ISSN No:-2456-2165

An Efficient Method for Data Embedding and Image Encryption by using Dna and Chao's Theory

Athira K.S
M. Tech Cyber Security, Department of CSE
Sree Narayana Gurukulam College of Engineering,
Kadayiruppu, Kerala, India

P Krishna Kumaran Thampi
Associate Professor, CSE Dept.
SNGCE, Kadayiruppu, Kerala

Abstract:- **The evolution of computer network technology, digital images are broadcast in public communication network. So that ensuring the security of digital image attracts more attention. In the proposed work we propose cryptography DNA encryption and chaos theory which combines the encryption and reversible data hiding techniques for embedding. In order to this techniques used to achieve primary concerns of security. In this method firstly, input image is converted into RGB components. These RGB matrix are transformed into two DNA encoded matrix. Chen's hyper chaotic map is applied for odd pixel value based DNA encoded matrix and Lorenz chaotic map is used for even pixel value based DNA encoded matrix to produce the chaotic sequence separately. To interchanging the pixel position of two DNA encoded matrix with chaotic sequence. Final step is to perform an add operation which can add two matrices to get the resultant encrypted image. Next stage for embedding, For data embedding the repeating process of histogram equalization can be performed. The proposed algorithm was analyzed and evaluated using data set of different images. The experiment result shows the strength of the proposed algorithm.**

Keywords:- *DNA Cryptography, Chen's hyper chaotic map, Lorenz chaotic map, RDH Algorithm.*

I. INTRODUCTION

Due to the revolutionary growth of digital communication to ensure the security of image and information has become a challenging area. The lack of security in an digital image can cause easyaccess by the hackers and it can further use for illegally purpose. All kind of implementation are carried out in secured digital image applications must be ensure the standard security requirement such as confidentiality, integrity and authentication. As a result image encryption technology is prime concern in different areas like telemedicine, military, E-Commerce, cloud computing, financial transaction and mobile phone applications. In telemedicine the patient information are in the form of electronic medical images and also doctors wants to communicate the secret information with their patients, Information will be embedded into animage and transmitted. In order to enhance the security features, we can also embedded source camera information in the target image. So that if any attack occurs we can easily retrieve the source information. Secure data transmission are possible in images using Image encryption and data embedding methods.Different techniques are available for image security and one of the technique is encryption. Encryption is procedure by which the input image is converted into an cryptic image using a key. A user can retrieve the input image by applying a decryption method on the cipher image. The common algorithms are used in Encryption process rsa and aes. The next part of an data transmission is data embedding. Usually we can see that image embedding are done by lsb embedding.

In cryptography recent techniques called DNA image encryption based on chaotic theory have been implemented. Combination of both cryptography and chaotic theory based method can improve the encryption level. The DNA computation of an image is complex and hence it is used only in encryption. The different types of chaotic maps are used in image encryption, the purpose of using chaotic sequence in an digital image is to increase the security of encrypted image. A novel Reversible Data Hiding (RDH) is proposed in this work. RDH is also called an lossless data embedding and it is used as an information career.

The proposed techniques provides security for images and data. The flow of the proposed technique include various stages. The image encryption part consist of the technique called DNA encryption and chaotic theory and The data embedding part consist of RDH method. The different stages of this system is clearly explained in fig 1.

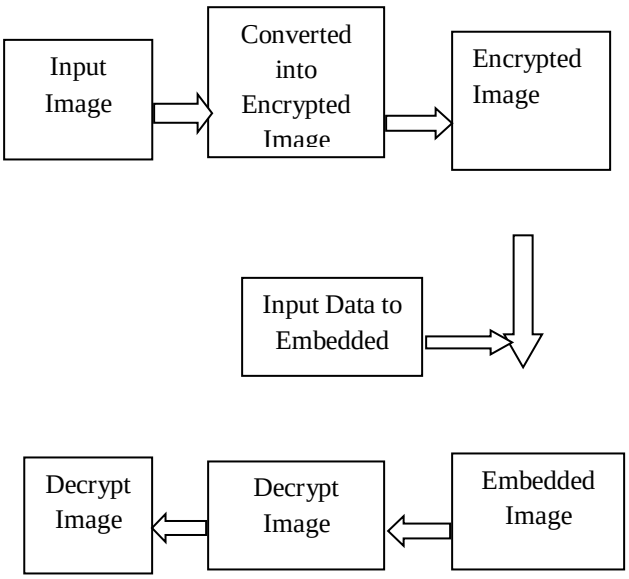

Fig 1:- Proposed System Design

II. LITERATURE SURVEY

There have been a number of surveys about image encryption and data hiding in literature. A comparative study is performed in this section to give completeness to this work. The result shows that various kinds of encryption and decryption are applied in different applications such as military information, telemedicine applications etc.

In [1], authors presented AES encryption method for images. In this existing method, Firstly image is divided into matrix format and applying each round of AES algorithm. Before going for an encryption must be set the initial key for encryption. In decryption process the same kind of rounds are carried out in reverse manner.

In [2], authors have proposed another encryption method for images in his work. The work mainly focus on RSA encryption. It is a public key cryptosystems. For an encryption to selected encryption key (two large prime number) is used in encryption stage and converted into encrypted format. The encryption key is a public one and decryption key is private one.

In [3], authors have connoted a technique which is based on the Blowfish algorithm. It is symmetric block encryption. In this technique the key length is variable and having the range 32 to 448 bits. Each of the encryption rounds are done by using permutation and XOR operation in an image.

In [4], authors proposes LSB substitution for data hiding. In this work the new methods are implemented in proposed system. Usually LSB methods are for encryption part cover image is converted into stego images by using key. For decryption the same key is used to recover the image. But in this paper used combination of LSB technique and PVD.

In [5], authors introduced a new area in steganography in colour images in frequency domain or more precisely that in Discrete Cosine Transform (DCT) domain. It is used for an to hide the data into image. In this method image is divided in to low, middle and high frequency components. Usually embedding process are done in middle component of image.

In [6], authors proposed a method for embedding are Cryptography and Digital Watermarking. It is mainly focused on medical images. The proposed algorithm having two stages, water marking embedding procedure and water marking extraction procedure. The embedding are done in RONI region of image. In extraction process are also started from RONI that means its a reversal of embedding process. It provides image integrity and authenticity.

III. PROPOSED SYSTEM

A. Methodology

In the proposed system or in any other embedding system there are two stages of processing namely image encryption and data embedding. Here also we have two stages of operation, encryption and hiding. Encryption process can be further divided into DNA encoding and chaotic sequence generation. Next step is data hiding, we are embedding text fileby using RDH algorithm. Finally at the destination or receiver end the image need to be decrypt by performing the reverse operation encryption stage. Fig 2. shows the Overview of the proposed method.

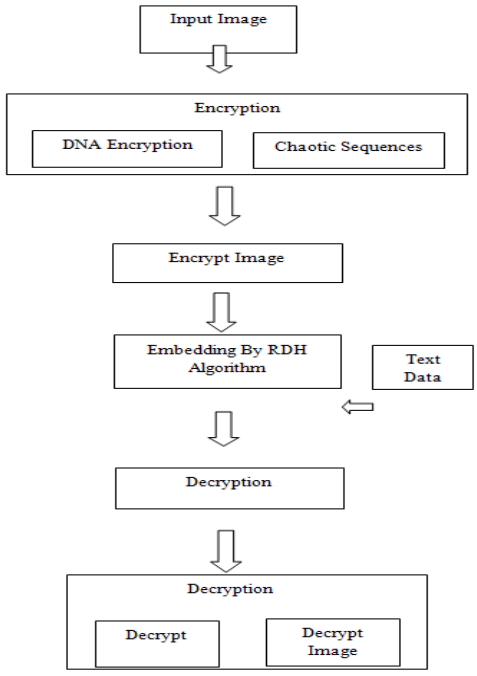

Fig 2:- Overview of Proposed Method

ISSN No:-2456-2165

B. DNA Cryptography

DNA stands for deoxyribonucleic acid in medical dictionary which is an unbreakable component in human body, like this type of component we are proposing an unbreakable DNA encryption technique using chaos theory[7]. Fig 3. shows the process of transformation to get an encrypted image.

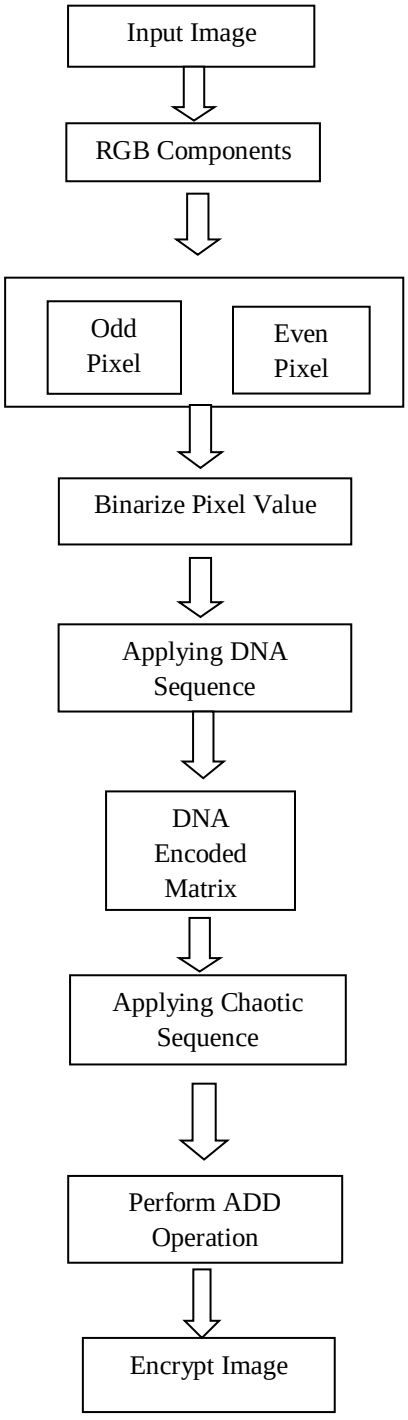

Fig 3:- DNA Encryption Process

In the proposed model the initial step is to extract the RGB component of target image. That is generating odd value pixels and even value pixels of the input image. Next step is to binarize the generated odd and even value pixels. After generating the odd and even pixels these binary image need to be encoded using a DNA standard. The index values of Chen's hyper sequences are used to scramble the DNA encoded odd matrix and similarly Index values Lorenz chaotic sequences are used to scramble the DNA encoded even matrix. Final step is to perform an add operation which can add two matrices to get the resultant encrypted matrix.DNA computing has many advantages, such as high speed, energy efficiency, and economical information storing.

C. Chaotic System

Chaos theory is a branch of mathematics and studies complex system. Chaotic based image encryption to provide secure image transfer. In the proposed work choose the Chen's chaotic mapping Lorenz chaos mapping and as a chaotic system. Chen's chaotic sequences are very complex in nature and also its very difficult to predict and analyze this sequences so these type of chaotic maps are suitable for generating random sequences in encryption processes. Chen's chaotic sequences described as following functions[8].

$$X_1 = a_1(y_0 - x_0) \quad (1)$$

$$Y_1 = x_0z_0 + d_0x_0 + c_2y_0 - q_0 \quad (2)$$

$$Z_1 = x_0y_0 - b_1z_0 \quad (3)$$

$$Q_1 = x_0 - k_1 \quad (4)$$

Where x_0 , y_0 , z_0 and q_0 are positional variable and a_1, b_1, c_1 and d_1 are control parameters. The value of k is in range from -0.7 to 0.7.

Like Chen's chaotic map, Lorenz chaos system are also very complex to predict and analyze. Since these type of systems are high dimensional chaotic map in which it is more unpredictable. This type of system provide high security for digital image encryption and transmission.

Lorenz chaotic sequences described as following functions[8].

$$K_1 = \sigma (L - k) \quad (5)$$

$$L_1 = rK - L - KM \quad (6)$$

$$M_1 = KL - BM \quad (7)$$

Where K, L and M are arbitrary parameters and σ=10, r=28, B=8/3 are positive constants.

D. DNA Encryption Algorithm

ISSN No:-2456-2165

DNA encryption algorithm can be summarized using following steps [8]:

Algorithm: DNA Encryption

Input **:** I(M,N)

Output: Encrypted I'(M,N)

Step 1: Start

Step 2 : Input image I(M,N) where M is the row size and N is the column size

Step 3: Input image is divided into odd pixels and even value pixels. The odd image is O(M,N) and even image is E(M,N)

Step 4: Binarize the odd value and even value pixels.

Step 5: Binary images are restored into DNA encoded odd and even matrices

Step 6: Generate Chaotic systems, Chen's hyper chaotic sequences A and B are sorted the generated values in increasing order as A_1 and B_1, Lorenz chaotic sequences AA and BB are sorted the generated values in increasing order as AA_1 and BB_1

Step 7: These index values of the sequences to scramble the pixels

of image.A_1 and B_1 used to scramble the pixels of O(M,N) and A_1 and B_1 used to scramble the pixels of E(M,N).

Step 8: Add the binary images O(M,N) and E(M,N)to obtain resultant image Z(M,N).

Step 9: The resultant image Z(M,N) transformed into encrypted image using DNA encoding. The encrypt image is I'(M,N)

Step 10: Stop

E. DNA Encryption Methodology

In this method first to generate odd pixel and even pixel images and these images transformed into binary images separately[8]. The DNA sequences A=[0 1], T=[1 0], G=[1 1] and C=[0 0] is applied for even image and A=[0 0],T=[1 1],G=[0 1] and C=[1 0] is applied for odd image. Finally DNA encoded matrix is obtained.

Different patterns of DNA coding are are shown in Table 1.

	1	2	3	4	5	6	7	8
A	00	00	01	01	10	10	11	11
T	11	11	10	10	01	01	00	00
G	01	10	00	11	00	11	01	10
C	10	01	11	00	11	00	10	01

Table 1. DNA Patterns

Next stage for an encryption to scramble the pixel position of DNA encoded matrix using sorted index value of generated chaotic sequence. Finally perform add operation to get an encrypted image. The Table 2. shows the results of ADD operation which is unique[8].

Add	T	A	C	G
T	C	G	T	A
A	G	C	A	T
C	T	A	C	G
G	A	T	G	C

Table 2. DNA Add Operation

The encrypted image can be decrypted using reverse process of encryption technique an d SUB operation shown in Table 3.[8].

Sub	T	A	C	G
T	C	G	T	A
A	A	C	G	T
C	T	A	C	G
G	G	T	A	G

Table 3. DNA Sub Operation

F. Data embedding

Data embedding is the process of hiding text data or any data in the target image. Figure shows the functional block diagram of data embedding process.

- *Reversible Data Hiding*

Reversible data hiding[9], or lossless data embedding, embeds invisible data into a digital image in a reversible fashion. There are many methods for reversible data hiding among this histogram based methods are more efficient. In the proposed system we have chosen histogram based method because it can enhance a visual quality. This techniques can be employed to recover the original image to their pristine form after the hidden data extracted.

- Histogram based data embedding

The input to this data embedding process is the encrypted image obtained after the DNA based chaos theory encryption. The first step of histogram based data embedding is to obtain the histogram of the encrypted image. After obtaining the histogram, highest two bins in the histogram are taken for data embedding, so histogram equalization can be perform by repeating this process. In order to embed the data we need to compare the encrypted image pixel value with the two peak bins of the histogram. If there is a match occurs, then that particular position can be used to embed the text data[10]. Before embedding a pre-processing is needed for the text data, in which the text data is to be converted into ASCII format followed by binary conversion.

Fig 4. shows RDH and Histogram Embedding process.

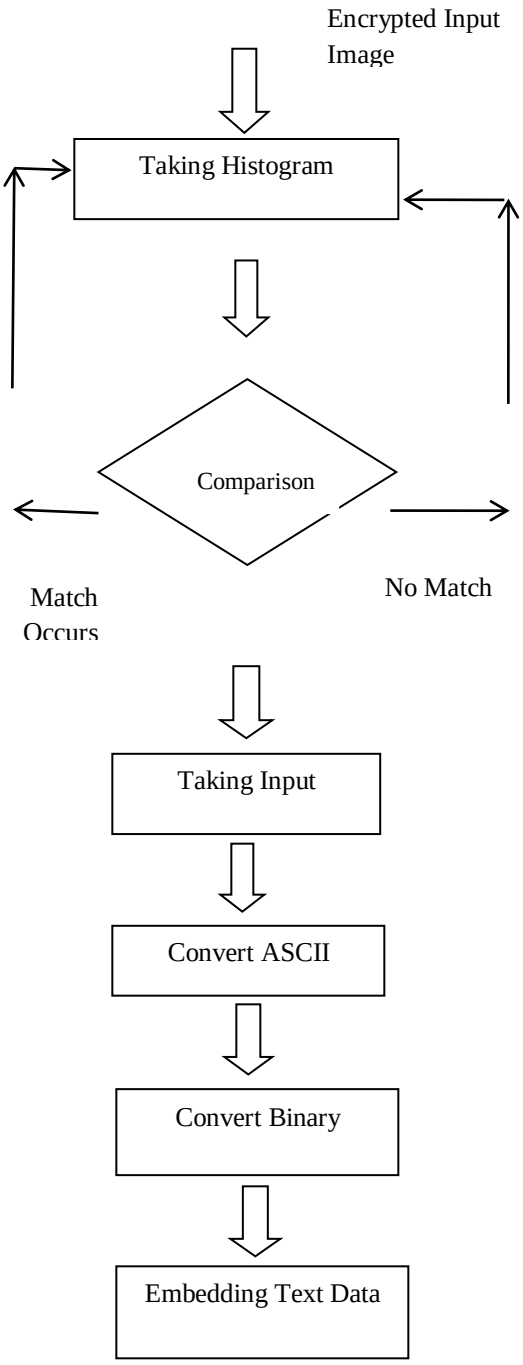

Fig 4:- RDH and Histogram Embedding process.

The data embedding performed using followed equations[10].

ISSN No:-2456-2165

$$i' = \begin{cases} i - 1, & \text{for } i < I_s \\ I_s - b_k, & \text{for } i = I_s \\ i & \text{for } I_s < i < I_R \\ I_R + b_k, & \text{for } i = I_R \\ i + 1, & \text{for } i > I_R \end{cases} \quad (8)$$

where i' is the modified pixel value, and b_k is the k-th message bit (0or 1) to be hidden. By applying Eq(8) to every counted in h_I, totally $h_I(I_s) + h_I(I_R)$ binary values are embedded.

G. Decryption

Decryption is generally reverse process of encryption. In the proposed methodology we need to decrypt the input image as well as the input text data. The higher peak value and lower peak value can be represented as I_s , I_r respectively. The peak values I_s and I_r are needed to extract the embedded text data. In simple we are performing the reverse operation of data embedding by histogram. Text decryption can be performed using following equations.

Text decryption can be performed using following equations[10].

$$b'_k = \begin{cases} 1, & \text{if } i' = I_s - 1 \\ 0, & \text{if } i' = I_s \\ 0, & \text{if } i' = I_R \\ 1, & \text{if } i' = I_R + 1 \end{cases} \quad (9)$$

Where b'_k is the k-th binary value extracted from the marked image I'. In a similar way we can perform the input image decryption from the encrypted image. The following equations can be used to perform the image decryption [10].

$$i = \begin{cases} \text{+1}, & \text{for } i' < I_s - 1 \\ & \text{for } i' = I_s - 1 \text{ or } i' = I_s \\ & \text{for } i' = I_R \text{ or } i' = I_R + 1 \\ i + 1, & \text{for } i' > I_R + 1 \end{cases} \quad (10)$$

IV. RESULT AND ANALYSIS

The proposed method is successfully implemented on the standard image data set. The standard input image lena.tif is shown in Fig 5. In our proposed encryption algorithm DNA map rule as specified in map rules Table 3.1. By using this map rule to get an DNA encoded even and odd matrix. To scramble the pixel position of both DNA encoded even and odd matrix by using generated sorted order of two chaotic sequence like chen's and lorenz sequence. Finally to attain Encrypted image using add operation of both encoded matrix. The ADD operation is specified in Table 3.2.

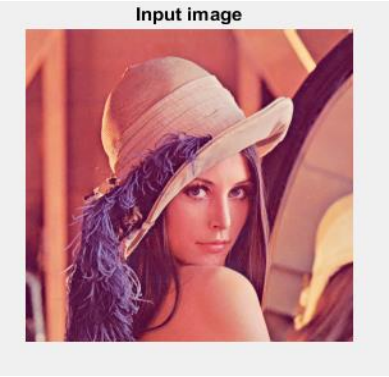

Fig 5:- Input Image

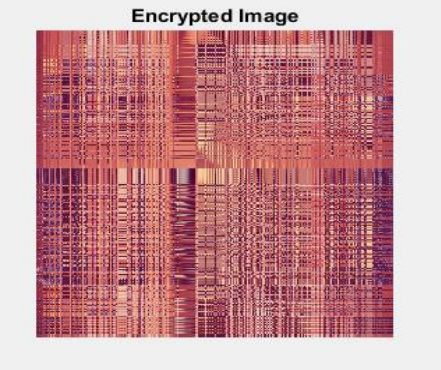

Fig 6:- Encrypted Image

For embedding process, First we have to take the histogram of image and After obtaining the histogram, highest two bins in the histogram are taken for data embedding, so histogram equalization can be perform by repeating this process. In order to embed the data we need to compare the image pixel value with the two peak bins of the histogram. If there is a match occurs, then that particular position can be used to embed the text data. Here after encryption process to get an encrypted image we need to embed the text data. Fig 6. shows entered text data to embedded in an image and also decrypt the text data.

ISSN No:-2456-2165

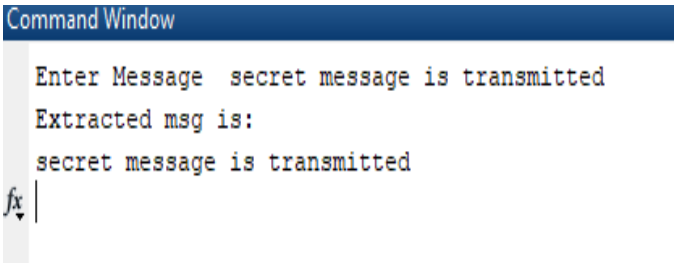

Fig 7:- Data to embedded and extracted

After extracting text data have to extracting input image also. Fig 8. extracted input image.

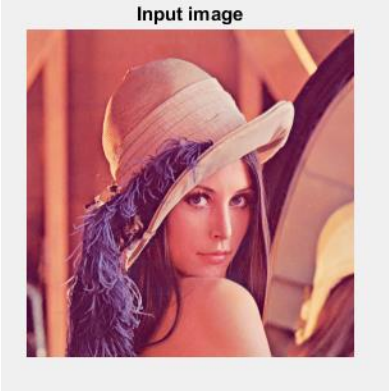

Fig 8:- Extracted input image

The performance analysis show that the proposed algorithm provides high security. The Fig 9. shows the histograms of the input image, Encrypted image and Decrypt input image respectively.

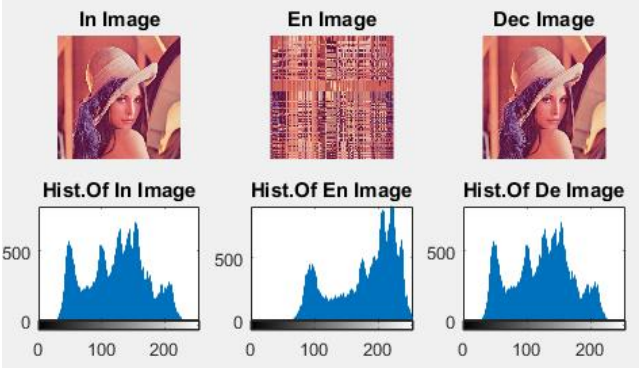

Fig 9:- Histogram Analysis

From the histogram analysis we can see that the output image having the same histogram of input image and histogram of encrypted image is changed.

V. CONCLUSION

In this work we introduce method for image encryption and data embedding. Both theoretical analysis and experimental results show that the proposed cryptosystem has high security. The DNA cryptography is used for encryption. Chaotic sequence are used to scramble the pixels position of DNA matrix and after add operation is used to get an encrypted matrix. For an embedding, the first step of histogram based data embedding is to obtain the histogram of the image. The repeating histogram equalization are used to embedded the data. The result analysis show that the DNA encryption scheme is effective, it has strong sensibility and high security. The chaotic sequence are enhance the encryption level.

REFERENCES

[1]. Qi Zhang and Qunding.(2014),"Digital Image Encryption Based On Advanced Encryption Standard(AES) Algorithm", Fifth International Conference on Instrumentation and Measurement, Computer, Communication and Control.

[2]. Ali E. Taki El_Deen and El-Sayed A. El-Badawy, Sameh N. Gobran, "Digital Image Encryption Based on RSA Algorithm", IOSR Journal of Electronics and Communication Engineering (IOSR-JECE),Volume 9, Issue 1, 2014.

[3]. Pia Singh and Karamjeet Singh, "Image Encryption and Decryption Using Blowfish Algorithm in MATLAB",International Journal of Scientific & Engineering Research, Volume 4, Issue 7, 2013.

[4]. Mohanjeet Kaur and Mamta Juneja, "A New LSB embedding for 24-bit pixel using MultiLayered Bitwise XOR", 2014.

[5]. Rajib Biswas, Sayantan Mukherjee and Samir Kumar Bandyopadhyay, "DCT Domain Encryption in LSB Steganography", 5th International Conference on Computational Intelligence and Communication Networks, Mathura, 2013.

[6]. AliAI-Haj, Noor Hussein and Gheith Abandah,"Combining Cryptography and Digital Watermarking for Secured Transmission of Medical Images",2nd International Conference on Information Management (ICIM), 2016.

[7]. Qian Wang, Qiang Zhang and Changjun Zhou,"A Multilevel Image Encryption Algorithm Based on Chaos and DNA Coding", Fourth international on conerance on Bio -Inspired Computing, 2009.

[8]. Prema T. Akkasaligar and Sumangala Biradar, "Secure Medical Image Encryption based on Intensity level using Chao's theory and DNA Cryptography", IEEE International Conference on Computational Intelligence and Computing Research, 2016.

[9]. Jun Tian, "Reversible Data Embedding Using a Difference Expansion",IEEE transactions on circuits and systems for video technology, vol. 13, 2003.

[10]. Hao-Tian Wu,, Jean-Luc Dugelay and Yun-Qing Shi, "Reversible Image Data Hiding with Contrast Enhancement", IEEE signal processing letters, vol. 22, 2015.