A High Quality Cryptography Based Image Steganography Using ASCII Differencing and Three LSB Bits Insertion Method

Tajinder Singh, Sukhjit Singh, Gurvinder Singh

Abstract— **For making more secure data transfer from sender to receiver through a channel due to fast growing in internet, various techniques are used. In thesis paper, we use steganography technique which is based on cryptography. Our Proposed work is divided into two methods. One works on Individual ASCII Code Digit Pair Differencing in which, we encrypt the original data in ASCII Code differencing by constructing digit pair of each ASCII code digit as an individual digit pair vertically. Then horizontally grouping of ASCII code of Key and individual ASCII code difference generate the cipher text string and other works on insertion of lower and reduced higher decimal value in three least significant bits of pixels of cover image. In this, the entire cipher text string is embedded into a cover image having dimensions of 512*512 using proposed method into three Least Significant Bits of pixels.The experimental results show that the proposed method is highly efficient in hiding the information and also secured against attacks. Besides, the embedded secret information can be extracted from cipher image without the assistance of original image. Since peak signal-to-noise ratio (PSNR) and MSE are extensively used as a quality measure of cipher images, the reliability of PSNR and MSE for cipher image is also evaluated in the work described in this paper.**

*Index Terms—*ASCII code difference, Cipher- Image, Cipher – Text, Indexed Image, LSB, Original information.

I. INTRODUCTION

Cryptography is derived from Greek words: kryptós, "hidden", and gráphein, "to write" - or "hidden writing" [7].Cryptography is a process which keep the original information safe in transmission channel. Cryptography converts the original information into non-understandable form and transmits this non-understandable data over an insecure channel. The unauthorized person cannot know the original information from this non-understandable data. Only authorized person has the capability to convert the non -understandable data to readable/understandable one[1]. cryptography converts plaintext to cipher text using Encryption process and decrypt cipher text to plain text

Mr. *Tajinder Singh,* *Lecturer, ECE Department, G.T.B.K.P.C., Punjab, India.*
Mr. *Sukhjit Singh,* *Assistant Professor, ECE Department, G.T.B.K.I.E.T., Punjab, India.*
Mr. *Gurvinder Singh,* *Assistant Professor, ECE Department, G.T.B.K.I.E.T. ,Punjab, India.*

using decryption process. The original information is said to be Plain Text and converting data in non-understandable form is called Cipher Text [4]. Now while we want to transfer the information to the other person, then there is most necessity of information security. For transferring the information confidentially, we use mostly a technique which is called Steganography. The steganography$[5,6]$ is a way of hiding the information from unauthorized person.The word "Steganography" technically means "covered or hidden writing". The purpose of steganography is covert communication to hide the information from a third party. In past times, the information were hidden on the back of wax tables, written on the stomachs of rabbits, or tattooed on the scalp of slaves. Invisible ink has been used for serious espionage by spies and terrorists. In modern terms, Steganography uses the media such as text file, image, audio, video as a cover or carrier to conceal the original information. In this paper, an image is used as a cover or carrier for hiding the original information. There is a least significant bit (LSB) [10] insertion method which is mostly used for embedding information in a cover image. The last bit of a byte is known as a LSB. This is 8th bit of a byte. In this method, the information is embedded by replacing the LSB of some or all bytes of an image with the bits of information.. For example a grid for 3 pixels of a 24-bit image can be as follows:

$$(00101100 \quad 00010101 \quad 11010100)$$

$$(10100111 \quad 11010100 \quad 00101100)$$

$$(11011010 \quad 11101101 \quad 01100001)$$

When the number 175, which binary representation is 10101111, is embedded into the least significant bits of this part of the image, the resulting grid is as follows:

$$(00101101 \quad 00011100 \quad 11011101)$$

$$(10100110 \quad 11000101 \quad 00001101)$$

$$(11010011 \quad 10101101 \quad 01100011)$$

In this paper, the original information is encrypted into cipher-text using proposed first method called ASCII differencing method and concealing this cipher-text into RGB cover image of 512*512 using proposed second method

called Three LSB Bits insertion method.

II. PURPOSES

Cryptography provides following security purposes to keep the original data in privacy, no any change of data and so on. [1].

A. *Confidentially*: Information which is transmitted by any channel can be accessed only by the authorized person.

B. *Authentication:* It tells about the checking the identification of sender for ensuring that the received information is arriving from an authorized person or a wrong person .

C. *Integrity:* No body without the sender and receiver can be modify the given encrypted data .

.

D. *Non repudiation:* Requires that neither the sender, nor the receiver of information be able to deny the transmission.

E. *Access control:* Nobody can access the information without authorized person .

III. PROPOSED WORK

The Proposed work is divided into two algorithms.

A. Encoding Algorithm
B. Decoding Algorithm

A. Encoding Algorithm:

a) *Encryption:*

- Take the original information as a Plain -Text.

- Take the random keys to encrypt the Plain -Text.

- Convert each character of plain- text and random keys into its ASCII code and measure its ASCII length.

- Construct digit pair of each ASCII code digit as an individual digit pair vertically.

- Calculate the magnitude of difference of each individual digit pair.

- Now grouping the 1st & 2nd digit and 2nd &3rd digit of ASCII code of random keys and Individual ASCII code differences. Here two groups G1 & G2 will construct from one Individual ASCII code difference and two groups G3 & G4 will construct from ASCII code of random key. Now total four groups are made G1,G2,G3,&G4

- Now XOR operation between G1 & G3 groups and G2 & G4 groups.

- Bytes constructing from XOR operation creates new Cipher- Text.

b) *Embedding:*

- Take a RGB Cover Image of 512*512 for embedding the Cipher- Text.

- Convert the RGB Cover Image into Indexed Image.

- Segmentation of the indexed Image into small segments having size of 2*2.

- Convert the Cipher- Text.into Binary Stream having 8 bit bytes.

- Divide each 8 bit byte into a binary stream having 3 bits into a row and convert into decimal number.

- Constructing two tables in one of which decimal numbers Less than 4 and in other decimal numbers More than 3.

- Taking 1's compliment of more than 3 Data Table.

- Now converting these Less than 4 and 1's compliment of More than 3 Data Tables in the form of binary stream having 3 bits in each row for embedding into selected pixel segments.

- Now select the pixel segment and convert it into binary equivalent.

- Pick the 1st bit of first row of one Data Table and replace it with 8th bit of selected pixel.

- Pick the 2nd bit of first row of one Data Table and replace it with 7th bit of selected pixel.

- Pick the 3rd bit of first row of one Data Table and replace it with 6th bit of selected pixel.

- Now it will create a new binary stream having 8 bits. Convert this binary stream into its decimal number. This decimal number represents the new created pixel value.

- Repeat all steps for embedding the remaining data bits of both data tables into the selected segments and creating new segments with new created pixel values.

- Create a new matrix from these new segments.

- Now constructing RGB Cipher Image from Indexed Cipher Image making by writing new matrix.

B. Decoding Algorithm:

a) *Extraction:*

- Take the RGB Cipher-Image having cipher text.

- Convert the RGB Cipher Image into Indexed Cipher Image.

- Segmentation of the indexed Image into small segments having size of 2*2.

- Convert the New Pixel Value into binary stream having 8 bit bytes.

- Choose the Last three LSB Bits and convert into its decimal number.

- Reconstruct the Less than 4 and More than 3 Data Tables.
- Taking 1's Compliment of only More than 3 Data Table.
- Reposition the Less Than 4 Data Table and More Than 3 Data Table.
- Convert decimal number into binary stream having 3 bits of each and making 8 bit byte in each row.
- Convert each 8 bit byte into character which is Cipher-Text.

b) Decryption:

- Now convert the Cipher Text into decimal number and subtract the constant number from decimal number and then it convert into binary number.
- Here ASCII difference is used as a key for decrypting the Cipher-Text. Now grouping the 1st & 2nd digit and 2nd & 3rd digit of ASCII code differences. Here two groups G1 & G2 will construct from one Individual ASCII code difference.
- Now XOR operation between Group G1 & binary equivalent of one character of Cipher-Text and G2 & binary equivalent of next character of Cipher-Text.

- With XOR operation, the sequence of random keys used at encryption process has accessed in decryption process.

- Calculate the magnitude difference of each individual digit pair vertically made from ASCII difference and accessed keys and concate the each individual digit pair difference and convert into character. Repeat this process for accessing the remaining characters of original information.

Fig 2. Indexed Image

Fig 3. Cipher- Image

Table 1.

Experiment results of Proposed Method

Fig 1. Cover Image

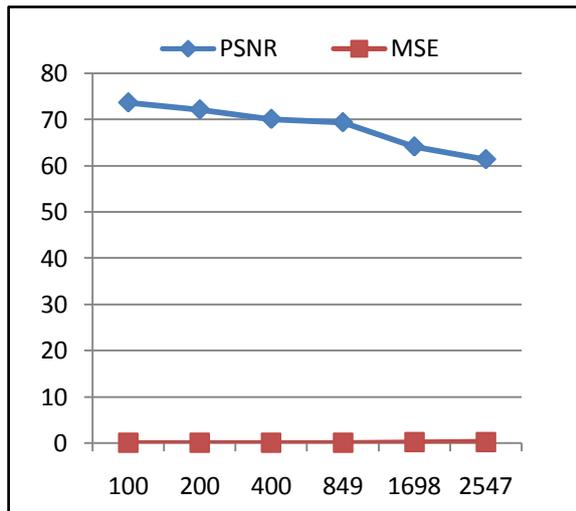| PROPOSED METHOD			
S.NO	Cipher Text	PSNR (In dB)	MSE
1	100	73.6770	0.0528
2	200	72.1626	0.0629
3	400	70.1099	0.0796
4	849	69.3892	0.0865
5	1698	64.1267	0.1586
6	2547	62.2107	0.1977

Fig 4. Graph of PSNR and MSE of Proposed Method

IV.   CONCLUSION

In this paper, we have provided proposed method for securing Original Information by using ASCII Code Individual digit pair differencing and Three LSB Bits Insertion Method.Each character of original information is encrypted with random keys using ASCII Code Individual digit pair differencing in form of cipher text. After generating cipher text, a RGB cover image of size 512*512 is used for hiding the original information and decrypt after its extraction with proposed method. Experimental results show cipher image with good parameter values after embedding the different length of original information in form of cipher text.

REFERENCES

[1]   M. Agrawal, P. Mishra, "A Modified Approach for Symmetric Key Cryptography Based on Blowfish Algorithm", International Journal of Engineering and Advanced Technology , Volume-1, Issue-6, ISSN: 2249 – 8958, , August 2012.

[2]   S.Kruti R, B. Gambhaya, "New Approach of Data Encryption Standard Algorithm", International Jouranal of Soft Computing and Engineering, Volume 2 , Issue 1,March 2012.

[3]   G.C. Kessler, "An Overview of Cryptography", 3 october 2013.

[4]   H. V. Desai, "Steganography, Cryptography, Watermarking: A Comparative Study", Journal of Global Research in Computer Science, Volume 3, No. 12, December 2012.

[5]   Silman, J., "Steganography and Steganalysis: An Overview", *SANS Institute*, 2001.

[6]   Provos, N. & Honeyman, P., "Hide and Seek: An introduction to steganography", *IEEE Security and Privacy Journal*, 2003.

[7]   http://en.wikipedia.org.

[8]   S. Arora, S. Anand, " A New Approach for Image Steganography using Edge Detection Method", International Jouranal of Innovative Research in Coumputer and Communication Engineering, Vol. 1, Issue 3, May 2013.

[9]   A. Mathur, "A Research paper: An ASCII value based data encryption algorithm and its comparison with other symmetric data encryption algorithms" , International Journal on Computer Science and Engineering, Vol. 4 ,No. 09 , ISSN : 0975-3397, Sep 2012.

[10] Chan, C.K. Cheng, L.M., " Hiding Data in Images by Simple LSB Substitution" ,pattern recognition. Vol 37, 2004, Pergamon.