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

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 3, Issue 12, December 2014

Random Scan Algorithm for Image Steganography in Scilab for Security Purposes

Ishant Premi[1], Mrs. Sukhjinder Kaur[2]

Lecturer, Electronics and Communication Dept. Thapar Polytechnic College, Patiala, India[1]

Associate Professor, Electronics and Communication Dept. Sri Sukhmani Institute of Engineering & Technology, Dera Bassi, India[2]

Abstract: In this paper, after entering the Secret Key the encrypted data is generated by determining their class. After that encrypted data is hidden in random bits of cover image using XORing method. By doing XORing the probability of pixel variation reduces as compared to replacing method as done in LSB or Modified LSB method. In this paper calculate the MSE, PSNR and Correlation Factor for Random Scan Algorithm in Scilab. In this paper also draw histograms between Cover image and Stego image to show how much Pixels variation.

Index Terms: Steganography, MSE, PSNR.

INTRODUCTION

Internet users frequently need to store, send, or receive private information. The most common way to do this is to transform the data into a different form. The resulting data can be understood only by those who know how to return it to its original form. This method of protecting information is known as encryption.

Before the invention of digital means, traditional methods were being used for sending or receiving messages. Before phones, before mail messages were sent on foot. For the messages where privacy was of prime concern, the ways of implementing security were following:

1. Choosing the messenger capable of delivering the message securely.
2. Write the message using such notations that actual meaning of the message was concealed.
3. Hide the message such that even its presence can’t be predicted.

Nowadays Steganography and Cryptography are well known and widely used techniques that manipulate information in order to cipher or hide their existence respectively.

Steganography is the art and science of communicating in a way which hides the existence of the communication. Cryptography scrambles a message so it cannot be understood; the Steganography hides the message so it cannot be seen. Even though both methods provide security, a study is made to combine both cryptography and Steganography methods into one system for better confidentiality and security.

A Steganography system consists of three elements: cover object (which hide the secret message), the secret message and the stego object (which is the cover object with message embedded inside it) [1].

Figure 1: shows the fundamental block diagram of Steganography. In Steganography cover image and secret data is read then embedding algorithm applied for the secret data to hide in cover object. After the Stego object is transmitted. At receiver side recovery algorithm applied on stego object for extracting secret data.

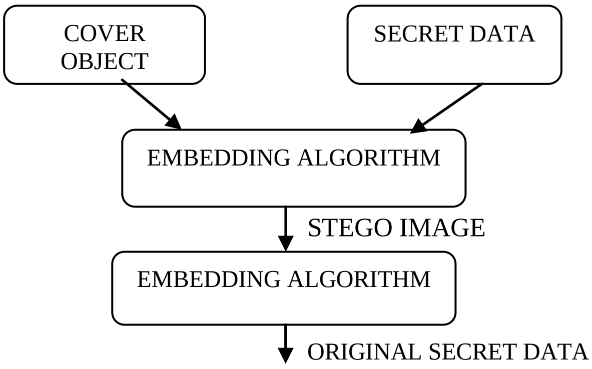


Figure 1: Block Diagram of Steganography [2]

1. Characterization of Steganography

In Steganography techniques a message embed inside a cover image. Various features characterize the strength and weaknesses of a method.

1.1 **Capacity**

The capacity in data hiding indicates the total number of bits hidden and successfully recovered by the Stego system.

1.2 **Robustness**

Robustness refers to the ability of the embedded data to remain intact if the system undergoes transformation like linear and non linear filtering, addition of random noise, rotation, scaling and compression.

1.3 **Undetectable**

The embedded algorithm is undetectable if the image with the embedded message is consistent with a model of the source from which images is drawn. Undetectability is directly affected by the size of the secret message and the format of the content of the cover image.

1.4 **Invisibility (Perceptual Transparency)**

The concept of Invisibility based on the properties of the human visual system. The embedded information is imperceptible if an average human is unable to distinguish between carriers that contain hidden information and others do not. It is important that the embedding occurs

DOI 10.17148/IJARCCE.2014.31245

without a significant degradation or loss of perceptual quality of the cover.

1.5 **Security**

The embedded algorithm is to be secure if the embedded information is not subject to removal after being discovered by the attacker and it depends on the total information about the embedded algorithm and secret key [3].

There are many application of Steganography in the area of featured tagging, secret communication, covert communication, copy right protection, military and intelligence agencies, TV broadcasting, Multimedia content copyrights etc.

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

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]

$$MSE=\frac{1}{M*N}\sum_1^M \sum_1^N (Fij-Gij)^2$$

M: numbers of rows of cover image
N: number of column of Cover Image
Fij: Pixel value from cover image
Gij: 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].

$$PSNR=20\log_{10} 255-10\log_{10} MSE$$

3. **Correlation Factor**: Correlation factor is one of the performance parameter. Correlation coefficient 'r' is the measure of extent and direction of linear combination of two random variables. If two variables are closely related, the correlation coefficient is close to the value 1. On the other hand, if the coefficient is close to 0, two variables are not related [5].

$$r=\frac{\sum_i(Xi-Xm)(Yi-Ym)}{\sqrt{\sum_i(Xi-Xm)^2}\sqrt{\sum_i(Yi-Ym)^2}}$$

Where
Xi - pixel intensity of original image
Xm- mean value of original image intensity
Yi- pixel intensity of encrypted image
Ym - mean value of encrypted image intensity

For Steganography the Correlation factor should be 1 for ideal Case so no dissimilarity in Stego image as compared to cover image.

In this paper calculate MSE, PSNR and Correlation factor for Random Scan Method.

RANDOM SCAN METHOD

1. Let suppose Cover image pixel values:

11001100	01011010	00001010	01010101
10101010	01010101	10110011	11110000

2. Let suppose message data values: 01101011
3. Using XORing Random Scan Method Stego Pixel values.

Cover image	11001100	01011010	00001010	01010101
Message Bits	00000011	00000100	00010000	01000000
Stego Image	11001111	01011110	00011010	00010101

In XORing method the probability of bits variation reduces as compared to LSB Replacing method.

RANDOM SCAN ALGORITHM

Transmitter Side

1. Read the cover image.
2. Read the message.
3. Enter the Secret key.
4. Generate the encrypted message by determining their class.
5. Read the Encrypted message and convert into binary format.
6. Hide the Encrypted data in Random bits of cover image by doing XORing of cover image with data bits.
7. Mean square error (MSE) is calculated by comparing the stego image with cover image.
8. Peak Signal Noise Ratio (PSNR) is calculated from MSE.
9. Correlation Factor calculated between Cover image and Stego Image.
10. After hiding data Stego image is transmitted.

Receiver Side

1. At the Receiver side the Secret key enter and if they match then only Extraction of data is Possible.
2. After matching the Secret Key XORing of cover image and Stego image is done to extract the encrypted data bits from stego image.
3. Then Original message is generated by subtracting the data bits from their class.

The security level increases in this proposed method because

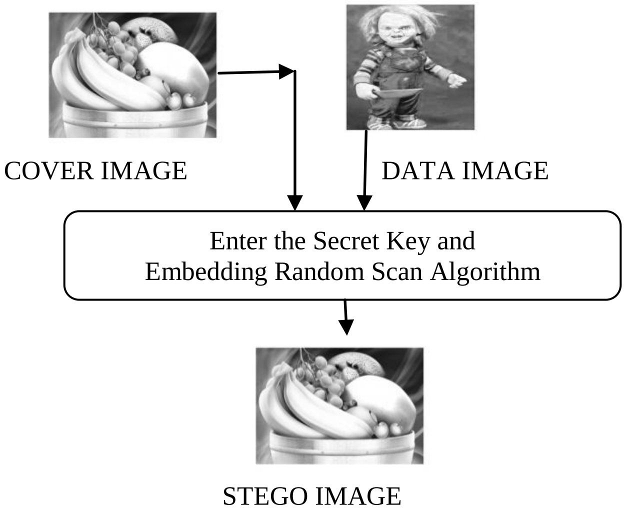
1. The Secret Key for Embedding and extracting the data.
2. The Encrypted data generated by determining their class.
3. By doing XORing the data bits with cover image pixels bits again encrypted data generated.

Simulation Results

In this paper we simulate Random Scan Method in Scilab-5.4.1(64 bit).Scilab is a freely distributed open source scientific software package, first developed by researchers from INRIA and ENPC, and now by the Scilab Consortium. It is similar to Matlab, which is a commercial product. Yet it is almost as powerful as Matlab. Scilab consists of three main components:

- an interpreter
- libraries of functions (Scilab procedures)
- libraries of Fortran and C routines

Scilab is specialized in handling matrices (basic matrix manipulation, concatenation, transpose, inverse, etc.) and numerical computations. Also it has an open programming environment that allows users to create their own functions and libraries [11]. The results of this method as follows:

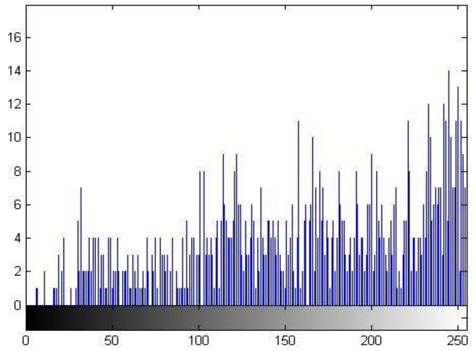


BLOACK DIAGRAM FOR RANDOM SCAN METHOD

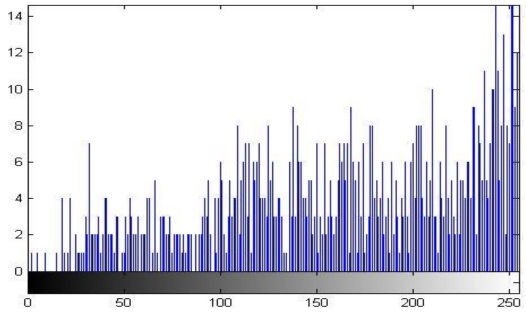
1. MSE and PSNR for Proposed Method

COVER IMAGE SIZE	32*32
DATA IMAGE SIZE	16*16
MSE	31
PSNR	33dB
Correlation Factor	0.99

2. Histograms for Cover Image



2. Histograms for Stego Image



CONCLUSION

In this paper encrypted data is hiding using Random Scan method in Scilab. The following advantages of proposed method

1. High Security of data because of Secret key and Encryption data is hiding.

2. In existing methods up to 4 bits from LSB side data is hiding but in this method up to 8 bits hide the data and even with acceptable PSNR.

3. In this the correlation factor comes 0.99 so its show that Stego image approximate looks like Cover image even after hiding the data.

REFERENCES

[1] A. Joseph Raphael and Dr. V. Sundaram "Cryptography and Steganography –an Survey" *International Journal of Computer Technology Application*, vol 2, pp. 626-630, 2012.

[2] Himanshu Gupta , Prof Ritesh Kumar and Dr. Soni Changlani "Enhanced Data Hiding Capacity using LSB-Image Steganography Method" *International Journal of Emerging*Technology *and Advanced Engineering"* vol 3,June 2013.

[3] Zaidoon Kh. AL-Ani, A.A.Zaidan, B.B.Zaidan and Hamdan.O.Alanazi "Overview-Main Fundamental for Steganography" *Journal of Computing*, vol 2, March 2010.

[4] Bassam jamil Mohd,saed Abed and Thaier Al-Haneh,sahel Alouneh, "FPGA hardware of the LSB Steganography method" *International Conference on Computer, Information and Telecommunication Systems (CITS)*, pp 1-4, 2012.

[5] S. Thenmozhi and M. Chandrasekaran "A Novel Technique for Image Steganography Using Nonlinear Chaotic Map" *7th International Conference on Intelligent Systems and Control (ISCO), pp. 307-311, 2013.*

[6] Dr. Diwedi Samidha and Dipesh Agrawal, "Random Image Steganography in Spatial Domain", *International Journal of Computer Science and Information Security*, vol 7, pp. 3, March 2013.

[7] Ankita Ganorkar and Sujata Agrawal "Releaving the Hidden Secret with LSB Steganography" *International Journal of Innovative*

Research in Electrical, Electronics, Instrumentation and Control Engineering, vol. 1, Issue 3, June 2013.

[8] Deshpande Neeta, Kamalapur Snehal and Daisy Jacobs "Implementation of LSB Steganography and its evaluation for various bits" *IEEE 1st International Conference on Digital Information Management*, India, pp.173-178, December 2006.

[9] 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.

[10] H.Wang,S. Wang, "Cyber warfare: Steganography vs Steganalysis", *Communications of the ACM*, vol. 47, no. 10, pp. 76-82, October 2004.

[11] *http://en.wikipedia.org/wiki/Scilab*

DOI 10.17148/IJARCCE.2014.31245