Applied Mathematics & Information Sciences Letters
An International Journal

http://dx.doi.org/10.12785/amisl/010305

Data hiding schemes based on the formal improved exploiting modification direction method

Wen-Chung Kuo[1,*], *Shao-Hung Kuo*[2] *and Yu-Chih Huang*[3]

[1]Department of Computer Science and Information Engineering, National Yunlin University of Science & Technology, Yunlin 640, Taiwan, R.O.C.
[2]Graduate School of Engineering Science and Technology Doctoral Program, National YunLin University of Science and Technology, Yunlin 640, Taiwan, R.O.C.
[3] Department of Information Management, Tainan University of Technology, Taiwan, R.O.C.

Received: 23 Mar. 2013, Revised: 27 Jul. 2013, Accepted: 29 Jul. 2013
Published online: 1 Sep. 2013

Abstract: Steganography is an important strategy in the field of data security. Its main purpose is to hide secret information by embedding it in a cover image. The quantity of data that can be hidden in a single cover image is also very important. Recently, a high capacity technique called Exploiting Modification Direction (EMD) data hiding was introduced by Zhang and Wang. In order to enhance embedding quality, Lee et al. proposed an improved scheme using the change data base method. However, both of these schemes use a fixed equation to calculate and store secret data, so if their encoding formula is disclosed, the secure data will be compromised. In this paper, we propose two kinds of weight-changing evaluation of the high capacity EMD data hiding strategy. The major contribution of these two proposed schemes are their embedding formulas can be made public; one of them uses the table checking method to change the weighting evaluation of the high capacity EMD data-hiding strategy, and the other uses formal high capacity EMD data hiding. Experimental results show that the proposed scheme not only retains high embedding capacity and stego image quality of the original scheme but is also more secure than the LWC-scheme.

Keywords: Cover image, Data hiding, Stego image, Steganography, Security.

1 Introduction

The internet has become part of daily life. However, many dangers are hidden behind the convenience of the internet; for instance, personal information can be intercepted during transmission, modified, and used illegally. The information must thus be secured. A possible method is stenographic data hiding. In general, an equation is used to hide secret messages inside of a cover image, called a stego image, which can be safely delivered to recipients.

Data hiding focuses not only on security and capacity, but also on imperceptibility and robustness. We focus on data security and data hiding capacity in this paper. Many data hiding methods have been proposed. Most data hiding techniques use the least significant bit (LSB) position to hide the secret information. In other words, the secret information is converted into a binary bit stream, which is injected into the LSB[2,5,6] .

Exploiting Modification Direction (EMD) was proposed by Zhang and Wang to increase the capacity of secret information in a cover image[7]. In the EMD method, only one of two pixels is modified. From a spatial point of view, the two pixels can only be in one of five states: shifted upward, downward, left, right, or not moved at all. Lee *t al.*'s[3] improved EMD is a technique that uses two pixels at a time, and gives both pixels a fixed evaluation value (LWC-scheme). However, there are concerns about the security of the LWC-scheme and Zhang-Wang's scheme; both use fixed evaluation values, so once their encryption techniques become public, the security will be compromised. In this paper, we propose two high capacity EMD data hiding techniques with changing evaluation values; the stego images remain secure even if formulas are made public. One of the proposed schemes uses table checking to change the weighting evaluation value in a high capacity EMD data

* Corresponding author e-mail: simonkuo@yuntech.edu.tw

hiding system. The other scheme uses a formal equation with eight pairs of weighting evaluation values.

The rest of this paper is organized as follows. In Section 2, we review the Zhang-Wang scheme[7] and the LWC scheme[3]. We introduce the two proposed high capacity EMD data hiding techniques with changing evaluation values in Section 3 and Section 4, respectively. We present the experimental results and compare them with the LWC-scheme in Section 5. Finally, the conclusion is given in Section 6.

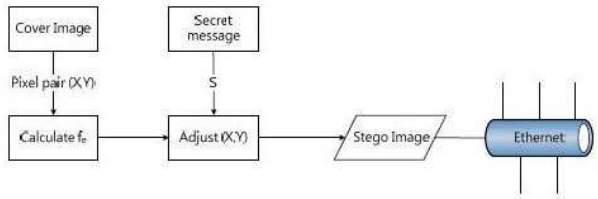

Fig. 1: Procedure of data hiding in [3]

2 Review of Data Hiding Technology based on EMD method

Many data hiding techniques have the problem of balancing image distortion and data hiding capacity. This problem was solved by Zhang and Wang's EMD data hiding theory which provides higher data capacity and higher PSNR (above 50dB). In this section, the Zhang-Wang scheme[7] and the LWC scheme[3] are discussed in detail.

2.1 EMD Data Hiding Scheme

The EMD method uses directional modification of data hiding. Secret information is injected into a group of cover image pixels as a series of binary codes, so the group has n pixels and the binary code is injected into $(2n+1)$-ary. During the EMD data hiding procedure, pixels of cover image are listed as $g_1, g_2, \ldots, g_n$, where n represents the number of pixels in a pixel group. Before the hiding procedure, the pixels are converted into a $(2n+1)$-ary structure; for instance, a group of $(1111101110010111)_2$ is converted into a $(30211412)_5$ 5-ary structure (two adjacent pixels are selected as a group). For the conversion and pixel group, we defined the extraction function as:

$$f(g_1, g_2, \ldots, g_n) = [\sum_{i=1}^{n} (g_i \cdot i)] \bmod (2n+1) \quad (1)$$

where g_i is the value of the pixel i and n is the number of pixels. For example, when i is equal to 2, two pixels, g_1 and g_2, are considered. Therefore, the extract function is $f(g_1, g_2) = 1 \times g_1 + 2 \times g_2 \bmod 5$. However, the EMD method has a drawback - the best hiding bit rate is in 5-ary. When n is increased, the number of pixels in a group increases, and the hiding bit rate decreases [7].

2.2 The Data Hiding Procedure with High Capacity EMD

Lee *et al.*[3] first converted secret data from the binary array to 8-ary, i.e., this changes the data hiding capacity from 1 bit to 3 bits. For pixels, they only use two adjacent pixels (e.g. X and Y) as well as the Zhang-Wang scheme. Let f_e be the extraction function that defines the weighting value using the value of the first pixel times 1 and using the value of the second pixel times 3. The two numbers are then summed and modulo 8 is performed to get a remainder which can be a reference pointer for the secret codes. This is different from the first EMD extraction function[**?**]The extraction function f_e and hiding procedure are shown in Eq.(2) and Fig.1, respectively.

$$f_e(X,Y) = (1 \times X + 3 \times Y) \bmod 8. \quad (2)$$

2.2.1 Embedding the Secrete Information s by Using High Capacity EMD

In the LWC-scheme, the high capacity EMD data hiding procedure can be divided into three steps as shown.

Step1.Pair up all the pixels in the cover image.
Step2.Substitute each pair of (X,Y) into Eq.(2)
Step3.Adjust (X,Y) such that the secret message by using following relationships:
(A1-1)Let $X' = X$ and $Y' = Y$, when $s = f_e(X,Y)$.
(A1-2)Let $X' = X+1$ and $Y' = Y$, when $s = f_e(X+1,Y)$.
(A1-3)Let $X' = X-1$ and $Y' = Y$, when $s = f_e(X-1,Y)$.
(A1-4)Let $X' = X$ and $Y' = Y+1$, when $s = f_e(X,Y+1)$.
(A1-5)Let $X' = X$ and $Y' = Y-1$, when $s = f_e(X,Y-1)$.
(A1-6)Let $X' = X+1$ and $Y' = Y+1$, when $s = f_e(X+1,Y+1)$.
(A1-7)Let $X' = X+1$ and $Y' = Y-1$, when $s = f_e(X+1,Y-1)$.
(A1-8)Let $X' = X-1$ and $Y' = Y+1$, when $s = f_e(X-1,Y+1)$.

2.2.2 Extracting Secret Information s using High Capacity EMD

There are three steps for extracting hidden information:

Step1.Pair up the disguised pixels in the stego-image.
Step2.Obtain the $F^{'}$ function by substituting each pair of $(X^{'},Y^{'})$ into the f_e extraction function.

$$F^{'} = (1 \times X^{'} + 3 \times Y^{'}) \bmod 8.$$

Step3.Convert the value of F' into a secret message in the original binary form.

3 Improved Version of High Capacity EMD Hiding Technique with Lookup Table

The original EMD[7] and improved EMD[3] methods both use a change of weighting value along with modulo to find a proper position for any point in the surrounding area. The weighting value of the LWC-scheme extraction functions is similar to that of the Zhang-Wang scheme; both are fixed which makes them vulnerable to crackers. In order to strengthen security, we now propose two improved schemes which use an adaptable hiding technique in Sections 3 and 4.

3.1 The Formal form of Improved High Capacity EMD Hiding Technique

We introduce a strategy that improves the security of high capacity EMD hiding. The extraction function fs (X,Y) is similar to that of the LWC-scheme shown as in Eq.(3):

$$f_s(X,Y) = (a \times X + b \times Y) \bmod 8. \quad (3)$$

where each pair (X,Y) represents the neighbor pixels X and Y. Then, we adjust the value of X or Y with the secret data s using the following relationships:

(R-1)Let $X^{'} = X$ and $Y^{'} = Y$, when $d_0 = (s - f_s(X,Y)) \bmod 8$.
(R-2)Let $X^{'} = X + 1$ and $Y^{'} = Y$, when $d_1 = a = (s - f_s(X,Y+1)) \bmod 8$.
(R-3)Let $X^{'} = X - 1$ and $Y^{'} = Y$, when $d_2 = 8 - a = (s - f_s(X-1,Y)) \bmod 8$.
(R-4)Let $X^{'} = X$ and $Y^{'} = Y + 1$, when $d_3 = b = (s - f_s(X,Y+1)) \bmod 8$.
(R-5)Let $X^{'} = X$ and $Y^{'} = Y - 1$, when $d_4 = 8 - b = (s - f_s(X,Y-1)) \bmod 8$.
(R-6)Let $X^{'} = X + 1$ and $Y^{'} = Y + 1$, when $d_5 = a + b = (s - f_s(X+1,Y+1)) \bmod 8$.
(R-7)Let $X^{'} = X + 1$ and $Y^{'} = Y - 1$, when $d_6 = 8 + a - b = (s - f_s(X+1,Y-1)) \bmod 8$.
(R-8)Let $X^{'} = X - 1$ and $Y^{'} = Y + 1$, when $d_7 = 8 - a + b = (s - f_s(X-1,Y+1)) \bmod 8$.

In other words, given the coefficient pair (a,b), we can get the modified data pair $(X^{'},Y^{'})$ with the secret data s by using the relationship from (R-1) to (R-8).

Theorem 1. If the (a,b) coefficient pair can satisfy the following four requests:

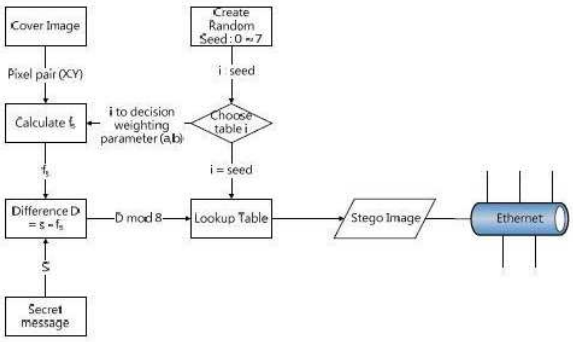

Fig. 2: Procedure flow of data hiding

Request 1.$a \neq b$,
Request 2.$a + b \mod 8 \neq 0$,
Request 3.$(a+b)$ is divisible by 2,
Request 4.$\gcd(a,b) = 1$ and $a + b \leq \lfloor \frac{8}{4} \rfloor = 4$,

then the coefficient pair (a,b) satisfies $f_s = a \times X$ $b \times Y \bmod 8$. That is to say, there are 8 coefficient pairs: $(1,3)$, $(1,5)$, $(7,3)$, $(7,5)$, $(3,1)$, $(5,1)$, $(3,7)$, and $(5,7)$, which can be used in $f_s = a \times Xb \times Y \bmod 8$.

Proof. Let set $S = \{0,1,2,3,4,5,6,7\}$ and set $A = \{a+b, a-b, -a+b, 0, -a, -b, a, b\}$. The symbol $|A|$ represents the number of valid elements in set A. According to the four requests, we can find out the following results.

1.If $a = b$, then the pairs of set $B = \{(a,b)\} = \{(1,1), (2,2), (3,3), (4,4), (5,5), (6,6), (7,7)\}$ cannot be used in $f_s(X,Y)$. Therefore, $|B| = 7$.
2.If $a + b \bmod 8 = 0$, i.e., $a = -b \bmod 8$, then the pairs of set $C = \{(a,b)\} = \{(1,7), (2,6), (3,5), (4,4), (5,3), (6,2), (7,1)\}$ do not satisfy $f_s(X,Y)$. Therefore, $|C| = 7$, i.e., there are 7 pairs in this case.
3.If $(a+b)$ is not divisible by 2, the pair (a,b) cannot generate 2,4, or 6 using $f_s(X,Y)$. For example, when (a,b) is equal to $(1,2)$, element 4 is not in set A. There are 24 pairs in this case.
4.Finally, if $\gcd(a,b)$ is not equal to 1, then element 1 is not in set A. Hence, there are 4 pairs in this case.

To sum up the four requests above, there are only 8 valid pairs of coefficients, i.e., $(1,3)$, $(1,5)$, $(7,3)$, $(7,5)$, $(3,1)$, $(5,1)$, $(3,7)$, and $(5,7)$, such that $f_s = a \times X + b \times Y \bmod 8$.

Consequently, we use seeds to decide the weighting value. A random weighting value is used to check the modulo table to determine which way to change the pixel pair (X, Y) in the cover image. Our embedding flow chart and 8 way adjustment table, are shown in Figs.2 and 3, respectively.

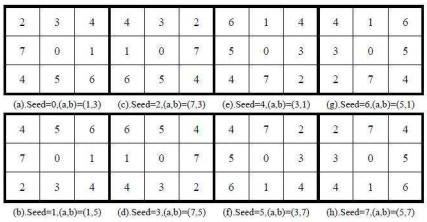

Fig. 3: Weighting parameters with different pair(a,b)

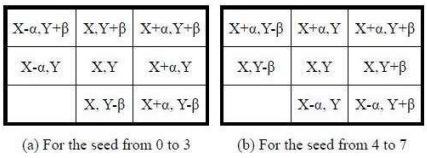

Fig. 4: Weighting values α and β in modulo table

3.2 Embedding the procedure

In order to improve this scheme, an efficient algorithm will be proposed in this subsection. Some notations are defined to assist our introduction of the proposed scheme.

Algorithm FIER scheme (Embedding Algorithm for Formal form of Improved High Capacity EMD Hiding Scheme with Relations):

Input: The cover image I_{C-FIER} and the binary secret data M

Output: The stego-image I_{S-FIER}

Step 1.Pair up the pixels in cover image I_{C-FIER}.

Step 2.Choose a random number seed to decide (a,b).

Step 3.Obtain the f_s values by substituting each pair of (x_i,x_{i+1}) into Eq.(3).

Step 4Compare f_s values and secret data s.

If s is equal to $f_s(x_i,x_{i+1})$, then the stego pair of pixels $(y_i,y_{i+1})=(x_i,x_{i+1})$.

Otherwise, the pair of pixels $(y_i^{'},y_{i+1}^{'})$ will to be modified by using the coefficient pair (a,b) and the relationships from (R-1) to (R-8).

For instance, we first obtain a pair of pixel values $(X,Y)=(100,113)$. The seed is 2, i.e., $(a,b)=(7,3)$, and secret data $s=6$. After we substitute $(100,113)$ into the extraction function f_s, we obtain $f_s=7$. The difference $d=(6-7) \bmod 8=7$. According to Fig.3(c), we can quickly obtain the result $(X+1,Y)$ when the difference is $7(-1 \bmod 8=7)$ and $s=2$; in other words, we can get this stego pixel pair $(101,113)$ from $(100,113)$ with Fig.3(c).

4 The Formal Improved High Capacity EMD Hiding Technique

The main idea of improved version of the high capacity EMD scheme (shown in section 3) is using a look-up table quickly get the changed pixel from hidden image, and also quickly get the secret information during extraction. However, the drawback of this scheme is the need for additional storage of eight tables. In order to extract the secret message successfully, these additional tables must be transmitted to the receiver by a secret channel. Hence, it will consume spaces for storage and bandwidth during transmission. Now, we modify these additional eight tables to condensed into two characteristics tables shown in Fig.4 (a) and (b), respectively. The detailed relationship between (α,β) and seed is shown in the Table 1. Specifically, each seed also has a corresponding weighting value (a,b), and (α,β). Finally, the relationships between all the corresponding values are shown in Table 1.

From Fig.4 (a) and (b), the EMD method picks a pair of pixels, and gets the remainder by passing the pair through modulo to find the value in the surrounding area. For the modulo table, all of them use the difference 0 as the center, then the different weighting value generalized function including α and β is designed to match the Fig.4 condition. Furthermore, we can simplify the relationship between (a,b) and (α,β) in Table 1 by using Algorithm 1.

Algorithm 1
Input: a and b
Output: α and β
If $(a+b) \bmod 4=0$, then
  If $\lfloor \frac{a+b}{8} \rfloor=0$, then $\alpha=1$ and $\beta=1$,
  Else $\alpha=-1$ and $\beta=-1$,
  Else if $a<b$, then $\alpha=1$ and $\beta=-1$,
  Else $\alpha=-1$ and $\beta=1$.

Below, we provide an example to explain the embedded procedure in our proposed scheme.

Example 1. If the secret data is $s=6$ and there is a pixel pair $(X,Y)=(190,143)$ with a seed of 2. Therefore, we get the stego pixel pair $(191,143)$ with the following steps.

Step 1.Using Algorithm 1, we can find out weighting pair $\alpha=-1$ and $\beta=1$ when the seed = 2 and $(a,b)=(7,3)$.

Step 2.Calculate the difference D between the secret data $s=6$ and f_s when the pixel pair $(190,143)$ is substituted into the extraction function f_s. I.e. $D=-1 \bmod 8=7 \bmod 8=7$.

Step 3.Substitute α and β into Table 1, so $(190,143)$ is transformed into $(191,143)$ such that $f_s(191,143)=s=6$.

Table 1: Relationship of generalized equation

Difference	Seed : $0 \sim 3$		Seed : $4 \sim 7$	
$d = s - f_s(X,Y)$	$X^{'}$	$Y^{'}$	$X^{'}$	$Y^{'}$
$d = s - f_s(X,Y) = 0$	$X^{'} = X$	$Y^{'} = Y$	$X^{'} = X$	$Y^{'} = Y$
$d = s - f_s(X,Y) = 1$	$X^{'} = X + \alpha$	$Y^{'} = Y$	$X^{'} = X$	$Y^{'} = Y + \beta$
$d = s - f_s(X,Y) = 2$	$X^{'} = X - \alpha$	$Y^{'} = Y + \beta$	$X^{'} = X + \alpha$	$Y^{'} = Y - \beta$
$d = s - f_s(X,Y) = 3$	$X^{'} = X$	$Y^{'} = Y + \beta$	$X^{'} = X + \alpha$	$Y^{'} = Y$
$d = s - f_s(X,Y) = 4$	$X^{'} = X + \alpha$	$Y^{'} = Y + \beta$	$X^{'} = X + \alpha$	$Y^{'} = Y + \beta$
$d = s - f_s(X,Y) = 5$	$X^{'} = X$	$Y^{'} = Y - \beta$	$X^{'} = X - \alpha$	$Y^{'} = Y$
$d = s - f_s(X,Y) = 6$	$X^{'} = X + \alpha$	$Y^{'} = Y - \beta$	$X^{'} = X - \alpha$	$Y^{'} = Y + \beta$
$d = s - f_s(X,Y) = 7$	$X^{'} = X - \alpha$	$Y^{'} = Y$	$X^{'} = X$	$Y^{'} = Y - \beta$

Table 2: Relationship between α and β

Seed	0	1	2	3	4	5	6	7
(a,b)	$(1,3)$	$(1,5)$	$(7,3)$	$(7,5)$	$(3,1)$	$(3,7)$	$(5,1)$	$(5,7)$
A	1	1	-1	-1	1	1	-1	-1
B	1	-1	1	-1	1	-1	1	-1

Table 3: The Formal Form of Extraction Function

$X-(-1)^{\lfloor \frac{seed}{4} \rfloor} \cdot \alpha$ $Y+(-1)^{\lfloor \frac{seed}{4} \rfloor} \cdot \beta$	$X-(-1)^{\lfloor \frac{seed}{4} \rfloor} \cdot \lfloor \frac{seed}{4} \rfloor \cdot \alpha$ $Y-(1-\lfloor \frac{seed}{4} \rfloor)(-1)^{(1-\lfloor \frac{seed}{4} \rfloor)} \cdot \beta$	$X+\alpha, Y+\beta$
$X+(1-\lfloor \frac{seed}{4} \rfloor)(-1)^{(1-\lfloor \frac{seed}{4} \rfloor)} \cdot \alpha$ $Y+\lfloor \frac{seed}{4} \rfloor \cdot (-1)^{\lfloor \frac{seed}{4} \rfloor} \cdot \beta$	X, Y	$X-(1-\lfloor \frac{seed}{4} \rfloor)(-1)^{(1-\lfloor \frac{seed}{4} \rfloor)} \cdot \alpha$ $Y-\lfloor \frac{seed}{4} \rfloor \cdot (-1)^{\lfloor \frac{seed}{4} \rfloor} \cdot \beta$
	$X+\lfloor \frac{seed}{4} \rfloor \cdot (-1)^{\lfloor \frac{seed}{4} \rfloor} \cdot \alpha$ $Y+(1-\lfloor \frac{seed}{4} \rfloor)(-1)^{(1-\lfloor \frac{seed}{4} \rfloor)} \cdot \beta$	$X+(-1)^{\lfloor \frac{seed}{4} \rfloor} \cdot \alpha$ $Y-(-1)^{\lfloor \frac{seed}{4} \rfloor} \cdot \beta$

4.1 Formal Version of High Capacity EMD Hiding Technique

In order to get the formal form of extraction function $f_s(X,Y)$, we combined different seeds and the relationship between α and β as shown in Table 3.

For example, when the seed is 6, the value of α and β are -1 and 1, respectively. The results are the same as Table 4.

4.2 Embedding Procedure

Algorithm FHCEMD-scheme (Embedding Algorithm for Formal form of Improved High Capacity EMD Hiding Scheme):

Input: The cover image $I_{C-FHCEMD}$ and the binary secret data M

Output: The stego-image $I_{S-FHCEMD}$

Step 1.Pair up the pixels in cover image $I_{C-FHCEMD}$.

Step 2.Choose a random seed to determine (a,b).

Step 3.Follow Algorithm 1, using the random seed to calculate the coefficients α and β.

Step 4.Obtain the f_s values by substituting each pair of (x_i, x_{i+1}) into Eq.(3).

Step 5.Compute the difference d between the value $f_s(x_i, x_{i+1})$ and secret data s. If s is equal to $f_s(x_i, x_{i+1})$, the pixel pair (y_i, y_{i+1}) equals (x_i, x_{i+1}). Otherwise, the pair of stego-image pixels (y_i, y_{i+1}) will be found by using the Table 5 and d.

Example 2. If secret data $s = 5$ and pixel pair $(X,Y) = (120,223)$ with seed of 6, then the stego pixel pair is $(120,222)$ by Algorithm FHCEMD-scheme.

Step 1.Using Algorithm 1, we find $(\alpha,\beta) = (-1,1)$ when the seed is 6 and weighting pair $(a,b) = (5,1)$.

Step 2.Calculate the difference d between the secret data s and $f_s(120,223) = 7$. I.e. $d = (s - f_s) \bmod 8 = 7$.

Step 3Substitute $d = 7$, $\alpha = -1$ and $\beta = 1$ into Table 5, so $(120,223)$ is shifted to $(120,222)$ because $f_s(120,222) = s = 6$.

5 Experimental Results and Security analysis

The experimental results and security analysis were implemented in Matlab on a PC having an Intel(R)

Table 4: Shifting of X and Y when $\alpha = -1$, $\beta = 1$

$X+1,Y+1$	$X,Y+1$	$X-1,Y+1$
$X+1,Y$	X,Y	$X-1,Y$
	$X,Y-1$	$X-1,Y-1$

Fig. 5: Cover image

Fig. 6: Stego image

Pentium(R) 4 3.00GHz 2.99GHz CPU and 2GB of memory running Windows XP Professional. Eight common standard grayscale test images (Airplane, Baboon, Boat, Elaine, Gold Hill, Lena, Pepper and Tiffany shown) were extracted from the USC-SIPI image database[8]. The processed cover images (512×512) are shown in Fig.5. Both schemes still retain the same high capacity as the LWC-scheme.

5.1 Experimental Results

Here, we compare the stego-image's quality between LWC-scheme and our proposed scheme in Table 5 showing the performance of the proposed scheme is similar to that of the LWC-scheme. The Peak Signal to Noise Ratio (PSNR) is used in this paper to evaluate image quality. The PSNR of a gray level image is defined as Eq.(4).

$$PSNR = 10 \times \log_{10} \frac{255^2}{MSE} \tag{4}$$

$$MSE = \frac{1}{M \times N} \sum_{x=1}^{M} \sum_{y=1}^{N} (I(x,y) - I^{'}(x,y))^2$$

Where M and N represent the length and width of the image. $I(x,y)$ and $I^{'}(x,y)$ denote the cover image pixel value and the stego image pixel value at position (x,y)), respectively.

We also compared the improvement in storage space. The first improved version of EMD (in section 3) uses table checking to find the data hiding strategy quickly. However, the drawback of this strategy is that extra space is required to store several tables. The formal EMD scheme does not require extra space (in section 4).

5.2 Security analysis

In this subsection, we focus our discussion on the enhanced security features of the proposed scheme.

For the LWC-scheme, fixed coefficients are used in the extraction function. Therefore, it does not provide any security mechanism against disclosure when the embedding procedure is made public.

In order to increase security, we propose the parameters of the extraction function can be modified during the hiding procedure. The parameters change rates are $131,072$ ($\frac{512\times512}{2}$) times during the hiding procedure. Therefore, only knowledge of the seed can recover the secret data from the stego image because these parameters for determining are dependent on the seed selection. The algorithm specifics of our proposed scheme can be openly publicized while the LWC-scheme cannot.

Finally, the functionality of the proposed scheme is compared with LWC-scheme, and we summarize the comparisons in Table 6.

6 Conclusion

Two kinds of weight changing of high capacity EMD schemes were proposed and implemented. One uses table checking to change the weighting evaluation of a high capacity EMD scheme and the other uses a formal form to implement the high capacity EMD data hiding scheme. Two proposed schemes improve the security of EMD.

Acknowledgement

The authors are grateful to the anonymous referee for a careful checking of the details and for helpful comments that improved this paper and acknowledge the financial support by the National Science Council of Taiwan under grant NSC NSC 102-2218-E-150 -001.

Table 5: Comparison of PSNR values between [3] and our proposed scheme Unit: dB

	Airplane	Baboon	Boat	Elaine	Gold Hill	Lena	Pepper	Tiffany
LWC-scheme[3]	50.16	50.17	50.17	50.18	50.17	50.17	50.18	50.16
Our scheme I	50.17	50.16	50.18	50.17	50.17	50.17	50.17	50.17
Our scheme II	50.17	50.16	50.18	50.17	50.17	50.17	50.17	50.17

Table 6: Functionality comparison table

Functionality	LWC-scheme[3]	Our proposed scheme(I)	Our proposed scheme(II)
Algorithm can be public	No	Yes	Yes
The Extraction function's parameters	Fixed	Random	Random
Embedding method (Extraction function)	Lookup table	Lookup table	Formal Form
Embedding Capacity	1.5 bpp	1.5 bpp	1.5 bpp
Average PSNR	50.17 dB	50.17 dB	50.17 dB

References

[1] C. C. Chang and W. C. Wu, "A novel data hiding scheme for keeping high stego image quality," *Proceedings of the 12th International Conference on MultiMedia Modelling*, Bijing, China, January, 225-232 (2006).

[2] A. Ker, "Steganalysis of LSB matching in grayscale images," *IEEE Signal Processing Letters*, **12**, 441-444 (2005).

[3] C. F. Lee, Y. R. Wang, and C. C. Chang, "A steganographic method with high embedding capacity by improving exploiting modification direction," *IIHMSP 2007*. Third International Conference on, **1**, 497-500 (2007).

[4] J. Mielikainen, "LSB matching revisited, " *IEEE Signal Processing Letters*, **13**, 285-287 (2006).

[5] R. Z. Wang, C. F. Lin, and J. C. Lin, "Image hiding by optimal LSB substitution and genetic algorithm, " *Pattern Recognition*, 34, 671-683 (2001).

[6] H. C. Wu, N. I. Wu, C. S. Tsai, and M.S. Hwang, "Image steganographic scheme based on pixel-value differencing and LSB replacement methods, " *IEE Proceedings- Vision, Image and Signal Processing*, **152**, 611-615 (2005).

[7] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Comm. Letters*, **10**, 1-3 (2006).

[8] [8]A. G. Weber. "The USC-SIPI Image Database. Version 5," httpG//sipi.usc.edu/database/.

Wen-Chung Kuo received the B.S. degree in Electrical Engineering from National Cheng Kung University and M.S. degree in Electrical Engineering from National Sun Yat-Sen University in 1990 and 1992, respectively. Then, He received the Ph.D. degree from National Cheng Kung University in 1996. Now, he is an associate professor in the Department of Computer Science and Information Engineering at National Yunlin University of Science & Technology. His research interests include steganography, cryptography, network security and signal processing.

Shao-Hung Kuo He is currently pursuing his PhD in Graduate School of Engineering Science and Technology-Doctoral Program at National Yunlin University of Science and Technology, Republic of China. He current research interests include data hiding, image processing and information security.

Yu-Chih Huang is Associate Professor of Information Management at Tainan University of Technology. She was the Director of Information Management (2007–2008) at Tainan University of Technology. She received the PhD degree in Mechanical Engineering at National Cheng Kung University in 2000. Her main research interests are: RFID information management systems, system analysis and design, information education and signal processing, e-business and applications.