proposed method is consisted of embedding and extracting procedures. In the embedding procedure, the secret digits are embedded into a c^n-ary notational system in a group of pixels with c as a constant parameter, which implies there will be c status for a pixel to be changed for embedding a secret digit. In the extracting procedure, the secret data can be completely extracted from the stego-image. In a group of the proposed method, at most n pixels need to be modified, and each pixel has c modifications.

3.1 Embedding Procedure

Let S be a series of binary secret data and I be a gray-level image of $W\times H$ pixels. S is divided into N pieces with L bits and each secret piece is converted into a secret digit d based on c^n-ary notational system. The proposed method

firstly selects a key α to pseudo-randomly permute all pixels in I. After that, the proposed method partitions the permuted pixels into a series of groups. Each group contains n permuted pixels and is denoted as a vector, $G_n=(g_1, g_2, \ldots, g_n)$. In EMD method, only one pixel is changed at most by either increasing or decreasing one; otherwise, no modification is needed. The modification interval for a pixel to carry secret digit in the EMD method is [-1, 1], which narrows the interval's limit on the embedding capacity. In order to improve the capacity, the proposed method allows at most n pixels can be modified and the number of modifications for each cover pixel is c. Hence, the modification interval of the pixel in the proposed method is $[-\lceil 0.5\times(c-1)\rceil+1, \lceil 0.5\times(c-1)\rceil]$ where c is even; otherwise, the minimum modification interval of the pixel is $[-\lceil 0.5\times(c-1)\rceil, \lceil 0.5\times(c-1)\rceil]$ if c is odd.

In the proposed method, the weight vector is defined as $W_{n,c}=(w_1, w_2,\ldots, w_n)=(c^0, c^1,\ldots, c^{n-1})$. For example, let n and c be 3 and 2, respectively, so that $W_{3,2}=(2^0, 2^1, 2^2)=(1, 2, 4)$ and the minimum modification interval is [0, 1]. Similarly, when n and c are given as 2 and 4, the weight vector and modification interval are $W_{2,4}=(4^0, 4^1)=(1, 4)$ and [-1, 2], respectively. Therefore, when n and c are given, the proposed method generates a minimum modification interval which then creates a minimum modification vector MV. Accordingly, a modulus function k as shown in Equation (4) is formulated. The function is a kind of a mapping which transforms an n-dimensional vector to a value k within the range from zero to (c^n-1), and it can also be observed by a corresponding mapping with possible c^n combinations of pixel changes. Tables 2 and 3 display the corresponding mappings with n=3, c=2 and n=2, c=4, respectively, while k is calculated as follows: Let each row in the Table 2 be a vector, which is denoted as a minimum modification vector $MV=(mv_1, mv_2,\ldots, mv_n)$. Then, the k is formulated as:

$$k=\left(\sum_{i=1}^{n} mv_i \times w_i\right) \bmod c^n \tag{4}$$

Let us consider the case with n and c set as 3 and 2, respectively. $W_{3,2}$ and MV are given as (1, 2, 4) and (0, 1, 1) (see Table 2). Note that k is computed as 6 = (0×1+1×2+1×4) mod 2^3. For the second case, k is 4 as generated by (0×1+0×2+1×4) mod 2^3.

Thus, the new embedding function f_c is used as weighted sum function for modulo c^n for each group, and f_c can be calculated as follows:

$$f_c(g_1, g_2, \ldots, g_n)=\left[\sum_{i=1}^{n}(g_i \cdot w_i)\right] \bmod c^n \tag{5}$$

The modified pixel value vector G_n' can be computed by Equation (6):

$$G_n' = G_n + MV_t, \tag{6}$$

where

$$t=(d-f_c) \bmod c^n, \tag{7}$$

and MV_t is the minimum modification vector for $k = t$ associated with the parameters c and n.

After embedding phase, if the modified pixel value g_i' is less than 0 or more than 255, then the pixel will be in underflow and overflow situations. To solve the underflow fand overflow problems, the new modified pixel value g_i'' is calculated with Equation (8):

$$G_n''(g_1'', g_2'', \ldots, g_n'')=\begin{cases} g_i''=255-Max, & \text{if } g_i''>255 \\ g_i''=0-Min, & \text{if } g_i''<0 \\ g_i''=g_i, & \text{otherwise} \end{cases}, \tag{8}$$

where Max and Min are the maximal and minimal values in the modification interval, respectively. After that, G_n'' is used to embed the secret digit using Equations (5~8). After all secret digits are embedded, the modified pixels are pseudo-randomly re-permuted using the same key α to generate the stego-image I'.The embedding steps of our proposed method are summarized as follows:

Step 1. Calculate f_c value with G_n according to Equation (5).

Step 2. If $d \neq f_c$, compute the value t using Equation (7). Otherwise, go to Step 6.

Step 3. Find the minimum modification vector MV_t, and compute the modified pixel value vector G_n' by Equation (6).

Step 4. Check G_n' whether the underflow or overflow occurs. If G_n' is showing underflow or overflow, go to Step 5. Otherwise, go to Step 6.

Step 5. Calculate G_n'' according to Equation (8), and reset G_n as $G_n = G_n''$.

Step 6. Read next G_n and d, and go to Step 1 until all secret digits are embedded.

Figure 1 displays the flowchart of embedding procedure in our proposed method. We use the following two examples to demonstrate how to embed a secret digital d into a group G_n with and without underflow/overflow in the embedding procedure of proposed method.

Example 1. Assume that n and c are equal to 3 and 2, respectively. Therefore, $W_{3,2}$ is (1, 2, 4). A group G_3 with three cover pixels is given as (200, 203, 208). The to-be-embedded secret bit stream $S=101_2$ is converted into a secret digit d =5 such as d=5 mod 2^3 in a 2^3-ary notational system.

Step 1. Compute f_c value with the G_3 according to Equation (5). In this case, f_c value is 6 because f_c = (200×1+203×2+208×4) mod 2^3=6.

Step 2. Since (d=5)≠(f_c=6), the value of t is set as 7 using Equation (7) (i.e. t =(5-6) mod 2^3=7).

Step 3. For the value t=7, n =3 and c=2, we can derive the corresponding modification vector MV_7 =(1,

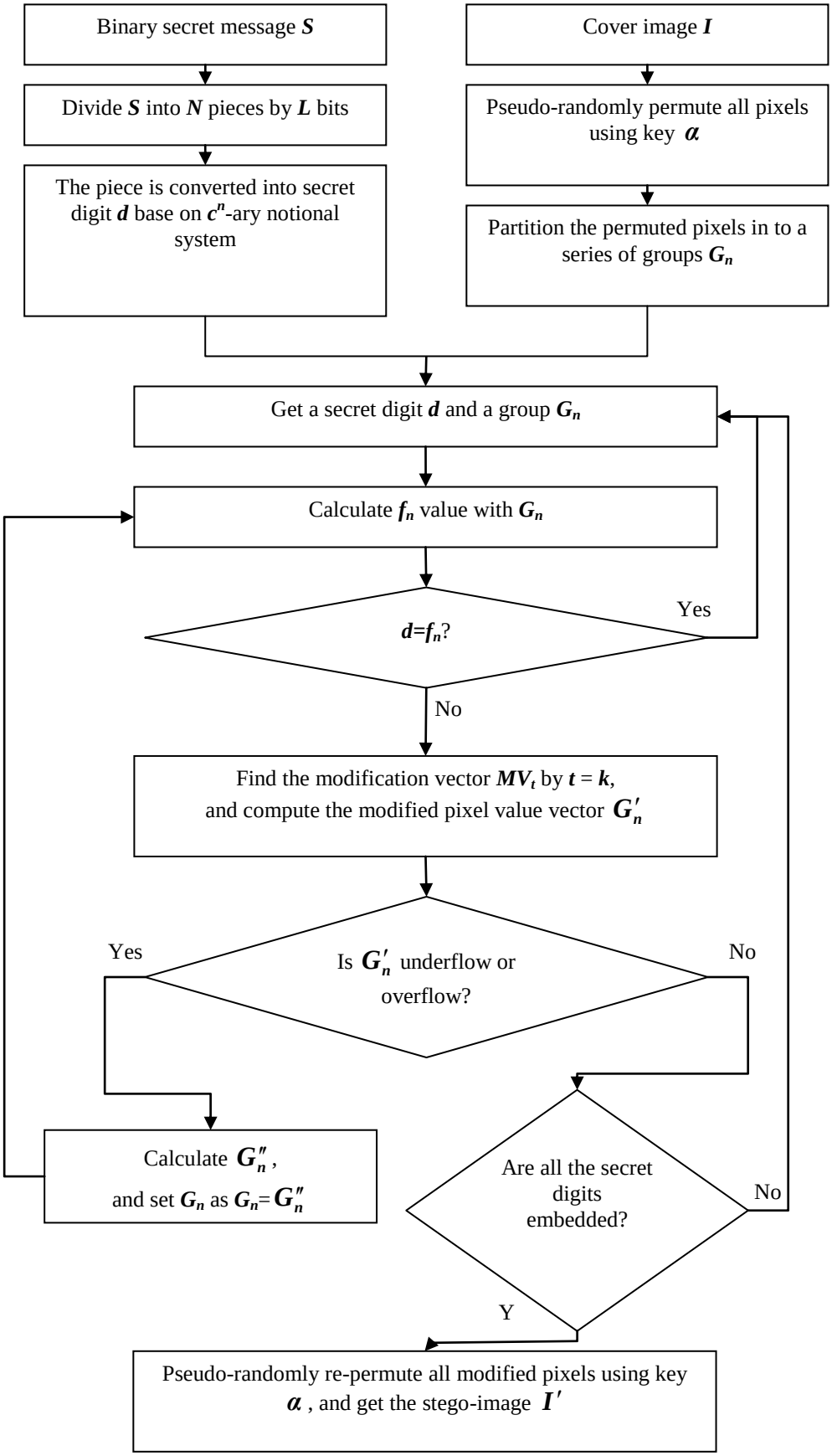


Figure 1: Flowchart of embedding procedure in our proposed method.

1, 1) for k=t=7, could be derived from $t = \left\lfloor \sum_{i=1}^{n} (mv_i \times w_i) \right\rfloor \bmod c^n$ for i=1, 2 and 3. Namely, 7=(1×2^0+1×2^1+1×2^2) mod 2^3. From Table 2, the minimum modification vector MV_7 for the 8th case with (1, 1, 1) is also obtained. Then, according to Equation (6), the modified pixel value vector G_3' turns to (201, 204, 209) (i.e. $G_3' = (200+1, 203+1, 208+1) = (201, 204, 209)$).

Example 2. Let n and c be 2 and 4, respectively. The G_2 is given as (255, 255), and $W_{2,4}$ is given as (1, 4). S=1000_2 is converted into a secret digit d=8 (i.e. d=8 mod 4^2=8) in a 4^2-ary notational system.

Step 1. Compute f_c value with G_2 according to Equation (5). In this case, the value of f_c is 11 because f_c = (255×1+255×4) mod 4^2=11.

Step 2. Since d is smaller than f_c (i.e. 8 < 11), the value of t is 13 from Equation (7) (i.e., 13= (8-11) mod 4^2=(1×4^0+(-1)×4^1) mod 4^2). We also can look up Table 3 and find the corresponding minimum modification vector MV_{13} for k=t=13, which is the two-element vector (1, -1). Thus, according to Equation (6), the modified pixel value vector G_2' is set as (256, 254) by G_2'=(255+1, 255-1)=(256, 254).

Step 3. Since g_1' is overflow now, it should be adjusted such that the secret digit can be embedded. In this case, the maximal value in the modification interval=[-1, 2] is 2; so G_2 is modified into G_2''=(255-2, 255)=(253, 355) using Equation (8). After that, G_2 is set as G_2''.

Step 4. Re-computer f_c value with the G_2. According to Equation (5), f_c equals 9 (i.e. f_c = (253×1+255×4) mod 4^2=9).

Step 5. Since d=8 is smaller than f_c=9, the value of t is 15 from Equation (7) (i.e. t= (8-9) mod 4^2=15).

Step 6. The corresponding modification vector MV_{15} is given as (-1, 0) such that k=t=15=((-1)×4^0+0×4^1) mod 4^2. Therefore, the modified pixel value vector G_2' is modified to (253, 255) (i.e. G_2'=(253-1, 255+0)=(253, 255)).

3.2 Extracting Procedure

Same as the embedding procedure, all the pixels of stego-image I' are pseudo-randomly permuted using key α. After that, the permuted pixels are partitioned into a series of groups, where each group G_n' contains n permuted pixels such as $G_n' = (g_1', g_2', \ldots, g_n')$. The secret digit d can be extracted from G_n' by extracted function f_c'. The extracted function f_c' is defined as follows:

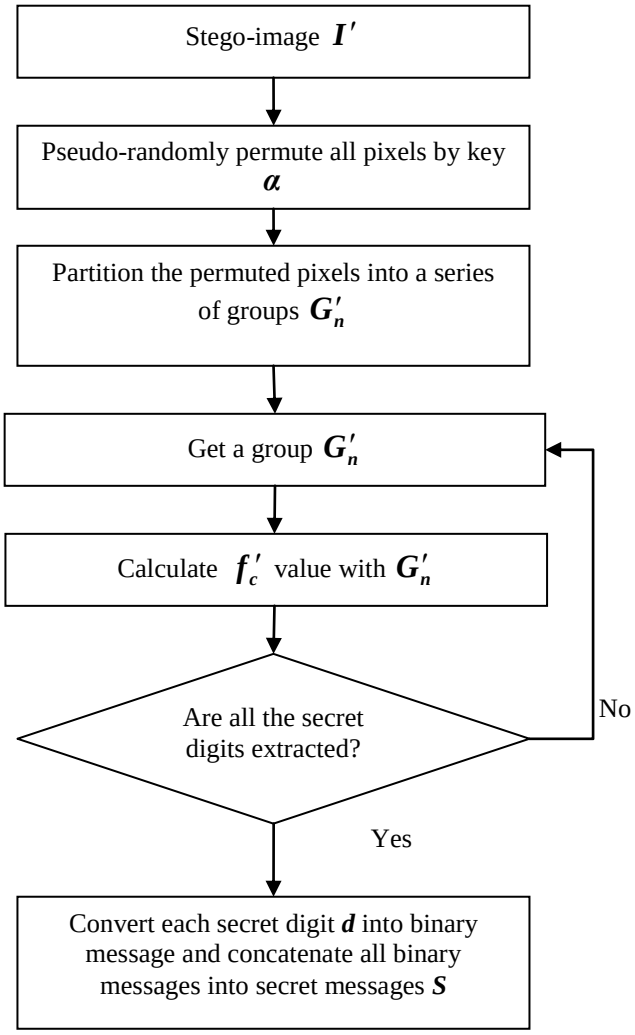


Figure 2: Flowchart of extracting procedure in our proposed method

The value of f_c' is equal to the secret digit d. While all secret digits are being extracted, all the binary messages are concatenated to recover the secret message S. Figure 2 shows the flowchart of extracting procedure in our proposed method.

Example 3 illustrates how to extract a secret digit d from a group G_n' below.

Example 3. Assume that n and c equal to 3 and 2, respectively. G_3' is given as (201, 204, 209), and $W_{3,2}$ is (1, 2, 4). According to Equation (9), the secret digit d is calculated as d= f_c' =(201×1+204×2+209×4) mod 2^3=5, and the secret message S=101_2 is in its binary representation.

4 Experimental Result

The aim of this section is to investigate the performance of the proposed method and to compare it with Wang *et al.*'s method [10], EMD-2 method [4], Lee *et al.*'s method [5],

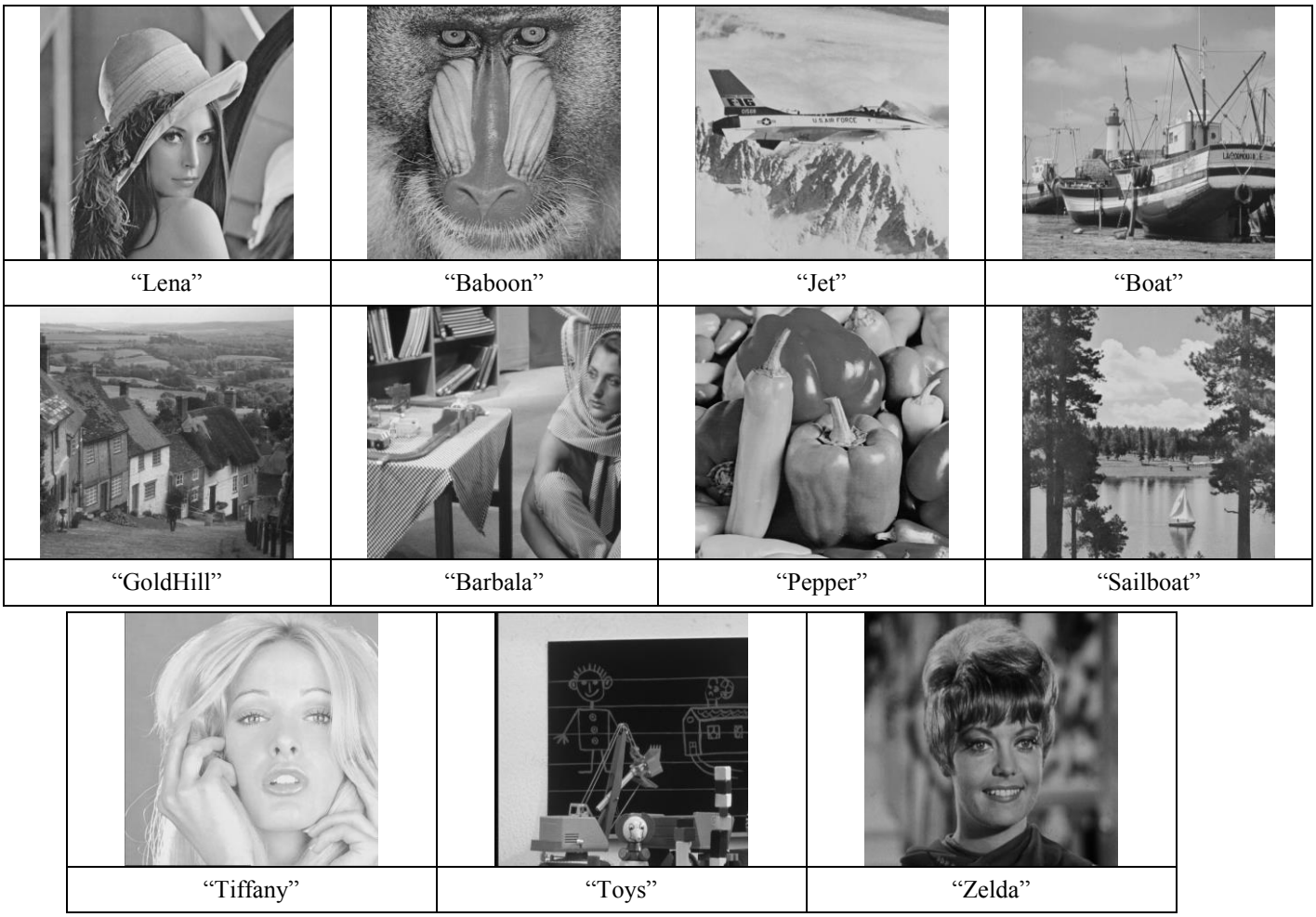


Figure 3: The test images

Lee *et al.*'s method [6], and EMD [12]. In the experiments, the gray-level images with size of 512×512 "Lena", "Baboon", "Jet", "Boat", "GoldHill", "Barbala", "Pepper", "Sailboat", "Tiffany", "Toys", and "Zelda" are used as test images shown in Figure 3.

The peak signal to noise ratio (***PSNR***) [4] is used to evaluate the image quality. The ***PSNR*** is defined as follows:

$$\boldsymbol{PSNR} = 10 \times \log_{10} \frac{255}{\boldsymbol{MSE}} \text{dB}, \tag{10}$$

MSE is the mean squared error and is computed as follows:

$$\boldsymbol{MSE} = \frac{1}{\boldsymbol{H} \times \boldsymbol{W}} \times \sum_{i=1}^{\boldsymbol{H}} \sum_{j=1}^{\boldsymbol{W}} (\boldsymbol{x}_{ij} - \bar{\boldsymbol{x}}_{ij})^2, \tag{11}$$

where $\boldsymbol{H}$ and $\boldsymbol{W}$ are the height and width of image, respectively; $\boldsymbol{x}_{ij}$ is the original pixel value at coordinate $(\boldsymbol{i}, \boldsymbol{j})$, and $\bar{\boldsymbol{x}}_{ij}$ is the modified pixel value at coordinate $(\boldsymbol{i}, \boldsymbol{j})$. The embedding rate (***R***) is employed to calculate the number of secret bits carried by one pixel. The embedding rate is formulated as

$$\boldsymbol{R} = \frac{\text{The number of embedding bits}}{\boldsymbol{H} \times \boldsymbol{W}} (\text{bpp}). \tag{12}$$

4.1 Parameter Selection

The first experiment investigates two parameters $\boldsymbol{n}$ and $\boldsymbol{c}$ to observe how the parameters affect embedding performance. Table 4 presents the embedding capacity and the image quality of proposed method with different $\boldsymbol{n}$ and $\boldsymbol{c}$ for image "Lena." By Table 4, results showed that only the parameter $\boldsymbol{c}$ controls the embedding capacity and the image quality. When $\boldsymbol{c}$ is increasing, the embedded rate will increase and the ***PSNR*** of stego-image will decrease. The theoretical embedding rate $\boldsymbol{R}$ of the proposed method is presented as the following equation, and it shows that the embedding capacity depends on the parameter $\boldsymbol{c}$.

$$\boldsymbol{R} = (\log_2 \boldsymbol{c}^{\boldsymbol{n}}) / \boldsymbol{n} = [\boldsymbol{n} \cdot (\log_2 \boldsymbol{c})] / \boldsymbol{n} = \log_2 \boldsymbol{c}. \tag{13}$$

Accordingly, the embedding capacity of our proposed method determined by the parameter $\boldsymbol{c}$ is scalable. The adjusted parameter $\boldsymbol{c}$ provides the proposed method the flexibility in both embedding capacity and image visual quality.

Table 4: The ***PSNR*** and ***R*** of the proposed method with different ***c*** and ***n*** for "Lena"

n \ ***c***	***c***=2		***c***=3		***c***=4		***c***=5		***c***=6	
	PSNR (dB)	***R*** (bpp)	***PSNR*** (dB)	***R*** (bpp)	***PSNR*** (dB)	***R*** (bpp)	***PSNR*** (dB)	***R*** (bpp)	***PSNR*** (dB)	***R*** (bpp)
n=2	51.14	1.00	49.90	1.58	46.38	2.00	45.13	2.32	43.14	2.58
n=3	51.13	1.00	49.90	1.58	46.36	2.00	45.12	2.32	43.10	2.58
n=4	51.14	1.00	49.88	1.58	46.38	2.00	45.12	2.32	43.12	2.58
n=5	51.15	1.00	49.89	1.58	46.38	2.00	45.11	2.32	43.13	2.58
n=6	51.14	1.00	49.89	1.58	46.37	2.00	45.12	2.32	43.12	2.58
n=7	51.14	1.00	49.89	1.58	46.36	2.00	45.11	2.32	43.13	2.58

Table 5: The ***PSNR*** and ***R*** of the proposed method with different ***c*** and ***n***=2

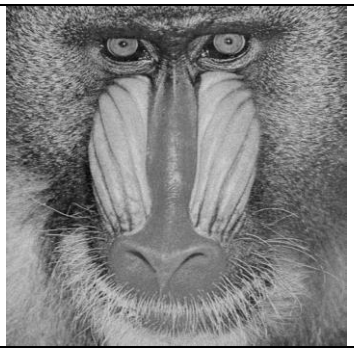
Image \ ***c***	***c***=2		***c***=3		***c***=4		***c***=27		***c***=28	
	PSNR (dB)	***R*** (bpp)	***PSNR*** (dB)	***R*** (bpp)	***PSNR*** (dB)	***R*** (bpp)	***PSNR*** (dB)	***R*** (bpp)	***PSNR*** (dB)	***R*** (bpp)
Lena	51.14	1.00	49.88	1.58	46.38	2.00	30.29	4.75	29.97	4.81
Baboon	51.14	1.00	49.89	1.58	46.35	2.00	30.30	4.75	29.98	4.81
Jet	51.14	1.00	49.89	1.58	46.36	2.00	30.32	4.75	29.99	4.81
GoldHill	51.14	1.00	49.89	1.58	46.36	2.00	30.28	4.75	29.96	4.81
Boat	51.14	1.00	49.90	1.58	46.36	2.00	30.30	4.75	29.96	4.81
Barbala	51.15	1.00	49.89	1.58	46.37	2.00	30.30	4.75	29.99	4.81
Pepper	51.13	1.00	49.89	1.58	46.36	2.00	30.31	4.75	29.98	4.81
Sailboat	51.14	1.00	49.89	1.58	46.35	2.00	30.30	4.75	29.98	4.81
Tiffany	51.14	1.00	49.89	1.58	46.35	2.00	30.20	4.75	29.98	4.81
Toys	51.13	1.00	49.88	1.58	46.36	2.00	30.31	4.75	29.98	4.81
Zelda	51.14	1.00	49.88	1.58	46.36	2.00	30.30	4.75	29.98	4.81

"Lena"		"Baboon"		"Jet"	
PSNR	51.14 dB	***PSNR***	51.14 dB	***PSNR***	51.14 dB
R	1 bpp	***R***	1 bpp	***R***	1 bpp
Capacity	262144 bits	Capacity	262144 bits	Capacity	262144 bits

"Boat"		"GoldHill"	
PSNR	51.14 dB	***PSNR***	51.14 dB
R	1 bpp	***R***	1 bpp
Capacity	262144 bits	Capacity	262144 bits

Figure 4: The ***PSNR***, ***R***, and embedding capacity of the proposed method(***n***=2, ***c***=2).

"Lena"	
PSNR	30.29 dB
R	4.75 bpp
Capacity	1245184 bits



"Baboon"	
PSNR	30.30 dB
R	4.75 bpp
Capacity	1245184 bits

"Jet"	
PSNR	30.32 dB
R	4.75 bpp
Capacity	1245184 bits

"Boat"	
PSNR	30.30 dB
R	4.75 bpp
Capacity	1245184 bits

"GoldHill"	
PSNR	30.28 dB
R	4.75 bpp
Capacity	1245184 bits

Figure 5: The ***PSNR***, ***R***, and embedding capacity of the proposed method (***n***=2, ***c***=27).

4.2 Embedding Rate versus Image Distortion in the Proposed Method

Since the parameter ***c*** dominates the embedding rate, the second experiment will focus on analyzing the embedded rate of the proposed method. Table 5 shows the ***PSNR*** and ***R*** of the proposed method with different ***c*** when ***n***=2 for the test images. Table 5 indicates that the proposed method can provide average values of ***PSNR*** at 51.14 dB~30.30 dB and average embedding rates at 1.00~4.75 bpp with different ***c***=2~27. However, it is difficult for human eyes to discriminate the difference between the original image and the stego-image when ***PSNR*** exceeds 30 dB. Therefore, the image quality of the proposed method with ***c***=27 is satisfied. In addition, the proposed method provides various image qualities and embedding capacities by adjusting ***c***, according to user application requirements. Figures 4 and 5 display the ***PSNR***, ***R***, and embedding capacity of the proposed method with ***n***=2, ***c***=2, and ***n***=2, ***c***=27 for a subset of test images, respectively with smooth images "Lena" and "Jet" and some are complex like "Baboon," "Boat", and "GoldHill."

4.3 Embedding Capacity versus Image Distortion for Related Methods

The third experiment was designed to compare the performance of the proposed method with those of the other image hiding methods based on the EMD method with similar conditions, including Wang *et al.*'s method [10], Lee *et al.*'s method [5], Lee *et al.*'s method [6], EMD-2 method [4], and EMD [12]. Table 6 shows the performances of the proposed method and the compared methods for the test images. In Wang *et al.*'s method, ***K*** is the parameter to control the capacity and image quality of stego-image. In this experiment, the average values of ***PSNR*** and ***R*** in Wang *et al.*'s method are 46.89 dB and 1.13 bpp while ***K*** is 1, respectively. In addition, when ***K*** is set to 70, Wang *et al.*'s method can provide an average ***PSNR*** value of 45.16 dB and embedding rate ***R*** of 1.99 bpp. In Lee *et al.*'s method, it keeps $(16 - p_m)$ most significant bits of a pixel-pair unchanged while altering p_m least significant bits to indicate the virtual modifications on a ***m***-dimensional pseudo-random vectors for carrying the secret data, where $m = 2^{p_m - 1} - 1$. The average values of ***PSNR*** and ***R*** in Lee *et al.*'s method [5] are 46.89 dB and 1.13 bpp when p_m is 4 and ***m*** is 7, respectively. However, Table 4 indicates that the ***PSNR*** and ***R*** of the proposed method are superior to that of Wang *et al.*'s [10] and Lee *et al.*'s methods [5]. Under similar conditions, the proposed method supplies the same ***PSNR*** and ***R*** with the EMD-2 method. However, the maximal embedding rate of the

Table 6: The performances of the proposed method and the compared methods

Method	Parameter	Measure	Lena	Baboon	Jet	GoldHill	Boat
Proposed method	n=2, c=3	***PSNR***(dB)	49.88	49.89	49.89	49.89	49.90
		R(bpp)	1.58	1.58	1.58	1.58	1.58
	n=2, c=4	***PSNR***(dB)	46.38	46.35	46.36	46.36	46.36
		R(bpp)	2.00	2.00	2.00	2.00	2.00
Wang *et al.*'s method[10]	K=1	***PSNR***(dB)	46.90	46.89	46.89	46.89	46.88
		R(bpp)	1.13	1.13	1.13	1.13	1.13
	K=70	***PSNR***(dB)	45.16	45.15	45.16	45.15	45.16
		R(bpp)	1.99	1.99	1.99	1.99	1.99
Lee *et al.*'s method[5]	m=7, p_m=4	***PSNR***(dB)	44.31	44.28	44.45	44.28	44.33
		R(bpp)	1.95	1.95	1.95	1.95	1.95
Lee *et al.*'s method[6]	n=4	***PSNR***(dB)	44.17	44.17	44.14	44.17	44.16
		R(bpp)	2.00	2.00	2.00	2.00	2.00
EMD-2 method[4]	n=2	***PSNR***(dB)	49.89	49.89	49.88	49.89	49.90
		R(bpp)	1.58	1.58	1.58	1.58	1.58
EMD method[12]	n=2	***PSNR***(dB)	52.11	52.13	52.12	52.09	52.08
		R(bpp)	1.16	1.16	1.16	1.16	1.16
LSB method[9]		***PSNR***(dB)	44.15	44.17	44.15	44.15	44.13
		R(bpp)	2	2	2	2	2

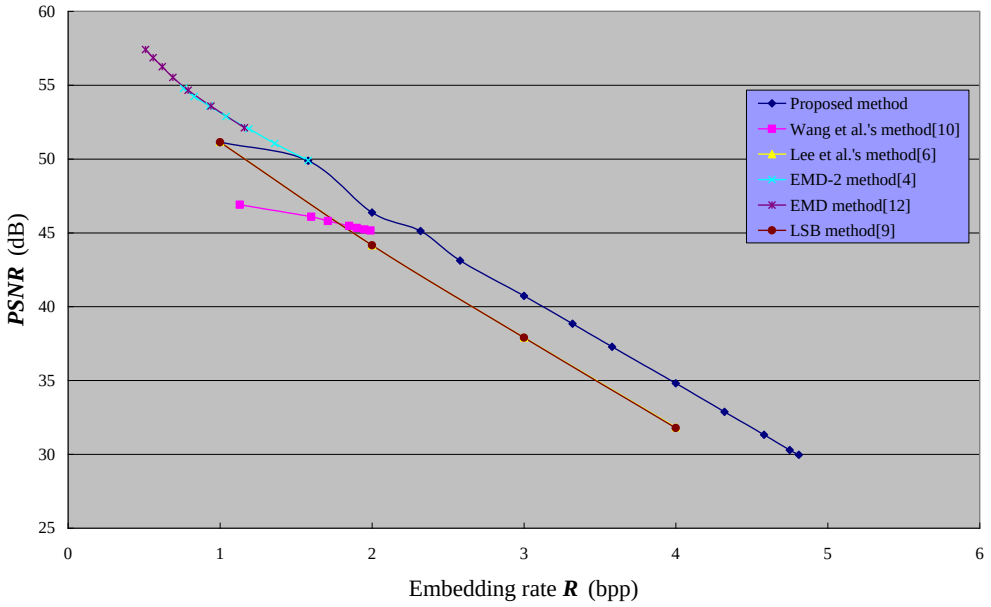


Figure 6: The performances of the proposed method and the compared methods for images "Lena"

proposed method (i.e. 4.75 bpp) is more than that of the EMD-2 method, which is 3.32 bpp and can be referred by [4]. Lee *et al.*'s method [6] develops a hiding method based on modulus function which provides the same performance as the LSB replacement method when compared using two criteria, namely visual quality and embedding capacity. Their average PSNR was 31.847 dB when the embedding rate was 4 bits for each gray-level pixel. Our proposed method is superior compared to the Lee *et al.*'s [6] and LSB replacement methods [9] with respect to visual quality and embedding capacity. From Table 6, when the embedding rate reaches 2 bpp, the PSNR value can be improved about 2.19 dB, which is 46.35-44.16, for the same capacity.

Figure 6 demonstrates the relationship between the ***PSNR*** and ***R*** for image "Lena" obtained by Wang *et al.*'s [10], Lee *et al.*'s [6], EMD-2 [4], EMD [12], LSB [9], and the proposed methods. The maximal embedding rate of Wang *et al.*'s method is close to 2 bpp and provides a ***PSNR*** value over 45 dB; Lee *et al.*'s and LSB methods provide a ***PSNR*** value of 31.78 dB when the maximal embedding rate is at 4 bpp. Although the EMD and EMD-2 methods generate a better image quality (i.e. over 50 dB), the maximal embedding rates of both methods can only achieve 1.16 and 1.58 bpp, respectively, which are not that high. Overall, the proposed method has shown the ability to provide the maximal embedding rate of 4.75 bpp and a good image quality than compared methods.

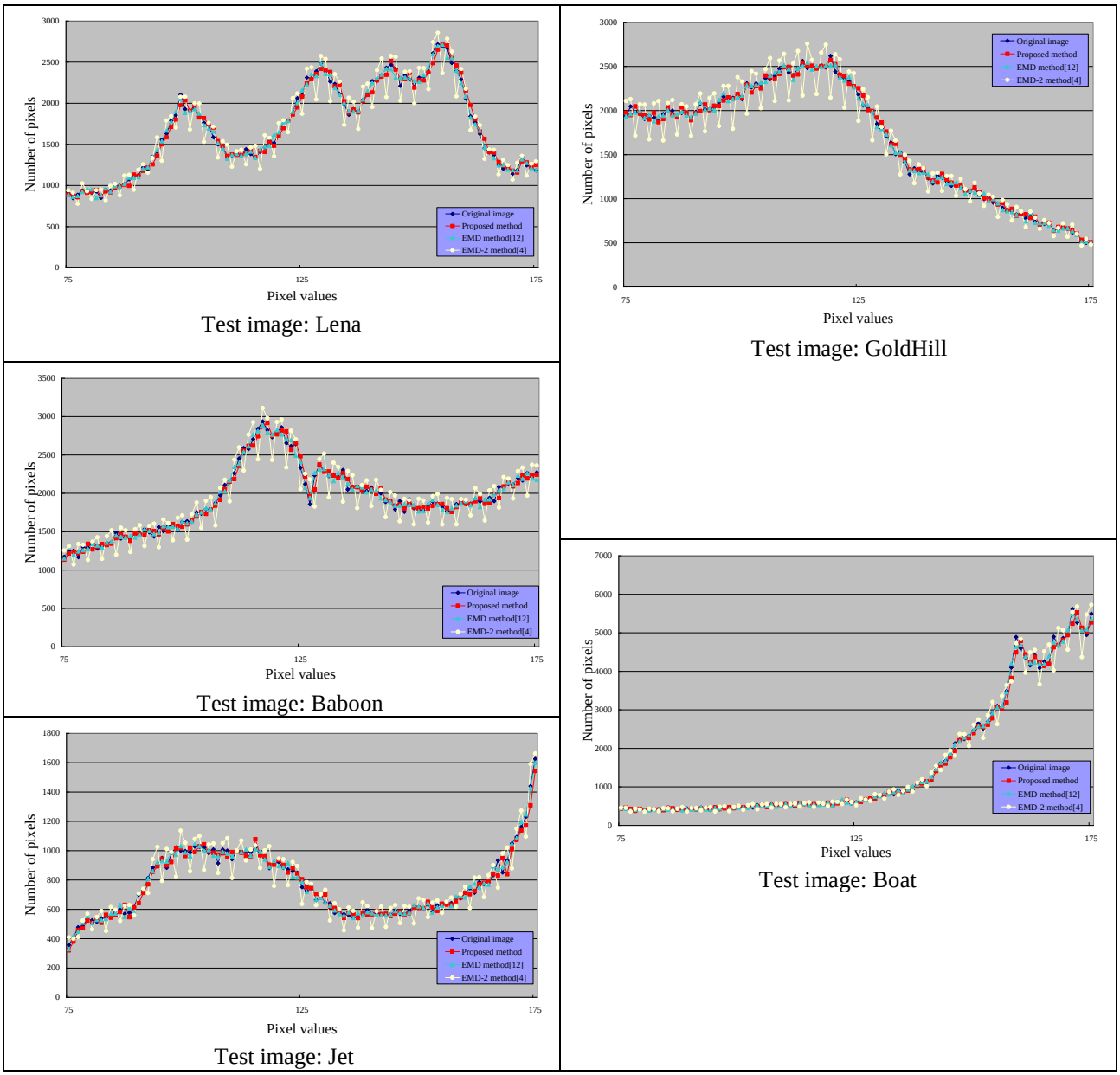


Figure 7: The histograms of the original test images and stego-images using the proposed, EDM, and EDM-2 methods

4.4 Imperceptibility Analysis for EMD-based Method

In the last experiment, in order to establish a fair comparison among the proposed method, EMD method, and EMD-2 method, we have embedded the same secret capacity into the test images "Lena," "Baboon," "Jet," "GoldHill", and "Boat." Figure 7 displays the pixel histograms of both original images and stego-images obtained by the proposed method, EMD method, and EMD-2 method in the test image. These histograms represent the frequency of pixel values between pixel values from 75 to 175. Also, comparing with our proposed method, EMD method and EMD-2 method, the curves of histogram in the proposed method and EMD method are both closer to that of the original image; this means that the less the modification made to the original image, the less the difference between the stego-image and original image. Compared with the original image histogram, minute differences are inevitable; therefore, the steganographic attack (i.e. statistic analysis) may be hardly detected.

5 Conclusion

The EMD method allows at most one pixel is modified in a group. Therefore, the maximal embedding rate of EMD method is 1.16 bpp when n is 2. To improve the embedding capacity of EMD method, a new high payload adjustment image hiding method is proposed in this paper. In the proposed method, n pixels in a group can be modified at most and each pixel has c different ways of modification. According to experimental results, the minimal and maximal embedding rates of our proposed method are 1 bpp and 4.75 bpp respectively with *PSNR* over 30 dB. As

the experiment results indicated, our proposed method provides a higher embedding rate and a better image quality of stego-image than the compared methods. Moreover, the proposed method can achieve certain degree of security with low computation. The users are granted the ability to adjust the embedding rate of the proposed method by using different *c* for various applications requirements.

References

[1] C. K. Chan and L. M. Cheng, "Hiding data in image by simple lsb substitution," *Pattern Recognition*, vol. 37, no. 3, pp. 469-474, 2004.

[2] C. C. Chang, C. C. Lin, C. S. Tseng, and W. L. Tai, "Reversible hiding in dct-based compressed images," *Information Sciences*, vol. 177, no. 13, pp. 2768-2786, 2007.

[3] S. Dumitrescu, X. Wu, and Z. Wang, "Detection of LSB steganography via sample pair analysis," *IEEE Transactions on Signal Processing*, vol. 51, no. 7, pp. 1995-2007, 2003.

[4] H. J. Kim, C. Kim, Y. Choi, S. Wang, and X. Zhang, "Improved modification direction method," *Computers & Mathematics with Applications*, vol. 60, no. 2, pp. 319-325, 2010.

[5] C. F. Lee, C. C. Chang, and K. H. Wang, "An improvement of EMD embedding method for large payloads by pixel segmentation strategy," *Image and Vision Computing*, vol. 26, no. 12, pp. 1670-1676, 2008.

[6] C. F. Lee and H. L. Chen, "A novel data hiding scheme based on modulus function," *Journal of Systems and Software*, vol. 83, no. 5, pp. 832-843, 2010.

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

[8] C. C. Thien and J. C. Lin, "A simple and high-hiding capacity method for hiding digit-by-digit data in images based on modulus function," *Pattern Recognition*, vol. 36, no. 12, pp. 2875-2881, 2003.

[9] L. F. Turner, "Digital data security system," *Patent IPN*, WO 89/08915, 1989.

[10] Z. H. Wang, T. D. Kieu, C. C. Chang, and M. C. Li, "A novel information concealing method based on exploiting modification direction," *Journal of Information Hiding and Multimedia Signal Processing*, vol. 1, no. 1, pp. 1-9, 2010.

[11] A. Westfeld and A. Pfitamann, "Attacks on steganographic systems," *Lecture Notes in Computer Science*, vol. 1768, pp. 61-76, 1999.

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

Chin-Feng Lee received Ph.D. degree in Computer Science and Information Engineering in 1998 from National Chung Cheng University in Taiwan. She is currently a professor in Department of Information Management at Chaoyang University of Technology, at Taichung. Her research interests include database design, data mining, image processing, and information hiding.

Chin-Chen Chang received his Ph.D. degree in computer engineering from National Chiao Tung University. He's 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. Professor Chang was an associate professor in Chiao Tung 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. 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 Youth Award of the R. O. C., 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., Chung-Shan Academic Publication Awards, Distinguished Research Awards of National Science Council of the R. O. C., Outstanding Scholarly Contribution Award of the International Institute for Advanced Studies in Systems Research and Cybernetics, Top Fifteen Scholars in Systems and Software Engineering of the Journal of Systems and Software, and so on. His current research interests include database design, computer cryptography, image compression and data structures.

Pei-Yan Pai received the B.S. degree in Department of Information Management from National Taichung Institute of Technology, Taichung, Taiwan, in 2002. He received the M.S. degree in Department of Information Management from Chao Yang University of Technology, Taichung, Taiwan, in 2007. In 2011, he obtained Ph.D. degree from the Department of Computer Science of National Tsing Hua University. His research interests include medical image analysis, pattern recognition and multimedia applications.

Chia-Ming Liu received the B.S. degree in 2009 and M.S degree in 2011 from Department of Information Engineering Computer Science of Feng Chia University, Taichung, Taiwan. His research interests include image processing and digital watermarking.