Suspection Less Steganographic Approach using Enigma Intermix Cube Encryption Technique

T. Gomathi, B. L. Shivakumar

Abstract*— *Steganography is a process of hiding one data behind an image. A text data or an image in one format is being hidden in other image or text data of the same format or of the different format. The data transmitted nowadays are being hacked easily by intruders, such that the purpose of secured transmission fails there. There are several traditional ways of transmitting data such as encryption, scrambling, watermarking, steganography, etc; the process of encryption involves changing data in one format to the other and transmitting. When the decryption method is known to the intruders then the data is easily available for them. Most of the encryption techniques are easy to predict. The process of scrambling involves shuffling the positions of the data in a format, which when applied in the reverse order or applied continuously will result in the original data. Watermarking is a process of embedding an image or text or logo in another image such that it is partially visible on the main data and hence it doesn't so well for secured transmission technique. Similarly the various traditional methods of steganography have some disadvantages. Some among them are listed below.

Index terms - Encryption, HVS (Human Visual System), LSB (Least Significant Bit), PSNR (Peak Signal Noise Ratio), Steganography

I. INTRODUCTION

The word ***steganography*** *i*s derived from the Greek words stegos meaning cover and grafia meaning writing defining it as covered writing. In image ***Steganography*** the information is hidden exclusively in images. ***Steganography*** is the art and science of secret communication .It is the practice of encoding/embedding secret information in a manner such that the existence of the information is invisible. The original files can be referred to as cover text, cover image, or cover audio. After inserting the secret message it is referred to as stego-medium. The ***Least Significant Bit (LSB)*** insertion is the most common spatial domain technique, which consecutively replaces the least significant bit of cover image with the message bits. This method exploits the natural weakness of ***Human Visual System (HVS)*** in recognizing the slight difference of colors. The LSB method changes some or all the 8th bit of image's data so that the image's alteration is not perceptible for any human eyes. In this manner, when using a color image the LSB of each of the red, green and blue Components can be used. Therefore, the potential capacity for hiding secret data in a color image is triple of the same image size in the Grayscale mode. Furthermore, when the data is embedded subsequently to all bytes of cover image, it would be rather easy to detect and extract the message. A moderately more secure method is to encrypt before performing ***Steganography*.**

Manuscript Received on September 22, 2014.

Prof., T. Gomathi, Research Scholar, Karpagam University, Coimbatore, India.

Dr. B. L. Shivakumar, Director, Department of Computer Application, Sri Ramakrishna Engineering College, Coimbatore, India.

The message image which is to be hidden is being encrypted so that the identifying the hidden image presence will become difficult. The protection of images is of particular interest in this paper. Traditional image encryption algorithms such as private key encryption standards (DES and AES), public key standards such as ***Rivest Shamir Adleman(RSA)***, and the family of ***Elliptic-Curve-based Encryption (ECC)***, as well as the ***International Data Encryption Algorithm (IDEA),*** may not be the most desirable candidates for image encryption, especially for fast and real-time communication applications. In recent years, several encryption schemes have been proposed. These encryption schemes can be classified into different categories such as value transformation, pixels position permutation, and chaotic systems. The security of image encryption has been extensively studied. Almost some encryption schemes based on permutation had already been found insecure against the cipher text-only and known/chosen-plaintext attacks, due to the high information redundancy, and it is quite understandable since the secret permutations can be recovered by comparing the plaintexts and the permuted cipher texts. Generally, chaos-based image encryption algorithms are used more often than others but require high computational cost. Moreover, a chaos system is defined on real numbers while the cryptosystems are defined on finite sets of integers. One-dimensional chaotic ***cryptosystems*** are limited by their small key spaces and weak security. In this paper, I present a new ***steganographic*** approach using ***LSB technique*** and a novel image encryption algorithm based on the principle of ***Enigma Intermix cube Algorithm***. The remaining of this paper is organized as follows in Section II describes the Existing image ***LSB Steganography algorithms***, Section III describes the proposed **LSB *Steganography*** along with the new ***Image encryption algorithm***, Section IV describes the Experimental results and tables and Finally I Conclude in Section V.

II. RELATED WORKS

A. LSB Algorithm

The traditional steganography technique is the least significant bits algorithm. It involves converting the data into binary format and then replacing them in the places of binary values of the cover image (the image which hides the data). This technique when used for hiding images behind images failed because of loss in data. The image which is to be hided is converted into binary form and the most significant bits (MSB) of it are alone replaced in the places of LSB of the cover image. This process will yield some amount of loss in the data at receiving side. Along with that the trace of image to be hidden will be seen on the Steganography output image.

B. Wavelet Transform

The wavelet transform involves converting image into frequency domain and then process with it. It will split the image into higher frequencies and lower frequencies and it prolongs when the decomposition level increases. After splitting of the image into various frequencies the data to be hidden can be embed along with them to form the stegano image. Thus this method also results in data loss in terms of frequencies since some frequencies are left out.

C. Bitplane Complexity Steganography

BPCS involves embedding secret information in true color images by replacing the complex areas in the cover image. This method consumes more time to perform the embedding algorithm and it always requires a 24 bit true color image as cover image. And all the above mentioned methods, on choosing an improper cover images will show traces when an image is hidden behind it. Also these methods will not attain a PSNR (peak signal to noise ratio) as infinity. Only a transmission with PSNR infinity will contain the secret image exactly without a loss.

III. PROPOSED APPROACH

Steganography is done in several ways like hiding text in image, audio in image or image behind image. This work implements a new method for hiding image behind image. The proposed system is designed to have a secure transmission with no trace of original image in the Steganography output. This approach uses Enigma Intermix cube encryption for secured data transmission along with LSB algorithm. The proposed work involves the following steps in it.

1) Image Importing
2) Pre-processing image
3) Encrypting image
4) Constructing stegano image
5) Transmitting data
6) Reconstructing Stegano image
7) Decrypting image
8) Calculating PSNR

A. Image Importing

The data chosen in our method is an image. The image to be hidden and the image which is to hide the secret image are to be chosen. The image chosen are true color RGB images and are processed as such. Any format of an RGB image can be chosen such as png, jpeg, tiff, etc,

B. Pre-Processing Image

Basically several images will not be of good quality, perfect size or with good brightness and contrast. Such images when taken for further processing may result unexpectedly. So every image should be enhanced in terms of quality and resized properly. Two Resizing process are done here.

1) The secret image is resized to a size of A x A (for ex, A=128).
2) The cover image is resized to a size of A x A.

C. Encrypting Image

Encryption is a process of converting data in one form to the other such that the input data which was in a easy understandable form goes difficult to understand and guess after encryption. There are several encrypting algorithms for images. Some among them are listed below.

i) Data Encryption Standard

The DES algorithm is one of the traditional encryption techniques used earlier. It involves encryption for data in the form of bits. For a 32-bit block it needs 48 bit key to encrypt it and for a 64 bit block of data it needs a 56 bit key to encrypt. Since the number of key bits is less the security is less in this technique. Moreover this method utilizes more time period to encrypt.

ii) Block based standards

The block based standards for encrypting involves converting the image into smaller blocks and transferring them into another form. These transferred blocks are again replaced in the same location. Since the entire process takes places only in terms of blocks the encrypted image consists of patterns with difference between each block in the image.

D. Enigma Intermix Cube Encryption

The encryption technique used in this work is called as enigma intermix cube encryption. This method involves the following steps.

***Step1*:** Consider a square matrix of image.
***Step2*:** Perform the sum of elements in all individual rows.
***Step3*:** If the sum of first row elements is even, perform a right circular shift of that particular row and perform left circular shift if it is odd.
Step4: Repeat step 3 for all rows.
Step5: Now perform column wise sum of all elements.
Step 6: If the sum of first column elements are even, perform a down circular shift of that particular row and perform up circular shift if it is odd.
***Step 7*:** Repeat step 6 for all columns.
***Step 8*:** Convert the finally obtained image matrix data into binary form with each pixel converted into 8 bits.
***Step9*:**Now perform an XOR operation between binary value of one single key letter say 'k' represented in 8 bits and every element in the binary value matrix.
Step 10: After performing XOR operation, the matrix is again converted into integers form. And that form the encrypted image.

The key letter can be any character such that it must have an ASCII value. That key value is always confidential between the sender and the receiver. The intruder can't guess that an XOR operation is being done and if known the key will be unknown.

E.Constructing Stegano Image

The encrypted image cannot be send as such to the receiver since it may be hacked by the intruders so the encrypted image is next put into a process of steganography. The method used to hide the message image is LSB algorithm. The following are the steps for constructing a stegano image.

Step 1: The encrypted image is now converted into binary

form such that each pixel value contains 8 bits of value.

Step 2: After converting the encrypted image into binary values it is split into LSB and MSB values.

Step 3: Cover image is also converted into binary values each comprising of 8 bits.

Step 4: After converting the cover image into binary values it is also split into LSB and MSB values.

Step 5: After the splitting process the MSB of Encrypted image is now combined with MSB of cover image. (i.e.) the LSB of cover image is replaced with MSB of Encrypted image.

Step 6: This process is repeated to all pixels in the Cover image and a new set of pixels values is obtained.

Step 7: Finally convert the binary values into integers and thus it forms the stegano image.

F. Transmitting Data

The stegano image after all process is transmitted to the receiver.

G. Reconstruction of Stegano Image

The stegano image received by the receiver is to be reconstructed to extract the information hidden. The reverse operation of the construction process is performed to reconstruct the image. After performing all steps the encrypted image will be obtained.

H. Decrypting Image

The encrypted image obtained is now applied with the steps of encryption in reverse manner. This process will yield the input secret image. The key character used in decryption process is also the same as in encryption.

IV. EXPERIMENTAL RESULT

I tried out the algorithm in the software called mat lab R 2013 a using the CPU Pentium.IV, here large data set was substituted and verified some among them is listed below in table. in this table I calculated PSNR value for all images and its formula it's given below

PSNR Calculation

After the decryption process the image at the receiver side and the original image is subjected to calculate PSNR. By the value of PSNR the loss in image recovering can be calculated. PSNR is calculated by using the formula,

$$PSNR = 10\log\frac{255^2}{MSE}$$

Where,

$$MSE = Mean\left[\sum([ORG - RECONSTRUCTED])^2\right]$$

ORG= Original image,
RECONSTRUCTED= Reconstructed image.

TABLE FOR CALCULATING PSNR VALUE FOR IMAGE

S.No	*Message Image*	*Cover Image*	*PSNR Using LSB*	*PSNR Using Encryption*	*Time Taken in Sec*
1	*Flower*	*Sunset*	*56.50*	*59.50*	*31.35*
2	*Flower*	*Orange*	*56.50*	*59.50*	*31.35*
3	*Baboon*	*Flower*	*64.35*	*67.35*	*31.24*
4	*Lena*	*Dark Evil*	*63.72*	*66.82*	*31.34*
5	*Checker Board*	*Balls*	*59.65*	*61.66*	*31.35*

Steganography using LSB Technique

Message Image: Flower
Cover Image: Orange

Fig. 1. Message Image

Fig. 1.1. Stegano Image

Fig. 1.2. Recovered Message Image

The Trace of Message Image located in the Stegano Image

Message Image: Flower
Cover Image: Orange

Fig. 2. Message Image Indicating a Smaller Portion

Fig. 2.1. Trace of Located Portion found in the Stegano Image

Steganography using LSB Technique along with Encryption
Message Image: Flower
Cover Image: Orange

Fig. 3. Message Image

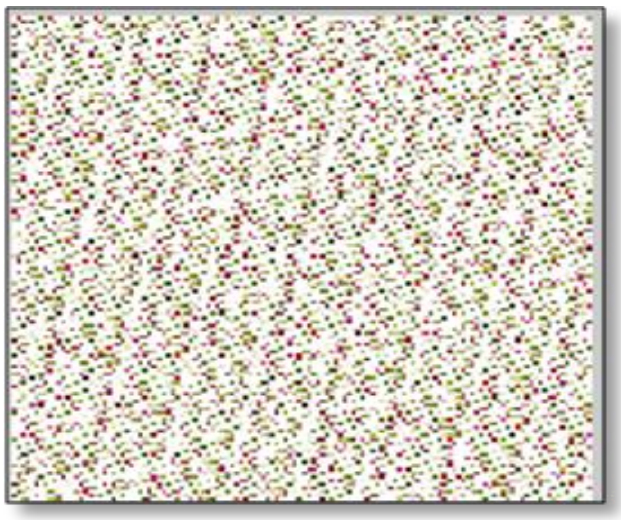

Fig. 3.1. Encrypted Message Image

Fig. 3.2. Stegano Image

Fig. 3.3. Recovered Message Image

Disappearance of the Trace of Message Image in the Stego Image
Message Image: Flower
Cover Image: Orange

Fig. 4. Message Image Indicating a Smaller Portion

Fig. 4.1. Located Portion not found in stegano Image

V. CONCLUSION

After comparing the existing and proposed method for the same Data I conclude that the proposed method produce ***PSNR*** high than the existing method so I conclude that the ***quality*** of the recovered image is *so* ***good*** that the image recovered in the existing method.

REFERENCES

1. R.Anderson and F. Petitcolas, "On the limits of steganography" IEEE Journal of Selected Areas in Communications, Vol. 16, No. 4, May 1998.
2. NielsProvos, Peter Honeyman, "Hide and Seek: An Introduction to Steganography," IEEE computer society, 2003.
3. K B Raja, Venugopal K R and L M Patnaik, "A Secure Stegonographic Algorithm using LSB, DCT and Image Compression on Raw Images", Technical Re-port, Department of Computer Science and Engineering, University Visvesvaraya College of Engineering, Bangalore University, December 2004.
4. An overview of image steganography by T. Morkel , J.H.P. Elo_, M.S. Olivier. Information and Computer Security Architecture (ICSA) Research Group Department of Computer Science University of Pretoria, 0002, Pretoria, South Africa.
5. Johnson,N.F.Jajodia,S.,"Exploring Steganography:Seeing the Unseen",Computer Journal, February 1998.
6. Fridrich, Miroslav Goljan, and Rui Du State University of New York, Binghamton.
7. J. V. Anand and G. D. Dharaneetharan, "New approach in steganography by integrating different LSB algorithms and applying randomization concept to enhance security," presented at the Proceedings of the2011International Conference on Communication, Computing, Rourkela, Odisha, India 474-476, 2011.