ISSN: 2277-9655
(I2OR), Publication Impact Factor: 3.785

IJESRT

INTERNATIONAL JOURNAL OF ENGINEERING SCIENCES & RESEARCH TECHNOLOGY

A NOVEL APPROACH TO ROBUST AND SECURE IMAGE STEGANOGRAPHY BASED ON HASH AND ENCRYPTION

Er. Parminder Singh*, Er.Parminder Singh Saini
Mtech. Student, ECE Deptt., Doaba Group of colleges, Kharar, Punjab, India
Assistant Professor, ECE Deptt., Doaba Group of colleges, Kharar, Punjab, India

DOI: 10.5281/zenodo.47027

ABSTRACT

There has been widespread use of digital data over the internet. The security of the data is of utmost concern for the users. Steganography and cryptography are two different techniques for data security. The main purpose of cryptography is to make message unintelligible, while steganography even conceals the existence of the hidden message. Digital images are excellent carriers of hidden information. In the present paper, a method has been proposed for LSB steganography which carries three fold security mechanism. The method uses Diffie-Hellman, RSA algorithm with a hash function. The proposed method ensures high data security, stability and ruggedness. The results of the proposed method have been compared based upon PSNR and MSE. These have been found to be very encouraging.

KEYWORDS:Steganography, Cryptography, RSA algorithm, Diffie-Hellman algorithm, Hash Function, PSNR, MSE, Cover Object, Stego-image.

INTRODUCTION

With the widespread deployment of the internet involving Online Banking, Online Shopping, Online funds transfer, Online messaging, Emailing etc. and advent of mobile telephony, Digital TV Broadcast, Video Conferencing, Video On Demand and Digital Data networks, there has been enormous flow of digital data transmitted between various users. However the data security comprising of authenticity, integrity, confidentiality etc. has become a big challenge these days. Over the years various data security techniques have emerged for reliable and secure communication like cryptography, steganography, digital watermarking etc.

Cryptography and steganography both have the same purpose i.e. to hide the messages in a specific medium. However, they have one distinct difference, the cryptography hides the contents of the secret message from third parties by making the message unintelligible whereas steganography even conceal the existence of the message altogether. Cryptography scrambles a message using cryptographic algorithms and secret keys so that it cannot be understood. Steganography deals with composing hidden messages so that only the sender and the receiver know that the message even exists. Since nobody except the sender and the receiver knows the existence of the message, it does not attract unwanted attraction. In cryptography, a cipher message for instance, might arouse suspicion on the part of the recipient while an invisible message created with steganographic methods will not. 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.

The concept of steganography is illustrated by following example: Let Alice wants to send a secret message (M) to Bob using a harmless medium as cover object (C) which can be sent to Bob without raising suspicion. Alice changes the cover object (C) to a stego-object (S) by embedding the secret message (M) into the cover object (C) by using a stego-key (K). Alice then can send the stego-object (S) to Bob without being detected by third person Charlie. Bob will be able to read the secret message (M) as he knows the stego-key (K) used to embed it into the cover object (C).

In a perfect system, a normal cover should not be distinguishable from a stego-object neither by a human nor by a computer looking for statistical patterns. But practically, this may not be always the case. To embed secret data into a

cover medium, the cover must contain a sufficient amount of redundant data or noise because in most steganography processes, this redundant data is replaced by the secret message. This limits the types of data that we can use with steganography.

There are several suitable carriers below to be the cover-object:

- Network protocols such as TCP, IP and UDP
- Audio that is using digital audio formats such as wav, midi, avi, mpeg, mpi and voc
- File and Disk that can hide and append files by using the slack space
- Text such as null characters, just like morse code including html and java
- Images file such as bmp, gif and jpg, where they can be both color and gray-scale.

Requirements of a good steganography technique

1) Invisibility: The prime feature of the steganography is that, the changes made in the stego object should be unnoticed by the human eye.

2) *Payload Capacity*: Since the steganography process carries a hidden secret message, it is required that cover object have sufficient embedding capacity even to carry long messages.

3) *Robustness against attacks*: Steganalysis is the technique to detect hidden information from a stego object. The steganography algorithm should be strong enough so that it cannot be easily detected.

4) *Independent of file format*: There are number of image formats being used over the internet, If only one type of format is used very frequently between two communicating parties, this may arise suspicion by the eavesdropper. The steganography algorithm should be flexible enough so that any type of image format can be used.

RELATED WORK

A brief review of the previous research work done in the field of secure steganography is presented in the following paragraphs:A LSB insertion steganography technique with RSA encryption have been proposed in the paper [1]. The data to be hidden is encrypted by using RSA algorithm and then the encrypted data is matched from users library of images and most suitable image is selected, so that there is less chance of detection of hidden data by steganalysis. Another paper [2] proposes LSB steganography using a secret key. The cover image is divided into three matrices (Red, Green and Blue). The secret key is converted into 1D array of bit stream. Secret key and Red matrix are used for decision making to replace hidden message either into Green matrix or Blue matrix. The reverse process is used to recover the hidden message at receiver end. The paper [3] proposes a secured steganography technique based on Random Function. The message to be hidden is encrypted using a random function and other random values. The function is generated based upon various parameters like length of secret message, length of a constant vector and threshold value. The proposed method achieves confidentiality and provides more security to data against detection. Another proposed technique is hash function with LSB based video steganography [4]. In this technique the hidden message bits replace the LSB positions of R, G, B values of cover frames. The positions of insertion in LSB are selected by a hash function. The results of this technique are compared based upon PSNR and MSE of stego video frames with respect to original video frames. The results are encouraging.

PROPOSED METHOD

The proposed method of LSB steganography is based on RSA algorithm, Diffie-Hellman Algorithm. These have been explained in following paragraphs.

RSA algorithm:

1) Take two prime numbers ‘p’ and ‘q’. Rabin-Miller primality test algorithm can be used to generate and verify the prime numbers.
2) Calculate modulus ‘n’ by multiplying ‘p’ and ‘q’. This number is used by both public and private keys.
3) Calculate the totient $\Phi(n) = (p-1)(q-1)$
4) Find the public key exponent, normally expressed as ‘e’ which is so chosen that $1<e<\Phi(n)$ and ‘e’ is co prime with $\Phi(n)$ i.e. $\gcd(e,\Phi(n)) = 1$ (gcd is greatest common divisor). The public key is a key pair of the exponent ‘e’ and the modulus ‘n’. It is represented as (e, n).
5) Private key is computed by using Extended Euclidean Algorithm. Private key component ‘d’ is calculated by solving the following equation.

$$(e.d) \bmod \Phi(n) = 1$$

6) The private key is expressed as (d, n)
7) Encryption is done for the message 'M' as: Ciphertext $C = M^e \bmod n$
8) Decryption is done as: Message $M = C^d \bmod n$

Diffie-Hellman algorithm

1) Alice and Bob, using insecure communication, agree on a huge prime number 'p' and a generator 'g'. They don't care if someone listens in.
2) Alice chooses some large random integer $X_A < p$ and keeps it secret. Likewise Bob chooses $X_B < p$ and keeps it secret. These are their "private keys".
3) Alice computes her "public key" $Y_A = g^{X_A} \bmod p$ and send it to Bob using insecure communication. Bob computes his public key $Y_B = g^{X_B} \bmod p$ and sends it to Alice.
4) Alice computes $K_A = (Y_B)^{X_A} \bmod p$ and Bob computes $K_B = (Y_A)^{X_B} \bmod p$
   $K_A = K_B$ because $K_A = K_B = g^{X_A X_B} \pmod p$

Both have shared secret key. They can use it to encrypt and decrypt the message.

Steps for the proposed method are given below:

Sender Side

1) A color image is selected as cover image. The secret text message is converted into binary form using ASCII codes.
2) A secret key is generated using Diffie Hellman algorithm and message data is encrypted in stage I.
3) RSA algorithm is applied to encrypt the data in stage II.
4) R,G,B (Red, Green and Blue) pixels values of the cover image are calculated.
5) Hash Function is applied to calculate the LSB positions for R, G and B pixel values where secret data bits are to be embedded.
6) The bits of secret message data are embedded into the LSB positions, given by the values of the hash function.
7) A stego image is formed and sent to the destination where the intended secret message is to be sent

Receiver Side

1) The received stego image is taken as input.
2) Using the known hash function, positions of embedded secret message data bits are calculated and secret data is extracted in encrypted form.
3) RSA algorithm is applied to decrypt the message in stage-I.
4) Diffie-Hellman algorithm is applied to decrypt the message in stage-II, thereby getting the original secret message.

The proposed technique is implemented in MATLAB. The Encryption and decryption is implemented in separate modules. To check the quality of stego image with respect to original cover image, the values of PSNR (Peak signal to noise ratio) and MSE (Mean Squared Error) have been calculated. PSNR represents the ratio between the maximum possible power of a signal and the power of corrupting noise that affects the fidelity of its representation. PSNR is often written in terms of the logarithmic decibel scale. It is defined via the mean squared error (MSE) that is given by

$$MSE = \frac{\sum_{m.n} [\, I_{cover}(m,n) - I_{stego}(m,n) \,]^2}{m*n}$$

Where 'm' and 'n' are the number of rows and columns, respectively, in the two input monochrome images (the original cover image Icover and its stego-image Istego).

The PSNR is then given by

$$PSNR = 10 \log_{10} \left[\frac{R^2}{MSE} \right]$$

Where, R is the maximum possible pixel value of the image. For 8 bit pixel value R=255

For color images with three RGB values per pixel, the PSNR is defined by

PSNR = 10 $\log_{10}$ [$\frac{R^2}{MSE(RGB)}$]

Where MSE(RGB) is the sum over all squared value differences divided by image size and by three

MSE(RGB) = $\frac{MSE(R)+MSE(G)+MSE(B)}{3}$

It is well known that an image with a PSNR value exceeding 30 dB is considered to be acceptable to human perception.

Hash Function:

The bits are embedded in the sequence of 3,3,2 for R,G and B pixel values, respectively. Which means out of 8 bits of secret data, 3 bits are embedded in Red value, next three in Green Value and 2 bits are embedded in Blue value of the pixels of cover image.

The Hash function is given as:

h = (j+i) mod n

where j varies from 1to8 (number of bits in a plane)

i is the total length of the message

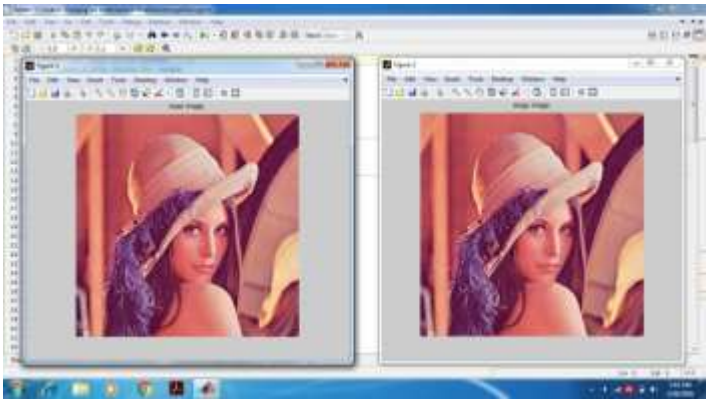
n is the total least significant bits in a plane which are to be replaced which is 4 in our case.

Depending upon the values given by hash function the respective LSB bits of the R,G,B values are replaced on transmitter side. Reverse procedure is adopted on receiver side.

RESULTS AND DISCUSSION

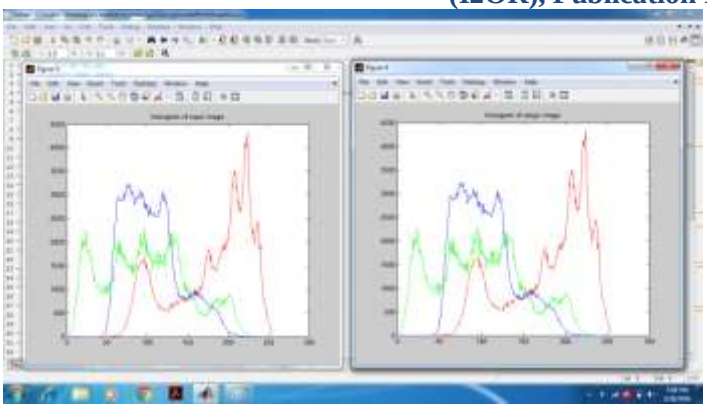
The proposed method has been tested on various types of color images with different formats. The secret messages of different lengths have also been used to test the proposed method. The results have been very encouraging. There is no noticeable visual difference between original image and stego image. Further, the PSNR of image have been calculated to compare distortion in the stego image which has been found to be very good with values more than 60db.

Figure:1



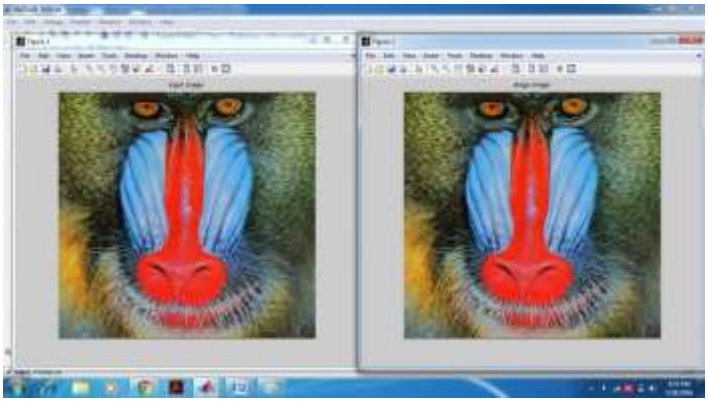
Input Image (lena.png) ***Stego Image***

Figure:2



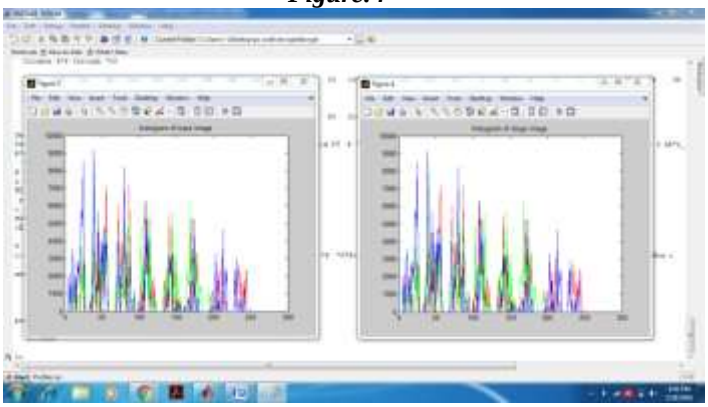
Histogram of input Image-lena(left) and stego image(right)

Figure:3



Input Image (baboon.bmp) ***Stego Image***

Figure:4

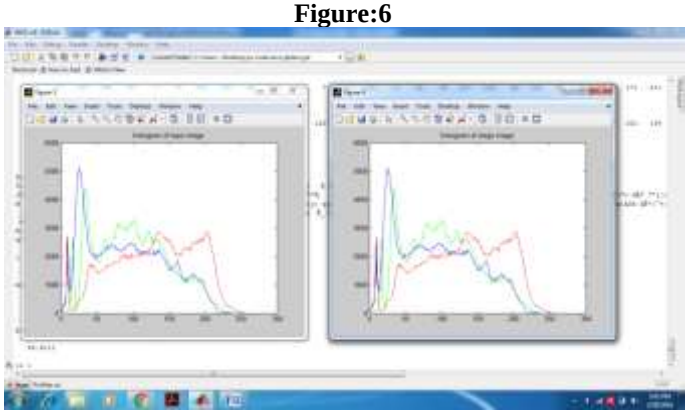


Histogram of input Image-baboon(left) and stego image(right)

Figure:5

Input Image (barbara.bmp) *Stego Image*

Figure:6

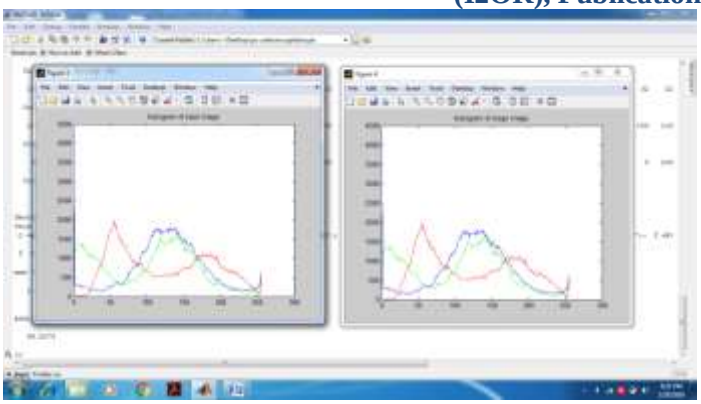


Histogram of input Image-barbara(left) and stego image(right)

Figure:7

Input Image (flower.jpg) *Stego Image*

Figure:8



Histogram of input Image-flower(left) and stego image(right)

Table 1. MSE and PSNR comparison of test images for different text lengths of secret message

No. of text Characters	Lena.png (512x512)		Baboon.bmp (500x480)		Barbara.bmp (720x576)		Flower.jpg (500x375)	
	mse	Psnr (db)	mse	Psnr (db)	mse	Psnr (db)	mse	Psnr (db)
21	1.1826×10^{-4}	87.4	1.124×10^{-4}	87.6	7.15×10^{-4}	89.6	1.4578×10^{-4}	86.5
87	4.6539×10^{-4}	81.4	4.9583×10^{-4}	81.2	3.0543×10^{-4}	83.3	6.24×10^{-4}	80.2
175	9.2061×10^{-4}	78.5	9.9861×10^{-4}	78.1	6.1005×10^{-4}	80.3	.0013	77.1
351	.0018	75.6	.0020	75.1	.0012	77.3	.0025	74.2
1055	.0054	70.8	.0059	70.4	.0035	72.7	.0074	69.4

Figures 1 to 8 show the input images, stego images and and their corresponding histograms. Figure 9 shows the values of MSE (mean squared error) and PSNR (peak signal to noise ratio) for different test images and their corresponding stego images for various sizes of secret messages. The results obtained are encouraging with PSNR values greater than 60 db. PSNR reduces with the size of the secret message. Also the higher resolution images show higher values of PSNR as compared to low resolution images for same secret message size.

CONCLUSION

The proposed method is very secure and rugged, as it uses three tier security mechanisms of Diffie-Hellman algorithm, RSA algorithm and hash function. In today's scenario of internet security, the method can be extremely useful for transmission of secret messages. As the method involves extensive computing at various stages and also if the message is very long, the processing time increases to some extent. But generally the secret messages are not very long and also with availability of high speed computers, the proposed method can be used very efficiently for secret communications.

REFERENCES

[1] Mamta Juneja, Parvinder Singh Sandhu, " Designing of Robust Image Steganography Technique Based on LSB Insertion and Encryption", 978-0-7695-3845-7/09 $25.00 © 2009 IEEE
[2] S. M. Masud Karim, Md. Saifur Rahman, Md. Ismail Hossain, "A New Approach for LSB Based Image Steganography using Secret Key", 987-161284-908-9/11/$26.00 □ 2011 IEEE
[3] Hamdy M. Mousa, "Secured Steganography Algorithm Based Random Function", 978-1-4799-0080-0/13/$31.00 ©2013 IEEE

[4] Kousik Dasgupta1, J.K. Mandal and Paramartha Dutta, "HASH BASED LEAST SIGNIFICANT BIT TECHNIQUE FOR VIDEO STEGANOGRAPHY (HLSB) ", International Journal of Security, Privacy and Trust Management (IJSPTM), Vol. 1, No 2, April 2012
[5] Shashikala Channalli, Ajay Jadhav, "Steganography an Art of Hiding Data", International Journal on Computer Science and Engineering Vol.1(3), 2009, 137-141, ISSN : 0975-3397
[6] Ravindra Gupta, Akanksha Jain, Gajendra Singh, "Combine use of Steganography and Visual Cryptography for Secured Data hiding in Computer Forensics", (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (3) , 2012,4366 – 4370
[7] T.C. Manjunath, Ushaa Eswaran, " Digital Steganography Implementation for Colored Images Using Wavelets", International Journal of Communication Engineering Applications-IJCEA
[8] Victor Onomza Waziri, Audu Isah, Abraham Ochoche, Shafi'i Muhammad Abulhamid, " Steganography and Its Applications in Information Dessimilation on the Web Using Images as Security Embeddment: A Wavelet Approach", International Journal of Computer and Information Technology (ISSN: 2279 – 0764) Volume 01– Issue 02, November 2012
[9] Vinaykumar M Kolli, Vaishakh B N, "Key Based Data Embedding Technique in Image Steganography", International Journal of Computer Applications (0975 – 8887) 2013
[10] Adnan Mohsin Abdulazeez Brifcani, Wafaa Mustafa Abduallah Brifcani, "Stego-Based-Crypto Technique for High Security Applications", International Journal of Computer Theory and Engineering, Vol.2, No.6, December, 2010, 1793-8201
[11] Vivek Jain, Lokesh Kumar, Madhur Mohan Sharma, Mohd Sadiq, Kshitiz Rastogi, " PUBLIC-KEY TEGANOGRAPHY BASED ON MODIFIED LSB METHOD", Volume 3, No. 4, April 2012 Journal of Global Research in Computer Science
[12] E. Yuva Kumar, P. Padmaja, "RSA Based Secured Image Steganography Using DWT Approach", Journal of Engineering Research and Applications ISSN : 2248-9622, Vol. 4, Issue 8(Version 1), August 2014, pp.01-04.