DATA HIDING METHOD with HIGH EMBEDDING CAPACITY CHARACTER

Wen-Chung Kuo simonkuo@nfu.edu.tw
Department of Computer Science and Information Engineering, National Formusa University, Yunlin 632, Taiwan, R.O.C

Jiin-Chiou Cheng chiou@mail.stut.edu.tw
Department of Computer Science and Information Engineering, Southern Taiwan University, Tainan 710, Taiwan, R.O.C

Chun-Cheng Wang 96g0216@webmail.stut.edu.tw
Department of Computer Science and Information Engineering, Southern Taiwan University, Tainan 710, Taiwan, R.O.C

Abstract

Recently, the data hiding method based on the high embedding capacity by using improved EMD method was proposed by Kuo et al.[6]. They claimed that their scheme can not only hide a great deal of secret data but also keep high safety and good image quality. However, in their scheme, the sender and the receiver must share the synchronous random secret seed before they transmit the stego-image each other. Otherwise, they can not recover the correct secret information from the stego-image. In this paper we propose an improved scheme based on EMD and LSB matching method to overcome the above problem, in other words, the sender does not share the synchronous random secret seed the receiver before the stego-image is transmitted. Observing the experimental results, they show that our proposed scheme acquires high embedding capacity and acceptable stego-image quality.

Keywords: Data-hiding, Cover-image, Stego-image, EMD, LSB match method.

1. Introduction

With the rapid development of network technology, vast multimedia data would be communicated over the network. Although network transmission is convenient and fast, the multimedia data passing through the network is often attacked and tampered by malicious attackers. From the literatures many people are devoted to study the security for multimedia data. In general there are two methodologies to deal with such work: one is the cryptography and the other is steganography. Using the cryptography methodologies, the only specific user with the private key can decrypt the ciphertext when the plaintext is encrypted. An attacker cannot find out the content of message even though he gets the encryption message from the Internet. Nevertheless, the ciphertext will still be insecure if the private key is stolen or broken. Another way to promote the security of multimedia data is to hide secret data behind a meaningful image. The major goal of data hiding scheme is

not only to raise the hiding amount in the stego-image but also keep the quality of the stego-image. In the past literatures, many well data-hiding schemes had be suggested [4,6,9].

In 2006, an efficient embedding scheme based on the Exploiting Modification Direction (for short, EMD-scheme) was proposed by Zhang and Wang [9]. The scheme uses the relationship of adjacent pixels to embed the secret data. The secret data will be embedded within two adjacent pixels, that is, only one of two pixels in the EMD scheme – add one, subtract one, or stay the same. From a spatial point of view, two pixels just have five situations - moving upward, downward, left, right, or not moving at all. From their experimental simulations and discussions, the EMD-scheme can enhance the capacity of secret message and the quality of the stego-image. Recently, Lee et al. [4] proposed an improved data-hiding scheme, say LWC-scheme, which catches both of two adjacent pixels at a time and improves the possible situations from five to eight. As a result of LWC-scheme, it can promote the capacity 1.5 times approximately the former. Since the data embedding process uses the fixed evaluating parameters in both of EMD-scheme [9] and LWC-scheme [4], they will be cracked easily and leak the secret message within the stego-image while their technology are disclosed. Therefore, some concerns about the security issues will be considered. Later, Kuo et al. (for short KWSK-scheme) [6] proposed two high capacity EMD data hiding techniques with changing-evaluating-value to improve the shortcoming of above schemes, in other words, the stego-images will still be safe even when it publishes the embedding formulas. According to KWSK-scheme, they used the synchronous generator of random numbers to minimize the possibility of message disclosure and improve the lack of open method but there is an open problem of synchronization of random seeds before the stego-image is transmitted between the sender and the receiver. In this paper, we will propose an improvement scheme based on EMD and LSB matching method to overcome the synchronization problem, in other words, the sender does not send the synchronous random secret seed to the receiver before the stego-image is transmitted. According to the experimental simulations and discussions, we show that the proposed scheme still keeps high safety and good image quality.

The rest of this paper is organized as follows. In Section 2, we will introduce the EMD-method, LSB matching method and LWC-scheme briefly. Then, we will propose the improvement scheme to overcome the synchronization problem and give the experimental result in Section 3 and Section 4, respectively. Finally, conclusions will be drawn in the Section 5.

2. REVIEW THE DATA HIDING SCHEME WITH HIGH EMBEDDING CAPACITY TECHNIQUES

2.1. The Exploiting Modification Direction Method

In 2006, Zhang and Wang [9] used the relationship of adjacent pixels to promote the data embedding scheme. In their method, they transfer the secret message into (2n+1)-ary system and then embed the modified secret message into a group of n pixels in cover image by using the following equation:

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

g_i is the i-th value of pixel and n is the number of pixels. Due to the limit of paper page, we cannot explain their embedding and extracting procedures in detail here. For more details about those methods, the reader can refer to the Ref. [9].

2.2. The High Embedding Capacity by Improving Exploiting Modification Direction (EMD)

According to Lee et al.'s analysis, they find only five situations - moving upward, downward, left, right, or not moving at all to embed the secret data into two adjacent pixels by using the EMD scheme. To elevate the capacity of EMD-scheme, Lee et al. improve the number of variable situations from five to eight and then propose a steganographic scheme [4] with high embedding capacity in 2007. Here, we just only describe the embedded procedure in LWC-scheme as following steps:

Step 1. Transfer the secret message to message s, which is 8-ary system.

Step 2. Take two adjacent pixels (X, Y) as a group and perform the following extraction process,

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

Step 3. Adjust (X, Y) according to the following rule:

(3-1) If $s = f_e(X,Y)$, $X = X$, $Y = Y$.

(3-2) If $s = f_e(X+1,Y)$, $X = X+1$.

(3-3) If $s = f_e(X\text{-}1, Y)$, $X = X\text{-}1$.

(3-4) If $s = f_e(X, Y\text{+}1)$, $Y = Y\text{+}1$.

(3-5) If $s = f_e(X, Y\text{-}1)$, $Y = Y\text{-}1$.

(3-6) If $s = f_e(X\text{+}1, Y\text{+}1)$, $X = X\text{+}1$, $Y = Y\text{+}1$.

(3-7) If $s = f_e(X\text{+}1, Y\text{-}1)$, $X = X\text{+}1$, $Y = Y\text{-}1$.

(3-8) If $s = fe(X\text{-}1, Y\text{+}1)$, $X = X\text{-}1$, $Y = Y\text{+}1$.

Therefore, the stego-image may be generated as soon as the above modified pixels are embedded into the original image. The secret data can be extracted by using the extracting procedure when the particular user receives the stego-image.

2.3. The Data Hiding Scheme with High Embedding Capacity Based on General Improving EMD Method

Observing Eq. (1) in EMD-scheme and Eq. (2) in LWC-scheme, both uses the change of weight value along with modulus to fulfill the proper position for any point from surrounding area. Although there are outstanding contributions on the hiding capacities in the two techniques, the parameters of embedding function are fixed and their algorithms have to be kept. Otherwise, they will be cracked and the secret message in stego-image will leak out. In order to improve such shortcoming, Kuo et al. [6] proposed two high capacity EMD data hiding techniques with changing-evaluating-value, in other words, the stego-image will still be safe even though it publishes the embedding procedure. The KWSK-scheme is summarized as following:

Step 1. Transfer the secret message s, which is 8-ary system.

Step 2. Take two adjacent pixels (X, Y) as a group.

Step 3. Compute the value of the extract function f_{seed} with a random seed. The extract function is defined as Eq.3:

$$f_{seed}(X,Y) = (X \times a + Y \times b) \bmod 8 \tag{3}$$

Where the coefficients a and b are decided by the modular table shown in Fig.1. Compute the difference $d = (s - f_{seed}) \bmod 8$. Adjust ($X$, Y) by the modular table and the seed.

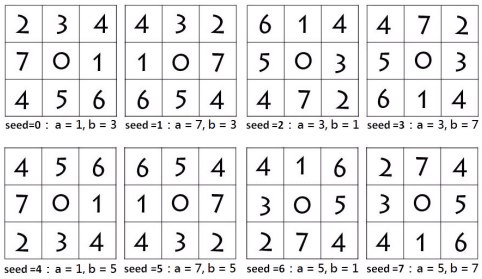

FIGURE 1: The modular tables for different weights.

Similar to the LWC-scheme, the stego-image is generated when the above modified pixels are embedded into the original image. Besides, the secret data will be extracted by using the extracting procedure when the particular user receives this stego-image. Form the experiment simulations, the KWSK-scheme [6] still maintains the high capacity and the image quality is almost the same as the LWC-scheme.

2.4. Least-Significant-Bit (LSB) Matching Method

In order to keep the embedding of the same amount of information as LSB matching and detect the secret data harder than the conventional LSB matching method, Mielikainen proposed a robust LSB matching method [5] in 2006. There are two major properties in his scheme as following:

$$f(l-1,n) \neq f(l+1,n), \forall l,n \in Z.$$

$$f(l,n) \neq f(l,n+1), \forall l,n \in Z.$$

Therefore, embedding message is performed for two pixels *X* and *Y* of a cover image at a time and then adjusting one pixel of the (*X*, *Y*) to embed two secret bits message s_1s_2. The embedding flowchart is shown in Fig.2 and the embedding procedure is described as following:

Step 1. If the LSB of *X* is the same as s_1, go to step 2.
Otherwise, go to step 3.

Step 2. If the value of $f(X,Y)$ is the same as s_2, do not change any pixel. Otherwise, the value of pixel *Y* is increased or decreased by 1.

Step 3. If the value of $f(X-1,Y)$ is the same as s_2, the value of pixel *X* is decreased by 1. Otherwise, the value of pixel *X* is increased by 1.

Where the function $f(X,Y)$ is defined as Eq.4:

$$f(X',Y') = LSB\left(\left\lfloor \frac{X'}{2} \right\rfloor + Y'\right) \tag{4}$$

Since this new LSB matching method just only increase or decrease 1 in two adjacent pixels, the difference of the two neighborhood pixel between cover image and stego-image is very small. Hence, it can keep high quality while hiding data.

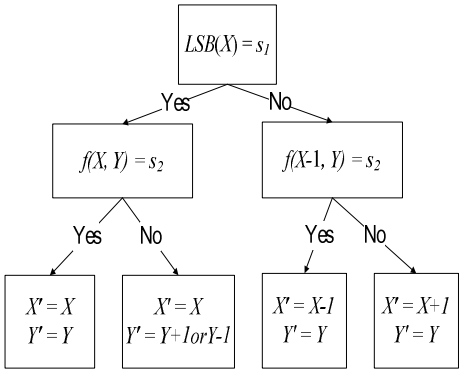

FIGURE 2: The LSB matching embedding procedure.

3. THE PROPOSED DATA HIDING SCHEME

By using more changes of weight, a robust embedded method can be proposed, which will enhance the security of the secret data within the stego-image[6]. Unfortunately, it needs to produce many random seeds before the stego-image will be processed and send them to the receiver for extracting secret message from the stego-image. How to transmit the additional information from sender to receiver is an important issue. However, such issue does not be discussed in [6]. In order to improve the lack, we will propose an efficient data hiding method based on the improved EMD and LSB matching methods, in which the seeds are embedded into stego-image at the same time and the receiver can extract these seeds and secret data from the stego-image.

3.1. The Embedding Secret Message Procedure

In our scheme, the embedding procedure is performed over three cover image pixels at a time. First, we embed the secret message by using the improvement EMD method, and then use the following functions f_1 and f_2 to embed the random seeds into the stego-image.

$$f_1(X,Y) = LSB(X+Y) \tag{5}$$

$$f_2(X,Z) = LSB(\left\lfloor \frac{X}{2} \right\rfloor + Z) \tag{6}$$

, where *X*, *Y*, *Z* are the first, second and third pixel in a group respectively. The flowchart of embedding message is shown in Fig.3. The steps are described as follows:

Step 1. Divide the modular tables into two groups G_0 and G_1 shown in Fig.4.
Step 2. Take three adjacent pixels (X, Y, Z) as a group.
Step 3. Let the result of a hash function $H(\cdot) = 0$ or 1. Compute the hash value $H(x_1||x_2||x_3||x_4||x_5||x_6)=i$ and decide to use group G_0 or G_1, where x_i is the ith bit of pixel X. Then, we also use the random generate to produce a seed $s_a \in \{0,1,2,3\}$.

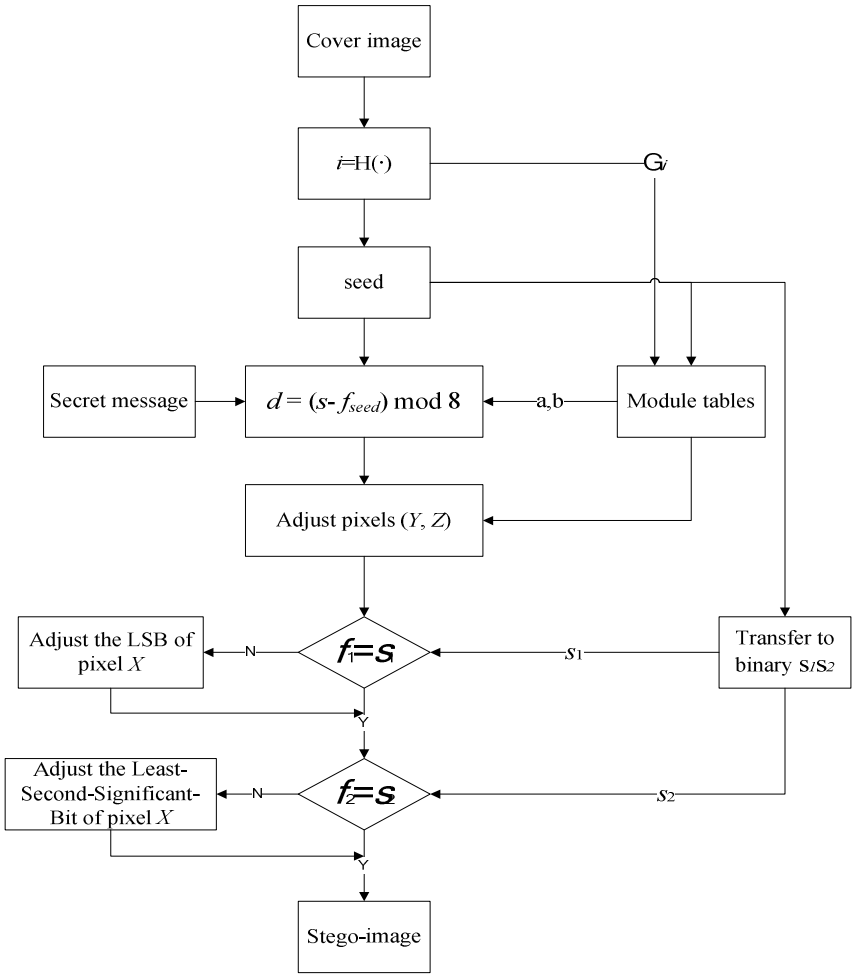

FIGURE 3: The embedding secret message procedure.

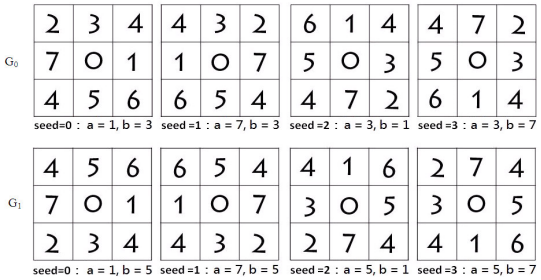

FIGURE 4: The group modular tables.

Step 4. Embed the secret message into pixels (Y, Z) by using the improved EMD method.
Step 5. Transfer the seed s_a to the binary stream s_1s_2.
Step 6. Compute v_1, which is the value of f_1, and check whether v_1 is equal to s_1 or not. If v_1 is equal to s_1, then keep the original LSB of pixel X. Otherwise, we adjust the LSB of pixel X.
Step 7. Compute v_2, which is the value of f_2, and check whether v_2 is equal to s_2 or not. If v_2 is equal to s_2, then keep the original Least-Second-Significant-Bit of pixel X. Otherwise, we adjust the Least-Second-Significant-Bit of pixel X.

3.2. The Extracting Secret Message Procedure

The flowchart of extracting secret message is shown in Fig.5. There are five steps in this procedure. Now, they are described as follows:

Step 1. Compute the value i, which is first six bits of pixel X of $H(\cdot)$, to decide group G_i.
Step 2. Extract the first bit of random seed s_1 by computing f_1.
Step 3. Extract the second bit of random seed s_2 by computing f_2.
Step 4. Transfer the binary s_1s_2 to decimal value to extract seed.
Step 5. Take pixels (Y, Z) and the weight of seed in G_i to extract the secret message by computing extract function f_{seed}.

Therefore, the receiver can recover the secret data by using the extracting procedure.

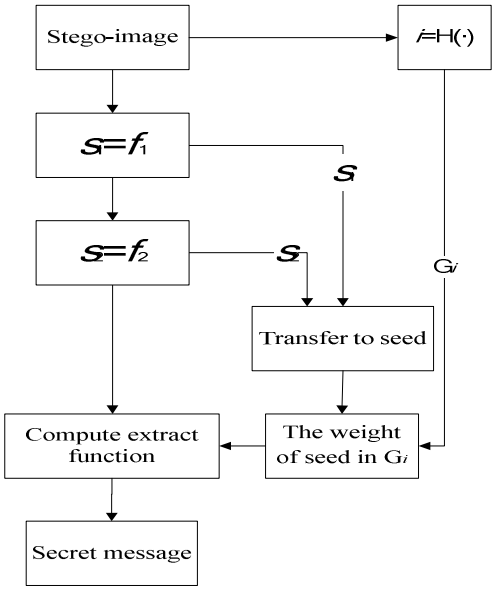

FIGURE 5: The extracting secret message procedure.

4. EXPERIMENTAL RESULT

We perform our scheme over Lena, Pepper, Baboon and Boat, which are common pictures and shown in Fig.6. These cover images are 512×512, 8bits and grayscale. The resultant stego-images are shown in Fig.7. We can't distinguish between cover-images and stego-images with human's eyes.

FIGURE 6: Cover images.

FIGURE 7: Stego-images.

Analysis of the stego-image's PSNR: From Tab.1, we can find out the stego-image's quality by using our method is lower than KWSK-scheme. In KWSK-scheme, Kuo et al. take two adjacent pixels as a group and each pixel is at most increased or decreased by 1. In our scheme, we take three adjacent pixels at a time and it is just only the second or third pixel to increased or decreased by 1 at most but the value of first pixel maybe be changed by difference 3 or 1 in each pixel group. Although the stego-image's quality in our scheme is not good as KWSW-scheme, there is an important merit is that it does not transmit the random number seeds before the sender and receiver communicates each other.

Analysis of embedding capacity: We take three pixels in a group to embed three bits at a time but Kuo et al. [6] take two pixels in a group to embed three bits. Therefore, the embedding capacity of our scheme is about 2/3 of KWSK-scheme and the experiment result shown as Table 1. Similarly, there is an important advantage in our proposed scheme which does not need the synchronous random number seed to carry although the embedding capacity in our scheme is less than KWSK-scheme.

Method	KWSK-scheme[6]		Our scheme	
	Payload (bits)	PSNR (dB)	Payload (bits)	PSNR (dB)
Lena	393,216	50.175	262,143	47.164

Pepper	393,216	50.179	262,143	47.170
Baboon	393,216	50.178	262,143	47.171
Boat	393,216	50.175	262,143	47.074

TABLE 1: The comparison between KWSK-scheme and our scheme.

5. CONCLUSION

In this paper, we propose an improved scheme by using the LSB matching method to embed seeds into the stego-image again to replace to transmit the synchronous random number seeds before the sender and the receiver commune each other, i.e., this can improve the defect of the synchronous random number seeds in KWSK-scheme. The experimental result shows that it can not only keep the acceptable image quality and security but also enhance convenience for transmission in our proposed scheme.

6. ACKNOWLEDGEMENT

This work is supported by National Science Council under NSC 98-2219-E-150-001.

7. REFERENCES

[1] FOR JOURNALS: F. Cayre, C. Fontaine, and T. Furon, “Watermarking Security: Theory and Practice,” IEEE Trans. on Signal Processing Vol.53, No.10, pp.3976-3987, Oct. 2005.

[2] FOR JOURNALS: 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, pp.225-232, January 2006.

[3] FOR JOURNALS: A. Ker, “Steganalysis of LSB Matching in Grayscale Images,” IEEE Signal Processing Letters, Vol.12, No.6, pp.441- 444, June 2005.

[4] FOR JOURNALS: C. F. Lee, Y. R. Wang, and C. C. Chang, “A Steganographic Method with High Embedding Capacity by Improving Exploiting Modification Direction,” IIHMSP 2007, Volume 1, Issue, pp.497 – 500, 26-28 Nov. 2007.

[5] FOR JOURNALS: J. Mielikainen, “LSB Matching Revisited,” IEEE Signal Processing Letters, Vol.13, No.5, pp.285-287, May 2006.

[6] FOR CONFERENCES: W. C. Kuo, L. C. Wuu, C. N. Shyi, and S. H. Kuo, “A Data Hiding Scheme with High Embedding Capacity Based on General Improving Exploiting Modification Direction method” HIS2009, Aug. 2009.

[7] FOR JOURNALS: R. Z. Wang, C. F. Lin, and J. C. Lin, “Image Hiding by Optimal LSB Substitution and Genetic Algorithm,” Pattern Recognition, Vol.34, No.3, pp.671-683, 2001.

[8] FOR JOURNALS: 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, Vol.152, No.5, pp.611-615, October 2005.

[9] FOR JOURNALS: X. Zhang and S. Wang, “Efficient Steganographic Embedding by Exploiting Modification Direction,” IEEE Comm. Letters, Vol.10, No.11, pp.1-3, Nov. 2006.