Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.1041 – 1045

RESEARCH ARTICLE

Data Hiding At 7th Bit (RGB) With Cryptography

Rashi Singh
Student
Deptt. Of Comp. Sc. & Engg.
G.I.T.M, Gurgaon, India
rashimac1@gmail.com

Gaurav Chawla
Associate Professor
Deptt.Of Comp. Sc.& Engg.
G.I.T.M, Gurgaon, India
chawla.gaurav17@gmail.com

Dr. Rajkumar Yadav
Department of Computer Science and Engineering,
UIET, MDU, Rohtak
rajyadav76@rediffmail.com

***Abstract*: In recent years it have been witnessed, the rapid development of the internet and telecommunication techniques. But with this development, the security of information is becoming very difficult. To tackle information security problem steganography and cryptography techniques are used. Where cryptography is to scramble the contents of secret message and in steganography the secret message is embedded into the cover medium. In this paper a new technique is discussed by combining both security techniques cryptography and steganography. Firstly information is encrypted by using multiple column transposition cryptography and then this message is hide behind any cover image on LSB 7th bit pixel. This method makes extraction of original message difficult. If hacker will come to know about message hidden in image then will not be able to know original message as it has to be encrypted through cryptography techniques.**

Keywords: **Steganography techniques: Cryptography; Information hiding; Information Security; Image Hiding.**

I. INTRODUCTION

Steganography is an important area of research in recent year involving a number of applications. Steganography is a technique used for hiding information in digital objects such as text, image, audio, video or sound file etc. By hiding information in digital image secure communication, copy - right protection and data authentication become possible. On the other hand cryptography is not to hide information but to encrypt it so that it can't be understand by unauthorized person. Steganography and Cryptography are parallel data security techniques and the techniques can be implemented side by side, in fact steganographic system can implement cryptographic data security. By combining these two techniques, first data is encrypted by cryptography then it is hidden into the cover image so that if steganography technique is broken then no will come to know the original message.

LSB is the very popular method used in steganography in which the message is hidden at the last bit of pixel. But it has disadvantage that if one changes all the last bit of pixels then the message can be destroyed.

So, to overcome this problem message is embedded at different location of the pixel value or the combination of different pixel values like:-

- 5th bit, 6th bit, 7th bit of pixel.
- 6th bit, 7th bit, 8th bit of pixel.
- 7th bit and 8th bit of pixel.
- 7th bit of pixel.
- 8th bit of pixel.

II. DESCRIPTION PROPOSED METHOD

To increase the capacity of image steganography we proposed a framework for hiding large volume of data much securely by combining cryptography technique i.e. multiple column transposition technique with Second LSB bit.

Multiple Transposition Method

Transposition technique changes the order of the letters in a message instead of replacing characters with other characters. it does not change (add or delete) any bit but only change the position of the bit so that it can't be able to understand. One of the transposition techniques is multiple round column transposition. In this technique the plain text is written in a row wise matrix form but is read as column wise all this is done by a key. The Key is something the sender and the recipient agree on beforehand. Key tells the size of the matrix. To encrypt plaintext the message is written in a rectangle, row by row, and reads the message off, column by column, but according to the order of the columns based on the key.

Transposition cipher is also of two types

- Regular columnar transposition cipher- An extra space of matrix is filled with null.
- Irregular columnar transposition cipher - An extra space of matrix is left blanks.
- In multiple round transposition cipher - The encrypted message is again encrypted with the help of key.

For example: - if we want to encrypt "COME HOME TOMARROW" by transposition cipher then it will be.

Message – "COME HOME TOMARROW"

Key – lions

So, according to key sequence of row will be 2, 1, 4, 3, 5.

2	1	4	3	5
C	O	M	E	H
O	M	E	T	O
M	A	R	R	O
W				

Encrypted message will be- "OMACOMWETRMERHOO"

In second column Transposition cipher this message is again encrypted

Message - "OMACOMWETRMERHOO"

Key – lions

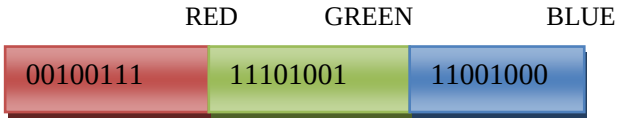
2	1	4	3	5
O	M	A	C	O
M	W	E	T	R
M	E	R	H	O
O				

Encrypted message will be- "MWEOMMOCTHAERORO

III. SECOND LSB METHOD [7th Bit]

24 Bit Image: In this method the message is to be embedded at the second last bit value i.e. 7th bit of a pixel to overcome the disadvantage of LSB method. In a computer images are represented as array of values. And these value represent the intensities of three color R(ed), G(reen), B(lue) where the total value of these three color describe a pixel value. This color model is called **the RGB model.** The 8 bit image can represent the total number of color 2^8 = 256 and a 24 bit image can represent 2^{24} = 16777216 colors. So, large bit value images are used to hide data.

For Example:-



If 101 =5 is embedded at 7th bit

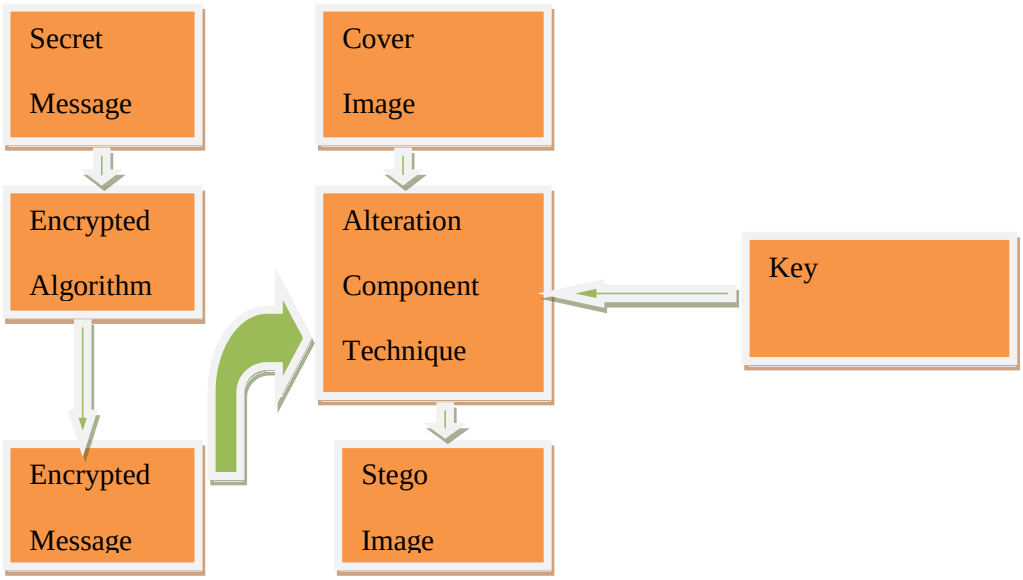
Once all the message characters are embedded into the cover-image, the target character (*) represented in bit by 101010, is inserted in the pixel of the cover-image immediately next to the one containing the last input character of the message. The target character is a special symbol and is known as Terminator Character. Because it is the last character that is embedded and after embedding the target character (101010), insertion process stops from next row onwards. This helps the decoding process to stop extracting of data from stego-image by informing that target character has come to end of data.

8 Bit Image: The 1 pixel of 8 bit image can represent 256 color only So the image should be chosen very carefully. Consider a palate with four color with palate position white(00), red(01), green(10), blue(11), similar to ARGB.We will try and hide the decimal number 10 represented in binary as 1010. The resulting raster is: 01 00 11 10, which corresponds to red, white, green, blue. These large changes in the image are very noticeable in a color image although an 8-bit gray scale image will produce relatively good results. There are multiple tools that implement LSB

IV. Proposed Encryption Algorithm

In this paper multiple column transposition cipher is used along with image hiding at 7th bit of pixel is used .the proposed algorithm is as follows:

1. Write the plain text message row-by-row in a rectangle according to key size.
2. Read the message column-by-column. However, it need not be in the order of columns 1, 2, 3 etc. It should be according to Key value etc.
3. The message thus obtained is the one time encrypted cipher text message.
4. Repeat step 1 and 2.
5. The message obtain is multiple round cipher text.
6. Select a cover image of size M*N as an input
7. A numeric key is selected (This key may be equal to *M* x *N*, where *M* and *N* denote the total number of the pixels in the horizontal and the vertical dimensions of the image).
8. The message to be hidden is embedded in RGB component only of an image.
9. Use a pixel selection filter to obtain the best areas to hide information in the cover image to obtain a better rate. The filter is applied to Second Least Significant Bit (LSB) i.e. 7th bit of every pixel to hide information, leaving most significant bits (MSB).
10. After this Message is hidden using Bit Replacement Method.



V. COMPARISION OF EMBEDDED DATA AT PROPOSED METHOD WITH LSB

The comparison is done to proof that proposed method is much better than the existing one. To prove it some examples are taken.

Example1: We want to insert an A (binary value 10000011) into a 24-bit image which uses the RGB color model. Each pixel uses eight bits for the intensity of red, green and blue. As we only want to change the least significant bits, we need 3 pixels for hiding the letter A.

	Red Component	**Green Component**	**Blue Component**
pixel 0	00100111	11101001	11001000
pixel 1	00100111	11001000	11101001
pixel 2	11001000	00100111	11101001

The changed sequence with the letter A (bit sequence 10000011) embedded would look like this:

	Red Component	**Green Component**	**Blue Component**
pixel 0	00100111	11101000	11001000
pixel 1	00100110	11001000	11101000
pixel 2	11001001	00100111	11101001

As we have make change at 4 bit position, If we change the 7th least significant bits, we need 3 pixels for hiding the letter A but the change would be on 2 bit place. This change is very minimum almost negligible from human eyes.

The changed sequence with the letter a (bit sequence 10000011) embedded would look like this:

	Red Component	**Green Component**	**Blue Component**
pixel 0	00100111	11101001	11001000
pixel 1	00100101	11001000	11101001
pixel 2	11001000	00100111	11101011

Example 2: if a pixel of the cover image with the LSB RGB (Red-Green-Blue code) color 26E9CB# is used, binary 00100110-11101001-11001011 to hide the message 100 i.e. 4, the result would be (00100111-11101000-11001010):

Table 2: Results with LSB method

	Hexadecimal	**Red**	**Green**	**Blue**
Original Value	26E9CB	38	233	203
Modified Value	27E8CA	39	232	202

Result: Results obtained hiding the message 100 in the pixel 00100110-11101001-11001011 with the Second LSB method i.e. 7th bit the result would be (00100110-11101001-11001001) The least significant bits of the pixel have changed, introducing a small distortion. So, SECOND LSB method that would introduce more efficiency and less distortion.

Using the same example, the 3 bits of information 100 will be introduced in the SECOND LSB bits of each color the result will be.

	Hexadecimal	**Red**	**Green**	**Blue**
Original value	26E9CB	38	233	203
Modified Value	26E9C9	38	233	201

In this case the changes are at LSB of all three colors.

VI. FUTURE WORK

As the concept of security is very wide. The speed at which new technologies are introduced, with the same speed breaking of that technologies are also come out. So security of information is always a topic of new search and new researches on cryptography and steganography will goes on. Every technique leaves some space for further improvement. The work can be extended to provide an alternative strategy for data compression which can further reduce the size of the data. Efficient cryptographic techniques can also be used along with the steganographic techniques to provide more security to the data.

VII. CONCLUSION

In this paper we have used both steganography and cryptography technique to make data more secure. In this proposed system cryptographic and steganographic security is combined to give two tier securities to secret data. The Second LSB Insertion technique used to hide the message in images and tested with various samples. To add more security, we introduced a new encryption and decryption algorithm for the message before hiding. The most important property of this method is that the message information is scattered randomly over the second last bit of the cover image pixels. The comparative analysis is also shown between the proposed method and existing method.

REFERENCES

[1] J.B. Sinclair. "Simulation of Computer Systems and Computer Networks: A Process-Oriented Approach". Feb.15, 2004.

[2] Ismail Avcibas, Nasir Memon, and Bulent Sankur, "Steganalysis Using Image Quality Metrics", IEEE transactions On Image Processing, Vol.12, No.2, February 2003.

[3] D. Artz, "Digital Steganography: Hiding Data within Data", IEEE Internet Computing, Vol. 5, No.3, pp. 75-80, 2001.

[4] I. Avcibas, B. Sankur, and N.D. Memon. "Steganalysis based on image quality metrics". Proc. Multimedia Signal Processing Conf., Oct. 2001.

[5] J. Fridrich, R. Du, and L. Meng. "Steganalysis of LSB encoding in color images". Proc. IEEE ICME Conference, July 2000.

[6] N. F. Johnson, S. Jajodia, "Steganalysis: The Investigation of Hidden Information", Proc. IEEE Information Technology Conf., pp. 113-116, 1998.

[7] N. F. Johnson, S. Jajodia, "Exploring Steganography: Seeing the Unseen", Vol. 31, No.2, IEEE Computer,pp. 26-34, 1998.

[8]Ahlfeldt; R.M., (2006) "Information Security in a Distributed Healthcare Domain". Ph.D. thesis, University of Sk¨ovde, Department of Communication and Information.

[9] Chandramouli R. and Memon N. (2001), "Analysis of LSB based Image Steganography Techniques", Proceedings of ICIP 2001, Thessaloniki, Greece, October 7−10.

[10] Deshpande N, Snehal K., "Implementation of LSB Steganography and Its Evaluation for Various Bits" K.K.Wagh Institute of Engineering Education & Research, Nashik India

[11] http://www.appliedtrust.com/resources/security/every-company-needs-tohave-a-security - program

