Data Security using Combination of Steganography and Cryptography

Muhammad Omer Mushtaq, Yasir Saleem, Muhammad Fuzail,
Muhammad Khawar Bashir, Binish Raza

Department of Computer Science & Engineering University of Engineering & Technology, Lahore, Pakistan

Abstract

With the passage of time data protection is the most evolving topic of Information Security. However steganogarphy is less used, Cryptography is employed worldwide extensively in this area. Combination of both is very effective which is discussed in this paper. This paper proposes the technique of securing data by first using cryptology and then encodes the encrypted data using steganography. This makes it almost impossible for any individual cryptanalyst or a steganalyst to intrude the hidden message unless existence of hidden communication as well as encryption technique is known to the intruder. This scheme can be used to transmit data securely and covertly over wired as well as wireless media.

I. INTRODUCTION

This research paper proposes a combined technique of cryptography and steganography. The data to be transmitted is first encrypted using RC4 then the encrypted data is read as bytes and then broken into bits. The isolated bits are then placed at specific bit patterns of the digital image. The resulting image colour is changed by very small grayscale levels as compared to the original image. This change is not perceivable for any third party. Quality and dimension of carrier image used is directly proportional to efficiency of the designed system.

Use of only Cryptography however makes data meaningless but visible for cryptanalyst and is an invitation for attack to any intruder [1]. Use of steganography however makes data hidden but if the existence is sensed by any means, any intelligent steganalyst can find the secret data by some strong statistical analysis [2].The proposed technique can be cornerstone among future security trends in symmetric session key distribution. However the carrier file used in this scheme is the digital image but this technique can also be applied to other digital media .Next section gives an overview of both cryptography and steganography and some technical background of researches already made in this area. Third and fourth sections explain the proposed system regarding cryptography and steganography respectively. Fifth section describes the software implementation of our scheme. And sixth section describes the conclusion of our proposed system.

II. TECHNICAL BACKGROUND

The art of hiding information within digital data by a way that any third party cannot feel the existence of hidden communication is termed as Steganography[3]. The information that is to be concealed and the data that is used as carrier of that information can be of any digital format [4]. Information is embedded or encoded in the carrier digital file using a particular algorithm or technique [5]. The carrier digital file is transferred to second party and the hidden information is extracted using exactly the same technique as was used at the sending end, provided the encoded data is not transformed by any means while it is being transferred from sender to receiver. The encoding technique is designed in a way that the carrier digital file after and before encoding remains ostensibly same. This makes it different from cryptography in which data is deformed but not invisible.

In most simple way Cryptography might be termed as converting data into a form that is meaningless for any third party[6][7]. Encryption and Decryption are two main processes performed at sender and receiver end respectively. Encryption is just like a lock that is closed with the key and receiver needs the key to open that lock. The locked information known as cipher text is meaningless for third party.

Vikas Tyagi [8] proposed a technique of steganography in combination with cryptography in which the secret data is encrypted using symmetric key algorithm then the encrypted data is hidden into an image using LSB pixel processing. The combination of both these techniques provides a secure transmission of secret data. However this technique is combining both famous data security techniques but can be criticised by a limitation of data to be encoded because this technique is using only a single bit as carrier of information that is if a colour image is taken as carrier of information each pixel might carry only three bits of information.

Jagvinder Kaur and Sanjeev Kumar [9] propose a steganographic model in which secret message or data is embedded into a cover-object that can be text, image, or any multimedia digital file. The secret data is encrypted with a setgo-Key that is only known by sender or receiver. The message is embedded using the intensity of the pixel values directly. Image or cover-object is divided into blocks of bits and one message bit is embedded in every block of original image bits. This technique however makes minimum degradation of the original image but also provide a very small limit of data to be embedded since only one message bit is added to a block of image.

Samir Kumar and Indre Kanta [10] proposed a technique for hiding data in an 8-bit colour image file. This uses a lookup table or palette instead of 24-bit RGB image. In palette based steganography least significant bits are used to hide the data. A palette generation algorithm is used to quantize the image in different blocks then the colours in palette are sorted to minimize the difference between the colours. It uses Euclidian distance to choose the RGB values of 24-bit image compared to the RGB value of every colour in the palette [11] . Information will be hiding by changing the LSB of image with the bit values in palette. This technique provide a secure and fast system for internet and mobile communication due to light weight of image that can store small amount of data. Small amount of data again dictates the limitation of secret information that can be transmitted. Also the absence of cryptography makes the carrier image vulnerable for attack.

Adnan Gutub [12] proposed a new merging technology of utilizing LSB within image and random pixel manipulation methods and stego-key. Pixel used for hiding data is selecting random fashion depends on stego-key .Two LSB of one colour channel used to indicate the existence of data in the other two channels. Security is improved because the selection of indicator channel is not fixed. Indicator channel is selected in sequence. The test of this technique shows attractive results in the storage capacity of data-bits that to be hidden in relation to RGB image. However the technique for hiding data is efficient but not using encryption can be a threat in case some statistical analysis is performed at the pixels' bits.

Tanvir and Adnan Abdul-Aziz [13] proposed a new technology for image based steganography. A comparison is represented between the previous technology (Pixel Indication) and new proposed technique that is Intensity Based Variable-bit by showing experiments. The variable numbers of bits are stored in the channel of RGB image. The number of data bit storage is decided on the bases of actual colours of the image. The data bits are stored in one of two channels of the image other than the indicator channel depends on the colour values. The lower colour value channel will store data in its LSB. The selection of colour scheme is at runtime and depends on the cover media. The technique might be efficient as the presence of data in each pixel is not sure for the attacker but processing each pixel in image can give required data as there is no encryption on data and the data is hidden but present in its original form.

Juan and Jeus [14] proposed a technique of steganography in spatial domain. Technique uses the LSB steganography by hiding data in only one of the three colours at each pixel of cover image. To choose the colour for hiding information Pair analysis is used then LSB Match method is applied so that the final colour is as close to possible to the original one in the scale of colours. The proposed technique is however immune to visual, statistical and histograms attacks but limitation of data to be hidden is demerit of the technique and also data is not encrypted so a good statistical analysis might easily give the secure data to the intruder.

III. RC4 CIPHER

Both sender and receiver use the RC4 cipher which is fast and easy to implement in software as well as in hardware. RC4 cipher has variable key length. In our scheme we use the minimum key length of 32 bytes or 256 bits.

First of all an array state S is declared of 256 bytes shown in Figure 1[15]. S[i] =i ,where i={0,1,2,3… 254,255}

S
0
1
2
3
4
• • •
253
254
255

Figure 1: State Vector S

After that a temporary array vector T is declared whose length is same as of S. T is initialized by replicating the K vector containing the user defined key shown in Figure 2[15].

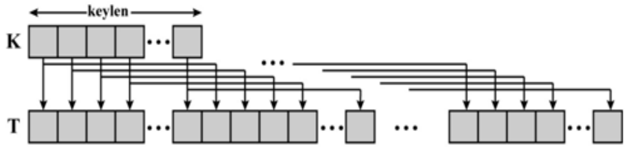


Figure 2: Initial State of T

Values of S are permuted by vector T. It is described by Figure 3[15]in which each ithbyte of S is swapped with jthbyte of S.

And j = (j + S[i] + T[i]) mod 256 [j initially set to zero]

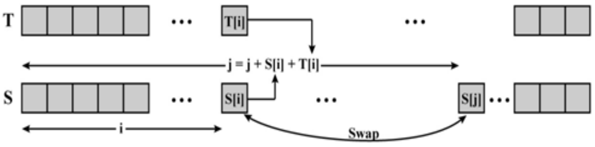


Figure 3: Initial Permutation of S

After the permutation, a temporary index t of S is generated by the ith and jth bytes of S which gives us the Random Key Stream Byte k given by algorithm:

$$k = S[t]$$

Where j& t are

$$j = (j + S[i]) \bmod 256$$

$$t = (S[i] + S[j]) \bmod 256$$

With generation of every k, S vector is again permuted at the end of each iteration as shown in Figure 4[15].

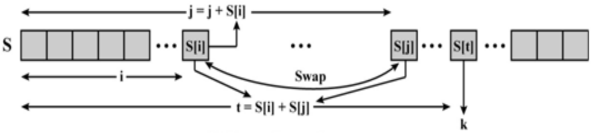


Figure 4: Stream Generation

Cipher byte is generated by the bitwise XOR operation between random key that is generated by above process and plaintext data. Figure 5 shows this procedure .In the same way at decryption end plain text is obtained from bitwise XOR of key (same key as was used at Encryption) with cipher text.

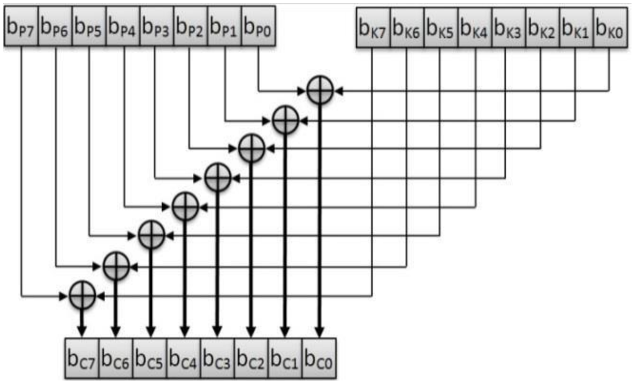


Figure 5: Cipher Text Generation

IV. STEGANOGRAPHY

The system reads the cipher text as a stream of bytes and for placement of different colour planes in the pixel, each byte is broken into group of bits. For the proposed system there are 6 possible combinations of bits' groups by dividing a byte (8 bits).The designed system rely on these 6 combinations of bits' that have any value only as more combinations make grayscale value somewhat perceivable. Any combination of bits' groups constitutes a byte which is mapped to a pixel at its different colour planes (most probably red, green and blue).

Cipher Byte is broken into groups of bits in different ways. In all ways essentially there are three groups simply shown by Figure 6 where C_{g1}, C_{g2}& C_{g3} are chosen from set

C = {2, 3, 4} in a way that to complete a byte, that is

$$C_{g1} + C_{g2} + C_{g3} = 8 \qquad \ldots 1$$

C_{g1}	C_{g2}	C_{g3}

Figure6: Cipher Byte Division

Choice of these numbers is explained by the following calculations. Let the chosen values for C_{g1}, C_{g2}& C_{g3}be

$$C_{g1} = 4$$

$$C_{g2} = 2$$

$$C_{g3} = 2$$

Then the change in grey levels of whole pixel due to C_{g1}willbe $C_{g1}' = 2^4 = 16$

Similarly

$$C_{g2}' = 2^2 = 4$$

$$C_{g3}' = 2^2 = 4$$

So the total change Δ_c in grey levels of the pixel due to these bits' change is given by

$$\Delta_c = C_{g1}' + C_{g2}' + C_{g3}'$$

$$\Delta_c = 24$$

Other possible combination for Figure 6 can be

$$C_{g1} = 3$$

$$C_{g2} = 3$$

$$C_{g3} = 2$$

Δ_c for this choice is 20 which is even a better choice. Value 4 cannot be chosen for any two of C_{g1}, C_{g2}& C_{g3}because it will not satisfy the Equation 1. In a similar fashion not all C_{g1}, C_{g2}& C_{g3}can be 3 or 2 at the same time. Hence it forms six possible combinations that are shown in Figure 7.

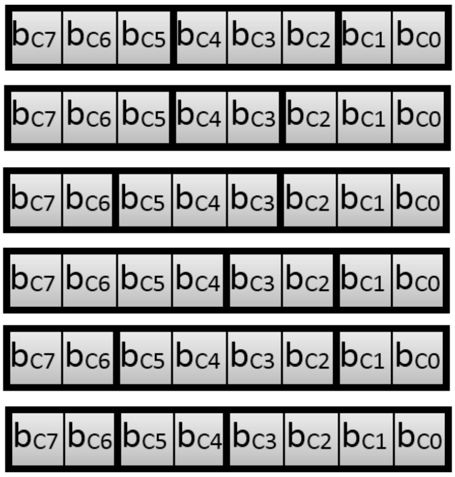


Figure 7: Possible Cipher Byte Division

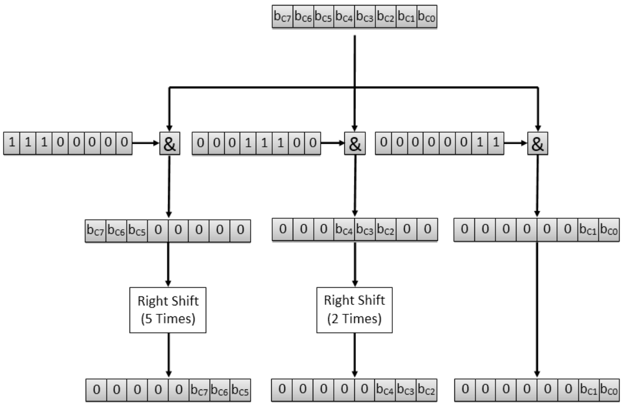


Figure 8: Isolation of Cipher Byte

A simple bitwise AND operation is performed to break the bits into groups ,for instance process of first possible bits-groups having 3, 3 and 2 bits is shown in Figure 8. First combination is result of bitwise AND operation of cipher byte Cb with 11100000 and then shifting it 5 bits-places towards right. The shifting is performed to move the meaningful bits at LSB positions and place 0 at rest of the bits which will help to map the value at desired place in colour plane of pixel using bitwise OR which are explained in next few lines. Group2 is result of bitwise AND operation of Cb with 00011100 and require shift of 2 bits-places to move the meaningful bits at LSB positions. Group3 is simply the result of bitwise AND of Cb with 00000011 without any shift. Brief overview of Steganographic process of above operation for 1st combination of Figure 7 is shown in Figure 9.

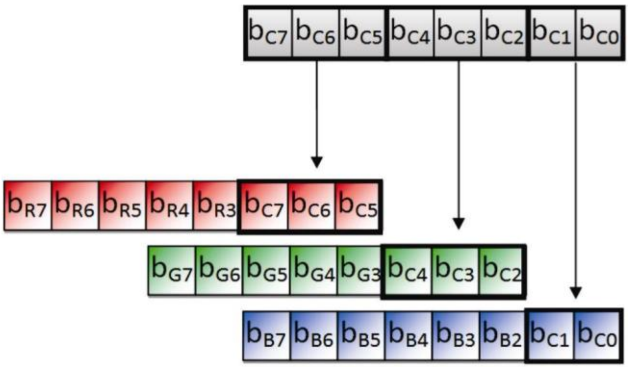

bC7 bC6 bC5 bC4 bC3 bC2 bC1 bC0
bR7 bR6 bR5 bR4 bR3 bC7 bC6 bC5
bG7 bG6 bG5 bG4 bG3 bC4 bC3 bC2
bB7 bB6 bB5 bB4 bB3 bB2 bC1 bC0

Figure 9: First Cipher Byte Division

Figure 10 shows overview of Steganographic process for second possible combination from Figure 7.

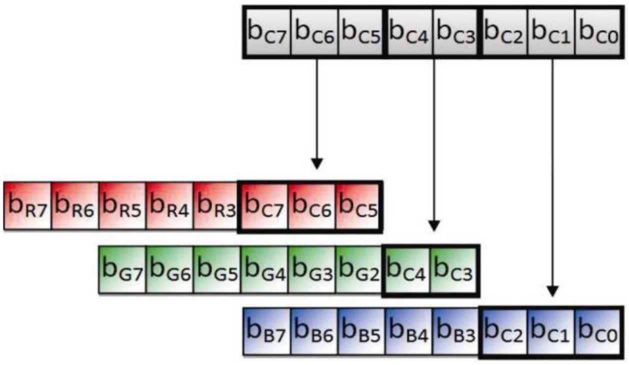

bC7 bC6 bC5 bC4 bC3 bC2 bC1 bC0
bR7 bR6 bR5 bR4 bR3 bC7 bC6 bC5
bG7 bG6 bG5 bG4 bG3 bG2 bC4 bC3
bB7 bB6 bB5 bB4 bB3 bC2 bC1 bC0

Figure 10: Second Cipher Byte Division

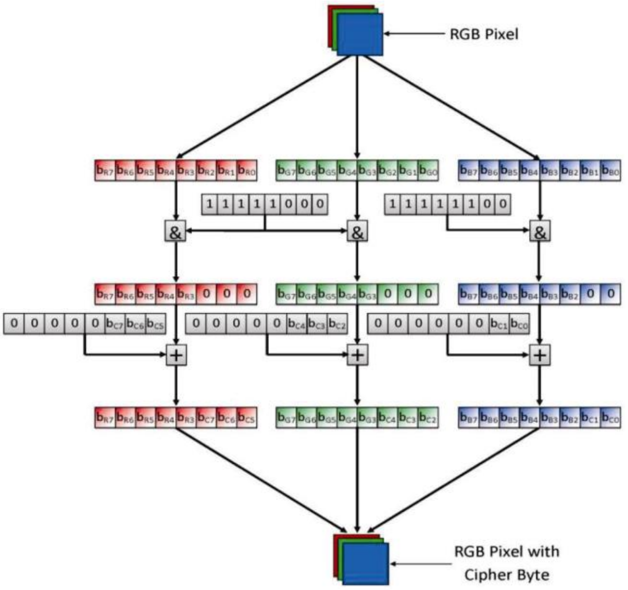
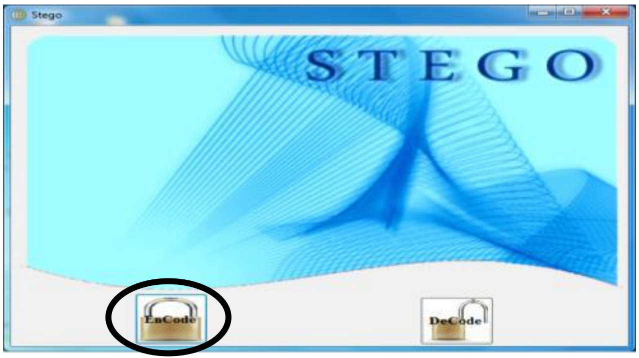
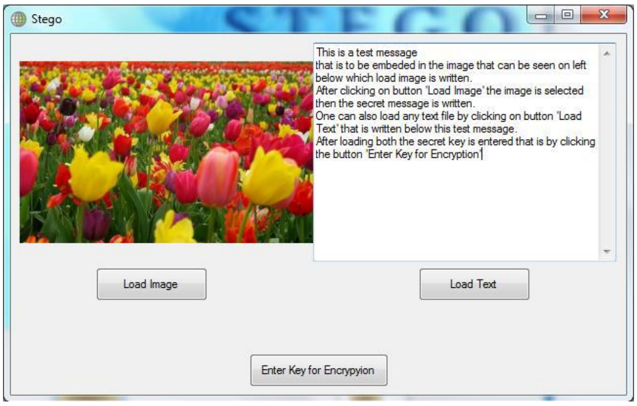

RGB Pixel
bR7 bR6 bR5 bR4 bR3 bR2 bR1 bR0
bG7 bG6 bG5 bG4 bG3 bG2 bG1 bG0
bB7 bB6 bB5 bB4 bB3 bB2 bB1 bB0
1 1 1 1 1 0 0 0
1 1 1 1 1 1 0 0
&
bR7 bR6 bR5 bR4 bR3 0 0 0
bG7 bG6 bG5 bG4 bG3 0 0 0
bB7 bB6 bB5 bB4 bB3 bB2 0 0
0 0 0 0 0 bC7 bC6 bC5
0 0 0 0 0 bC4 bC3 bC2
0 0 0 0 0 0 bC1 bC0
+
bR7 bR6 bR5 bR4 bR3 bC7 bC6 bC5
bG7 bG6 bG5 bG4 bG3 bC4 bC3 bC2
bB7 bB6 bB5 bB4 bB3 bB2 bC1 bC0
RGB Pixel with
Cipher Byte

Figure11: Complete Process

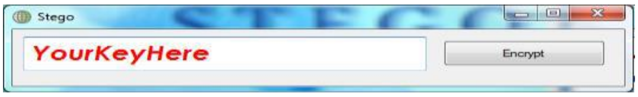
The whole process shown in Figure 8 gives us isolated bits at LSB positions which are then mapped to respective color-bits of pixel by performing bitwise AND operation with color-bits of pixel .

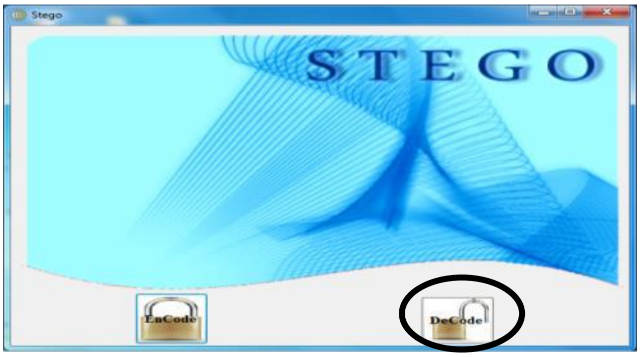
Taking the above instance of groups in the RGB pixel, red and green color bits are performed bitwise AND operation with 11111000 (to place C_{g1} and C_{g2} respectively) and blue color bits with 11111100. This operation makes the last bits vacant so that the isolated bits of cipher text can be placed here which is done by performing bitwise OR of cipher with respective color bits. The whole process above is explained in the Figure 11.

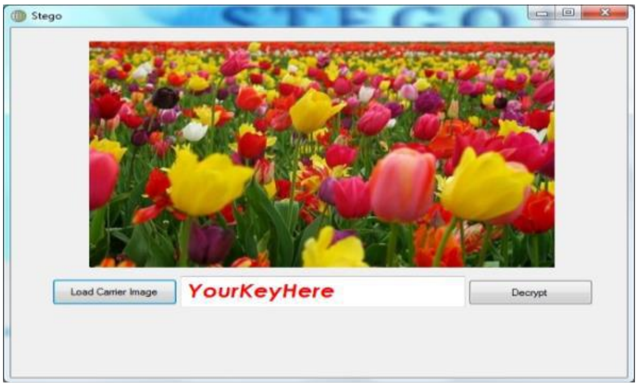


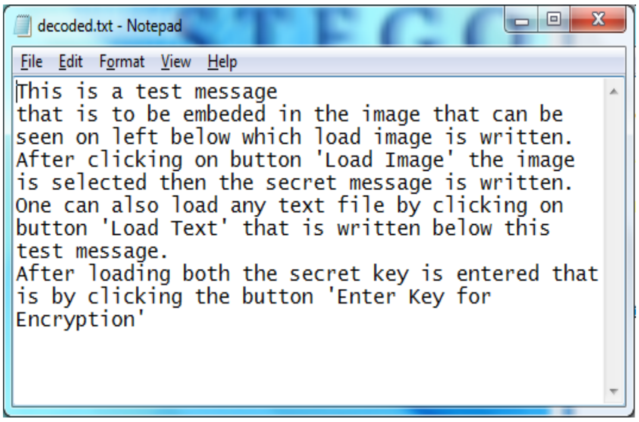


This is a test message
that is to be embeded in the image that can be seen on left below which load image is written.
After clicking on button 'Load Image' the image is selected then the secret message is written.
One can also load any text file by clicking on button 'Load Text' that is written below this test message.
After loading both the secret key is entered that is by clicking the button 'Enter Key for Encryption'









```
This is a test message
that is to be embeded in the image that can be
seen on left below which load image is written.
After clicking on button 'Load Image' the image
is selected then the secret message is written.
One can also load any text file by clicking on
button 'Load Text' that is written below this
test message.
After loading both the secret key is entered that
is by clicking the button 'Enter Key for
Encryption'
```

II. REFERENCES

[1]. Phad Vitthal S., Bhosale Rajkumar S., Panhalkar Archana R. *"*A Novel Security Scheme for Secret Data using Cryptography and Steganography" *I.J. Computer Network and Information Security*, 2, 36-42, 2012.

[2]. Shivendra Katiyar, Kullai Reddy Meka, Ferdous A. Barbhuiya, Sukumar Nandi, "Online voting system powered by Biometric security using Steganography", International conference on Emerging Applications of Information Technology, pp. 288-291, 2011.

[3]. Aniello Castiglione, Bonaventura D'Alessio, Alfredo De Santis, "Steganography and secure communication on online social networks and online photo sharing", International conference on Broadband and Wireless communication, Communication and applications, pp. 363-368, 2011.

[4]. D. Artz, "Digital Steganography: hiding data within data", IEEE Internet Computing, Vol. 5, Issue-3, pp. 75-80, 2001.

[5]. Piyush Marwaha, Paresh Marwaha, "Visual Cryptographic Steganography in Images", Second International conference on Computing, Communication and Networking, pp. 1-6, 2010.

[6]. S. Usha, "A secure triple level encryption method using cryptography and steganography", International Conference on Computer and Network Technology, Vol. 2, pp. 1017-1020, 2011.

[7]. K Suresh Babu, K B Raja, Kiran Kumar K, Manjula Devi T H, Venugopal K R, L M Patnaik, "Authentication in secret information in Image Steganography", TENCON, pp. 1-6, 2008.

[8]. Mr . Vikas Tyagi, Mr. Atul kumar, Roshan Patel, Sachin Tyagi, Saurabh Singh Gangwar, " Image Steganography using least significant bit with cryptography ", Journal of Global Research in Computer Science , Volume 3, No. 3, March 2012

[9]. Jagvinder Kaur, Sanjeev Kumar, "Study and Analysis of Various Image Steganography Techniques", IJCST Vol. 2, Issue 3, September 2011

[10]. Prof. Samir Kumar Bandyopadhyay, Indra Kanta Maitra, "An Application of Palette Based Steganography" , International Journal of Computer Applications (0975 – 8887) Volume 6– No.4, September 2010

[11]. Gao Hai-ying, Xu Yin, Li Xu, Liu Guo-qiang, "A steganographic algorithm for JPEG2000 image", International conference on Computer Science and Software Engineering, Vol. 5, pp. 1263-1266, 2008.

[12]. Adnan Gutub, Mahmoud Ankeer, Muhammad Abu-Ghalioun, Abdulrahman Shaheen, Aleem Alvi, "Pixel indicator high capacity technique for RGB image based Steganography" WoSPA 2008 – 5th IEEE International Workshop on Signal Processing and its Applications, University of Sharjah, Sharjah, U.A.E. 18 – 20 March 2008.

[13]. Mohammad Tanvir Parvez, Adnan Abdul-Aziz Gutub, "RGB Intensity Based Variable-Bits Image Steganography," apscc, pp.1322-1327, 2008 IEEE Asia-Pacific Services Computing Conference, 2008

[14]. Juan José Roque and Jesús María Minguet, "SLSB: Improving the Steganographic Algorithm LSB", 7th International Workshop on Security in Information Systems, 57-66, (2009).

[15]. William Stallings, "Cryptography and Network Security", 5th Edition, Publisher: Prentice Hall, 2005.

****