JNNCE Journal of Engineering & Management – A Peer Reviewed Bi-annual Journal
Available online @ https://jjem.jnnce.ac.in
ISSN: 2582-0079 (O)
https:// www.doi.org/10.37312/JJEM.2019.030209
Indexed in International Scientific Indexing (ISI)
Impact Factor Value: 1.025 for 2018-19
Volume: 3, Issue: 2
July - December 2019
Date of Publication: 12-30-2019

A Novel Technique for Steganography using LSB Method

Jishi B Nair
4th Semester, Dept of MCA,
JNNCE, Shimoga
jishupapu@gmail.com

Dr. Raghavendra.S.P
Assistant Prof., Dept of MCA,
JNNCE, Shimoga
raghusp.bdvt@gmail.com

Abstract
This paper provides a novel approach and gives brief survey on various steganographic strategies for encryption of the information. Steganography is a method of converting the information into the image. This paper helps to know the phrases related with steganography using LSB substitution method, experimental result and accuracy is examined on different datasets. Results obtained are satisfactory compared to the state of the state of the art methods.

1. Introduction

1.1Evolution of steganography and Cryptography

The security of the information is the most important factor of information technology and communication. To provide security to the information over the internet, the two techniques are used Steganography and Cryptography.

1.2 Steganography

The process of enclosing the data or the information within something to provide security for the information that is being transferred with the intension of being unobserved. In Greek, stegano means covered and graphy means writing, hence the name Steganography.

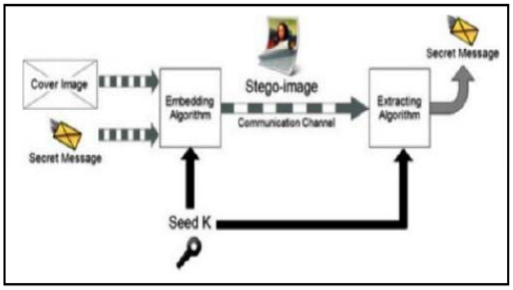


Fig1: Block Diagram of Steganography

Steganography is accomplished on varieties of data sets, according to the application requirement some of these classification is depicted in the following diagram.

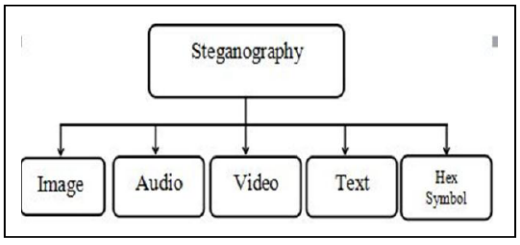


Fig 2: Steganography Classification Diagram

1.3 Cryptography

Cryptography coverts the information in such a way that no one can understand it, the person who holds the key can only

read it. In Greek Crypto means secret and Graphy means writing.

1.4 Importance of Steganography over Cryptography

Though the encryption of information allows secure communication and the need of a key to read the information is important and the encryption cannot be removed by the attacker, it is easy for him to make changes to the file and make it unreadable. On the other hand, Steganography provides secure and protected communication. The attacker will not be able to even detect that the information is embedded. Even if the attacker detects the presence of hidden message it is almost impossible to alter the content.

2. Literature Survey

Various researchers have made significant contribution in the area of steganography few of them have been discussed in this paper.

Alpa Agath [1] etal have proposed a novel technique an overview about the concepts of cryptography and steganography. Moreover, it presents a fair comparative analysis between various selected encryption algorithms on various parameters such as key size, block size, speed of encryption, level of security provided by algorithm, and memory usage. Danny Adiyan [2] etal have discussed concepts on steganography will be combined with vigenere cipher. Steganography utilizes the weakness of the human eye in viewing the image file; steganography also uses mathematical calculations in inserting messages into the image file. Deepali V. Patil [3] etal have discussed ideas on Review Paper on image steganography. This paper deal with the concept of Steganography by explaining firstly the meaning of Steganography and the terms related to it.Dr. Amit Kumar Goel[4] and etal has discussed in their project on the strength of stenography methods to enhance the security of communication over an open channel.Govind R. Suryawanshi [5] etal have discussed concept on Analysis of Effect of Spatial Domain Steganography Technique on DCT Domain using Statistical Features for Digital Images. This paper focuses on the different spatial domain Steganography techniques and their artifacts that leaved after data hiding. Alpa Agath [6] etal have discussed concept on Critical Analysis of Cryptography and Steganography. This paper focuses on overview about the concepts of cryptography and steganography. Moreover, it presents a fair comparative analysis between various selected encryption algorithms on various parameters such as key size, block size, speed of encryption, level of security provided by algorithm, and memory usage.B.G.Aagarsana[7] etal have proposed Image Steganography Using Secured Force Algorithm For Hiding Audio Signal Into Color Image. This paper deals with o hide audio signal into color image using AES algorithm and circular LSB algorithm.Amit Kumar[8] etal have disscussed on Result Analysis of DWT and LSB based Audio Steganography. This paper concentrates on providing high level of security, maximum embedding capacity; efficiency and reliability for secret communication using image processing and steganographic techniques.Blerim Rexha [9] etal have proposed Efficiency of LSB and PVD Algorithms Used in Steganography Applications. This paper deals with different parameters that affect efficiency of LSB and PVD algorithms, impact of carrier type, format, and size.Amit Kumar[10] etal have discussed about DWT and LSB based Audio Steganography- A Review .This paper deals with existing position of art literature in digital audio steganography technique. In this paper a completely unique methodology for digital audio steganography someplace encrypted

concealed data is embedded by adaptively modifying wavelet packet coefficients of host audio signal.

3. Methodologies

The proposed methodology focuses on different types of techniques involved in steganography, which are capable of producing image that I embedded with secrete message. The efficiency of this method is calculated by computing Mean Square Error (MSE) and Peak Signal to Noise Ratio (PSNR).

3.1 LSB Substitution Method

If we want to hide the information within the images LSB method is used. One bit of secret information is substituted in the 8th bit of each byte of file which is used as carrier.

3.2 Optimum Pixel Adjustment Procedure

OPAP is used to minimize the disturbance or distortion caused by LSB substitution method. The pixel value is adjusted in OPAP method after hiding the secret data. By doing this the quality of the stego image is increased without making changes to the data which is hidden.

3.3 IP Approach (Inverted Pattern)

In IP approach before embedding secret message has been processed. The secret images are checked to be inverted or not inverted before embedding. To record the transformation which is treated as secret key to be re-embedded, bits are used.

3.4 IP method using Relative Entropy

Instead of calculating the MSE for inverting pattern approach, relative entropy is calculated.

3.5 The hiding streams of 1's and 0's

This method uses the 0's and 1's present for hiding. In this method hidden data is converted into binary. The occurrence of 1's and 0's are computed and substituted in the pixels of cover image. The occurrence of 1's is placed in the odd columns of the pixel and the occurrence of 0's is placed in even columns.

3.6 Pixel value differencing

This method can provide a stego image which is of high quality. The quantity of bits inserted is dependent on the quality of the pixel i.e., edge area or smooth area.

3.7 The mod method

By subtracting any remainder obtained from dividing with 10the embedding is done.

3.8 The MOD 10 based method

After dividing the gray value of the pixel by 10, the data is hidden in the remainder obtained. The key determines whether the information is similar as the remainder or 10-remainder.The quality of the stego image is increased by this key.

3.9 DCT

A transform domain technique, the proposed methodology uses DCT for hiding messages in specific areas of cover image. In this technique, pixels are split into 8X8 blocks. Each block encodes one secrete message.

The function of LSB technique is to embed the message in the image. In this method initially message is encrypted and then it is embedded in the image at LSB position. The values of entropy and correlation of steno image and original image is measured after embedding. The method is said to be safe if both the values are same. Before sending it to the receiver, numerous vertical and horizontal blocks are created at the sender side. The secret transformation table is rebuilt by the receiver after sorting the secrete message from the encrypted image. Only secrete information is transferred instead of transferring whole transformation table. Security, capacity and imperceptibility are the three main things which are covered in this topic. In steganograhic technique, to hide the data inside the image new algorithms are generated. To embed the data inside the image, Pixels are used. The stego image has been saved in the popular JPEG format.

4. Proposed Methodology

In the Proposed methodology we are going to consider the category of images defined as input image $f(x,y)$ and Message image $m(x,y)$ along with the cover image $c(x,y)$.

The Stego image $s(x,y)$ is obtained by combining the cover image $c(x,y)$ and message image $m(x,y)$.

Furthermore the extracted message image $e(x,y)$ can be obtained by extracting cover image from stego image which is depicted as below:

Inspite of being simple, LSB technique have the disadvantage of causing distortion when the embedded bits for each pixel exceeds three in number, which is noticeable .Image Encryption approach provides lower payload. It requires more computational work when the key size is larger. The methodology compresses the key size to provide more payloads.

$$f(x,y) = \sum_{i=1}^{x} \sum_{j=1}^{y} f(x,y) \quad (1)$$

$$c(x,y) = \sum_{i=1}^{x} \sum_{j=1}^{y} c(x,y) \quad (2)$$

$$m(x,y) = \sum_{i=1}^{x} \sum_{j=1}^{y} m(x,y) \quad (3)$$

$$s(x,y) = \sum_{i=1}^{x} \sum_{j=1}^{y} c(x,y) + \sum_{i=1}^{x} \sum_{j=1}^{y} m(x,y) \quad (4)$$

$$e(x,y) = \sum_{i=1}^{x} \sum_{j=1}^{y} s(x,y) - \sum_{i=1}^{x} \sum_{j=1}^{y} c(x,y) \quad (5)$$

$$e(x,y) = \sum_{i=1}^{x} \sum_{j=1}^{y} m(x,y) \quad (6)$$

MSE: It represents the cumulative squared error between the compressed and the original image represented as mse It is calculated using:

$$mse = \frac{1}{R*C} \sum_{i=1}^{R} \sum_{j=1}^{C} \left(x_{ij} - x'_{ij}\right)^2 \quad (7)$$

Where R and C are the dimensions of the image. Matrix x_{ij} represent the original image. x'_{ij} represent the stego image.

PSNR (Peak Signal to Noise Ratio): represents the measure of the peak error.

PSNR is estimated using:

$$psnr = 10 \log 10 \left[\frac{I*I}{mse}\right]_{db} \quad (8)$$

Where I is the maximum possible value of the pixel in an image. PSNR is measured in decibels.

5. Experimental Results

These are the following results obtained when experiment is done for various inputs. These are the results we get when we give the LSB to be substituted is 3.

(a) MSE & PSNR evaluation

(b) Cover Image

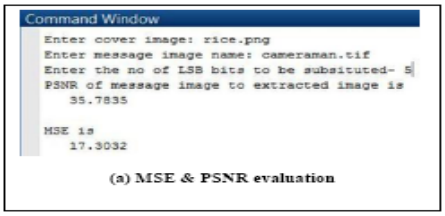
(c)Message Image

(d) Stego Image

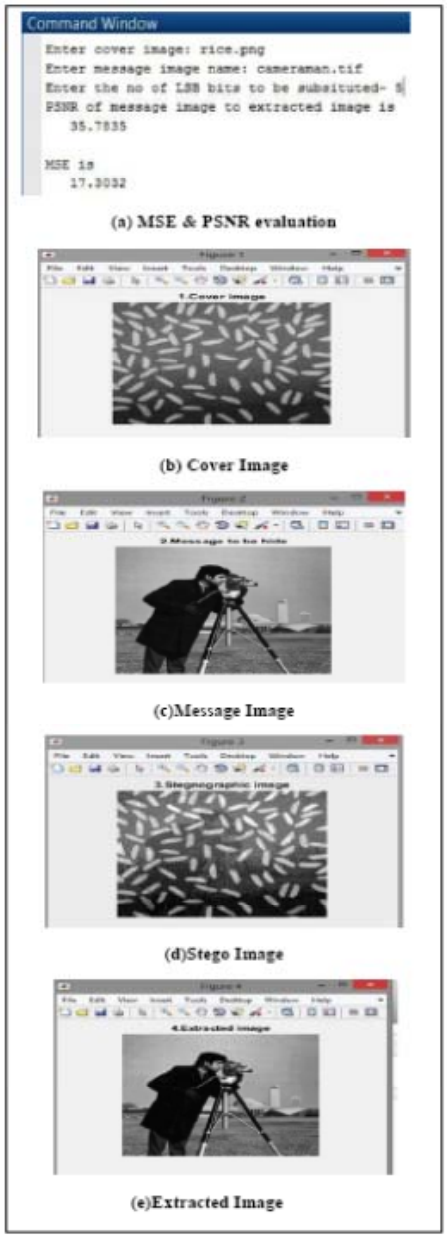
(e)Extracted Image

These are the results we get when we give the LSB to be substituted as 5.

The success rate is calculated using 2 parameters first one is and the other is PSNR.



(a) MSE & PSNR evaluation



(a) MSE & PSNR evaluation

(b) Cover Image

(c)Message Image

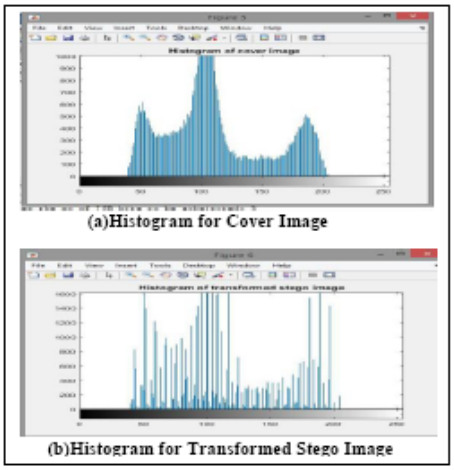
(d)Stego Image

(e)Extracted Image

Fig: 4 Experimental results for LSB value 5

These are the histograms that we get for the cover image and the transformed stego image.

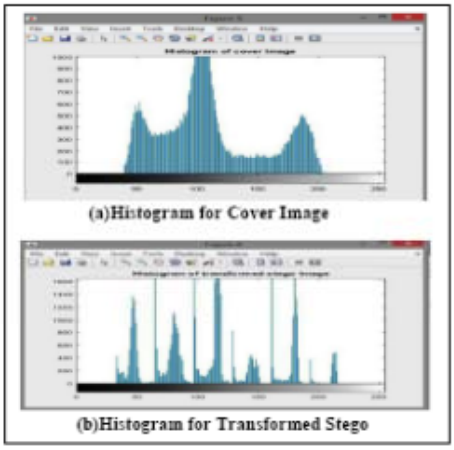
The below histograms are obtained when we alter the LSB to 3 bits and 5 bits respectively.



(a)Histogram for Cover Image

(b)Histogram for Transformed Stego Image

Fig: 5 Charts for Histogram with LSB 3



(a)Histogram for Cover Image

(b)Histogram for Transformed Stego

Fig: 6 Charts for Histogram with LSB 3 and 5

6. Conclusion

Since last few years, the steganography is one of the eye catcher for image cover media. This paper provides an introduction of steganography and introduces few methods of steganography which facilitates embedding of the data. These methodologies are more helpful and convenient way for identifying the stego images and also the image media relating to security of images. We can estimate the high embedding rate by using the quantitative steganalytic technique. The

Accuracy of around 82.7% obtained for LSB 5 with value of around 17.3.

References

1. Alpa Agath, Chintan Sidpara, Darshan Upadhyay, “Critical Analysis of Cryptography and Steganography”, International Journal of Scientific Research in Science, Engineering and Technology, Volume 4 | Issue 2 | Print ISSN: 2395-1990 | Online ISSN: 2394-4099, IJSRSET, 2018.
2. Danny Adiyan Z.1, Tito Waluyo Purboyo2 and Ratna Astuti Nugrahaeni3, “Implementation of Secure Steganography on Jpeg Image Using LSB Method”, International Journal of Applied Engineering Research ISSN 0973-4562 Volume 13, Number pp. 442-448, 2018.
3. DeepaliV.Patil1, Mr.Shatendra Dubey2, “Review paper on image steganography”, International Journal of Research in Computer Applications and Robotics ISSN 2320-7345-2014.
4. Sumit Kumar Moudgil, Dr. Amit Kumar Goel Professor, “Steganography on Audio Wave Tenth Layer by Using Signal to Noise Ratio Test and Spectrogram Analysis”, International Journal of Applied Engineering Research ISSN 0973-4562-2018.
5. Govind R. Suryawanshi , Dr. Suresh N. Mali ,“Analysis of Effect of Spatial Domain Steganography Technique on DCT Domain using Statistical Features for Digital Images”,International Journal of Applied Engineering Research ISSN 0973-4562 -2018.
6. Alpa Agath, Chintan Sidpara, Darshan Upadhyay, “Critical Analysis of Cryptography and Steganography” National Conference on Advanced Research Trends in Information and g technologies,| Online ISSN: 2394-4099 - 2018.
7. B.G.Aagarsana1, Anjali, T.Kirthika, S.Siva Kumar, “Image Steganography Using Secured Force Algorithm for Hiding Audio Signal into Color Image”, International Research Journal of Engineering and Technology (IRJET) - 2018.
8. Amit Kumar and Kamal Niwaria, “Result Analysis of DWT and LSB based Audio Steganography”, International Journal of Engineering and Management Research, ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962 -2018.
9. Blerim Rexha1, Petrit Rama2, Bujar Krasniqi3* and Gentiana Seferi4, “Efficiency of LSB and PVD Algorithms Used in Steganography Applications”, International Journal of Computer Engineering and Information Technology, E-ISSN 2412-8856 (Online)-2018.
10. Amit Kumar and Kamal Niwaria, “DWT and LSB based Audio Steganography- A Review”, International Journal of Engineering and Management Research, ISSN (ONLINE): 2250-0758, ISSN (PRINT): 2394-6962 -2018