



Raster Scan Technique for Secure Communication in Steganography

Yogita Birdi¹, Harjinder Singh²

PG Student [ECE], Dept. of ECE, University College of Engineering, Punjabi University, Patiala, India¹

Assistant Professor, Dept. of ECE, University College of Engineering, Punjabi University, Patiala, India²

ABSTRACT: Steganography is an art of hiding the fact that communication is taking place, by concealing information in other information. In this paper data is encrypted and for hiding Raster Scan technique is proposed. This technique is similar to Raster Scan principle of displaying an image on CRT display. In this work Mean Square Error and Peak Signal Noise Ratio is calculated for the proposed technique and the results are compared with existing techniques. Histograms are also drawn between existing results and proposed work to show the variation.

KEYWORDS: Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Least Significant bit (LSB).

I.INTRODUCTION

In today's world, the communication is the basic necessity of every growing area. Everyone wants the secrecy and safety of their communication. The mechanisms used for secure communication are cryptography and Steganography [1].

In cryptography, the message is modified in an encrypted form with the help of encryption key which is known to sender and receiver only. On the other hand Steganography is an art and science of communicating in such a way that it hides the existence of the communication. The word "stegano" means hidden and "graphei" means writing. The main idea of steganography is to send message between two parties without any suspicions from intruders [2].

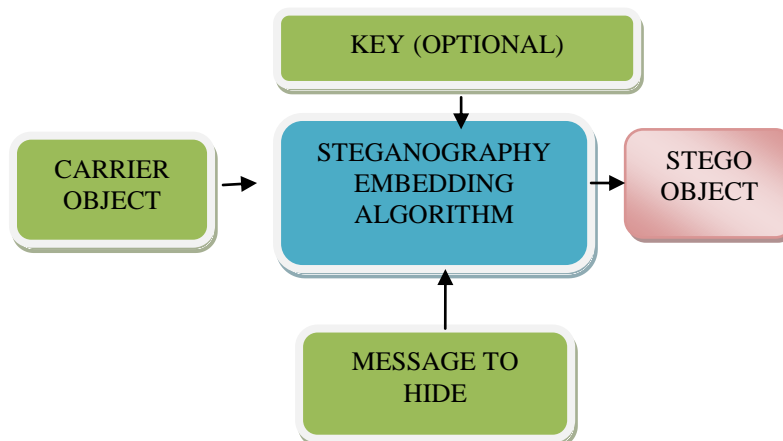
The basic model of steganography consists of three components [3].

1. The Carrier Image
2. The Message
3. The Key

1. The Carrier Image: The carrier image is also called the cover object that will carry the message that is to be hidden.

2. The Message: A message can be anything like data, file or image etc.

3. The Key: A key is used to decode/decipher/discover the hidden message. The key is optional in Steganography.



Basic Model of Steganography

To measure the imperceptibility of steganography several metrics are used. The metrics indicates how similar or different the stego image with the cover image is.



International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

The following metrics are used

1. **Mean Squared Error (MSE)** is computed by performing byte by byte comparisons of the cover image and stego image. The Computation expressed as[4]

$$MSE = \frac{1}{M*N} \sum_{i=1}^M \sum_{j=1}^N (F_{ij} - G_{ij})^2$$

M: number of rows of cover image
N: number of columns of cover Image
F_{ij}: Pixel value from cover image
G_{ij}: Pixel value from Stego Image

Higher value of MSE indicates dissimilarity between Cover image and Stego image.

2. **Peak signal to noise ratio (PSNR)** measures in decibels the quality of the stego image compared with the cover image. The higher the PSNR better the quality. PSNR is computed using the following equation [4].

$$PSNR = 20 \log_{10} Peak - 10 \log_{10} MSE$$

II. LITERATURE SURVEY

Juneja et al. [5] in this paper enhanced Least Significant bit technique is proposed. Least significant bit is the most common technique used for hiding the secret information in any digital media like image, text or audio/ video. LSB refers to replacement of first bit of image with the bit of secret message from LSB side. Although LSB is simple and useful for the user but it can be detected by attackers during transmission of data on the network. There are many versions of LSB like Edge LSB, random LSB, and Enhanced LSB.

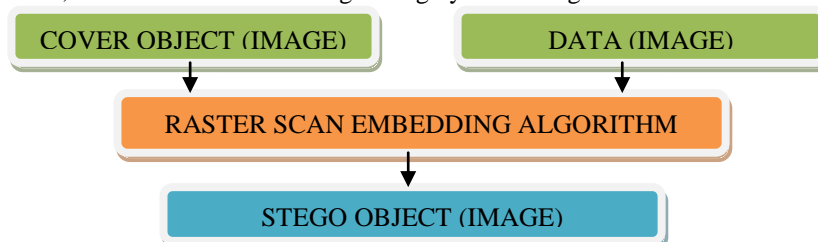
Samidha et al. [6] in this paper, many steganography techniques can be used like Least Significant bit, layout management scheme. Along with this technique, some more techniques are proposed, based on selection of random pixels from an image and again secret data is hidden in random bits of these randomly selected pixels.

Tanni et al. [7] in these paper, gray level values of the image pixels are modified. It provides one to one mapping between the binary data and the selected pixels in the image. A set of pixels are selected from the image. Firstly, all the odd selected pixels are made even by changing gray level by one unit. Then, a comparison is made by selecting first bit from the message and first bit of the pixels. If the first bit is even (0) then all pixels have even gray level and are not modified at all. But if the first bit is odd (1) then gray level of the pixels is decremented by one unit to make its value odd. Thus, gray level of all the pixels is modified accordingly.

In this paper we take motivation from ref. [5, 6] and proposed a new technique for data hiding. In this technique data is hiding based on Raster Scan principle used in CRT or television for displaying images. In these proposed technique data first hide from Left to right then right to left. For proposing Raster Scan technique data is hiding using modified LSB technique.

III. PROPOSED WORK

In this proposed model, the RGB color cover image and gray scale image data are read simultaneously. After that, raster



Block diagram of Proposed Technique



International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

Scan principle applied on data and data is hiding using modified LSB technique so that little bit variation in Stego image. To measure the imperceptibility of stego image, MSE and PSNR are calculated and compared with the existing algorithms.

Proposed Algorithm for Raster Scan Technique

1. Read the cover image.
2. Read the data and convert into binary format.
3. Hide the encrypted data using Raster Scan principle in cover image by doing XORing of cover image with data bits.
4. Mean square error (MSE) is calculated by comparing the stego image with cover image.
5. Peak Signal Noise Ratio (PSNR) is calculated from MSE.
6. Plot Histogram for MSE and PSNR and compare with existing results.

Example:

1. Cover Image Pixel values

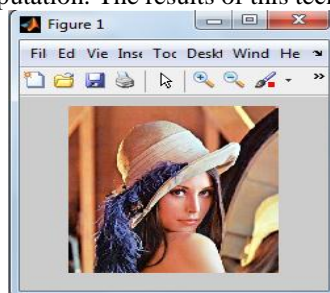
10101100	01010111	00110011	11001100
10010010	00011100	11111100	01011011
00011000	11110000	00111000	10101010
10101011	10101111	00000001	11000011

2. Data to hide-01101000,10101100,01001100,11001100
3. Encrypted Data to hide-
10010111,01010011,10110011,00110011
4. Message will be hidden using following technique.

101011 11	010101 01	001100 01	110011 10
→			
100100 01	000111 01	111111 00	010110 11
←			
000110 11	111100 00	001110 11	101010 10
→			
101010 00	101011 11	000000 00	110000 11
←			

IV.SIMULATION RESULTS

In this implemented Raster Scan Technique using modified LSB technique in MATLAB 2013. MATLAB, which stands for **MA**Trix **LAB**oratory, is a state-of-the-art mathematical software package, which is used extensively in both academia and industry. It is an interactive program for numerical computation and data visualization, which along with its programming capabilities provides a very useful tool for almost all areas of science and engineering. It is one of the leading software packages for numerical computation. The results of this technique as follows:



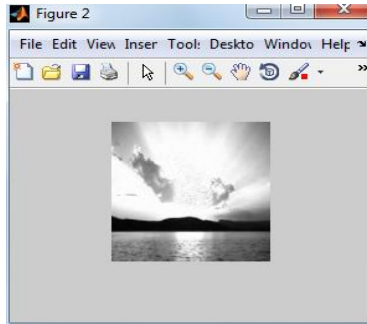
Cover Image (512x512)



International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

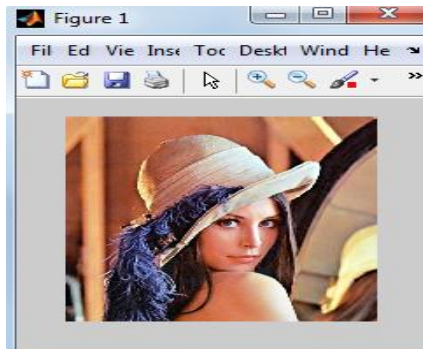
Vol. 4, Issue 6, June 2015



Data (128x128)



Encrypted Data (128 x128)



Stego Image (512 x 512)

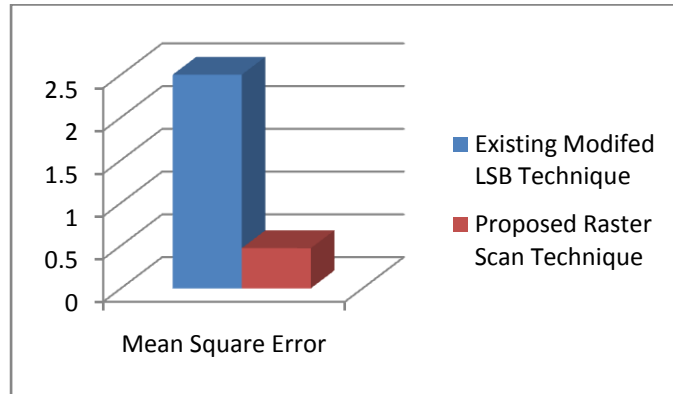
	Existing Modified LSB Technique[4]	Proposed Raster Scan Technique
Mean Square Error	2.5	0.47
Peak Signal to Noise Ratio	44.1dB	51.37dB



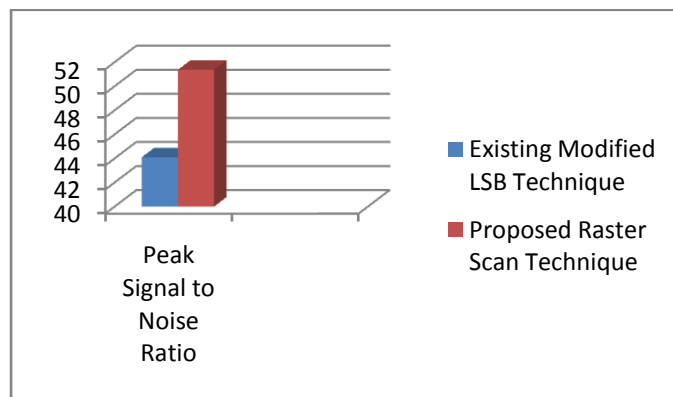
International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015



Histogram for Mean Square Error



Histogram for Peak Signal to Noise Ratio

V.CONCLUSIONS

In this paper Raster Scan algorithm is implemented using existing modified LSB technique for image hide in a cover image. In our work the negative of original image hide in cover image so it's difficult to extract the original image from over image because

- a) Pixels hide left to right then right to left.
- b) Even if an unknown person extracts the image from cover image they get the negative of original image.

Also in proposed algorithm in place of replacing Exoring of cover pixel with data pixel is done. Due to this probability of pixel variation reduces and PSNR value increases.

REFERENCES

- [1] Jasleen Kour, Deepankar Verma, "Steganography Techniques- A review paper", International Journal of Engineering Research in Management and technology, vol. 3, pp. 132-135, may 2014.
- [2] Gunjan Chugh, Rajkumar Yadav, and Ravi Saini, "A new image steganographic approach based on Mod factor for RGB images", International Journal of signal processing, image processing, and pattern recognition, vol. 7, pp. 27-44, 2014.
- [3] Md. Khalid Imam Rahmani, Kamiya Arora, and Naina Pal, "A crypto-Steganography: A Survey", International Journal of Advanced Computer Science and application, vol.5, 2014.
- [4] Bassam Jamil Mohd, Saed Abed and Thaier Al-Hayajneh and Sahel Alouneh, "FPGA hardware of the LSB Steganography", International Conference on Computer, Information and Telecommunication Systems (CITS), pp. 1-4, 2012.
- [5] M.Juneja, P.S. Sandhu, "Data Hiding with Enhanced LSB Steganography and Cryptography for RGB Color Images", International Journal of Applied Research , ISSN: 2249-555X , vol. 3(5), pp. 118-120, May 2013.
- [6] Dr. Diwedi Samidha, Dipesh Agrawal, "Random Image Steganography in Spatial Domain", International Journal of Computer Science and Information Security Publication March 2010, vol 7, March 2013.



ISSN (Print) : 2320 – 3765
ISSN (Online): 2278 – 8875

International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 4, Issue 6, June 2015

- [7] A. T. Al-Taani and A.m. AL-Issa, "A novel Steganographic method for gray level images", International journal of computer and information engineering, 2009.
- [8] A. Gupta and R.Garg, "Detecting LSB Steganography in Images"2012.
- [9] J. Madison, S.D. Dickman, "An Overview of Stegano- graphy", 2007.
- [10] M.M Amin, M. Salleh, S. Lbrahim,M.R.K Atmin,and M.Z.I Shamsuddin,"information hiding using steganography", IEEE 4th National Conference on Telecommunication Technology Proceeding, Shah Alam.Malaysia,pp.21-25,January 2003.