Volume 6, Issue 9, September 2016 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Digital Communication using LSB based Image Steganography Technique

Arpita Anil Harne
Research Scholar, Shivaji University, Kolhapur, Maharashtra, India

Abstract*— In this present digital scenario secure and invisible communication between two parties is the prime requirement. Steganography is the technique of hidden communication. It not only hides the message contents, instead it hides the existence of the message. It hides the message in such a way that message will be imperceptible to the human eyes. Least Significant Bit (LSB) Technique is Spatial Domain Technique. It hides the secret message inside an image. In this technique the least significant bit of the cover image is used for concealing the bit value of secret message, for providing higher security in digital communication.

Keywords – Steganography, LSB, Stego Image, Cover Image, Spatial Domain, MSE, PSNR, NC

I. INTRODUCTION

Secure communication is the prime requirement of today's digital world. Everyone wants to exchange their information without any degradation. Secret message should reach to the destination without scramble its original message contents. Some illegal eavesdroppers every time try to hack that secret data. For providing security to this secret data in digital medium there are various techniques are available. Like Cryptography, Steganography, Digital watermarking etc.

Steganography technique is one of technique used for securely data transmission over digital media. Any type of information like text, image, audio, voice etc. should be sent securely over the internet. Using Steganography technique secret information can embedding within a cover object. Basically Steganography word is derived from two Greek words "Stegos" and "Grafia" i.e. Steganographic, where Stegos means covered and Grafia means writing it means covered writing [1]. Using Steganography Technique any type of secret information can send securely. In this technique secret message is concealed inside a cover object. There are different types of Steganography Techniques are available based on the cover object. Cover Objects can be image, Audio, Video, Protocols etc.

Some basic terms used in image Steganography are as follows.

Message: It is the secret information which user wants to communicate with others.

Cover Medium: It is the medium in which user hides their message.

Steganography Algorithm: Using different Steganography algorithms user can embedded their secret data within a carrier medium.

Stego Image: After hiding message inside a cover image, it is called as stego image i.e. cover image + hidden message = Stego image.

In my research work I will implement spatial domain Steganography technique LSB for hiding text message. There are different Steganography techniques are available for this. But I will use LSB Image Steganography Techniques for concealing message contents. Here text message contents will conceal inside a cover image.

In spatial domain Steganography technique message bits are directly embedded in the pixel values of the cover image. LSB, MSB, PVD etc. are the examples of this domain. This technique provides higher embedded capacity without changing any integrity of the cover image. In Least Significant Bit Techniques (LSB) Technique the least significant bits of the cover image are used for concealing the bit values of the secret message [2].

Following fig.1 shows the Image Steganography Technique for text data hiding inside an image. After hiding text message inside an image, it is called stego image.

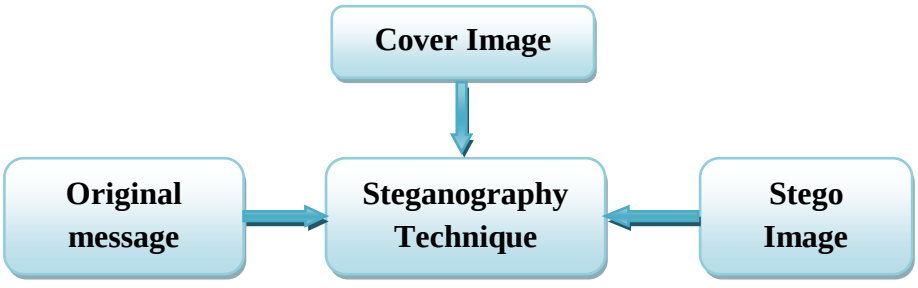

Fig.1 Image Steganography Technique

After hiding text message inside a cover image using Least Significant Method (LSB), the quality of stego image can be measured using following parameters PSNR, MSE, NC, Payload Capacity, Robustness, Invisibility etc [2].

MATLAB is a powerful and interactive tool for image processing. It provides many mathematical functions and inbuilt function for implementing different image related techniques. I will implement LSB image Steganography technique in MATLAB 7.8.0 (R2009a).

II. RELATED WORK

Now we are living in a digital world. Here secure communication over digital media is the foremost requirement of any organization. Secure communication means when two parties are communicating with each other then third party do not understand it. Many organizations share their confidential data over internet, so they want to reach their confidential data securely to the destination. Nowadays secure communication over internet is the most important factor of almost all fields. The term security means protection of any confidential data from unauthenticated access or different types of attacks.

There are various techniques are available for providing security to secret communication over internet. Cryptography, Steganography, Digital Watermarking etc. Techniques provide security to digital communication. These techniques use various methods for providing security. Sometimes for providing higher security various techniques can be merged [1]. For providing greater security, sometimes cryptography and Steganography both techniques are used. First encrypt the secret message using cryptography after then this encrypted message is concealed within any cover medium using Steganography [1] [2].

Image Steganography is the most popular form of Steganography. Image Steganography techniques are mainly implemented in two types of domain. (i) Spatial Domain (ii) Transform Domain.

Under Spatial Domain LSB, MSB, PVD etc. techniques are implemented and under Transform Domain DCT, DWT, DFT etc. techniques are implemented [3][4]. In LSB (Least Significant Bit) Technique first secret message and cover image file are converts into bit stream i.e. in binary form. Then using LSB algorithm message bits are concealed in LSBs of each pixel of image. Whereas in MSB (most significant technique) technique secret message are stored MSBs of each pixel value of cover image.

DCT (Discrete Cosine Transformation) and DWT (Discrete Wavelet Transformation) Techniques are implemented in transform domain. In this domain pixel values of cover image are transformed from spatial domain to frequency domain. After Transformation message bits are stored in the transformed coefficients of cover image. In DCT techniques DC coefficients are used for storing secret message bits. Here 8 * 8 or 16 * 16 quantization tables can be used for embedding secret data inside an image.

For providing greater security, various Steganography techniques like spatial domain and transform domain techniques can be combined, Even though various Steganography techniques can be combine with cryptography, watermarking techniques also [4] [5].

MSE (Mean Square Error), PSNR (Peak Signal to Noise Ratio), NC (Normalized Coefficients), Independent of file format etc. are the various parameters are available for evaluating Stego image quality after embedding massage data inside an image[5]

These image Steganography techniques may be applied on different file formats for data hiding like bmp, gif, jpeg etc. LSB image based Steganography technique is applied on these file formats for data hiding and result will be compared using parameters. In case of payload capacity LSB Technique in BMP file provides greater data hiding capacity compare to GIF and JPEG [6][7].

After analyzing various spatial domain and Transform domain techniques we can see that concealed data inside an image using spatial domain Steganography technique is more robust to various image manipulation operations like geometric attacks, rotating ,cropping, compressing etc. Whereas when using Transform domain techniques, concealed data is robust against low pass filtering, addition of noise, signal processing attacks etc [8].

III. PROPOSED ALGORITHM

A. Spatial Domain Image Steganography Techniques

In Spatial Domain Steganography Techniques direct pixel values of Image are used for embedding secret message bits, in such a way after hiding massage bits inside an image the image will be seen as earlier i.e. there should be no difference between original carrier image and Stego Image (after embedding data inside an image is called as stego image) and will not destroy the integrity of cover image. LSB (Least Significant Bit) is one of the spatial domain techniques.

B. LSB (Least Significant Bit) Technique

It is the common and simplest method for concealing secret message inside an image. In this method first secret message and cover image both are converted into binary stream. The least significant bit means nothing but 8th bit. Secret message bits will hide using this least bit. In this implementation 8 bit color images are used as a cover image [5] [6].

Basically in LSB technique message bits are hidden in least significant bit value of cover image. Here I've taken 8 bit color Image for data hiding. This color image is further divided into 3 planes R (Red), G (Green), B (Blue).

We can hide the message bits into any single plane but for increasing payload capacity and providing better security, we will hide our message bits into these 3 R, G, and B planes.

C. Algorithm for embedding text message inside an image

(i) First of all cover image and secret message are converted into binary stream.

(ii) For concealing text message, here I have taken 225*225*3 size color image, in which Red, Green and Blue planes.

(iii) In confidential message each character is represented by 8 binary bits i.e. (01110110).

(iv) Secret message embedding, inside an image starts from top to bottom of cover image.

(v) Each message bit is concealed inside a pixel value of Red, Green and Blue plane consecutively of cover image.

(vi) As we have seen above each pixel of cover image can contain 3 bits of confidential message.

These steps will repeat until all message bits hide into the cover image. These steps have implemented in MATLAB using LSB Steganography technique.

Following fig.2 shows the pictorial representation of Least Significant Bit (LSB) Steganography Technique for embedding secret message inside a cover image.

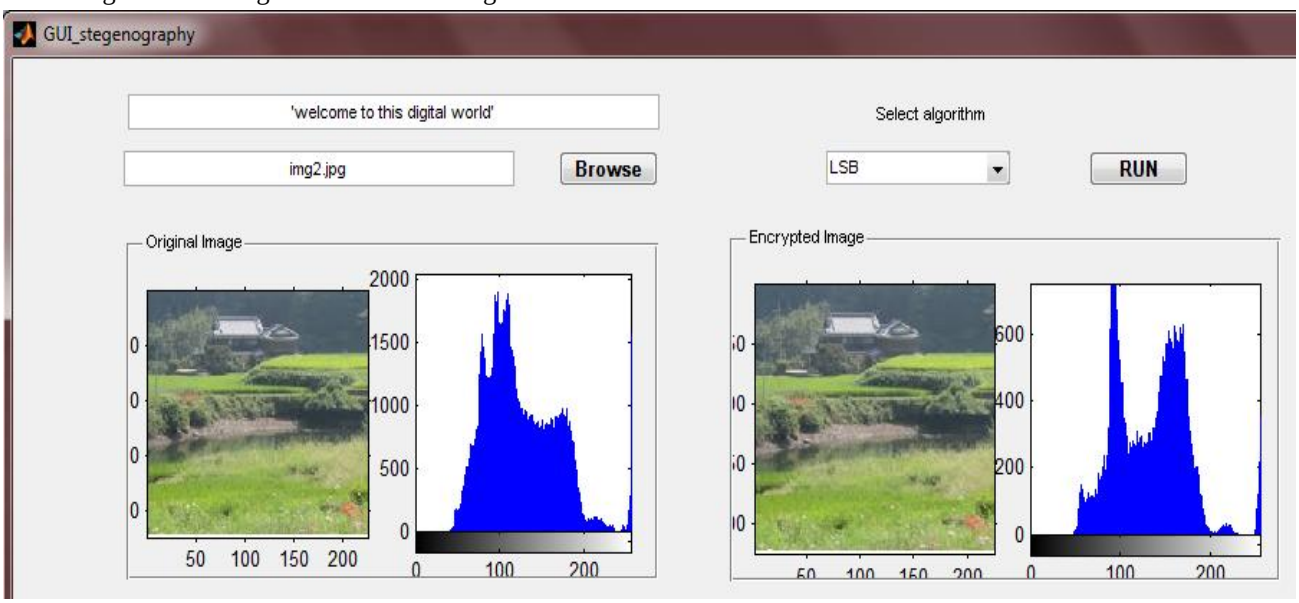

Fig. 2 Graphical representation of original cover image and Stego image with its histogram

D. Algorithm for extracting text message from stego image

(i) First Stego Image is converted into bit stream.

(ii) Cover image LSBs of R, G and B planes contains the Secret Message bits.

(iii) Reserve i * j * 3 (width*height*plane) size array for storing extracted secret message bits. Assign first all array value to 1.

(iv) For i=1 to width

For j = 1 to height

For k=1 to planes

{

Perform bit AND between Stego image bits and Hex value '0000 0001', for extracting message bits.

After shifting bits perform OR between shifted bits and extracted message bits for extracting whole message from stego image.

}

(v) Store all extracted message bits into a variable and present it in the form of original message format.

IV. PERFORMANCE EVALUATION RESULT

After embedding secret message inside an image using LSB Steganography algorithm, the result can be analysed using following parameters.

Payload Capacity

It is the size of the secret message which can be concealed in the cover image. In this technique payload capacity is 3bpp as shown in fig. 3.

Invisibility

It is the concept on invisibility after hiding the secret message bits in the cover image, i.e. cover image and stego image have to be identical. In this technique invisibility is high as shown in fig.3.

Mean Square Error (MSE)

It is the measurement of mean square error between cover image and stego image [4]. The value of MSE should be minimum.

$$MSE = \frac{\sum_{M,N}[I1(m,n)-I2(M,N)]^2}{M*N}$$

Peak Signal to Noise Ratio (PSNR)

It is mainly used for measure the quality of stego image.PSNR can be measure using following formula [4]. Its value should be high as shown in fig.3.

$$PSNR = 10 \log_{10} \frac{256^2}{MSE}$$

Independent of file format

It shows the different Steganography algorithms can use any type of file for concealing the secret data.

Robustness against image manipulation

After applying rotating, cropping, adding noise ,compression etc. operation on stego image, it should not effect on hidden data.

Normalized Coefficient (NC)

It shows the similarities between original message data and extracted message data after embedding the message inside an image.

After applying LSB Steganography Technique evaluated results are shown in the following fig.3.

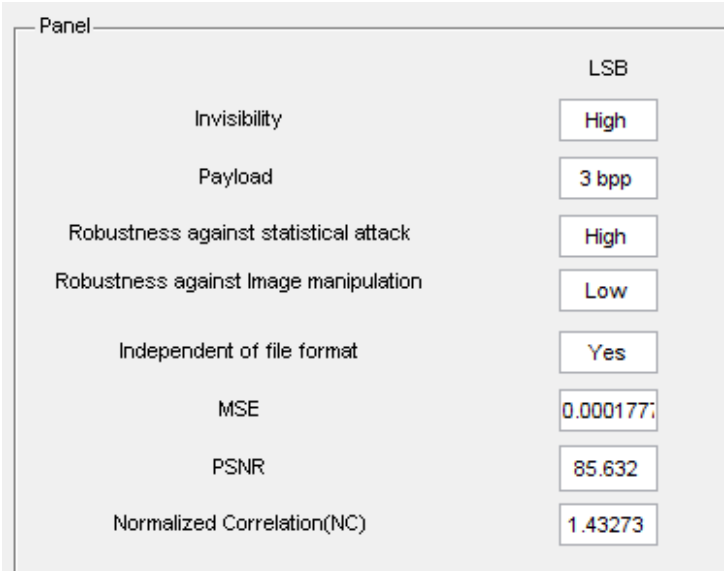

Fig.3 Performance Evaluation chart after applying LSB Steganography Technique.

V. CONCLUSION AND FUTURE WORK

In this research work I have implemented LSB Spatial Domain Steganography techniques for secret data transmission. I have tried to provide best results for secret data embedding .After implementing this technique results are evaluated using parameters MSE, PSNR, NC, Robustness against image manipulation, Robustness against statistical attack, Invisibility.

After analyzing values of these parameters we have seen that invisibility and robustness against statistical attack is high in this technique, payload capacity is also high i.e. 1bit of cover image can store 3 bits of secret message. I have implemented this technique using different file formats like .jpg, .png, .bmp etc. and evaluate their results using MSE and PSNR graph. This technique has also implemented using various sizes of images.

REFERENCES

[1] Vipul Sharme and Madhusudan, "Two New Approaches for Image Steganography Using Cryptography," Third International Conference on Image Information Processing 2015, pp. 202-207, Publisher: IEEE.

[2] S.Ashwin J.Ramesh ,S.Aravind Kumar and K.Gunavathi , "Novel and secure encoding and hiding techniques using image steganography: A survey," Emerging Trends in Electrical Engineering and Energy management(ICETEEEM),International Conference on 13-15 Dec 2012, pp.171-177, Publisher:IEEE

[3] Sumeet Kaur, Savina Bansal and R.K.Bansal, "Steganography and Classification of Image Steganography Techniques," International Conference on Computing for Sustainable Global Development (INDIACom) , Publisher: IEEE.

[4] C.P.Sumati, T.Santanam and G.Umamaheswari, "A study of Various Steganography Techniques Used for Information Hiding," International Journal of computer science & Engineering Survey,Vol.4, No.6, pp. 9-25 December 2013.

[5] R.Chandramouli and Nasir Memon, "Analysis of LSB based Image Steganography Techniques," 2001 International Conference on Image Processing, Volume: 3, pp. 1019 - 1022, Publisher: IEEE.

[6] K.Thangadurai and G.Sudha Devi, "An analysis of LSB based image Steganography techniques," Computer Communication and Informatics (ICCCI), International Conference on 3-5 Jan. 2014, pp.1 – 4, Publisher: IEEE.

[7] Amritpal Singh and Harpal Singh, "An improved LSB based image Steganography technique for RGB images," Electrical, Computer and Communication Technologies (ICECCT), IEEE International Conference on 5-7 March 2015, pp. 1- 4.

[8] Deepesh Rawat and Vijaya Bhandari, " A Steganography Technique for Hiding Image in an image using LSB Method for 24 Bit color Image," International Journal of Computer Application (0975-8887) Volume 64-No.20, February 2013.

