Improving Image Security using DES Encryption optimized with Huffman Coding in Steganography

Indu Maurya[a], S. K Gupta[b]

Research Scholar, CSE Deptt. B.I.E.T Jhansi[a]
A. P., CS&E Deptt., B.I.E.T Jhansi[b]
indumaurya42@gmail.com[a]
guptask_bi@rediffmail.com[b]

Abstract
The amazing development of internet advances and its applications require high state security of information during the hazardous correspondence on the network. For concealing information inside a cover image, image steganography method is used. The LSB based approach is the most well-known steganography method on account of its easiness and concealing capacity. All the image steganography method mostly centers on embedding procedure with less worried to the pre-processing, for example, encryption of secret image. The conventional algorithm does not give the pre-processing required to image-based steganography as they don't offer adaptability, robustness and high state of security. This work shows a remarkable method for image steganography in light of the Data Encryption Standard (DES) optimized with Huffman coding. DES utilizes 64-bit block size of plaintext and 56-bits of secret key and Huffman coding is utilized to diminish the number of bits per pixels required to represent it and furthermore decreases the transmission time for the transmission of images. The pre-processing give the high state of security as extraction of an image isn't conceivable without the learning of mapping standards of S – Box and the secret key of the function and furthermore the Huffman decoding rules. The proposed work is compared with the 20 implemented research models which are a combination of Chaos based Image Encryption and BTC (Bit truncating Compression) scheme in order to predict the percentage of improvement.

Keywords: Image Steganography, DES, Huffman Coding, Chaos Based Image Encryption, BTC scheme, Encoding, Decoding

1. Introduction

Steganography is the act of concealing private or delicate data inside something that seems, by all accounts, to be nothing out to the standard thing. Steganography is frequently mistaken for cryptology on the grounds that the two are comparative in the way that they both are utilized to ensure confidential data. The contrast between two is that steganography includes concealing data so it creates the impression that no data is covered up by any stretch of the imagination. In the event that a person or people see the object that the data is covered up within he or she will have no clue that there is any concealed data, thusly the individual won't endeavor to decode the data. What steganography basically does is exploit human recognition, human faculties are not prepared to search for records that have data within them, in spite of the fact that this product is accessible that can do what is called Steganography. The most well-known utilization of steganography is to conceal a document inside another record.

In this day and age, the correspondence is the fundamental need of each developing zone. Everybody needs the secrecy and safety of their imparting information. In our everyday life, we utilize numerous protected pathways like web or phone for exchanging and sharing data, yet it's not sheltered at a specific level. With a specific end goal to share the data in a disguised way two systems could be utilized. These components are cryptography and steganography. In cryptography, the message is altered in an encoded frame with the assistance of encryption key which is known to sender and receiver as it were. The message can't be gotten to by anybody without utilizing the encryption key. Be that as it may, the transmission of a scrambled message may effortlessly excite attacker's doubt, and the encoded message may hence be captured, assaulted or unscrambled brutally. To conquer the inadequacies of cryptographic methods, steganography strategies have been created. Steganography is the art of conveying such that it conceals the presence of the correspondence. Along these lines, steganography conceals the presence of information with the goal that nobody can distinguish its quality. In steganography, the way toward concealing data content inside any video and audio substance like the picture, sound, and the video is alludes as an "Installing". For expanding the secrecy of imparting information both the systems might be consolidated. Development of innovation and having quick Web make data to disperse over the world effectively and monetarily. This is made individuals to stress over their security and works. Steganography is a strategy that protects unapproved clients to approach the important information. The steganography and advanced watermarking give strategies that clients can conceal and mix their data inside

other data that make them hard to perceive by attackers. In the present data innovation period, the web has had a crucial impact on the correspondence and data sharing. Because of the fast advancement in Data Innovation and Correspondence and the Web, the security of the information and the data has to rise concerned. Consistently, secret information has been compromised and unapproved access of information has crossed the cut off points. Incredible measures ought to be taken to secure the information and data [1, 2]. Steganography joined with encryption will be a capable and effective device that gives an abnormal state of security [3].Steganography can be utilized as a part of a considerable measure of valuable applications. For instance, copyright control of materials, to upgrade the strength of an image web search tools and smart identity cards where the points of interest of people are implanted in their photos. Different applications incorporate video-sound synchronization, television broadcasting, TCP/IP packets where a one of a kind ID is installed in an image to investigate the system activity of specific clients. Steganography is the art and science of imperceptible correspondence. The word steganography is gotten from the Greek words "stegos" signifying "cover" and "grafia" signifying "writing" characterizing it as "secured composition". The presence of a message is secret. Steganography is typically executed computationally, where cover Works, for example, content records, pictures, sound documents, and video documents are changed such that a secret message can be inserted inside them. Keeping in mind the end goal to insert secret information into a cover message, the cover must contain an adequate measure of repetitive information or commotion. This is on account of in the inserting procedure Steganography really replaces this excess information with the secret message.

1.1. What is Steganography?

The word steganography is gotten from the Greek words "Stegos" which means cover and "Grafia" which means composing [1] characterizing it as secured composition. In image steganography, the data is concealed solely in images. Steganography is the art and science of secret correspondence. It is the act of encoding/implanting secret data in a way with the end goal that the presence of the data is undetectable. The first records can be alluded to as cover content, cover image, or cover audio. In the wake of embeddings the secret message it is alluded to as stego-medium. A stego-key is utilized for concealing/encoding procedure to limit identification or extraction of the installed information [2].

1.2. Steganography vs. Cryptography

Steganography Conceal the messages inside the Cover medium, numerous carrier file formats.

- Steganalysis means Breaking of steganography

Cryptography Encode the message before sending to the goal, no need of transporter/cover medium.

- Cryptanalysis means Breaking of cryptography

Cryptography is a technique for concealing data in a specific shape with the goal that exclusive the sender and authorized receiver can read and comprehend it. Steganography is the strategy for concealing data inside another non-secret report, picture, video, and so forth. In spite of the fact that postulations two terms appear to have a similar importance, they are really two unique ideas. Accordingly, we will examine the contrast amongst Cryptography and Steganography.

1.3 Overview

The word steganography originates from the Greek Steganos which signifies "secured" or "secret" and Grafia signifies "stating" or "drawing" i.e., Steganography implies truly "secured composition"[13]. Cryptography and steganography are generally utilized as a part of the field of information concealing away and has gotten critical consideration from both industry and the scholarly community in the current past. Previous hides the original information but latter conceals the very truth that information is covered up. Steganography gives an abnormal state of mystery and security by consolidating with cryptography. All through history, Steganography has been generally used to covertly convey data between individuals.

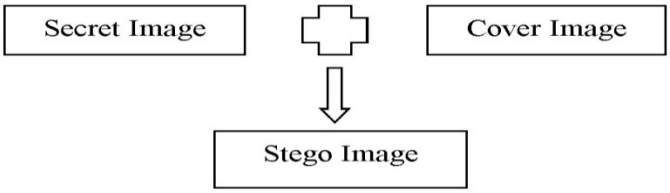


Figure 1: The Block Diagram of Steganographic system

2. RELATED WORKS

There are huge quantities of steganography installing strategies proposed in the writing. These strategies alter the cover image with various techniques. Be that as it may, the whole installing procedures share the generous objective of boosting the limit of the stego-channel [11]. In other words, the point is to implant at the most elevated conceivable rate while staying imperceptible to steganalysis attack. Spatial domain embedding procedure works on the central of tuning the parameter of the cover image (payload or aggravation) so the contrast between the cover image and the stego image is nearly nothing and indistinct to the human eyes. Steganography for the most part misuse human discernment since human faculties are not talented to search for the record that has concealed data inside them. Along these lines, steganography camouflages data from individuals endeavoring to hack them.

2.1. Peak Signal to Noise Ratio (PSNR)

PSNR can be defined as the measurement of the quality of the cover image and stego-image of sizes MxM (for 8-bit gray level) is calculated by using a following mathematical equation:

$$PSNR = 10 \times \log (255^2 / MSE)$$

dB is used to express the PSNR. PSNR represents the quality of image i.e. the higher the PSNR, lower in the difference between cover image and stego image and vice – versa.

2.2. Triangular Steganography

A few essential issues should be considered when contemplating Steganographic frameworks. They are Steganographic robustness, capacity, and security [2, 3]. The association between them can be communicated by the steganography triangle appeared in Figure 2. It speaks to adjust of the coveted attributes related with Steganographic technique. They are interdependent on each other and to enhance one component, either of different components should be sacrificed.

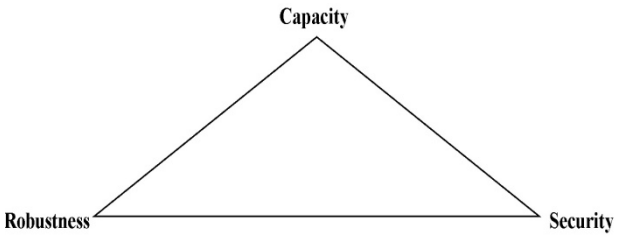


Figure 2: RCS Triangle(Robustness, Capacity, Security)

3. PROBLEM STATEMENT

The two main problems that arise in image encryption process are with respect to time it takes for its computation and its security level. For real- time image encryption, only those ciphers are preferable which takes the lesser amount of computational time without comprising security.

Many encryption methods have been proposed, and the most common way to protect large files is by using conventional encryption technique. Due to the complexity of their internal structure, some are not particularly fast in term of execution time. Critics believe that the most serious weakness of DES is in its key size (56 bits). The discussion shows that DES with a cipher key of 56 bits is not safe enough to be used comfortably.

4. OBJECTIVES

The main objectives to be achieved in this work are:

- To study various algorithms for data hiding and case study for the same.
- To design and implement DES (Data Encryption Standard) to get higher PSNR and more secure transmission.

- To evaluate results with previously designed algorithms to predict the percentage of improvement.

5. RESEARCH METHODOLY

(i) **Data Encryption Standard (DES)**: The Data Encryption Standard (DES) is a symmetric-key block cipher distributed by the National Institute of Standards and Technology (NIST). At the encryption site, DES takes a 64-bit plaintext and makes a 64-bit ciphertext; at the receiver site, DES takes a 64-bit ciphertext and makes a 64-bit block of plaintext. The same 56-bit cipher key is utilized for both encryption and decoding.

(ii) **Huffman coding scheme:** The Huffman coding plan furnishes a variable-length code with negligible average code-word length, i.e. slightest conceivable redundancy, for a discrete message source. (Here messages are grey values) Huffman coding utilizes a particular strategy for picking the representation for every image, bringing about a prefix code (at times called "without prefix codes", that is, the bit string speaking to some specific image is never a prefix of the bit string speaking to some other image). Huffman coding is such an across the board technique for making prefix codes that the expression "Huffman code" is generally utilized as an equivalent word for "prefix code" even when such a code isn't created by Huffman's algorithm.

In the paper Jeanne Chen[a], Wien Hong*[b], Tung-Shou Chen[a] and Chih-Wei Shiu[c], Steganography for BTC compressed images using no distortion technique, The Imaging Science Journal 2010 Vol 58.

They have only assumed the secret image as encrypted image. So I extend this approach to implement the detailed concept of DES.

Since DES is a symmetric encryption technique. So further we compare it with chaotic maps encryption methods.

6. Image Encryption using Chaos

One of the efficient and excellent encryption methods are Chaos-based Image Encryption. This is on the grounds that chaotic frameworks/maps have high affectability to their initial values and control parameters, chaotic property, non-convergence, and state ergodicity. Along these lines, numerous chaotic image encryption calculations have been created by specifically using existing chaotic frameworks/maps to their encryption processes [22, 23]. By and large, a chaos-based image encryption algorithm contains two bits: chaotic system and image encryption.
Chaotic systems/maps/frameworks in the image encryption algorithms can be divided into two categories: one-dimension (1D) and multi-dimension (MD). The MD chaotic maps have expanding operations in image security [24–26] because of their intricate structures and numerous parameters. However, numerous parameters expand the difficulty of their hardware/software executions and computation complexity [27]. On the other hand, 1D chaotic system has a basic structure and is anything but difficult to execute [27–31]. In any case, they likewise have three issues including:: (1) (1) the constrained or/and irregular range of chaotic behaviours [32,33]; (2) the vulnerability to low-computation-cost analysis using iteration and correlation functions [34]; and (3) the non-uniform information conveyance of output chaotic sequences. Thus, growing new chaotic systems with better disorderly execution are required.

6.1. Background

In the gathering of chaotic maps the 1D chaotic system/map has lots of utilization because of their simple/basic structures. In this section, we discussed the review of three 1D chaotic system/ maps: the Logistic Map, Tent Map and Sine Map. They will be utilized for our new chaotic Map.

6.1.1. Logistic map

One of the famous 1D chaotic map is the Logistic Map. The Logistic Map dynamical equation is simple but chaotic behavior is complex. Mathematically can be expressed in the following equation:

$$X_{n=1} = rX_n(1 - X_n)$$

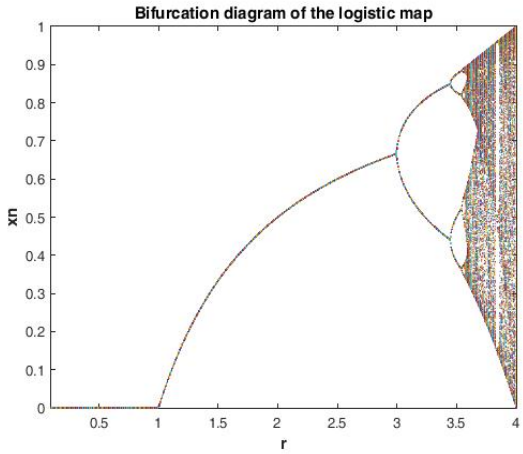


Fig. 7(a)

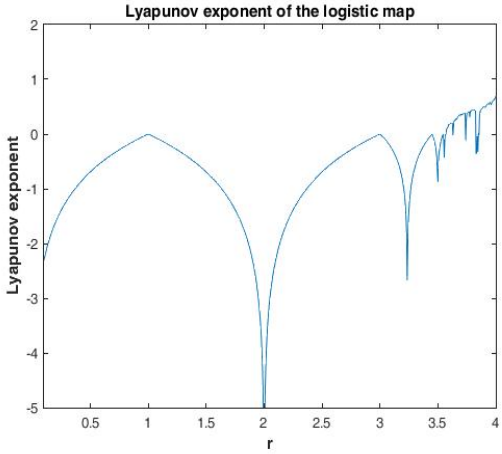


Fig. 7(b)

The Logistic Map bifurcation diagram and Lyapunov Exponent are presented in Figs. 7(a) and 7(b) to understand its chaotic behavior. In the bifurcation diagram shown in Fig. 7(a), a good chaotic behavior is shown by dotted lines and non-chaotic property is represented by the solid lines. Two major problems that exist in the Logistic map are: 1) chaotic range of logistic map is limited only within range [3.57, 4] and Even within this range, there exist some parameters which make the Logistic map with no chaotic behaviours and represented by the blank zone in its bifurcation diagram and plot of the Lyapunov Exponent represented in Fig. 7(b). For the Lyapunov Exponent, a good chaotic property of a chaotic map is shown by positive values. As shown in Fig. 7(b), the Lyapunov Exponents of the Logistic map are smaller than zero when parameter r<3.57. Second, the data range of the chaotic sequences is smaller than [0, 1] and showing the non-uniform distribution in the range of [0, 1]. These narrow down the applications of the Logistic map.

6.1.2. Tent map

The Tent map is known as a tent because of its tent-like shape in its bifurcation diagram. Mathematically can be expressed by the following equation:

$$X_{n+1} = \begin{cases} \dfrac{uX_n}{2} & X_i < 0.5 \\ \dfrac{u(1 - X_n)}{2} & X_i > 0.5 \end{cases}$$

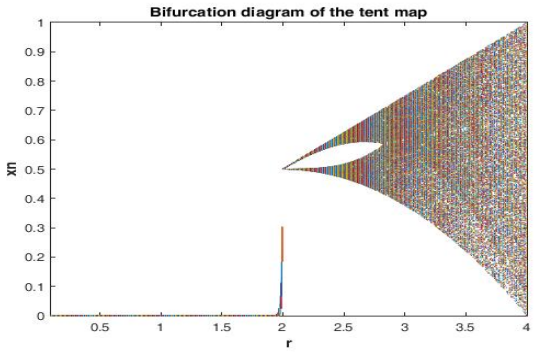


Fig. 7(c)

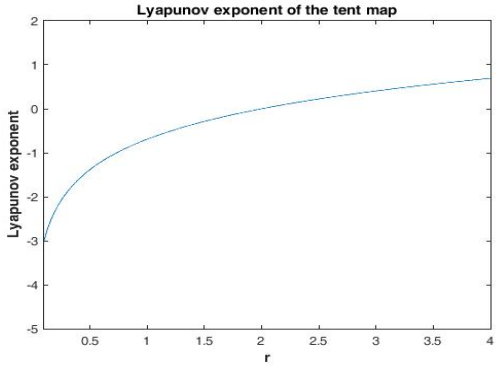


Fig. 7(d)

Bifurcation analysis represents its chaotic behavior in Fig. 7(c) and Lyapunov Exponent analysis represent its chaotic property in Fig. 7(d). Its chaotic range is [2, 4] proven by both analysis result. The same problem arises in Tent Map as the Logistic map: the chaotic range is limited and non-uniform distribution of the variant density function.

6.1.3. Sine Map

The chaotic behavior of Sine Map is similar as with the Logistic map. Mathematically can be expressed by the following equation:

$$X_{n+1} = a\ Sin\ (\Pi X_n)/4$$

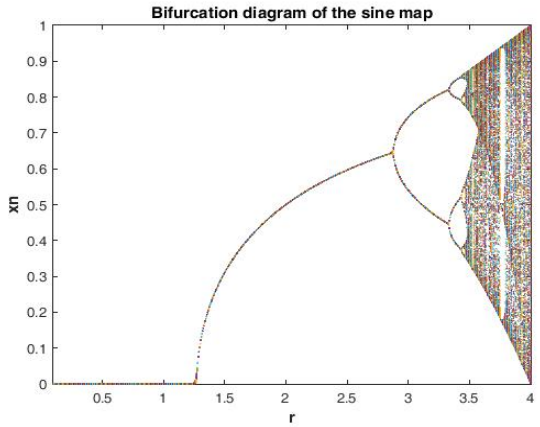


Fig. 7(e)

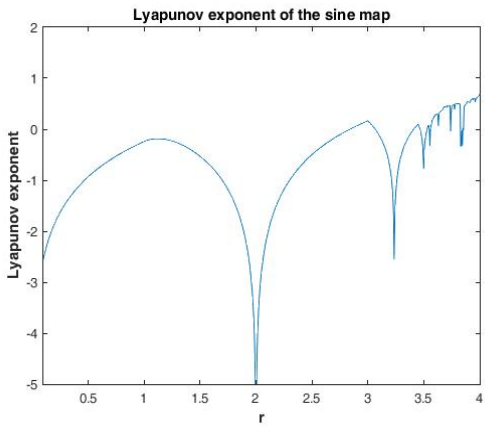


Fig. 7(f)

As shown in Figs. 7(e) and 7(f), its bifurcation diagram and Lyapunov Exponent of Sine Map are similar with bifurcation diagram and Lyapunov Exponent of the Logistic map in Figs. 7(e) and 7(f). Thus they have the same issues as discussed in Logistic Map.

7. Basic System Structure of Chaos-Based Image Encryption

Figure 8 shows the new chaotic system. It is a combination of two different 1D chaotic maps which is non-linear and considered as seed maps. Mathematically the chaotic system can be expressed by the following equation:

Where F (a, X_n) and G (b, X_n) represents two 1D chaotic maps (seed maps) with parameters a, b; mod: modulo operation, and n: the iteration number.

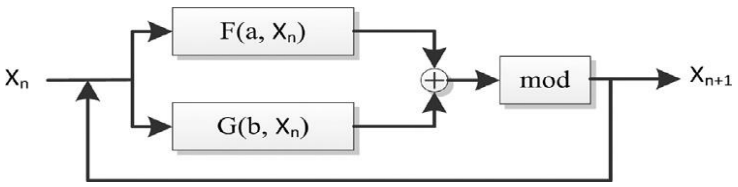


Figure 8: Chaotic system.

Since, there basic equations are different and the sensitivity of these maps are totally depends on Bifurcation diagrams and Lyapunov exponent.

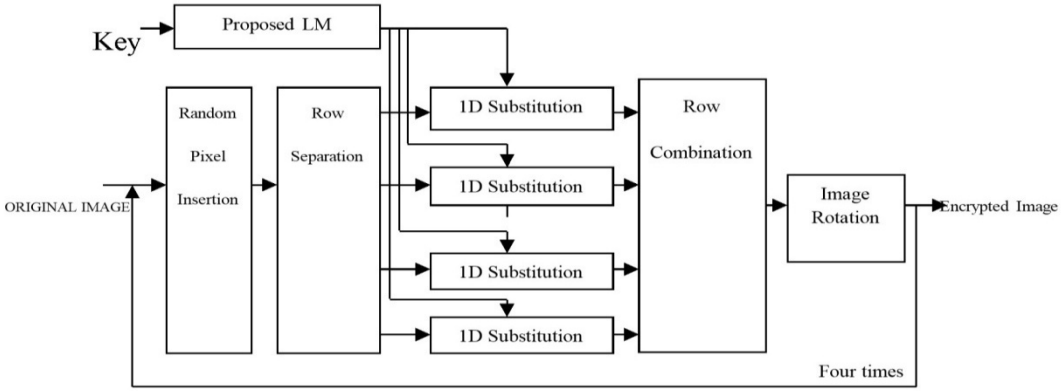
Since we started our work with Block Truncation Coding and combine these encryption methods along with steganography technique to evaluate the performance of implemented research models.

The implemented research models using BTC, Encryption methods and Steganography techniques are:

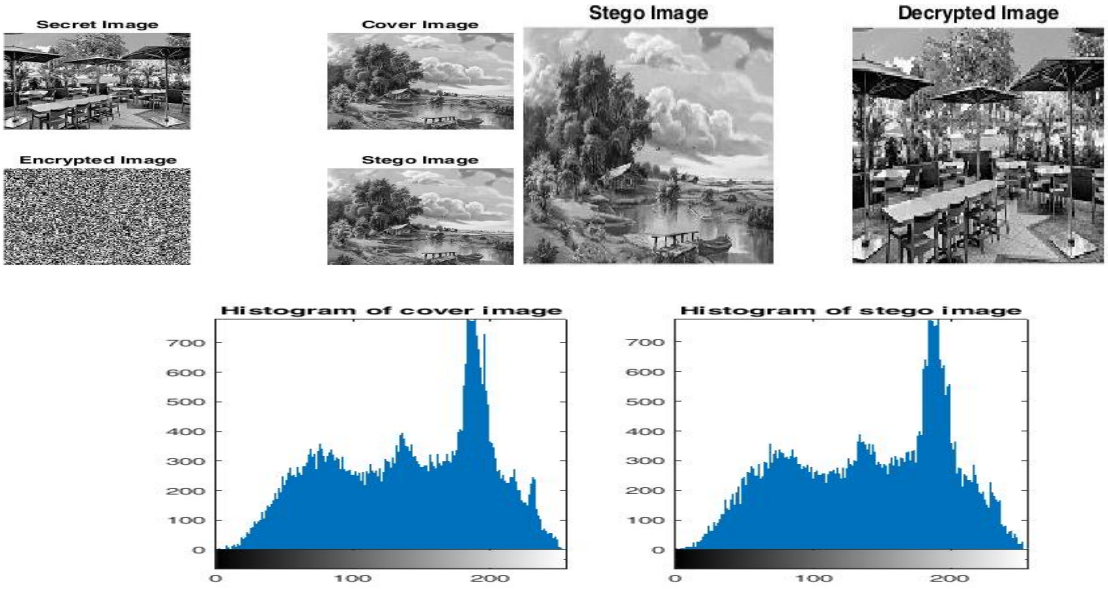
Logistic Map+ LSB
Tent Map+ LSB
Sine Map+ LSB
Logistic Map+ BTC+ LSB
Tent Map+ BTC+LSB
Sine Map+ BTC+LSB

Logistic Tent System+ BTC+LSB
Logistic Sine System+ BTC+LSB
Tent Sine System+ BTC+LSB

- **Logistic Map Encryption Technique**

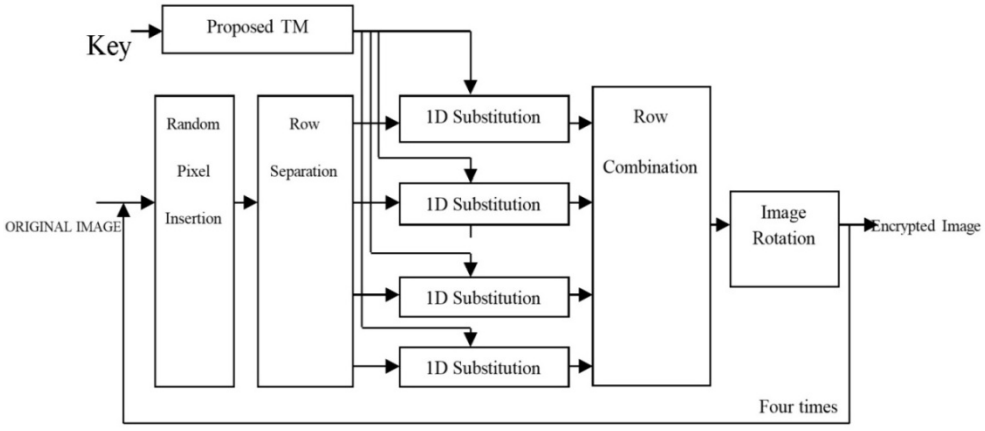


Logistic Map Encryption Technique + LSB

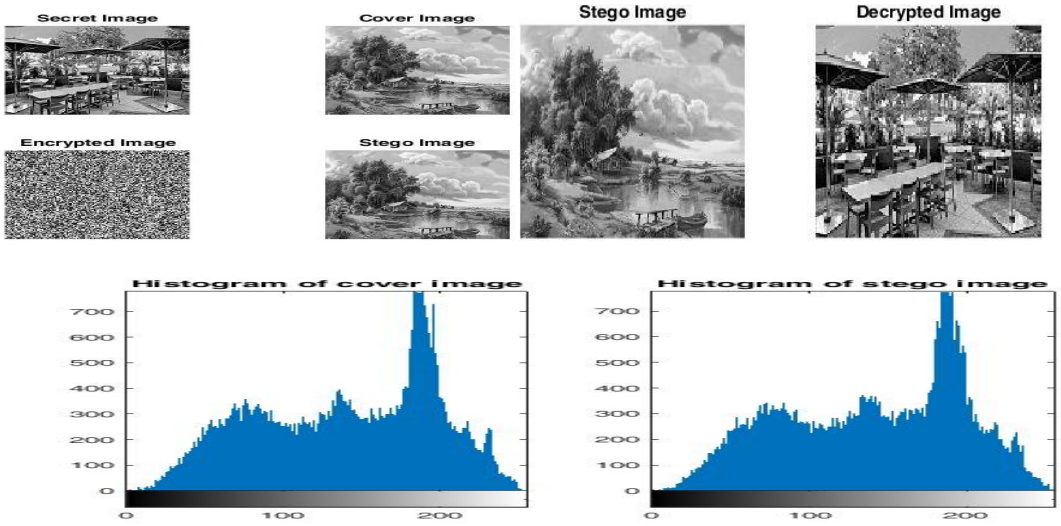


PSNR=44.02

- **Tent Map Encryption Technique**

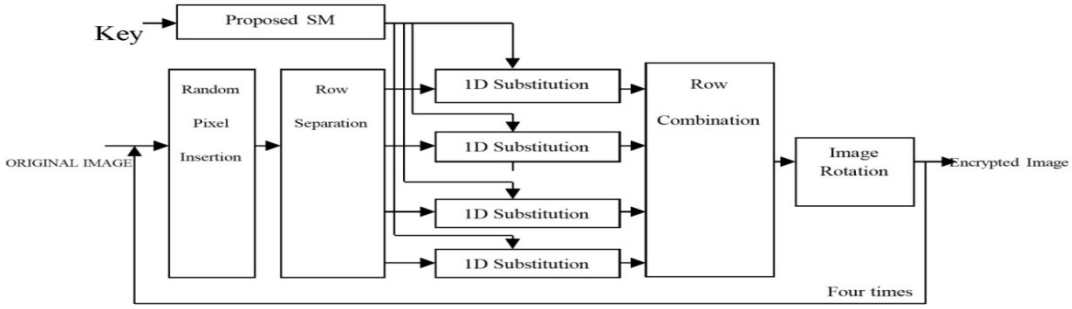


Tent Map Encryption Technique+ LSB

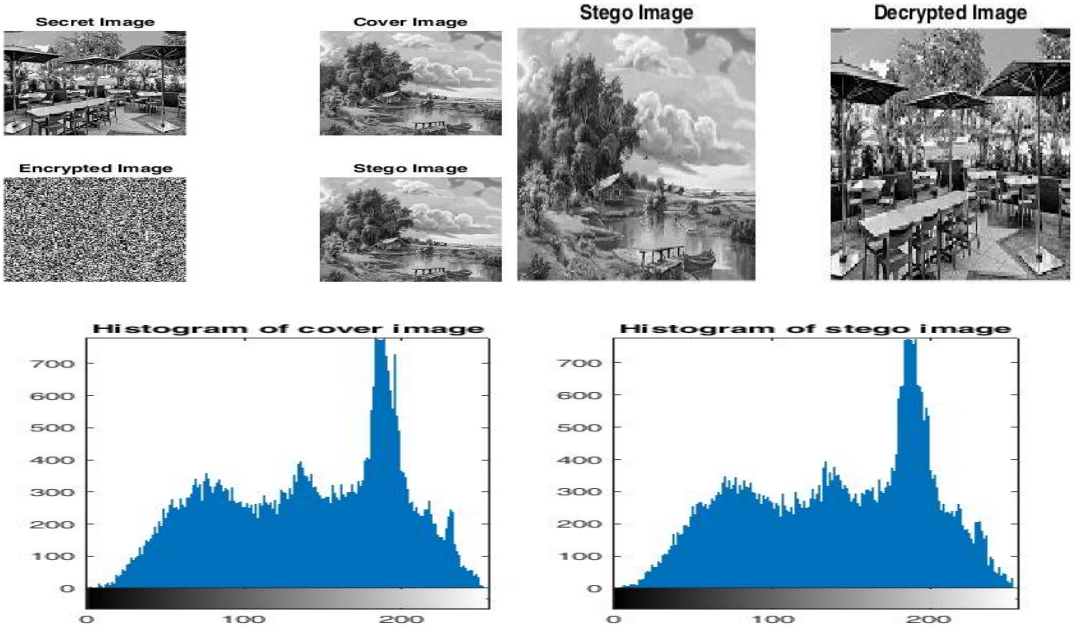


PSNR=44.10

- **Sine Map Encryption Technique**



Sine Map Encryption Technique+ LSB



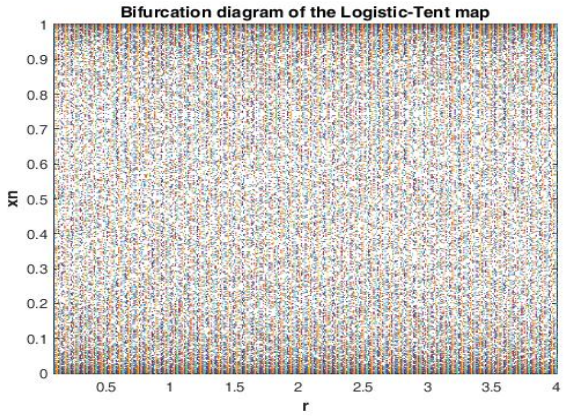
PSNR=44.06

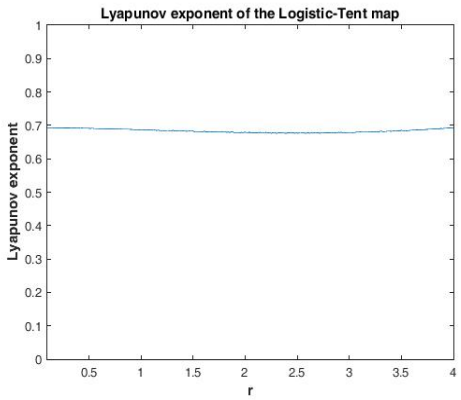
- **Logistic-Tent Encryption Technique**

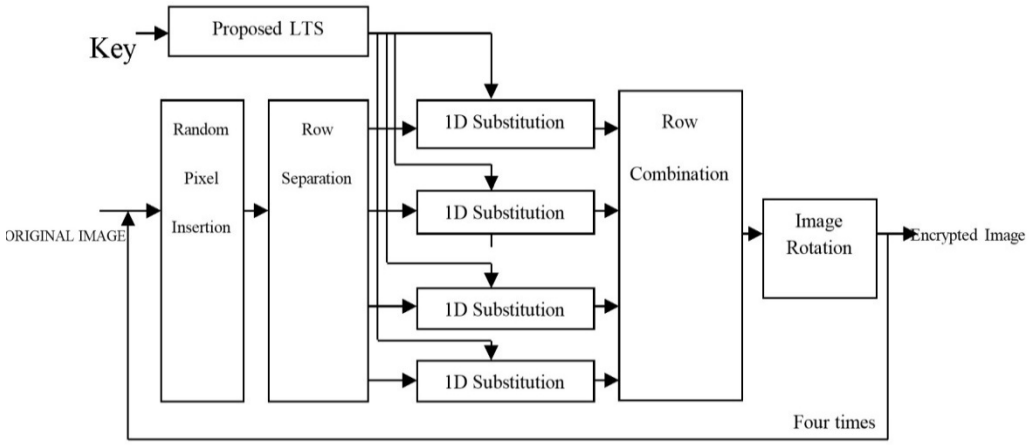
LTS mathematically can be expressed as follow:

$$X_{n+1} = (£(r, X_n) + \mathrm{r}((4 - r), X_n))mod1$$

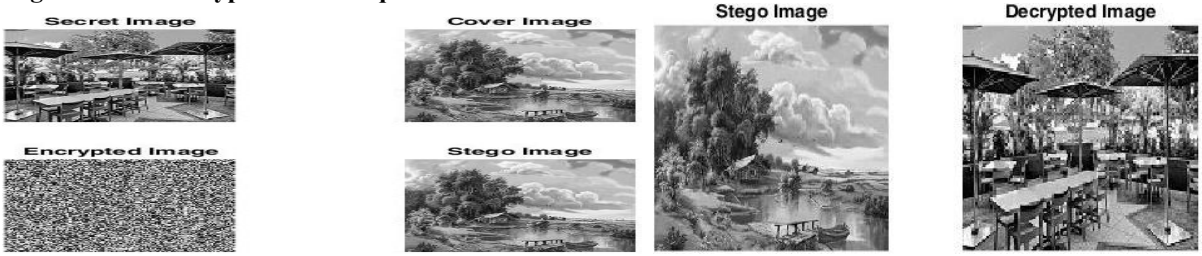
The bifurcation diagram of chaotic behavior and Lyapunov Exponent of the chaotic property of the LTS are represented in Fig 9(a) and 9(b), respectively.

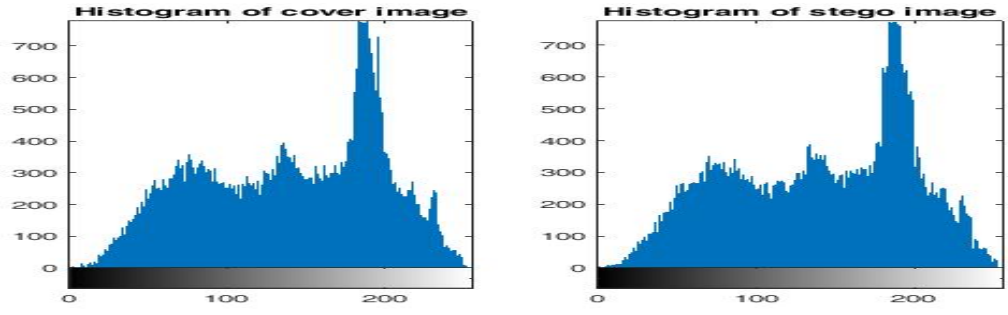






Logistic-Tent Encryption Technique+ BTC+ LSB





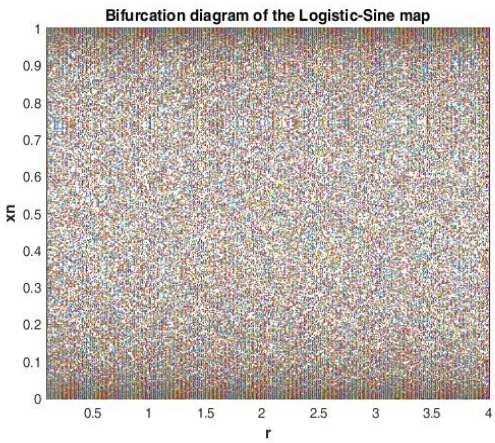
PSNR=45.50

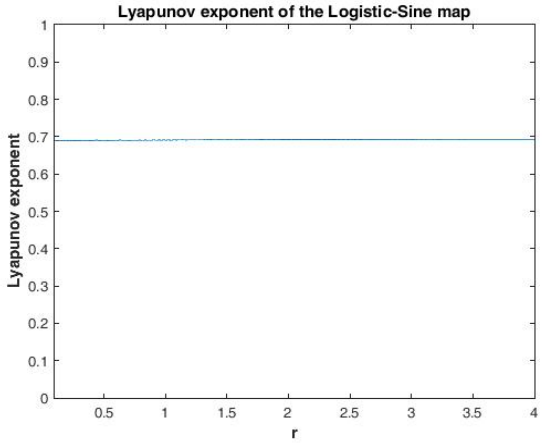
- **Logistic-Sine Encryption Technique**

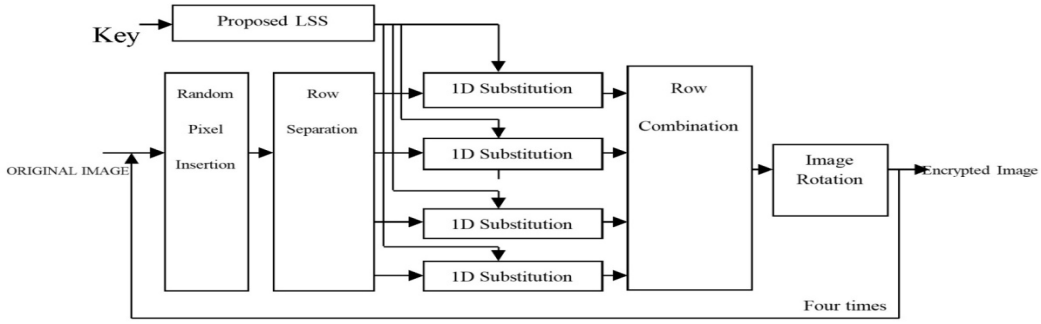
LSS mathematically can be defined as follow:

$$X_{n+1} = (rX_n(1 - X_n) + (4 - r)Sin(\Pi X_n)/4) mod 1$$

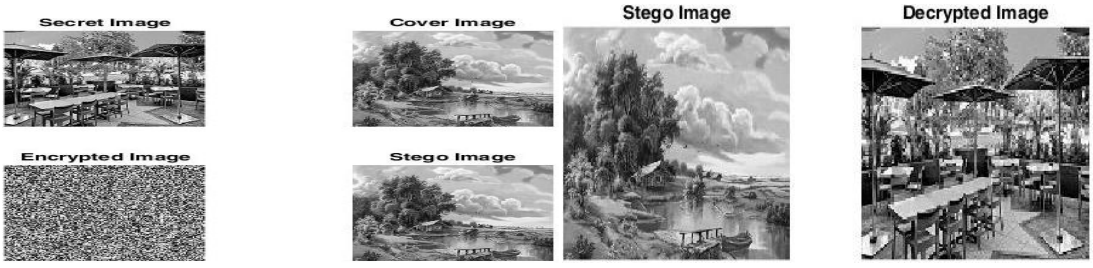
The bifurcation diagram of chaotic behavior and Lyapunov Exponent of chaotic property of the LSS are represented in Fig 9(c) and 9(d), respectively.

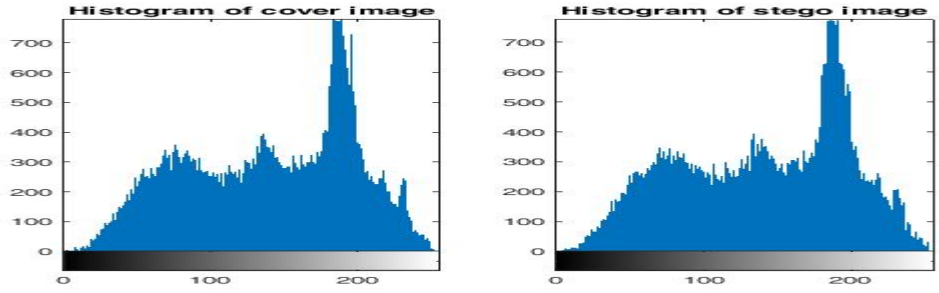






Logistic-Sine Encryption Technique+ BTC+ LSB





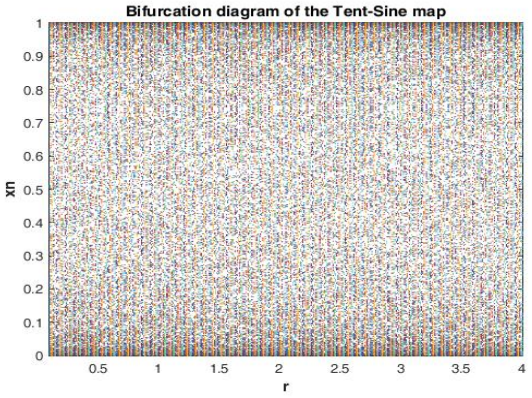
PSNR=45.21

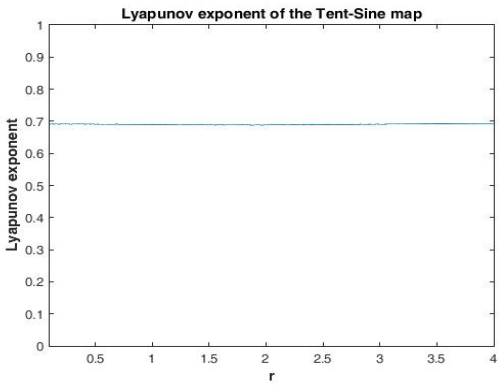
- **Tent-Sine Encryption Technique**

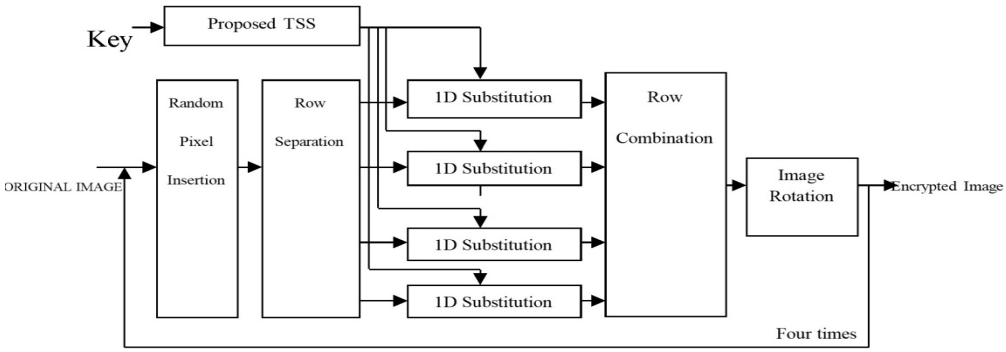
TSS mathematically can be expressed as follow:

$$X_{n+1} = (\mathrm{r}(r, X_n) + S((4-r), X_n))mod1$$

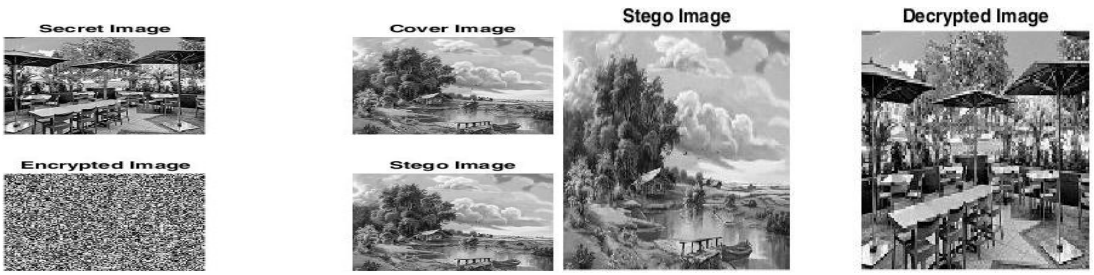
The bifurcation diagram of chaotic behavior and Lyapunov Exponent of chaotic property of the LTS are shown in Fig 9(e) and 9(f), respectively.

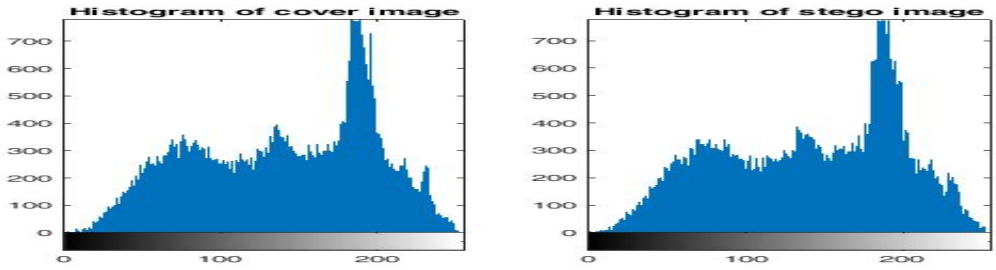






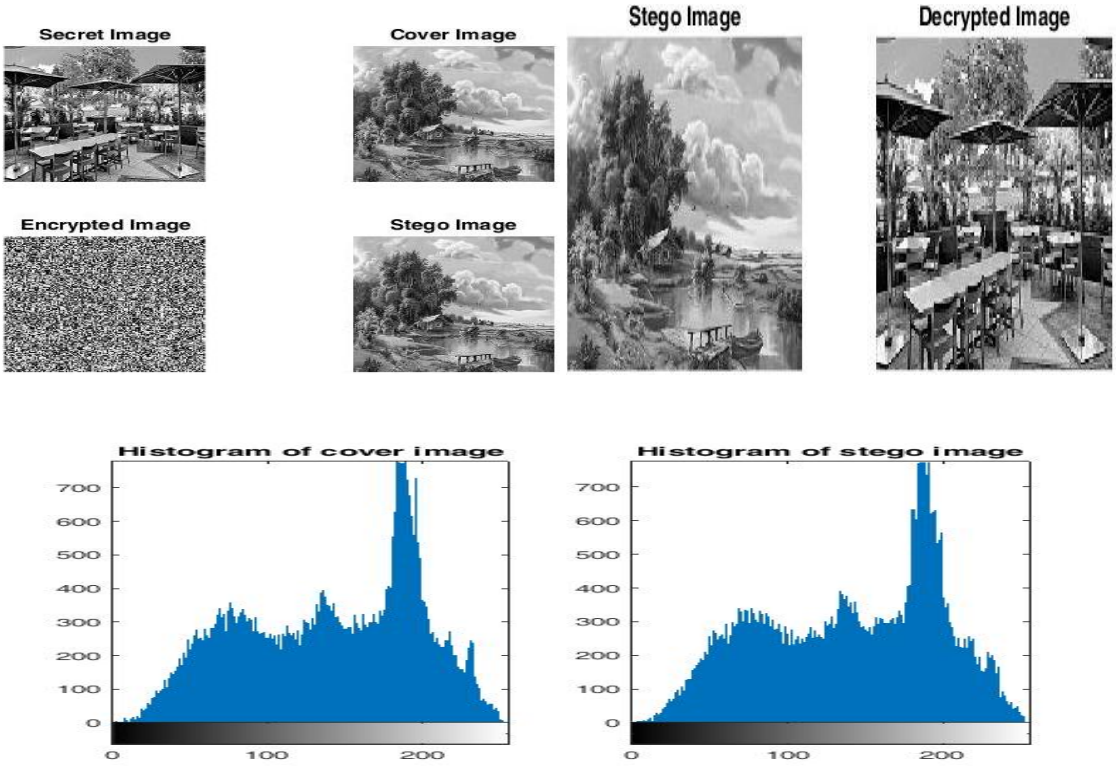
Tent-Sine Encryption Technique+ BTC+ LSB





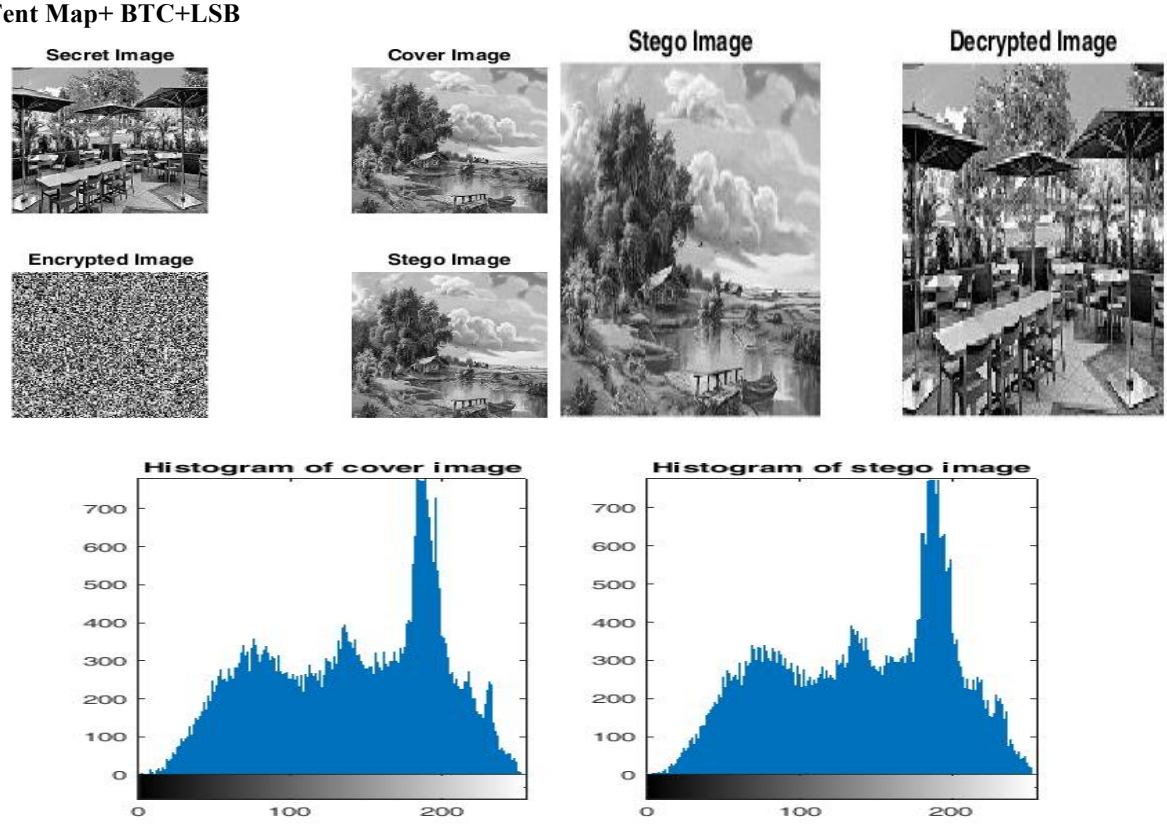
PSNR=45.13

Logistic Map+ BTC+ LSB



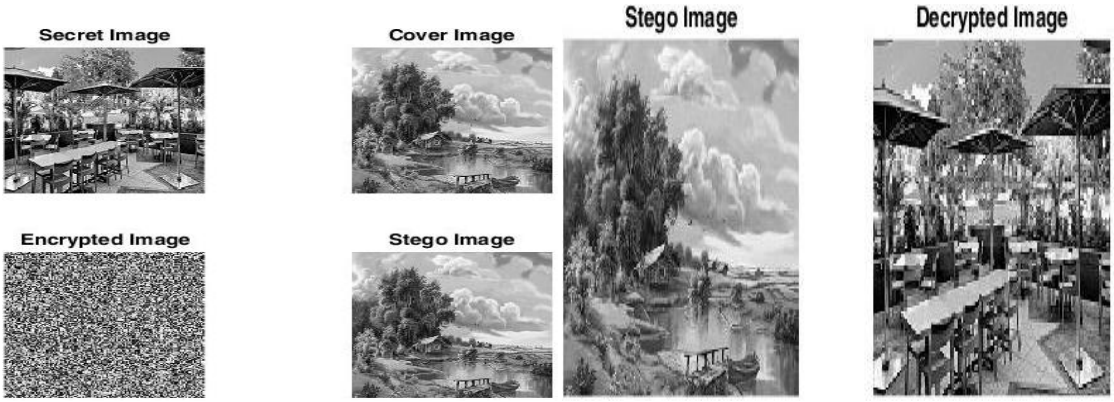
PSNR=44.95

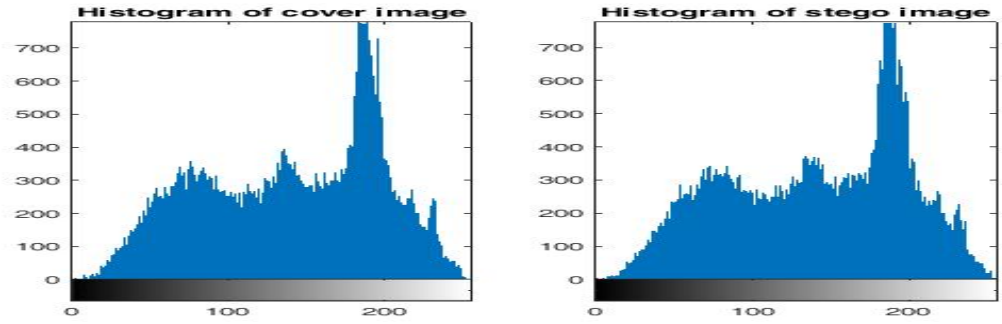
Tent Map+ BTC+LSB



PSNR=44.83

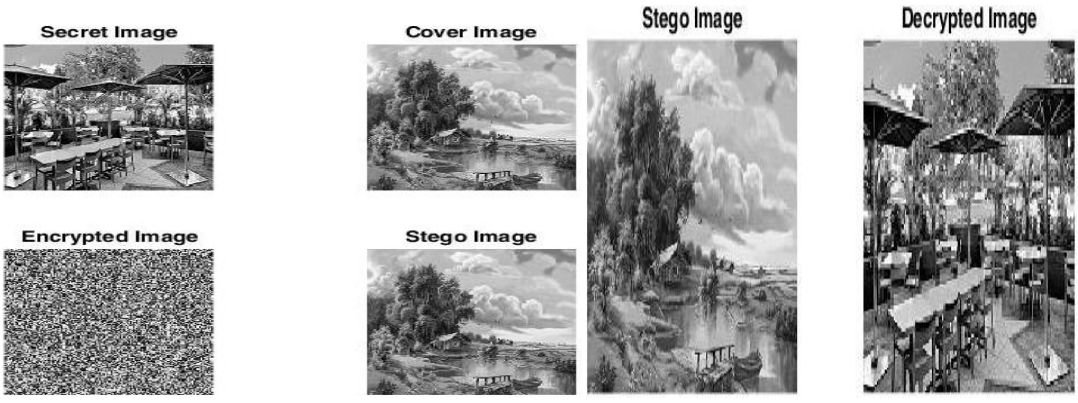
Sine Map+ BTC+LSB

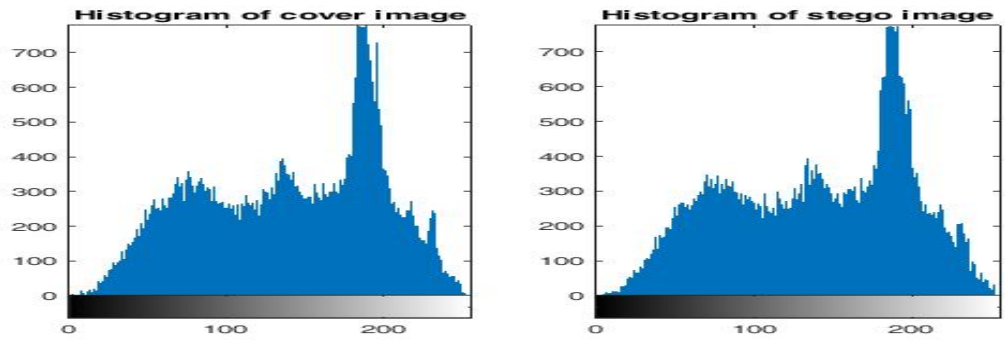




PSNR=45.37

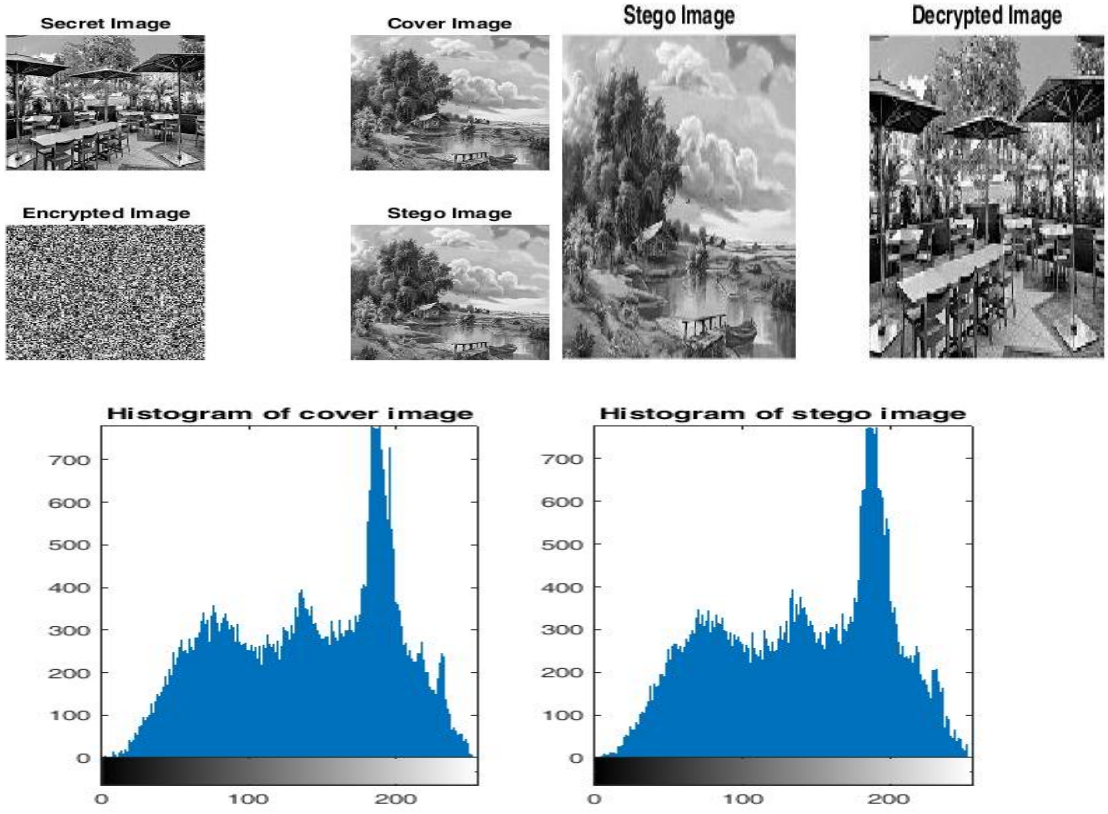
Logistic-Tent Map+ LSB





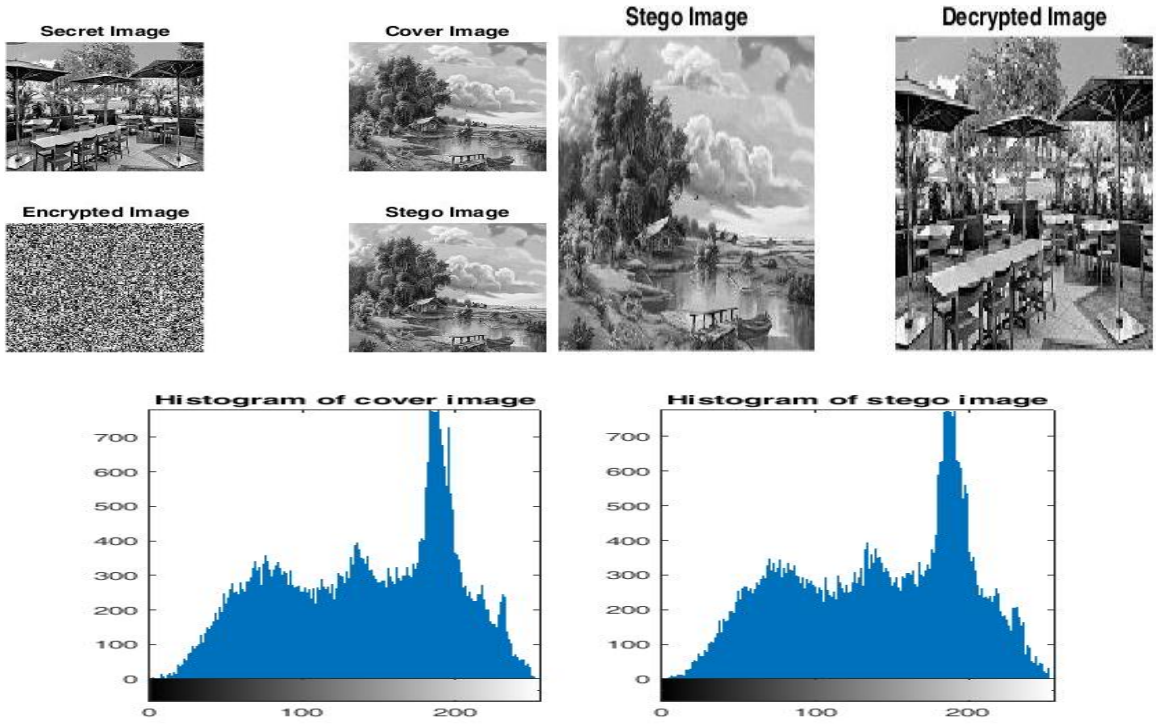
PSNR=44.12

Logistic-Sine Map+ LSB



PSNR=44.12

Tent-Sine Map+ LSB



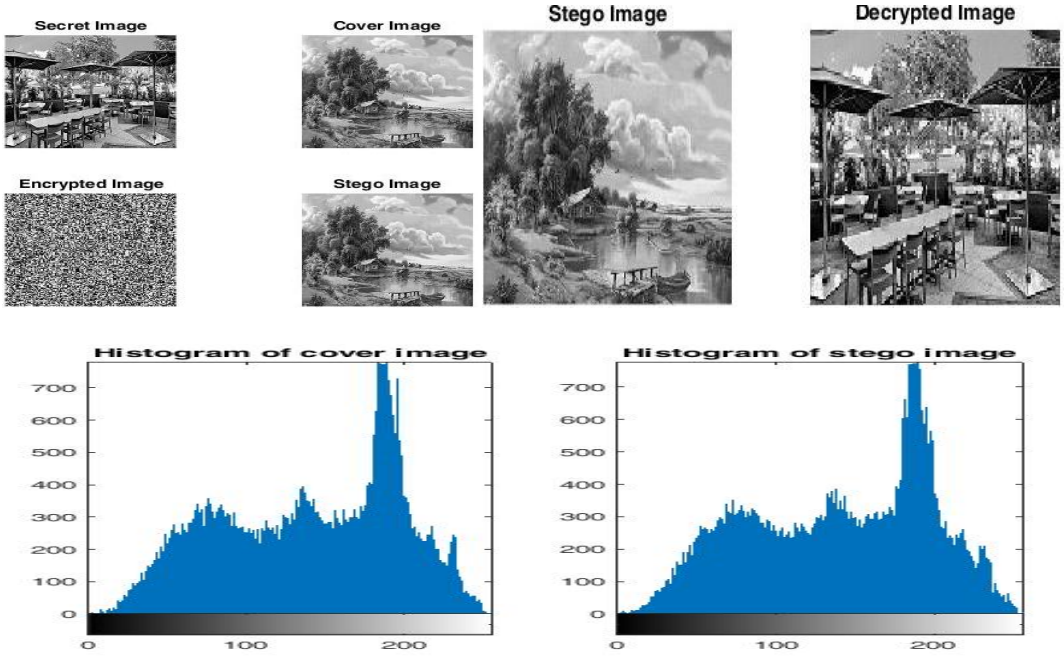
PSNR=44.14

Using Chaos based image encryption method we have seen that decryption will fail for a minute changes in the key as well as plaintext. Since our channel/data are prone to little amount of noise when transmitting through a channel. Even a very little addition of negligible amount of noise can leads to failure of decryption. For this reason we have used a DES method. It has no impact on addition of certain level of noise due to channel.

Now the implemented research models are:

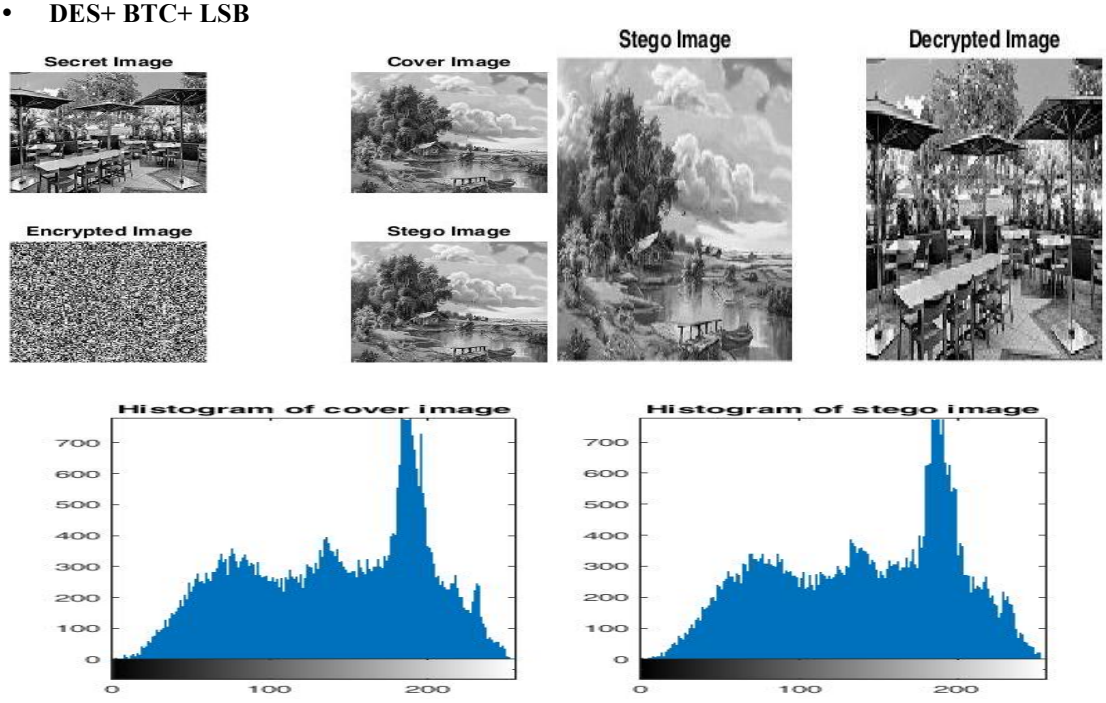
Data Encryption Standard (DES) + LSB
DES+ BTC+ LSB

- **DES+ LSB**



PSNR=44.16

- **DES+ BTC+ LSB**



PSNR=45.09

So If we compare DES+BTC+LSB to the Jeanne Chen[a], Wien Hong*[b], Tung-Shou Chen[a] and Chih-Wei Shiu[c], Steganography for BTC compressed images using no distortion technique, The Imaging Science Journal 2010 Vol 58. We have seen that the PSNR of implemented model (DES+BTC+LSB) is much higher than the previous paper.

Table 1: Comparison of PSNR

Jeanne Chen[a], Wien Hong*[b], Tung-Shou Chen[a] and Chih-Wei Shiu[c]	**DES+BTC+LSB**
PSNR(Different images)	**PSNR**
34.19	**45.09**
33.08	
29.62	
26.59	

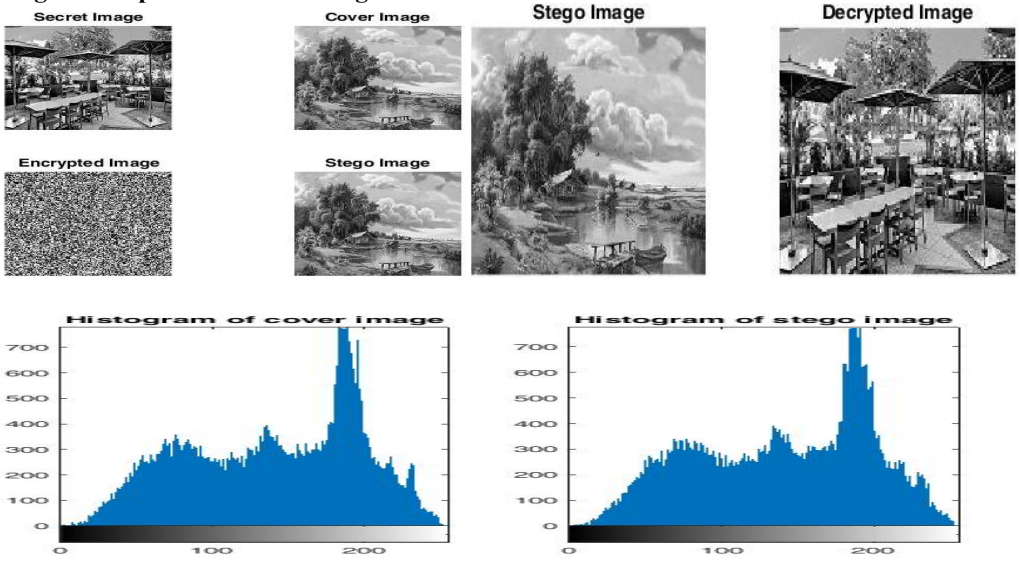
Again we started our research on other segment of this approach i.e. compression.BTC is a lossy compression technique and which is good if fine details from the image is not required. But we use steganography methods to share some highly secret and meaningful information. Therefore, information sharing without loss is much more important than channel constraints. In present condition, sufficient bandwidth is available around the globe with the invention of 3G, 4G, and 5G etc.

Huffman coding is a lossless compression approach. Therefore, we developed Huffman compression method and embed it in the model to conclude our work.

Now the implemented research models using Huffman coding along with encryption methods and steganography techniques are:

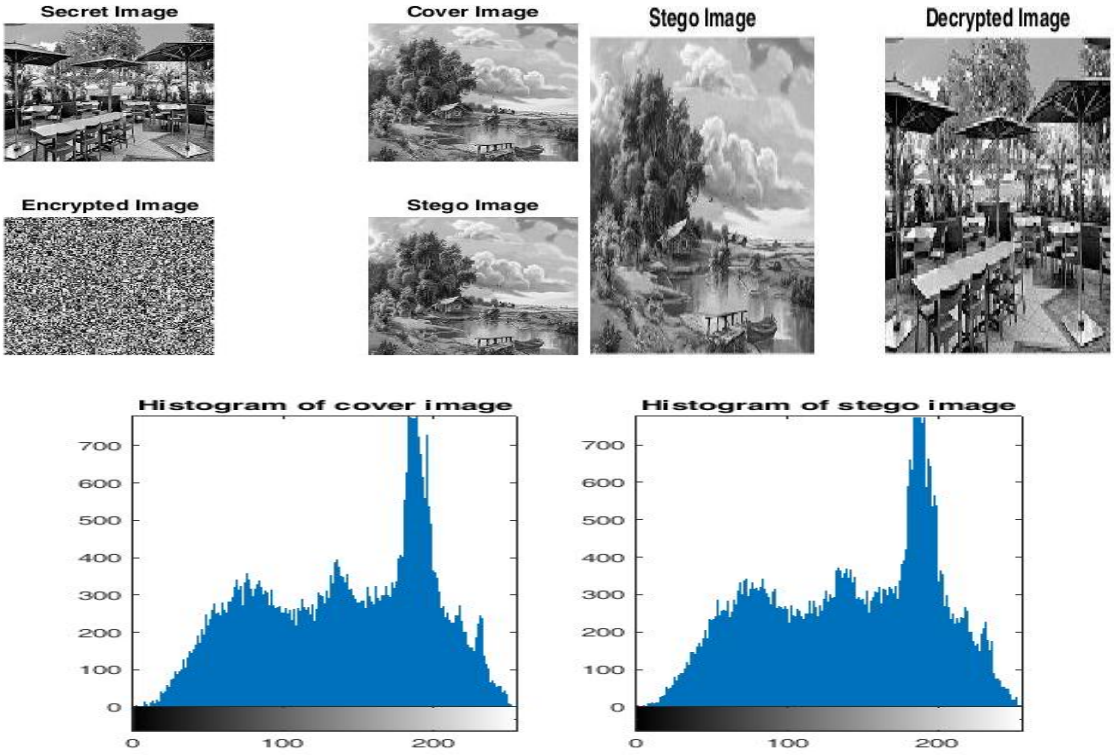
Logistic Map+ Huffman Coding+ LSB
Tent Map+ Huffman Coding+ LSB
Sine Map+ Huffman Coding+ LSB
Logistic Tent System+ Huffman Coding+ LSB
Logistic Sine System+ Huffman+ LSB
Tent Sine System+ Huffman Coding+ LSB
DES+ Huffman Coding+ LSB

- **Logistic Map+ Huffman Coding+ LSB**



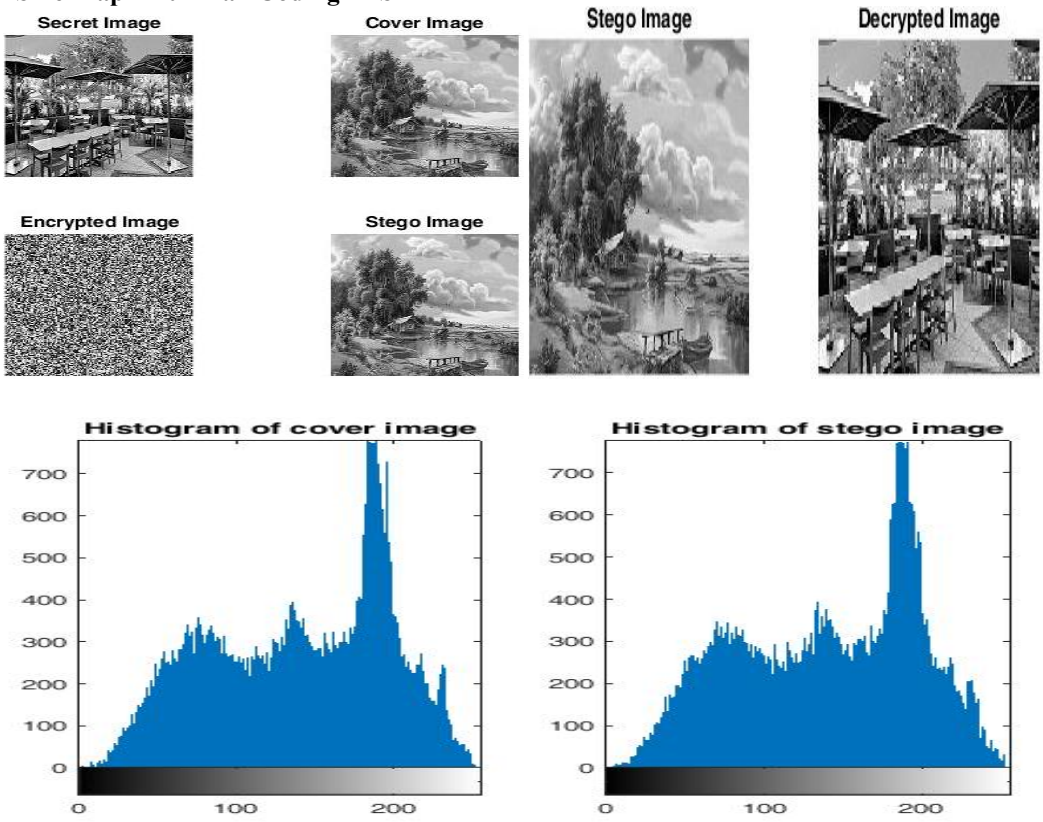
PSNR=46.28

- **Tent Map+ Huffman Coding+ LSB**



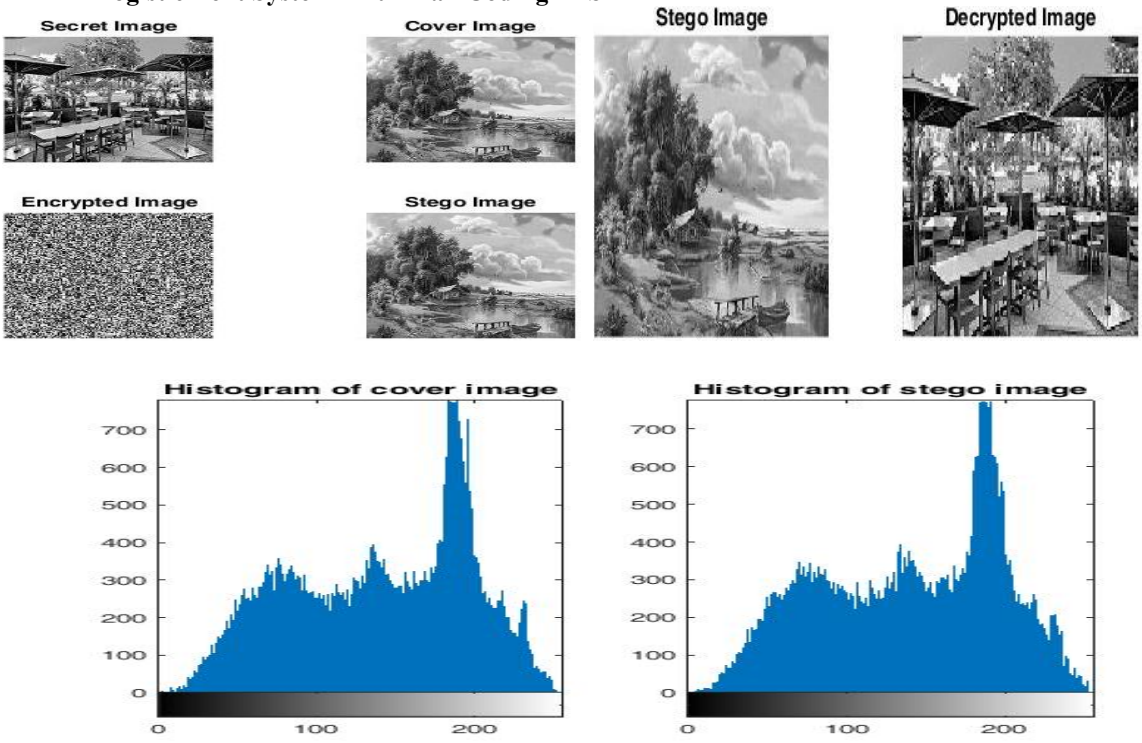
PSNR=45.20

- **Sine Map+ Huffman Coding+ LSB**



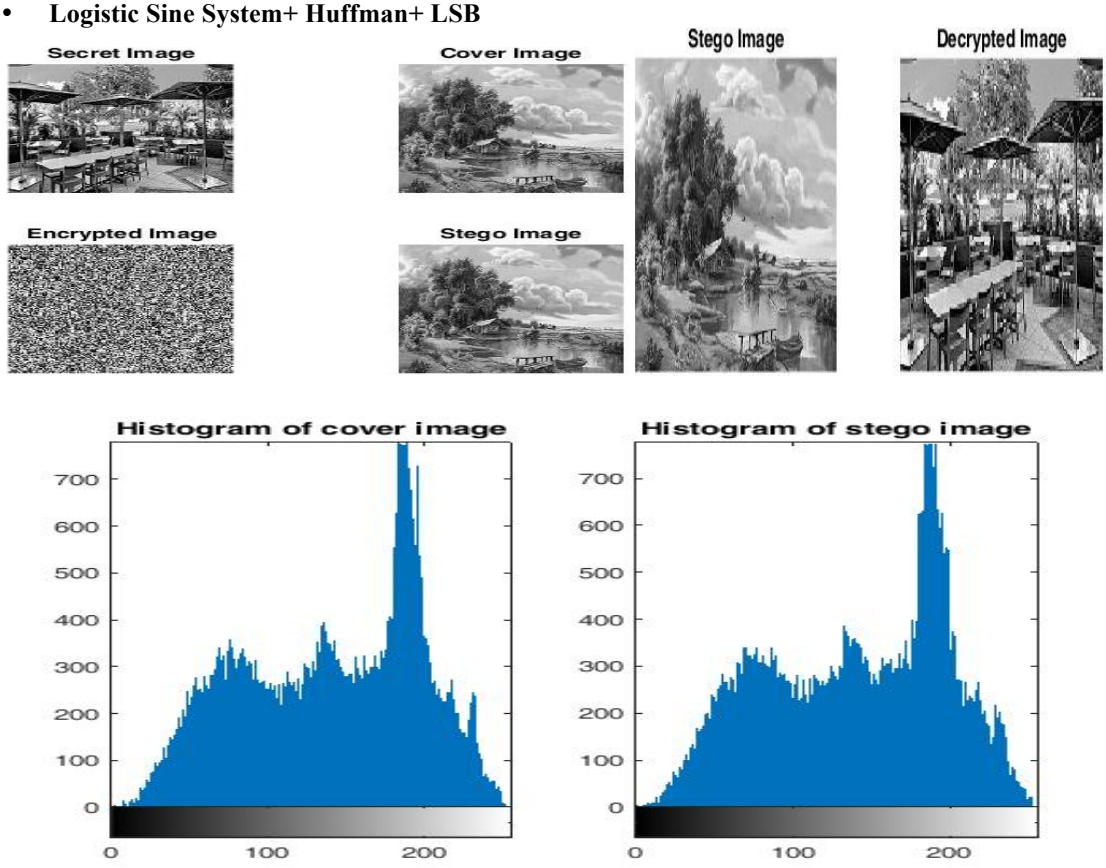
PSNR=46.01

- **Logistic Tent System+ Huffman Coding+ LSB**



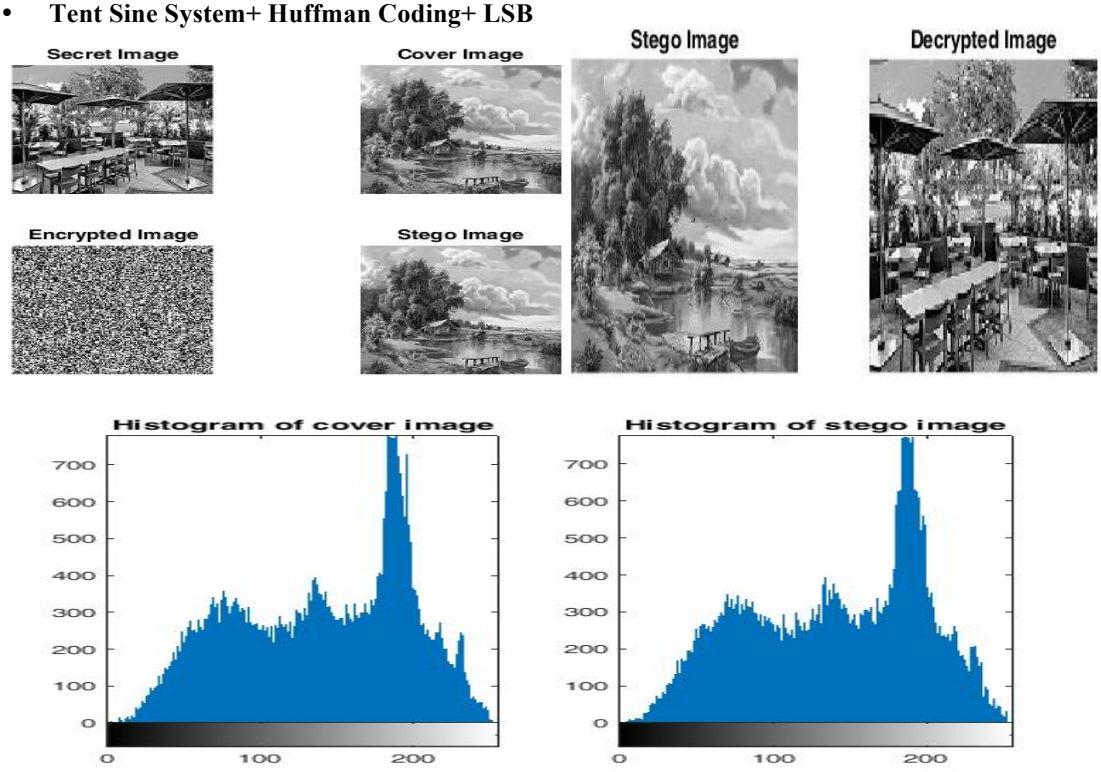
PSNR=46.03

- **Logistic Sine System+ Huffman+ LSB**



PSNR=45.62

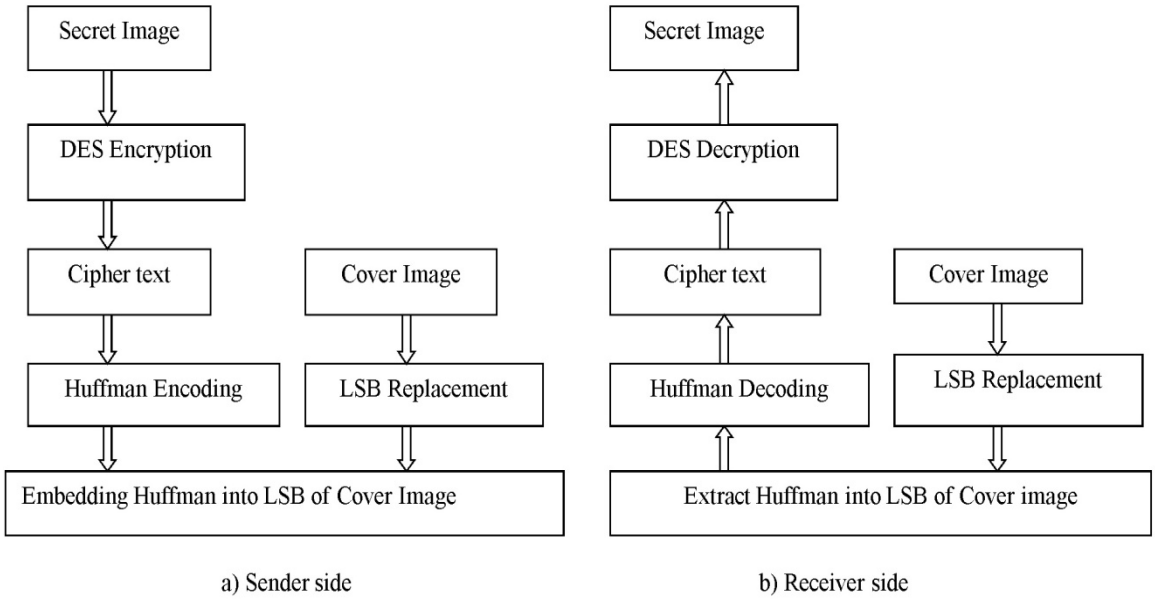
- **Tent Sine System+ Huffman Coding+ LSB**



PSNR=45.50

8. PROPOSED IMAGE STEGANOGRAPHY MODEL

Proposed steganography model is based on dual encoding using DES followed by Huffman coding. The DES encryption uses DES function comprising of permutation, substitution, S–Box mapping and secret key. The Huffman coding is done using probability density function of the histogram. The secret key is transmitted separately using different communication channel.



a) Sender side b) Receiver side

Figure 3: System Model

As per the requirement, we will take a secret image A and apply DES encryption on the image. Here we will get a 64*64 bit output = 4096 bits. These will be combined into pairs of 4 bits to give us a 16 grey level image of 16*16=256 pixels. This image still has the secret message. Now we can use the Probability density function of

the 16 grey levels to find the variable length code for the pixels in an image by creating a Huffman prefix dictionary. This '*MAY'* reduce the size of pixels to be embedded from 4 bits each to 2 bits or 3 bits depending on the frequency of their occurrence. And wherever the pixel with x intensity (0<=x<=15) exists, will be replaced by the Huffman code. The fundamental criticism about 56-bit DES encryption would be removed by this as the message cannot easily be decrypted without the correct Huffman Dictionary.
This will help us achieve our target to improve the security of DES algorithm. Other results may be that this reduces the size of the secret message and increase the embedding capacity. As Huffman is a variable length scheme, we cannot ascertain what will be the Average length of output. On the decoding end, the image LSB bits will be followed by reverse Huffman, which will provide us the ciphered message that can be passed through DES decryption and the secret image is regained.

By combining both these techniques the spatial real estate could thus be used more effectively.

8.1. Embedding procedure of an Image

Encoding Function: First take the secret image of size (e.g. of 64×64). Now convert each pixel intensity value of the secret image from decimal to binary. From the secret image, we have to take eight consecutive pixel values in order to form one block of 64 bits. Applying DES encoding function to this block:

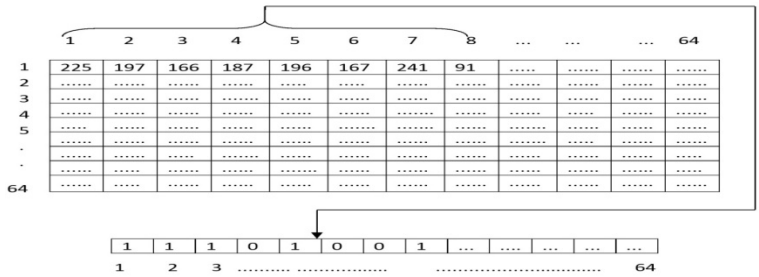


Figure 4: Block of 64 bits

1) **Initial / Inverse Initial permutation:** The 64 – bit takes as an input and this 64-bit passes through an IP here the bits are rearranged it will follow by a phase consisting of 16 rounds of the same function (f_k) to produce the 64-bit as a permutated output. The output of the 16th round will now pass through the inverse initial permutation by which the bits are restored to the original image.

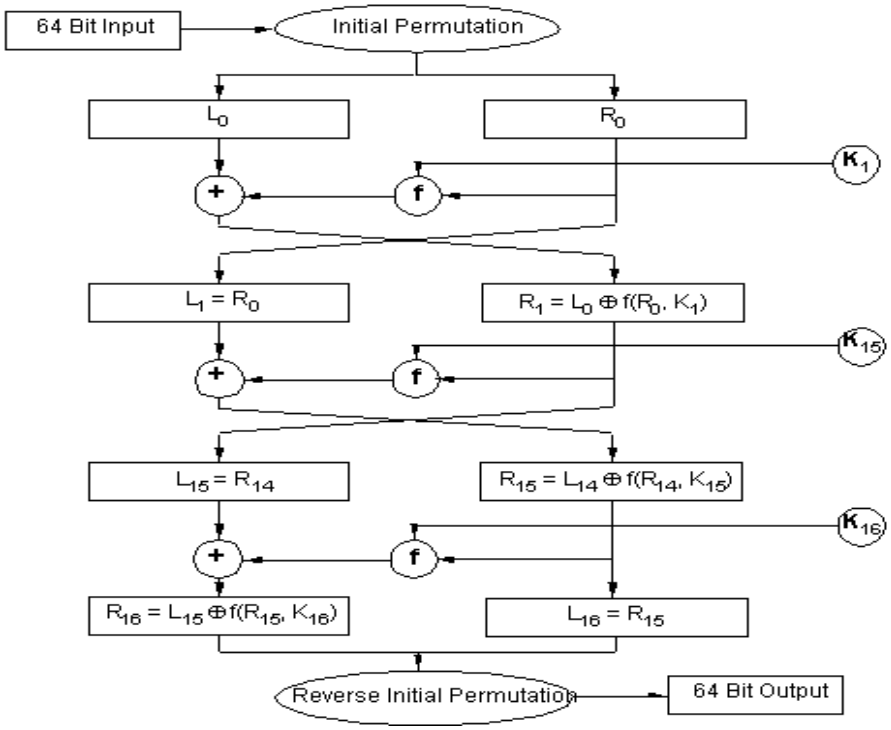


Figure 5: Encoding Function (DES) Detail

2) The function *f*: The function *f* is the most complex component of DES which includes both permutation and substitution functions. The function can be defined as follow:

$L_i = R_{i-1}$,
$R_i = L_{i-1}$ $F(R_{i-1}, K_i)$

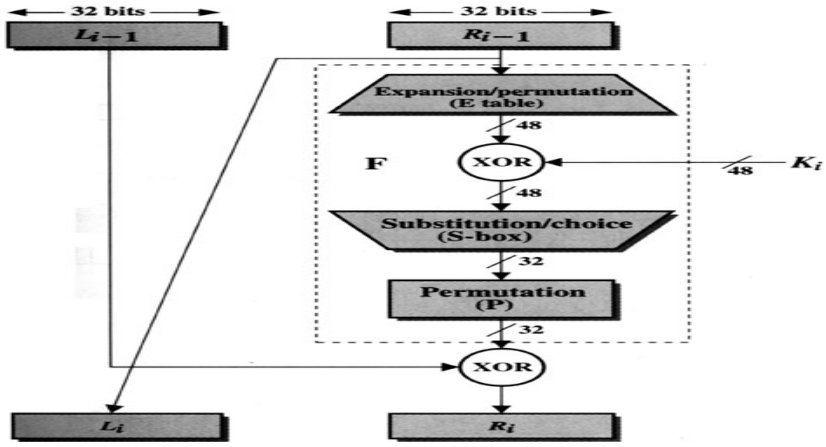


Figure 6: Single Round Detail

Here L and R are defined as the leftmost 32- bit and rightmost 32-bit of the 64 - bit first block of the eight consecutive pixels of the secret image. The R input is first expanded from 32-bit to 48-bit by using an expansion/permutation (E table) that involves duplication of 16 of the R bits. This 48-bit input is XORed with key K_i. This 48-bits result passes through an S-Box produce a 32 – bit output, which is again permuted to produce 32 – bit.

3) S- Box: The S-Box consists of a set of 8 Substitution-Boxes, which accepts six bits as an input and generates four bit as an output. First and last bits of input to box Si form a two-bit binary number to select one of four substitutions defined by four row in the table for Si. The middle 4-bits select from 4*16 definition table of Substitution boxes. The Substitution-Box definition table includes only a decimal value from 0 to 15 hence binary output of S-Box operation contain only 4 bit.

	0	*1*	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	*15*
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

Figure 7: S- Box Detail

Single Round Detail: For example, in S1 for input 101011, the row is 11 (row 3) and the column is 0101 (column 5).The value in row 3, column 5 is 9, so the output is 1001.The 32-bit output from the eight S boxes is then permuted and XOR with leftmost (L) 32bits is now input as 32-bits R for next round. One complete execution of DES gives eight-pixel value of secrete image into respective pixel values of an encrypted secret image.

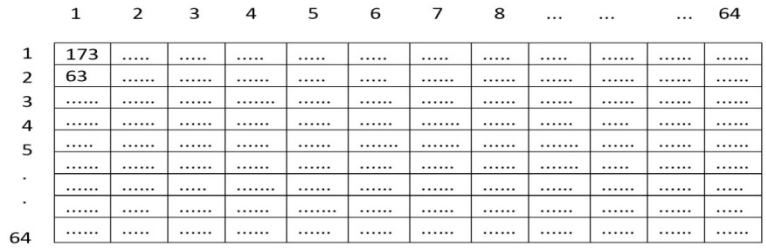


Figure 8: Encrypted secret image

4) Huffman Dictionary: make 2 bit pairs of pixels. Example (173)10 = (10101101)2 can be divided into 4 pairs {10}, {10}, {11}, {01} and find the probability density. Here probability occurrence of {10} (decimal value 2) is 2/4=0.5. PDF of {11} (decimal value 3) is 1/4=.25. PDF of {01} (decimal value 1) is 1/4=.25. Thus following is the dictionary:

10 are coded as 1.
11 are coded as 01.
01 is coded as 00.

Thus the output of (10101101) is coded as (110100) hence size of secret image is reduced. The compression ratio is 6/8.

5) Bit Division: Taking the Huffman output for the complete image, the values are embedded into 2 least significant bits of the cover image. After bit division we get value of b1 = 11, b2 = 01, b3 =00 and so on.

6) Insertion of Bit into the cover image: After receiving values of b1, b2, b3, these values are inserted into the cover image. These values are placed into the 2 bit LSB of the four consecutive pixels in the cover image. Taking the pixels one by one from the cover image, the 2 LSB bits are replaced by 11, 01 and 00 respectively.

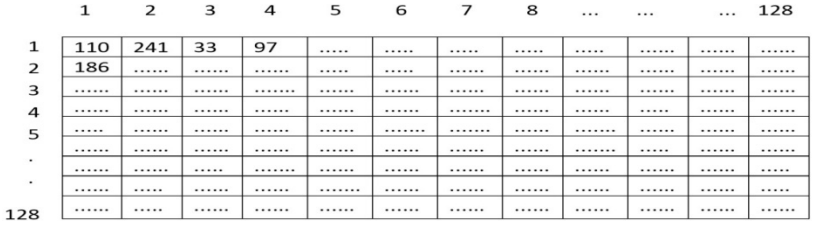


Figure 9: 128 bit cover image and perform LSB replacement

7) Formation of Stego-Image: The stego-image is formed after getting the new pixel value by replacing these values at their original position. Likewise, the pixels value on by one from encrypted secrete image and insertion into the cover image and replaced them. New stego-image is the resulting image.

8.1.1. Encoding procedure of an Algorithm

Input: A gray level Secrete Image (m × n), A gray Level Cover of size (2m × 2n);
Output: Stego Image of size (2m × 2n);
Steps:
1. Input eight-pixel value of the secret image form block of 64 bits to the image encoding Function (DES), which produces the encrypted secret image.
2. Pass it through Huffman encoding and form a dictionary to form a variable length code.
3. Divide the variable length code into 2 bits each.
4. Insert these pixel values into the LSB position in the cover image pixels one by one.
5. End.

8.2. Retrieval procedure of an Image

At the receiving end decoding of stego-image perform the following process:

1) Generate the 2 LSB bits from the stego-Image: The pixels are processed using the Huffman decoder to reconvert them to secret image pixels. Convert into binary values and take 2 LSB bits from four consecutive pixel values:

1 is decoded as 10.
01 is decoded as 11.

00 is decoded as 01.
Thus from b1=11, b2=01 and b3=00 we get {10}, {10}, {11} and {01}.

2) Concatenation of results: Now concatenating the input, the 8 bits of the first pixel value of encrypted secrete image is obtained as 10101101= 173

3) Formation of Encrypted Secrete Image: Now the generated value placed into first position. Likewise taking the next pixels from cover image extract the last 2-bit value from stego-image and use them to make 4-bit the process is repeated and the whole encrypted secret image is retrieved.

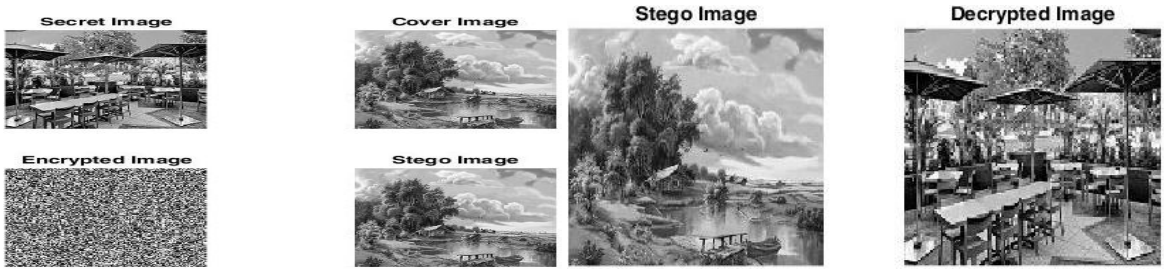
4) Formation of Secrete image: Now the eight consecutive pixel value from an encrypted secret image are again inputted to DES encoding function with same parameter and keys one by one (but used in reverse order) to obtain respective eight-pixels value of an original secret image.

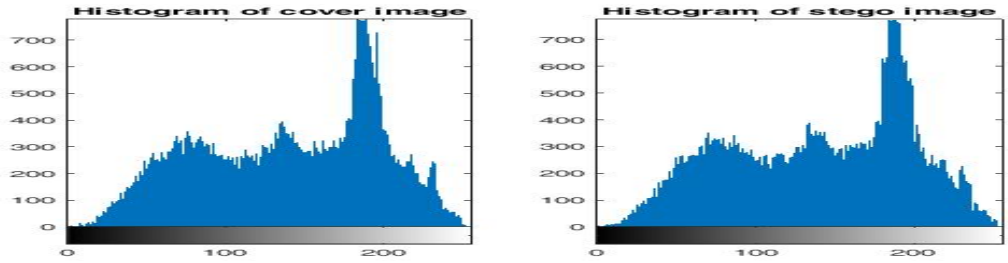
8.2.1. Decoding procedure of an Algorithm

Input: Stego-Image of size (2m × 2n); Output: A grey level Secrete Image (m × n);

Steps:
1. Input each pixel and take 2-bit LSB from 4 consecutive pixel value of the stego image.
2. Decode using the Huffman dictionary and concatenate four 2-bit LSB get 8-bits of each pixel of an encrypted secret image.
3. Now taking eight consecutive pixel value form block of 64 bits are input to decoding Function (DES) using same parameter but keys value used in reverse order getting first eight-pixel value of secret image.
4. End.

- **Data Encryption Standard+ Huffman Coding+ LSB**





PSNR=49.29

9. RESULTS

The proposed algorithm is compared with the implemented research models. Taking a secret image of size 64x64 bits and cover image of size 128x128 bits and Results and analysis of these entire implemented models are given below:

- **Data Encryption Standard + LSB**
- **Data Encryption Standard+ Huffman Coding+ LSB**
- **Logistic Map+ LSB**

- **Tent Map+ LSB**
- **Sine Map+ LSB**
- **Logistic Map+ Huffman Coding+ LSB**
- **Tent Map+ Huffman Coding+ LSB**
- **Sine Map+ Huffman Coding+ LSB**
- **Logistic Tent System+ Huffman Coding+ LSB**
- **Logistic Sine System+ Huffman+ LSB**
- **Tent Sine System+ Huffman Coding+ LSB**
- **Data Encryption Standard+ BTC+ LSB**
- **Logistic Map+ BTC+ LSB**
- **Tent Map+ BTC+LSB**
- **Sine Map+ BTC+LSB**
- **Logistic Tent System+ BTC+LSB**
- **Logistic Sine System+ BTC+LSB**
- **Tent Sine System+ BTC+LSB**

After analysing all the results the PSNR of all the implemented research models using different techniques given in the Table2

Table2: PSNR table of all the implemented research models

	Techniques	PSNR
1.	Data Encryption Standard+ LSB	44.16
	Data Encryption standard+ Huffman Coding+ LSB	49.29
	Data Encryption Standard+ BTC+ LSB	45.09
2.	Logistic Map+ LSB	44.02
	Logistic Map+ Huffman Coding+ LSB	46.28
	Logistic Map+ BTC+ LSB	44.95
3.	Tent Map+ LSB	44.10
	Tent map+ Huffman Coding+ LSB	45.20
	Tent Map+ BTC+ LSB	44.83
4.	Sine Map+ LSB	44.06
	Sine Map+ Huffman Coding+ LSB	46.01
	Sine Map+ BTC+ LSB	45.37
5.	Logistic-Tent Map+ LSB	44.12
	Logistic-Tent Map+ Huffman Coding+ LSB	46.03
	Logistic-Tent Map+ BTC+ LSB	45.50
6.	Logistic-Sine Map+ LSB	44.12
	Logistic-Sine Map+ Huffman Coding+ LSB	45.62
	Logistic-Sine Map+ BTC+ LSB	45.21
7.	Tent-Sine Map+ LSB	44.14
	Tent-Sine Map+ Huffman Coding+ LSB	45.50
	Tent-Sine Map+ BTC+ LSB	45.13

10. Conclusion

This work shows a remarkable method for image steganography in light of the Data Encryption Standard (DES) optimized with Huffman coding. DES utilizes 64-bit block size of plaintext and 56 - bits of secret key and Huffman coding is utilized to diminish the number of bits per pixels required to represent it and furthermore

decreases the transmission time for the transmission of images. The pre-processing give the high state of security as extraction of an image isn't conceivable without the learning of mapping standards of S – Box and the secret key of the function and furthermore the Huffman decoding rules. The proposed work is compared with the 20 implemented research models which are a combination of Chaos based Image Encryption and BTC (Bit truncating Compression) scheme in order to predict the percentage of improvement. After analyzing all the results the PSNR of all the implemented research models using different techniques given in the Table1shows that the DES optimized with Huffman coding have higher PSNR value as compared to other implemented research models.

References

[1] Yambin Jina Chanu , Themrichon Tuithung , Kh Manglem singh,“ A Short Survey on Image Steganography and Steganalysis Technique “ , IEEE Trans. ,2012 .

[2] Amitava Nag, Saswati Ghosh, Sushanta Biswas, Debasree Sarkar, Parta Pratim Sarkar " An Image Steganography Technioque using X-Box Mapping", IEEE Trans. International Conference Advances in Engineering, science and Mamagement (ICAESM- 2012) 709 -713.

[3] Ge Huayong, Huang Mingsheng, Wang Qian, "Steganography and Steganalysis Based on Digital Image", IEEE Trans. International Congress on Image and Signal Processing,(2011) 252-255.

[4] W. Luo, F. Huang, J. Huang, Edge adaptive image steganography based on LSB matching revisited, IEEE Trans. Inf. Forens. Security 5 (2) (2010) 201-214.

[5] Guilliang Zhu, Weiping Wang, “Digital Image Encryption algorithm based on pixel”, ICIS – 2010 IEEE International Conference 29-31 Oct 2010, pp – 769 – 772.

[6] Jasmin Cosic , Miroslav Bacai, “ Steganography and Steganalysis Does Local web Site contain “Stego” Contain “ , 52 th IEEE Trans. International Symposium ELMAR-2010, Zadar, Croatia 2009 ,pp 85 – 88.

[7] Zhang Yun-peng , Liu Wei “ Digital Image Encryption Algorithm Based on chaos and improved DES “, System, man and Cybernatics ,SMC 2009 , IEEE International Conference 11-14 Oct 2009, pp 474-479.

[8] J. Mielikainen, LSB Matching Revisited, IEEE Signal Process. Lett. 13 (5) (2006) 285-287.

[9] Saeed R. Khosravirad, Taraneh Eghlidos and Sharokh Ghaemmaghami, “Higher Order Statistical of Random LSB Steganography”, IEEE Trans. 2009, pp 629 - 632.

[10] Darrel Hankersson, Greg A. Harris, and Peter D. Johnson Jr.*Introduction to Information Theory and Data* Compression. CRC Press, 1997.

[11] Gilbert Held and Thomas R. Marshall. *Data and Image* Compression: Tools and Techniques

[12]http://en.wikipedia.org/wiki/Discrete_Fourier_transform

[13] Terry Welch, "A Technique for High--Performance Data Compression", Computer, June 1984.

[14] N Provos and P. Honeyman, "Hide and seek: An Introduction to Steganography", IEEE Security and Privacy, 2003, pp32-44.

[15] Donovan Artz" Digital Steganography: Hiding Data within Data ", Los Alamos National Laboratory, IEEE Trans. 2001, pp 75-80.

[16] K Suresh Babu , K B Raja, Kiran Kumar k, Manjula Devi T H, Venugopal K R, L M Pathnaik" Authentication of Secrete Information in Image Steganography", IEEE Trans. 13.

[17] Yang, Chunfang., Liu, Fenlin., Luo, Xiangyang., and Zeng, Ying., “Pixel Group Trace Model-Based Quantitative Steganalysis for Multiple Least-Significant Bits Steganography”, IEEE Transactions on Information Forensics and Security, Vol. 8, No. 1, January 2013.

[18] Swati malik, Ajit “Securing Data by Using Cryptography with Steganography” International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 5, May 2013

[19] Ishwarjot Singh ,J.P Raina,“ Advance Scheme for Secret Data Hiding System using Hop field & LSB” International Journal of Computer Trends and Technology (IJCTT) – volume 4 Issue 7–July 2013.

[20] G. Manikandan, N. Sairam and M. Kamarasan “A Hybrid Approach for Security Enhancement by Compressed Crypto-Stegno Scheme “, Research Journal of Applied Sciences, Engineering and Technology 4(6): 608-614, 2012

[21] Shabir A. Parah, Javaid A. Sheikh, G.M. Bhat, "Data Hiding in Intermediate Significant Bit Planes, A High Capacity Blind Steganographic Technique", International Conference on Emerging Trends in Science, Engineering and Technology , pp.192-197, July 2012.

[22] Michel K. Kulhandjian, Dimitris A. Pados, Ming Li, Stella N. Batalama, and Michael J. Medley, "Extracting spread-spectrum hidden data from digital media ", IEEE transactions on information forensics and security, vol. 8, no. 7, july 2013.

[23] Chang, Chin-Chen., Lin, Iuan-Chang., and Yaun-Hui YU., " A new Steganographic method for color and gray scale image hiding", Computer Vision and Image Understanding, ELSEVIER, Vol. 107, No. 3, pp. 183-194,2007.

[24] Bailey, K., and Curran, K., "An Evaluation of Image Based Steganography Methods", Journal of Multimedia Tools and Applications, Vol. 30, No. 1, pp. 55-88, 2006.

[25] Adnan Gutub, Ayed Al-Qahtani, Abdulaziz Tabakh, "Triple-A: Secure RGB Image Steganography Based on Randomization", International Conference on Computer Systems and Applications (AICCSA-2009), pp: 400-403, 10-13 May 2009.

[26] R.Amirtharajan, Sandeep Kumar Behera, Motamarri Abhilash Swarup, Mohamed Ashfaaq and John Bosco Balaguru Rayappan , "Colour Guided Colour Image Steganography" Universal Journal of Computer Science and Engineering Technology , 16-23, Oct. 2010, pp. 2219-2158.

[27] Anil Kumar , Rohini Sharma,"A Secure Image Steganography Based on RSA Algorithm and Hash-LSB Technique ",International Journal of Advanced Research in Computer Science and Software Engineering, Volume 3, Issue 7, July 2013.

[28] Gutub, A., Al-Qahtani, A., and Tabakh, A., "Triple-A: Secure RGB image steganography based on randomization", Computer Systems and Applications, AICCSA 2009, IEEE/ACS, pp. 400 – 403, 2009..

[29] Dr. Fadhil Salman Abed "A Proposed Method of Information Hiding Based on Hybrid Cryptography and Steganography ", IJAIEM, Volume 2, Issue 4, April 2013

[30] N.F. Johnson, S. Jajodia, Exploring steganography: seeing the unseen, IEEE Computer 31 (2) (1998) 26–34.

[31] J.C.Judge, Steganography: past, present, future. SANS Institute publication, <http://www.sans.org/ reading room/ whitepapers/ stenganography/ 552.php>, 2001

[32] F.A.P.Petitcolas, R.J.Anderson, M.G.Kuhn:"Information Hiding- A Survey", Process of IEEE, vol.87,no.7, pp.1062- 1078, July, 1999.

[33]Artz D (2001). "Digital steganography: hiding data within data" Internet Computing. IEEE, 5(3): 75-80

[34] Nassir Memon R. Chandramouli. Analysis of lbs. based image steganography techniques. In Proceedings of IEEE ICIP, 2001.

[35] L. Bao, Y. Zhou, C.L.P. Chen, H. Liu, A new chaotic system for image encryption, in: 2012 International Conference on System Science and Engineering (ICSSE), 2012, pp. 69–73.

[36] G.A. Sathishkumar, K. Bhoopathy bagan, N. Sriraam, Image encryp-tion based on diffusion and multiple chaotic maps, International Journal of Network Security & Its Applications, 3 (2) (2011) 181–194.

[37] A. El-Latif, L. Li, N. Wang, X. Niu, Image encryption scheme of pixel bit based on combination of chaotic systems, in: 2011 Seventh International Conference on Intelligent Information Hiding and Multimedia Signal Processing (IIH-MSP), 2011, pp. 369–373.

[38] M.I. Sobhy, A.E.R. Shehata, Methods of attacking chaotic encryption and countermeasures, in: Proceedings of 2001 IEEE International Conference on Acoustics, Speech, and Signal Processing (ICASSP '01), 2001, pp. 1001–1004.

[39] Chan, C. K. and Cheng, L. M. Hiding data in images by simple LSB substitution. Patt. Recogn., 2004, 37, 469–474.

[40] Chang, C. C., Lin, C. Y. and Hsieh, Y. P. Three-phase lossless data hiding method for the VQ index table. Fundam. Inform., 2008, 82, 1–13.

[41] Chen, J., Chen, T. S., Hsu, H. C. and Lin, Y. H. Using multi-ringed shadow image of visual cryptography to hide more secret messages. Imag. Sci. J., 2009, 57, 101– 108.

[42]Chuang, J. C. and Chang, C. C. Using a simple and fast image compression algorithm to hide secret information. Int. J. Comput. Appl., 2006, 28, 329–333.

[43] Delp, E. and O. Mitchell, O. Image compression using block truncation coding. IEEE Trans. Commun., 1979, 27, 1335–1342.

[44] Hong, W., Chen, T. S. and Shiu, C. W. Lossless steganography for AMBTC compressed images, Proc. 1st Int. Cong. on Image and signal processing: CISP 2008, Sanya, China, May 2008, IEEE, Vol. 2, pp. 13– 17.

[45] Lema, M. D. and Mitchell, O. R. Absolute moment block truncation coding and its application to color image. IEEE Trans. Commun., 1984, 32, 1148– 1157.

[46] Malvar, H. S. Fast progressive image coding without wavelets, Proc. IEEE Data Compression Conf., Snowbird, UT, USA, March 2000, IEEE, pp. 243– 252.

[47] Sharma, P. and Reilly, R. B. A colour face image database for benchmarking of automatic face detection algorithms, Proc. 4th EURASIP Conf. on Video/ image processing and multimedia communications, Zagreb, Croatia, July 2003, IEEE, Vol. 1, pp. 423– 438.