ANNALS OF FACULTY ENGINEERING HUNEDOARA
– INTERNATIONAL JOURNAL OF ENGINEERING
Tome X (Year 2012) – FASCICULE 3 (ISSN 1584 – 2673)

[1.] Jasvinder KAUR, [2.] Manoj DUHAN, [3.] Ashok KUMAR, [4.] Raj Kumar YADAV

MATRIX MATCHING METHOD FOR SECRET COMMUNICATION USING IMAGE STEGANOGRAPHY

[1-2.] DEENBANDHU CHHOTU RAM UNIVERSITY OF SCI. & TECH., MURTHAL, INDIA
[3.] KURUKSHETRA UNIVERSITY, KURUKSHETRA, INDIA
[4.] MAHARSHI DAYANAND UNIVERSITY, ROHTAK, INDIA

ABSTRACT: *In this paper, a new data hiding method for secret communication by using matrix matching is proposed. It does not use same pre specified bits of pixel value for insertion and retrieval of message. It makes changes to the bits of pixel value according to the matrix matching result. The pixels for insertion and retrieval of message are chosen by using pseudo random number generator that is seeded with a secret key which is shared between sender and receiver. Triple M method (Matrix Matching Method) makes the steganalyst harder because the stress of this method is not on same specific bits. Experimental result also shows that stego images visually indistinguishable from the original cover image.*
KEYWORDS: *Data hiding, Steganography, Cryptography, LSB method*

INTRODUCTION

Data hiding is a form of stenography that embeds data into cover media for the purpose of identification, annotation and copyright [1]. The important uses of data hiding in digital media are to provide proof of the copyright, assurance of content integrity and feature location. [2]. In this paper, 8 bit grayscale images are selected as cover media. These images are called cover image. When the data is hidden in cover image then it becomes stego image.

There are many techniques that hide the data in images [3-8]. The most popular and oldest technique for hiding data in digital image is LSB technique. In this method, least significant bit of pixel value is used for insertion of message. This method is very easy to implement and provide high capacity. An edge adaptive scheme which can select the embedding regions according to the size of secret message and the difference between two consecutive pixels in the cover image is proposed in [9]. LSB++ method, which improves over the LSB+ image steganography by decreasing the amount of changes made to the perceptual and statistical attributes of the cover image is given in [10].

In 2004, Potdar et al. proposes GLM (Gray level modification) technique [11], which is used to map data by modifying the gray level of the image pixels. Gray level modification Steganography is a technique to map data (not embed or hide it) by modifying the gray level values of the image pixels. GLM Steganography uses the concept of odd and even numbers to map data within an image. It is a one-to-one mapping between the binary data and the selected pixels in an image. From a given image a set of pixels are selected based on a mathematical function. The gray level values of those pixels are examined and compared with the bit stream that is to be mapped in the image. Initially, the gray level values of the selected pixels (odd pixels) are made even by changing the gray level by one unit. Once all the selected pixels have an even gray level it is compared with the bit stream, which has to be mapped. The first bit from the bit stream is compared with the first selected pixel. If the first bit is even (i.e. 0), then the first pixel is not modified as all the selected pixels

In the message hidden in 1st and 2nd bit plane method [12], Parvinder et al gives the concept of four algorithms, which insert each message bits four times. To avoid the pattern recognition and get more robustness each message bit is inserted four times i.e. as 00, 01, 10, and 11 at 1st and 2nd bit position in such a way that effect to original image is same as in the case, when message is hidden in least significant bit (0th bit plane). However these algorithms avoid the some of the disadvantages associated with least significant bit insertion method.

In this paper, a new data hiding scheme by using matrix matching method is proposed. On this basis of matching factor of columns, particular bits may be changed such that change in image quality is minimum. The MSE between the cover image and stego image is calculated. Experimental result shows that method our method provides less MSE than earlier method like LSB method, GLM method and parity checker method. Our method also removes two above discussed disadvantages associated with above said method.

The rest of the paper is organized as follows. Section 2 describes the proposed method. Section 3 derives the probability of matching of message bits with various columns of image matrix with selected pixels. Experimental results are shown in section 4. Finally, section 5 gives the conclusion of the paper.

MATRIX MATCHING METHOD

In this method, firstly we write our message in form of information matrix. The number of columns in information matrix will be 8. After that we select the 8 pixels using pseudo random number

generator for insertion of one row of information matrix. From the 8 selected pixels we will made selected pixel image matrix of size 8X8. The row of information matrix is inserted in that column of selected pixel image matrix which has the minimum effective change. The complete algorithm for insertion of the message is given below.

ALGORITHM

I. *Let C be the original 8 bit grayscale cover image of size $M_r \times M_c$ pixel which is represented by equations (1) & (2) :*

$$C = \{x_{ij},\ \ 0 \le i < Mr,\ \ 0 \le j < Mc\} \tag{1}$$

where,

$$x_{ij} \in \{0,1\ldots..,255\} \tag{2}$$

x_{ij}, is the intensity of pixel which is present at row number i and column j.
M_r, is the number of rows in the image.
M_c, is the number of the columns in the image.

II. *Let M be the message of length of n bits as shown in equations (3) & (4).*

$$M = \{mi,\ 0 \le i \le n\} \tag{3}$$

where,

$$mi\ \in \{0,1\} \tag{4}$$

m_i is the i^{th} message bit.

III. *Break the M into Q equal parts each of size 8 bit, such that*

$$Q = \{b_{ij},\ \ i \in (1,2,3,\ldots.8),\ j \in (1,2,3,\ldots.8)\} \tag{5}$$

IV. *Make the information matrix from the Q as (6) below:*

$$InformationMatrix = \begin{bmatrix} b_{11} & \ldots & b_{18} \\ . & \ldots & . \\ b_{q1} & \ldots & b_{q8} \end{bmatrix}_{Qx3} \tag{6}$$

where, $Q = \dfrac{M}{8}$

Size of Information Matrix will be Q×8.

V. *Generate the 8 pixel locations by using Pseudo Random Number Generator which are used for insertion of message.*

$$S.P. = \{P_i,\ \ i \in (1,2,3,\ldots.8)\} \tag{7}$$

where S.P. = Selected Pixel and

$$Pi = \{aij,\ i \in (1,2,3,\ldots.8),\ j \in (1,2,3,\ldots.8)\} \tag{8}$$

VI. *Now, generate the Selected Pixel Image Matrix (S.P.I.M.) using the 8 selected pixels as (9).*

$$S.P.I.M. = \begin{bmatrix} a_{11} & \ldots & a_{18} \\ . & \ldots & . \\ a_{81} & \ldots & a_{88} \end{bmatrix}_{8x8} \tag{9}$$

where S.P.I.M. is of order 8×8.

VII. *Now for inserting the i^{th} row of information Matrix calculate Matching Factor (M.F) for each column of selected pixel image matrix.*
Let R_i is the row of information matrix that we want to insert in the selected pixel image matrix, such that

$$Ri = \{b_{ij},\ \ j \in (1,2,3,\ldots.8)\} \tag{10}$$

M.F. for each column k (C_k) of selected pixel image matrix is calculated by formulae given in (11).

$$M.F.(C_k) = \sum_{j=1}^{8} x_{jk}\ ,\ where\ x_{jk} = \begin{cases} 1, & a_{jk} = b_{ij} \\ 0, & otherwise \end{cases} \tag{11}$$

Here $k \in (1,2,3,\ldots.8)$, $j \in (1,2,3,\ldots.8)$ and $i \in (1,2,3,\ldots.8)$.

VIII. *Calculate effective change for each column C_k which is given by following equation (12):*

$$EffectiveChange(C_k) = \frac{(8 - M.F.)}{2^{8-k}},\ \forall\ k \in (1,2,3,\ldots.8) \tag{12}$$

IX. *Now select the column C_s which has minimum effective change. Make the column C_s equivalent to R_i of information matrix such that*

$$a_{si} = b_{ji},\ \ \ j \in (1,2,3,\ldots.8) \tag{13}$$

X. *Store the binary value of selected column number in the core matrix. For each row of information matrix there will be three bits in core matrix as shown in equation (14).*

$$CoreMatrix = \begin{bmatrix} C_{11} & C_{12} & C_{13} \\ C_{21} & C_{22} & C_{23} \\ C_{31} & C_{32} & C_{33} \end{bmatrix}_{3x3} \tag{14}$$

XI. *Apply Huffman coding to core matrix to reduce the size of core matrix.*

XII. This reduced core matrix and key to pseudo random generator either may be embedded in the cover image itself or they may be sent out to the receiver end by (14) using public key cryptography or some other secret means.

The retrieval algorithm is just reverse of the insertion algorithm.

PROBABILITY OF MATCHING

The probability that the row R_i of information matrix has matching factor M.F. with the column C_k of selected pixel image matrix has been given by equation (15).

$$Prob(R_i, C_k, M.F.) = \sum_{M.F.=o}^{s} \frac{C_{s-M.F.}^{s}}{2^{s}} \quad (15)$$

RESULTS

This section discusses the result of using our proposed method hide data in image. The proposed technique has been tested on a database containing 20 images. We have applied the MSE (mean square error) and PSNR (peak signal to noise ratio) to compare Triple M (matrix matching method) with some existing investigated methods MSE and PSNR are calculated by using the well known formulae given in (16) and (17) respectively:

$$MSE = \frac{1}{[NxM]^2} \sum_{i=1}^{N} \sum_{j=1}^{M} [(X_{ij} - Y_{ij})^2 \quad (16)$$

$$PSNR = 10 \log_{10} \left[\frac{(255)_2}{MSE} \right] \quad (17)$$

Here: N, is the number of rows in cover image
M, is the number of columns in cover image
X_{ij}, intensity of $Pixel_{ij}$ in cover image
Y_{ij}, intensity of $Pixel_{ij}$ in Stego image

The results are calculated for message of different lengths. The results of PSNR comparison (in dB) of Triple M method with other existing methods is shown in Table 1.

Ten (10) standard cover images are from the database of entered images with their corresponding stego images are shown in Figure 1.

Figure 1 also shows the histogram of cover images and stego image respectively. For further evaluating the performance of triple M method, we have applied the matrix normalized cross- correlation which is defined by formulae (18).

$$NCC = \frac{\sum_{i=1}^{N} \sum_{j=1}^{M} (X_{ij} x Y_{ij})}{\sum_{i=1}^{N} \sum_{j=1}^{M} (X_{ij})^2} \quad (18)$$

Here, all the variables have the same meaning as in equation (16).

Table 1. Comparison of PSNR of Triple M with other existing methods

Cover image	Message length (inBytes)	Triple M	LSB	GLM	Parity checker
Baboon	1024	41.3	33.4	35.4	32.2
	4096	39.4	33.1	35.2	30.7
	8192	39.2	32.7	34.7	29.9
	16384	37.4	31.2	33.1	28.7
Jet	1024	43.2	34.1	36.2	33.1
	4096	43.1	33.2	35.1	32.8
	8192	42.5	32.1	35.0	32.5
	16384	37.1	30.7	34.1	31.5
Scene	1024	42.1	34.3	35.2	34.1
	4096	45.7	34.1	34.9	33.3
	8192	39.5	32.8	31.2	31.0
	16384	36.1	32.5	29.4	29.2
Tiger	1024	41.7	35.2	37.1	31.2
	2048	40.2	33.7	35.4	30.4
	4096	38.6	31.6	33.5	29.7
	8192	37.9	29.9	32.7	29.3

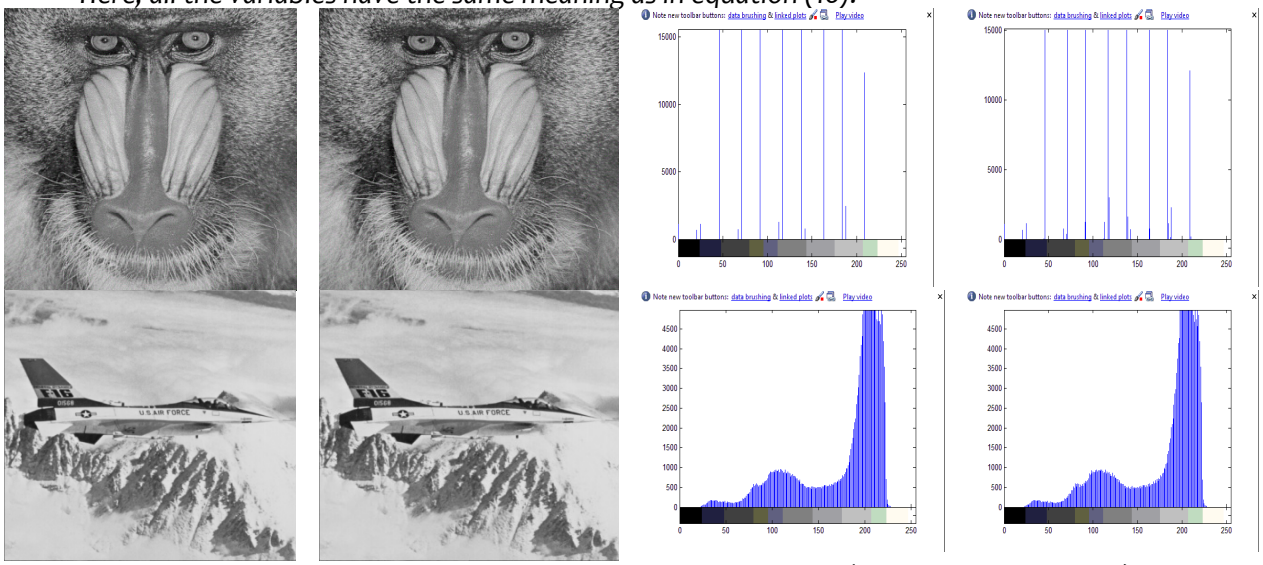

Figure 1. Cover Images with their corresponding stego images and histogram (message with 1024 Bytes) – Part 1&2

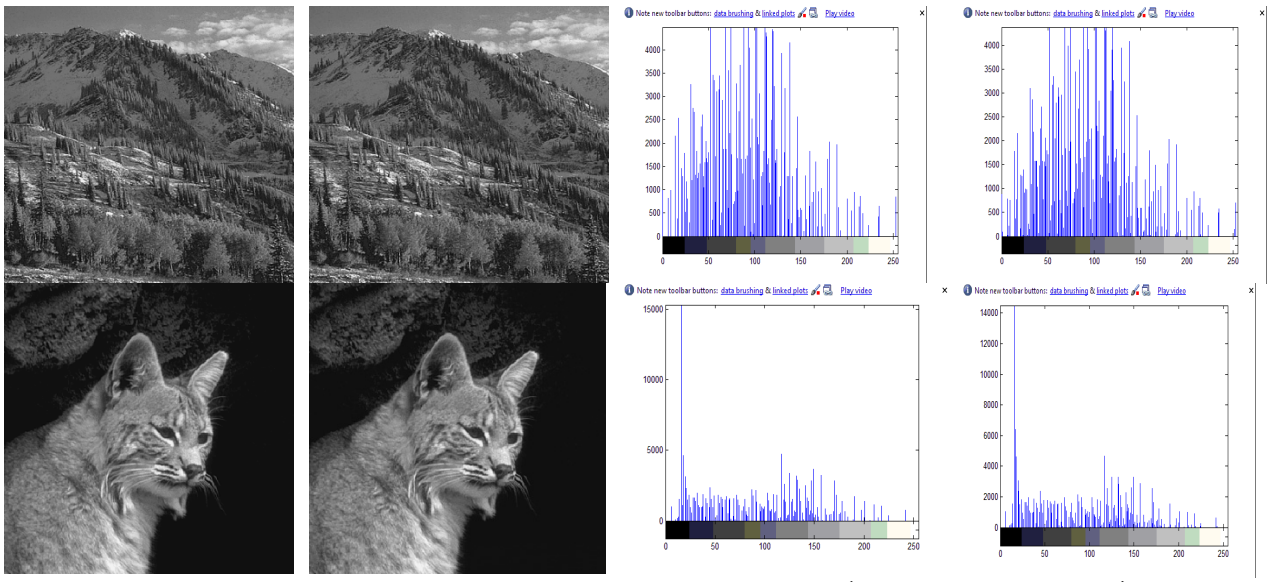

Figure 1. Cover Images with their corresponding stego images and histogram (message with 1024 Bytes) – Part 3&4

The result of NCC for 10 images is shown below in table 2.

High value of NCC shows that there is very less change in cover image and stego image. By using Triple M Method, the value of NCC will remain closer to 1 which shows that there is very little difference in cover images and their corresponding stego image.

Table 2. Result of NCC for 10 images

Cover Image	NCC
Image 1	1.0
Image 2	0.91
Image 3	0.85
Image 4	1.0
Image 5	0.89
Image 6	0.92
Image 7	0.91
Image 8	0.86
Image 9	1.0
Image 10	0.92

CONCLUSIONS

In this paper, a new data hiding method i.e. Triple M method has been proposed. This method removes the disadvantages associated with some existing investigated method. The experimental results show that it provides better PSNR values than some previous existing methods. Also, the NCC values come closer to 1, which shows that stego images are visually indistinguishable from their corresponding cover images. The stego images are very hard to differentiate from the cover images.

REFERENCES

[1.] R.J. Anderson, Information Hiding, Lecture Notes in Computer Science vol. 1174, May 1996.
[2.] Bender W. et.al. Applications for Data Hiding, IBM Systems Journal, 39 (3&4), pp 547-568, 2000.
[3.] T.S. Chen, C.C. Chang, M.S.Hawang, A Virtual Image Cryptosystem Based Vector Quantization, IEEE Trans. Image Process, 7 (10), pp 1485-1488, 1998.
[4.] L.M. Marvel, C.G. Boncelet, C.T. Retter, Spread Spectrum Image Stegnography, IEEE Trans. Image Process. 8(8), pp 1075-1083, 1999.
[5.] Ran-Zan Wang, Chi-Fang Lin, Ja-Chen Lin, Hiding Data in Images by Optimal Moderately Significant-Bit Replacement, IEE Electronics Letters, 36(25), pp 2069-2070, 2000.
[6.] K.L. Chung, C.H. Shen, L.C. Chang, A Novel SVD- and VQ- Based Image Hiding, Pattern Recognition Letters, 22(9), pp 1051-1058, 2001.
[7.] Ran-Zan Wang, CHI-Fang Lin, Ja-Chen Lin, Image Hiding by Optimal LSB Substitution and Genetic Algorithm, Pattern Recognition, 34(3), pp 671-683, 2001.
[8.] Chi-Kwong Chan, L.M. Cheng, Improved Hiding Data in Images by Optimal Moderately Significant-Bit Replacement, IEE Electronics Letters, 37(16), pp 1017-1018, 2001.
[9.] Weiqi Luo, Fangjun Huang, Jiwu Huang, Edge Adaptive Image Steganography Based on LSB Matching Revisited, IEEE Transactions on Information Forensics and Security, 5(2), pp 201-214, June 2010.
[10.] Ghazanfari K., Ghaemmaghami S., Khosravi S.R., LSB++: An Improvement to LSB+ Steganography, TENCON 2011 - 2011 IEEE Region 10 Conference, pp 364 – 368, Nov. 2011
[11.] Vidyasagar M. Potdar, Elizabeth Chang, Grey Level Modification Stegnography for Secret Communication, 2nd IEEE International Conference on Industrial Informatics, Germany, 2004.
[12.] Parvinder Singh, Sudhir Batra, HR Sharma, "Evaluating the Performance of Message Hidden in 1st and 2nd Bit Plane", WSEAS Transactions on Information Science and Applications, 2(8), pp 1220-1227, August 2005.
[13.] RG Van Schyndel, AZ Tirkel, CF Osborne, "A Digital Watermark", IEEE International Conference on Image Processing, 2, pp 86-90, Nov 1994.