Enhancement of LSB steganography using Exploiting Modification Direction

Prashanth Kumar K[1]
Student, M.Tech (DECS)
Department of E & C Engineering
St Joseph Engineering College,
Mangaluru, D.K, Karnataka, INDIA

Ms. Veena Desai[2]
Assistant Professor
Department of E & C Engineering
St Joseph Engineering College,
Mangaluru, D.K, Karnataka, INDIA

***Abstract*—In the conventional Least Significant Bit (LSB) steganography methods, the LSB plane of the image is replaced with secret bit. To overcome higher distortion and low payload capacity, Exploiting Modification Direction (EMD) method is proposed in this paper. Image steganography using Exploiting Modification Direction, embeds the data along pixel pair of image by incrementing or decrementing either pixel by one. Since the directions of modification are fully exploited, the proposed method provides high embedding efficiency that is better than LSB technique.**

Keywords—Steganography, Exploiting Modification Direction (EMD), Least Significant Bit (LSB)

I. INTRODUCTION

DATA hiding is a technique that conceals data into a carrier for conveying secret messages confidentially. Digital images are widely transmitted over the Internet; therefore, they often serve as a carrier for covert communication. Images used for carrying data are termed as cover images and images with data embedded are termed as stego images. After embedding, pixels of cover images will be modified and distortion occurs. The distortion caused by data embedding is called the embedding distortion. A good data-hiding method should be capable of evading visual and statistical detection while providing an adjustable payload. The primary goal of attack on steganographic systems, termed steganalysis, is to detect the presence of hidden data by finding statistical abnormality of a stego-media caused by data embedding Generally speaking, the more the secret data are embedded, the more vulnerable is the steganographic system to steganalytic attempts not be aware of the existence of the hidden secret message. This kind of data hiding technique is called as image steganography [1]. There are two types of image steganographic techniques: spatial domain and transform domain methods. Spatial domain algorithms embed information directly into the cover-image without performing other changes. They are easier to implement, but are not as robust. Transform domain algorithms embed secret information into a transform space. The advantage of these algorithms is good robustness; however, the disadvantage is less capacity. One of the basic methods of data embedding in spatial domain is least significant bit substitution method.

The least significant bit substitution method, a well-known data hiding method. In LSB embedding, the pixels with even values will be increased by one or kept unchanged. The pixels with odd values will be decreased by one or kept unmodified [2]. As a result, some structural asymmetry (never decreasing even pixels and increasing odd pixels when hiding the data) is introduced, and thus it is very easy to detect the existence of hidden message even at a low embedding rate using some reported steganalytic algorithms, such as the Chi-squared attack [3] and regular/singular groups (RS) analysis[4].

II. METHODOLOGY

A. LSB STEGANOGRAPHY

The LSB based Stegenography is one of the steganogrphic methods, used to embed the secret data in to the least significant bits of the pixel values in a cover image. e.g. 110 can be hidden in the first eight bytes of three pixels in a 24 bit image.

PIXELS: (00100111 11101001 11001000)
(00100111 11001000 11101001)
(11001000 00100111 11101001)
110 : (001101110)
RESULT: (00100110 11101000 11001001)
(00100111 11001000 11101001)
(11001001 00100111 11101000)

Here number 110 is embedded into first nine bytes of the grid and only 5 bits are changed.

The main disadvantage of this algorithm is that, to embed a single character it requires many pixels which causes more image distortion. So we need an advanced algorithm like Exploiting modification direction (EMD) to avoid this.

B. EXPLOITING MODIFICATION DIRECTION

The main idea of the EMD embedding scheme is that each $(2n + 1)$-ary notational secret digit is carried by n cover pixels, and only one pixel value increases or decreases by 1 at most. For each block of n cover pixels, there are $2n$

possible states of only one pixel value plus 1 or minus 1. The 2*n* states of alteration plus the case in which no pixel is modified form (2*n* + 1) different cases. Therefore, the (2*n* + 1)-ary notational secret digit is embedded into the cover pixels by changing the state. Before the data embedding procedure, the preprocess can convert the secret data into sequences of digits with (2*n* + 1)-ary notational representation. Suppose the gray values of pixels in a group are $p_1, p_2, p_3 \ldots p_n$, and the extraction function f as a weighted sum modulo (2n+1):

$$f(P_1, P_2 \ldots P_n) = \sum_{i=1}^{n} (P_i * i) \bmod (2n+1) \quad (1)$$

For the simplest case of $n = 2$, the secret data stream $S_{(2)}$ can be expressed as $S_{(5)}$ where $S_{(b)}$ denotes the *b*-ary notational system representation of secret data stream *S*. Thus, the 5- ary digits can conceal into blocks of two cover pixels by modifying at most one pixel value. Denote the gray values of a block of two cover pixels as *p*1 and *p*2, and the extraction function *f is* defined as a weighted sum modulo 5:

$$f(P_1, P_2) = \sum_{i=1}^{2} (P_i * i) \bmod 5 \quad (2)$$

Suppose that the transformed 5-ary secret digit *s* desired to be embedded into the cover pixels *p*1 and *p*2. According to the secret digit, the embedding process can be classified into 5 conditions [5].

Condition 1. If $(s - f(p1, p2)) \bmod 5 = 0$:
No modification is needed because the extraction function *f* can decrypt the correct secret data.
Condition 2. If $(s - f(p1, p2)) \bmod 5 = 1$:
Increase the pixel value *p*1 by 1.
Condition 3. If $(s - f(p1, p2)) \bmod 5 = 2$:
Increase the pixel value *p*2 by 1.
Condition 4. If $(s - f(p1, p2)) \bmod 5 = 3$:
Decrease the pixel value *p*2 by 1.
Condition 5. If $(s - f(p1, p2)) \bmod 5 = 4$:
Decrease the pixel value *p*1 by 1.
By the above operations, the stego-pixel value of the image is obtained, and hence we get stego image.

C. EMD EMBEDDING

The Block diagram of EMD embedding scheme is shown in Figure 1,

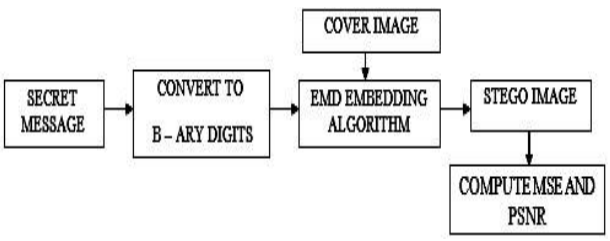

Figure 1: Block Diagram of EMD Embedding

User will enter the secret message through keyboard. This message will be there in ASCII format. The different steps in processing this message is as follows,
Step 1: Convert the message from ASCII character to B – ary digits.
Step 2: Cover image is gray scale image of any format. Take the pixel pair in raster scan order (Top left to Right bottom)
Step 3: Take the first digit and embed this in first pixel pair using EMD Embedding algorithm.
Step 4: Repeat the above step to embed other message digits.

D. EMD Extracting

The Block diagram of EMD extracting scheme is shown in Figure 2,

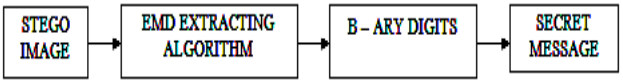

Figure 2: Block Diagram of EMD Extracting

Step 1: Take the pixel pair in raster scan order.
Step 2: Apply EMD extracting algorithm to extract the first digit.
Step 3: Go to next pixel pair and repeat the above procedure till all the digits are extracted.
Step 4: Covert the extracted digits back into character to get desired secret message.

III. RESULTS

The analysis of EMD based steganography has been done on basis of parameters like MSE and PSNR.
Mean Square Error (MSE):
It is the measure used to quantify the difference between the initial and the distorted or noisy image. MSE represents the mean square error between the cover image and stego image. A smaller MSE indicates that the stego image has better quality[2].

$$MSE = \frac{1}{MXN} \sum_{i=1}^{m} \sum_{j=1}^{n} I(i,j) - I'(i,j) \quad (3)$$

Peak Signal to Noise Ratio (PSNR):
The PSNR is the most popular criterion to measure the distortion between the cover image and stego-image. It is defined as follows [2]:

$$PSNR = 10 \log_{10} \left(\frac{255^2}{MSE} \right) \quad (4)$$

A higher PSNR indicates that the stego image has better quality.
Here, the symbols I(i, j) and I(i, j) represent the pixel values of the cover image and stego-image in the position (i, j), respectively, and *m* and *n* are the width and height of the original image.
Program is implemented using MATLAB. The proposed method is applied on 8-bit grayscale images. The messages are entered by the user and appended with "`" character to

make it total 100 characters. Results are compared with outputs of LSB Stegenography.

Figure 3 Cover image "lena.jpg"

Figure 4 Stego image embedded with secret data "engineering college"

Table 1 MSE and PSNR for different cover images

COVER IMAGE	MSE(LSB)	MSE(EMD)	PSNR(LSB) in dB	PSNR(EMD) In dB
lena	0.0011	8.6930e-004	62.9340	63.4350
desert	8.3387e-004	6.9452e-004	63.5253	63.9224
sea	7.8275e-004	6.2351e-004	63.6627	64.1566
castle	6.5626e-004	5.6521e-004	64.0454	64.3698

EMD Extracting algorithm is applied to the stego image to extract secret message "engineering college".

IV. DISCUSSION

LSB based steganography embed the secret message in LSB of cover image.EMD based steganography embed the secret messages using 5-ary notation system. This work implements EMD based steganography computing PSNR and MSE for result analysis. PSNR used as a quality measurement between two images. If PSNR ratio is high then images are better of quality. The PSNR value in the comparison table shows that EMD scheme has high payload capacity's calculated for EMD is less compared to LSB technique indicating less distortion in the stego image.

Table 1 shows the stego image quality by PSNR and MSE for the input message "engineering college".

V. CONCLUSION

Image steganography using EMD scheme provides more selectable cases so that the secret message can be conveniently hidden. The algorithm can be applied to color images in the similar manner. The result analysis shows the variation in the payload capacity in the case of EMD. It can be still enhanced by using more compact neighborhood set as in Adaptive Pixel Pair Matching [6].The visual quality of the image also can be improved by embedding the data along the edges of cover image using Edge Adaptive Techniques [7].

REFERENCES

[1] Xinpeng Zhang and Shuozhong Wang *"Efficient Steganographic Embedding by Exploiting Modification Direction"* , IEEE Communications letters, vol. 10, pp. 781-783, November 2006.

[2] Dr. Ekta Walia, Payal Jain and Navdeep *"An analysis of LSB & DCT based steganography"* Global Journal of Computer science and technology, vol. 10, pp. 4-8, April 2010.

[3] A. Westfeld and A. Pfitzmann, "*Attacks on steganographic systems"*, in proc. 3rd Int. Workshop on information Hiding, vol. 1768, pp. 61-76, 1999.

[4] A. D. Ker, "A General framework for structural steganalysis" , in proc. 9th Int. Workshop on Information Hiding, vol. 4567, pp. 204-219, 2007.

[5] Ruey-Ming Chao, Hsien Chu Wu, Chih-Chiang Lee and Yen-Ping Chu *"A Novel Image Data Hiding Scheme with Diamond Encoding"* Hindawi Publishing Corporation, Vol. 9, January 2009.

[6] Wien Hong and Tung – Shou Chen *" A Novel Data Embedding Method Using Adaptive Pixel Pair Matching"* , IEEE Transactions on information forensics and security, vol. 7, pp. 176-184, February-2012.

[7] Weiqi Luo, Fangjun Huang and Jiwa Huang, "*Edge Adaptive Image Steganography Based on LSB Matching revisited"* IEEE Transactions on information forensics and security, vol. 5, pp. 201-214, June-2010.

[8] Ruey Andrew D. Ker, *"Steganalysis of LSB Matching in Grayscale Images"* , IEEE Signal processing letters, vol. 12, pp. 441-444, June 2005.

[9] Chi – Kwong Chan, L. M Chang "*Hiding data in images by simple LSB substitution*" The Journal of pattern recognition society, vol. 37, pp. 469-474, August 2003.

[10] Rajashree Shitole, Satish Todmal "*A Novel Image Hiding Scheme by Optimal Pixel Pair Matching and Diamond Encoding*" IOSR Journal Of VLSI And Signal Processing, vol. 1, pp. 25-31, February-2013.