IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Row into Column Modify Stegano-algorithm

Rupali Jain[1], Jayshree Boaddh[2]

Student, Department of Computer Science, MIT, RGPV, Bhopal[1]

Faculty, Department of Computer Science, MIT, RGPV, Bhopal[2]

Abstract: Data security is maintained by assuming the consistency and accuracy of data over its entire life cycle. Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity, data integrity and denial of service. Here, we are proposing a Row into column Modify stegno-algorithm. This is an image steganography technique in which we proposed a way to hide message behind the cover image with improved value of PSNR and good NCC value**.**

Keywords: Steganography algorithm, pseudo-random generator, LSB method, data hiding, image steganography.

I. INTRODUCTION

Data security is maintained by assuming the consistency and accuracy of data over its entire life cycle. We use cryptography all for secret writing and verifying the correctness of message that are intended for the recipient. The message is usually encrypted from intelligible form to unintelligible form. On the other hand, Steganography conceal the existence of the message. Potential investigators find it very difficult to discover the hidden message. Data hiding does not easily allow access to the multimedia content. It provides various mechanisms to transmit secret messages which are hard to detect by the intruders. This work gives a smart overview of image steganography by proposing a new algorithm i.e. Row into Column Modify Stegno- Algorithm with its applications and its comparison with Matrix Matching Method [1]. The key features of our proposed algorithm include finding the most matching row of the message matrix with the first column (containing LSB of each random pixel) of the randomly selected pixels while previously author has tried to find the best column with minimum effective change with each row of the message matrix one by one.
We will hide data with the help of these techniques and then perform a comparison of result on the basis of PSNR and Normalized Cross Correlation.

II. RELATED WORK

A large number steganographic algorithms [2] have been developed in the literature, including different efficiencies in different parameters like invisibility, payload capacity, robustness against statistical attacks, robustness against image manipulation, independent of file format, unsuspicious files. Any algorithm should find the same set of parameters or any of them with improved values although memory requirements may be different. The simplest data hiding algorithm is the least significant bit data hiding algorithm [3].

The Least Significant Bit embedding technique is a technique which is used to hide the data behind the cover image such that it cannot be seen by human eye. The images used as cover image are generally in 8-bit or gray scale format. We emphasize strongly on Image Steganography providing a strong focus on the LSB technique. Select the message that is to be hidden behind the cover image. Embed the required number of bits in order to hide the MSB (Most Significant Bit) of the message behind the LSB (Least Significant Bit) of the cover image. Since the MSB contains the most important information of the image and the LSB contains the least important information of the image. Replacing the LSB of the cover image with the MSB of the message image will help us to form a stego image.

A new method was introduced by Kaur et al [1], to hide the message behind the cover image. After selecting the pixels randomly in cover image, we have to find the bits of the pixels where insertion has to occur such that they have got good matrix matching results with the bits of the message to be hidden.
The steganalyst jobs become harder as he is unable to crack easily about the location where changes have been made in the bits of the randomly selected pixels. Also, the stego images have been found almost similar to their corresponding cover images, the differences cannot be noticed by the human eye.

According to Rajkumar et al [4], parity checker method, as the name says, is all about the even parity and odd parity checking method. First find the binary value of the pixel if it contains the even number of 1's then it is said to have even parity and if pixel contains the odd number of 1's then it is called as odd parity. The method says insert 0 at the pixel location if its value contains the odd parity and insert 1 at the pixel location if pixel value contains the even parity. If the corresponding parity does not exist at a pixel location either for 0 or 1, then make corresponding parity at that pixel location (odd parity for 0 and even parity for 1) by adding or subtracting 1 to the pixel location.

Liu et al [5], proposed an adaptive matrix embedding method for grayscale images. The 2×4 pixel block is taken as a cover unit. The local correlation of the block is used to determine the message bit amount and choose the corresponding matrix embedding strategy. The method can embed less in image parts with high local correlation and more in image parts with low local correlation.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

III. PROPOSED METHOD

Matrix embedding is a previously introduced method that involves a coding procedure that can be applied to most steganographic schemes without requiring many changes. Embedding schemes that impose fewer embedding changes are more secure because they are less likely to disturb the statistics of the cover object to trigger detection. Here, we have been embedding our message only in the first column (containing LSB of each random pixel) each time. We have generated different matrices just to keep the information of cover image, message image, selected pixels in separate matrix. Actually, the pixel intensity of different pixels have been stored as elements for the cover image, message to be hidden, selected pixels (pixels that are selected using pseudo random generator to store the data bit of message to be hidden in their first column (containing LSB of each random pixel)). The message matrix and the selected pixel matrix are of dimensions 8x8 each. The pixels have been represented in 8-bit notation. The method includes choosing the best row of the message matrix to be inserted into the first column (containing LSB of each random pixel) of the selected pixel matrix. The best row has been decided by calculating the matching factor between all the rows of the 8x8 message matrix and the first column (containing LSB of each random pixel) of the 8x8 selected pixel matrix. The first column has been swapped with that row which has got maximum matching factor as compared to other rows. If more than one row has got same matching factor then the row has been allocated to the first column (containing LSB of each random pixel) on first come first serve basis. We keep the information of the respective row number in a new matrix. To improve the earlier work, here we are improving the PSNR and then NCC by embedding message only in first column (containing LSB of each random pixel), where as any one of the column has been chosen in base paper [1], depending upon the effective change. So in our method, the order of the selected row is represented in separate matrix while in base paper order of the column has been represented in core matrix.

Here, for selecting row number, Matching factor (MF) of each row has been found based on number of matched bits with the first column (containing LSB of each random pixel) of the selected pixel matrix (Row into column modify stegno-algorithm) rather than finding the minimum effective change of each of the 8 columns of the message matrix with each row (Matrix Matching method). In our method, the row with maximum matching factor has been placed in the first column while in matrix matching method (proposed earlier) the column with minimum effective change has been selected for replacement by the row.

IV. ROW INTO COLUMN MODIFY STEGNO-ALGORITHM

1. Select a 8-bit grayscale cover image.
2. Generate a cover matrix for this cover image with element x_{ij}.
3. Now divide the message to be hidden into n frames of 8-bit length each.
4. Generate matrix (for message) of dimension nx8 for the message matrix with element b_{ij}. Let each row be R1, R2,.....Rn.,each of length 8 bit.
5. Now find 8 locations of pixels using some pseudo-random sequence generator (for inserting each row) for each frame. Thus, n matrices(element a_{ij}) has been generated by pseudo-random generator for insertion of each row. Let each matrix be pixel matrix.
6. Our aim is to insert the each row of message matrix only into first column (containing LSB of each random pixel) of pixel matrix generated each time randomly.
7. The row of the message matrix has been decided by calculating Matching Factor(MF).
8. Matching factor=$\sum x_{jt}$ where x_{jt} =1 if $a_{jt} = b_{ij}$ and otherwise x_{jt}= 0 where i,j,t={1,2,3,....8}.
9. After calculating the M.F. of each row with the first column (containing LSB of each random pixel), row with maximum M.F. has been assigned to first column . If two or more rows have same M.F. then row is assigned to the first column on FCFS basis
10. Once the row has been assigned, we continue finding another row with maximum matching factor (from the remaining set of rows) with the first column (containing LSB of each random pixel) of new pixel matrix.
11. Similarly all the rows of the message matrix has been assigned to the first column of the pixel matrix generated randomly for each row.
12. Obtain the stego image after replacing the first column (containing LSB of each random pixel) of each pixel matrix by each row of maximum matching factor.
13. Now keep the order of the insertion of the row of the message matrix in a separate matrix.
14. Calculate Peak signal to noise ratio (PSNR) and Normalized Cross-Correlation (NCC).

At the receiver side, the separate matrix(containing the order in which rows has been inserted in first column) has been sent to the receiver. If the matrix is of small dimension then it can be sent directly else it is reduced in size using huffman coding by the sender itself.

The process of sending the separate matrix and the key required for pseudo-random generator (for generation of pixels) involves embedding them in the cover image or hiding them in some other secret manner. Later the steps of retrieval algorithm are found to be the reverse of the embedding algorithm.

V. EXPERIMENTAL RESULTS AND COMPARISON

The simulation environment used for the algorithm is MATLAB R2013a, Window-7/64-bits, Processor i3, 4 GB RAM. In base paper, the data hiding scheme by using matrix matching method is proposed. The author has calculated matching factor of columns, then the bits of these columns is changed such that change in image quality is minimum i.e. minimum effective change. The final core matrix which shows the column number in each row represents the particular columns in which insertion occurs. Later, he applied Huffman coding over this matrix to store this matrix such that it occupies less space. In our thesis, we are further working on a algorithm by proposing

DOI 10.17148/IJARCCE.2016.5111

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

a new idea to store the message only in the first column (containing LSB of each random pixel) in such a way that all the rows of the message matrix have been matched with the first column (containing LSB of each random pixel) of the selected pixel matrix. The row with the maximum matching bits or say the maximum matching factor has been assigned to the first column. Similarly, the other rows have been selected to assign to the first column (containing LSB of each random pixel) of the selected pixel matrix. Here, we have to store the order of the insertion of the rows in the core matrix. It has been noticed that for insertion a new selected pixel matrix has been generated using pseudo-random generator. The cover images used are lena.jpg, boat.png, jet.jpg, aero.bmp and baby.png and the messages to be hidden are land.jpg, barbara.jpg and pentagon.jpg. In the Matrix matching method [1], the PSNR values are less as compared to our proposed algorithm- Row into Column modify stegno-algorithm. Also, through our algorithm we found the value of NCC to be one or closer to 1 most of the times, this shows that there is very little difference between cover image and stego image.

The term peak signal-to-noise ratio (PSNR) calculated in decibel is an expression for the ratio between the maximum possible value (power) of a signal and the power of distorting noise that affects the quality of its representation

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

$$PSNR = 10\ log_{10}\left[\frac{(255)_2}{MSE}\right] \qquad (1)\ \&\ (2)$$

Where MSE is the mean square error is defined as the square of the difference between the pixel values of the original image and the stego image and then dividing it by size of the image. The Normalized Cross- Correlation (NCC) metric is the metric that is used to show the amount of deflection in the stego image with respect to the cover image after insertion of the message [6]. The higher value of NCC if closer to one, then it corresponds to very little difference between the cover images and their respective stego-images. NCC formula is:

$$NCC = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}(X_{ij}\,xY_{ij})}{\sum_{i=1}^{N}\sum_{j=1}^{M}(X_{ij})^2} \qquad (3)$$

N: Number of rows in cover image, M: Number of columns in cover image, Xij: Intensity of Pixel (ij) in cover image, Yij: Intensity of Pixel (ij) in Stego image.

Cover images:

Lena.jpg

boat.png

jet.jpg

aero.bmp

baby.png

Message images:

Land.jpg

Barbara.jpg

pentagon.jpg

DOI 10.17148/IJARCCE.2016.5111

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

Table I: PSNR values (in decibel) for different images obtained using row into column modify stegno-algorithm and matrix matching method

S.N.	Cover image	Message image	Size of message (Kilobytes)	Row into Column Modify Stegno-Algorithm		Matrix Matching Algorithm	
				PSNR	NCC	PSNR	NCC
1	Lena.jpg	land.jpg	4.03	61.09	1	51.88	0.9999
		Barbara.jpg	8.3	60.77	1	51.51	1
		Pentagon.jpg	15.8	58.44	1	51.55	1
2	Boat.png	land.jpg	4.03	61.6	1	51.67	1
		Barbara.jpg	8.3	61.39	1	51.62	1
		Pentagon.jpg	15.8	58.72	1	51.64	0.9999
3	Jet.jpg	land.jpg	4.03	60.79	1	51.72	1
		Barbara.jpg	8.3	60.52	1	51.62	1
		Pentagon.jpg	15.8	58.03	1	51.53	1
4	Aero.bmp	land.jpg	4.03	61.39	1	51.87	1
		Barbara.jpg	8.3	61.13	1	52.08	1
		Pentagon.jpg	15.8	58.63	1	51.28	1
5	Baby.png	land.jpg	4.03	60.9	1	51.74	0.9999
		Barbara.jpg	8.3	60.59	1	51.91	0.9998
		Pentagon.jpg	15.8	58.03	1	51.85	1

Table II: NCC value for different images obtained using row into column modify stegno-algorithm and matrix matching method

Row into Column Modify Stegno-Algorithm	**Matrix Matching Algorithm**
1	0.9999
1	1
1	1
0.9999	0.9999
0.9999	0.9998
1	0.9998
1	1
1	0.9999
1	0.9998
1	1

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 1, January 2016

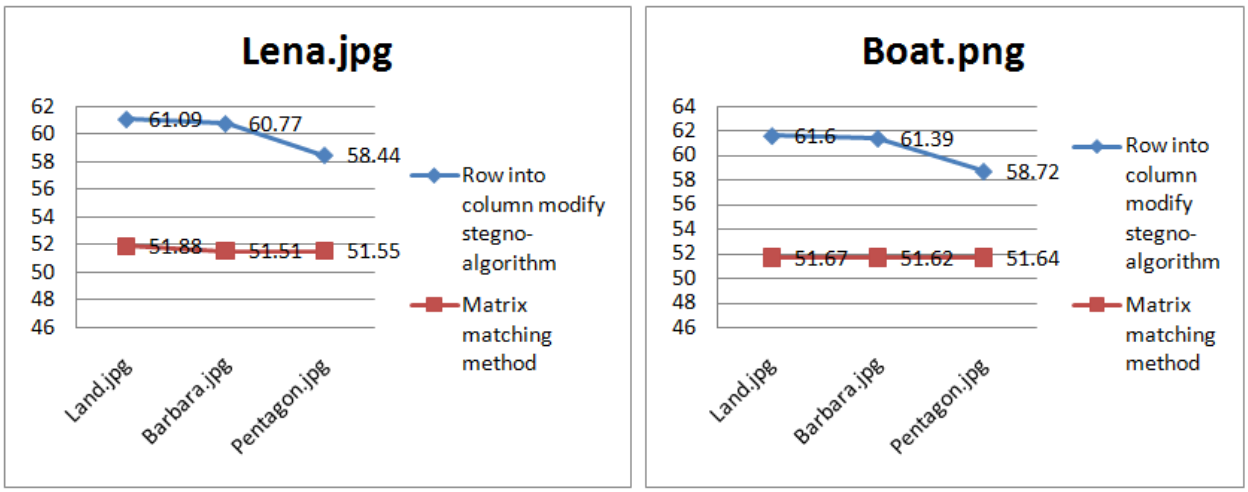

Fig 1. Graph showing PSNR values (in decibel) after hiding messages behind lena.jpg & boat.png

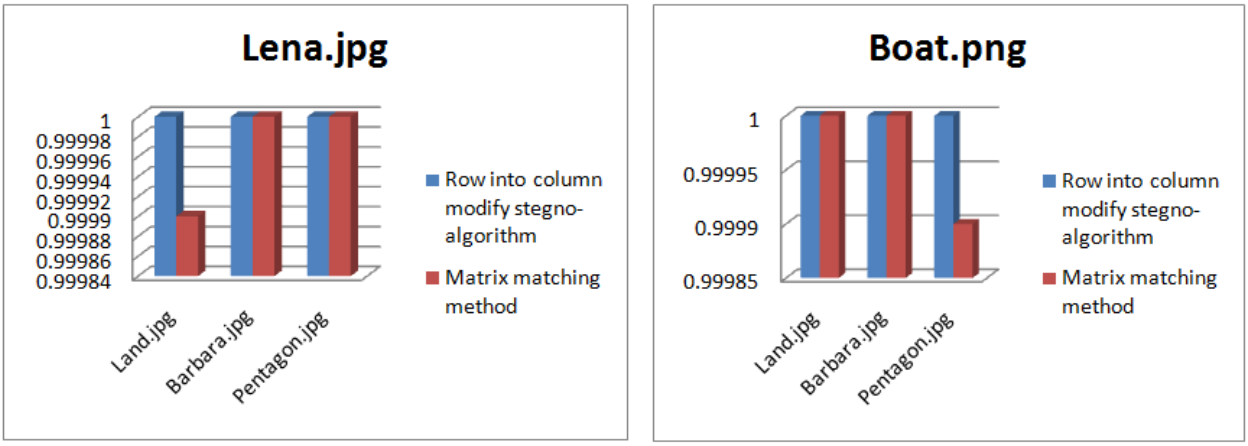

Fig 2. Graph showing NCC values after hiding messages behind lena.jpg & boat.png

VI. CONCLUSION

With the improved value of PSNR, our proposed algorithm Row into Column Modify stegno- Algorithm proved to be the better technique as compared to the Matrix Matching method. Also, when compared with the cover image, the stego image obtained can hardly be of any difference from it. The value of NCC help us to find the difference between the cover and its corresponding stego image as NCC value when 1 or closer to 1 then our stego image is said to be almost similar to the cover image. The Row into Column modify stegno- method gives better performance in the said parameters.

REFERENCES

[1] Kaur, J., Duhan, M., Kumar, A., Yadav, R.K.. Matrix Matching Method for secret Communication using image steganography. Fascicule 3. 2012. 45-48

[2] Umamaheswari, M., Sivasubramanian, S., Pandiarajan, S. Analysis of different steganographic algorithms for secured data hiding. IJCSNS International Journal of Computer Science and Network Security. 2010: 10 (8); 154-160

[3] Dey, S., Abraham, A. , Sanyal, S. An LSB data hiding technique using prime numbers. Third International Symposium on Information Assurance and Security, IEEE, 2007;101-106.

[4] Rajkumar, Rishi, R., Batra, S. A new steganography method for gray level images using parity checker. International Journal of Computer Applications. 2010: 11(11); 18-24

[5] Liu, G., Liu, W., Dai, Y., Lian, S. An adaptive matrix embedding for image steganography. IEEE, Third International Conference on Multimedia Information Networking and Security (MINES). 2011:642- 646.

[6] Chawla, G., Kamaldeep, Yadav, R., Ravi. Analysis of various image steganography techniques on the basis of normalized cross correlation (NCC). International Journal on Advanced and Innovative Research. 2012: 1(2);1-4

DOI 10.17148/IJARCCE.2016.5111