Random Scan Algorithm for Image Steganography in Scilab for Security Purposes

Ishant Premi¹, Mrs. Sukhjinder Kaur²

Lecturer, Electronics and Communication Dept. Thapar Polytechnic College, Patiala, India¹
Associate Professor, Electronics and Communication Dept. Sri Sukhmani Institute of Engineering & Technology, Dera Bassi, India²

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.

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
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]

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

- 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].

\[
PSNR = 20 \log_{10} \frac{255}{\sqrt{MSE}}
\]

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].

\[
r = \frac{\sum (X_i - \bar{X})(Y_i - \bar{Y})}{\sqrt{\sum (X_i - \bar{X})^2}(\sum (Y_i - \bar{Y})^2)}
\]

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:

<table>
<thead>
<tr>
<th>Cover image</th>
<th>11001100</th>
<th>01011010</th>
<th>00001010</th>
<th>01010101</th>
</tr>
</thead>
<tbody>
<tr>
<td>10101010</td>
<td>10100110</td>
<td>11101000</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. Let suppose message data values: 01101011

3. Using XORing Random Scan Method Stego Pixel values.

<table>
<thead>
<tr>
<th>Cover image</th>
<th>11001100</th>
<th>01011010</th>
<th>00001010</th>
<th>01010101</th>
</tr>
</thead>
<tbody>
<tr>
<td>Message Bits</td>
<td>00000011</td>
<td>00000100</td>
<td>00010000</td>
<td>01000000</td>
</tr>
<tr>
<td>Stego Image</td>
<td>11011111</td>
<td>01011110</td>
<td>00011010</td>
<td>00010101</td>
</tr>
</tbody>
</table>

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:

![Stegno Image Diagram](image)

**BLOACK DIAGRAM FOR RANDOM SCAN METHOD**

1. **MSE and PSNR for Proposed Method**

<table>
<thead>
<tr>
<th>COVER IMAGE SIZE</th>
<th>32*32</th>
</tr>
</thead>
<tbody>
<tr>
<td>DATA IMAGE SIZE</td>
<td>16*16</td>
</tr>
<tr>
<td>MSE</td>
<td>31</td>
</tr>
<tr>
<td>PSNR</td>
<td>33dB</td>
</tr>
<tr>
<td>Correlation Factor</td>
<td>0.99</td>
</tr>
</tbody>
</table>

2. **Histograms for Cover Image**

3. **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**


