IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 6 Issue 8, August 2019
ISSN (Online) 2348 – 7968
www.ijiset.com

A Novel Approach for Highly Secured and Robust Image Steganography

Sindhu Priya R
M.Tech
Electronics and Communication Engineering
B.M.S College of Engineering
Bangalore, India
sindussr@gmail.com

Dr. Meera A
Professor
Electronics and Communication Engineering
B.M.S College of Engineering
Bangalore, India
amira.ece@bmsce.ac.in

Abstract - Data hiding into image have become popular in present world. But there is always security issue as there is a high frequency of data transmitted that pose serious challenges like vulnerability, threats, and distributed denial of service attacks. The proposed technique of image steganography provides higher security, robustness and higher imperceptibility. This technique is more secure as the encrypted secret image is hidden in transformed cover images by deploying Chaotic based encryption schemes say Henon map and Lorenz map for confusion-diffusion process to evaluate the images free from the loopholes of security by implementing DWT (Discrete Wavelet Transform) and LSB (Least Significant Bit) for image hiding. Parameters say PSNR (Peak Signal to Noise Ratio), MSE (Mean Square Error), correlation coefficients in horizontal, vertical and diagonal directions, histograms and entropy have been calculated to justify aspects in terms of security and robustness.

Keywords - Confusion-Diffusion process, DWT, Henon map, Image Steganography, Lorenz map, LSB

I. INTRODUCTION

The recent surge in web technology led to increased social networking and sharing of on-line media. Data such as images, audio and video is transferred in huge volumes across the web. Obviously, data and privacy has to be secured. The way around to remove this obstacle is to use chaotic systems for image encryption to increase the security in the field of Steganography. Steganography and steganalysis play an important role in information hiding and extraction. steganography deals with techniques for hiding information and steganalysis detects the hidden information with little or no knowledge about the steganography algorithm or its parameters. Both Steganography and steganalysis are dealt in this paper. Steganography is the technique in which secret image is embedded into a cover image without affecting the perceptual quality of the cover image. Based on the medium used in steganography to embed the message, it is classified as image steganography, audio steganography and video steganography. Recently, steganography in text has also been proposed. In image steganography, the secret message is hidden inside an image such that the change in quality of the image cannot be noticed. In audio steganography, the secret message is hidden inside an audio file like a song or music without changing the original quality. In video steganography, the secret message is hidden inside a video file without disturbing the original quality of the video. In frequency domain steganography method, carrier image is first converted into frequency domain by using domain transforms such as Discrete Fourier Transform (DFT), Discrete Cosine Transform (DCT), Discrete Wavelet Transform (DWT), Fourier Mellin Transform (FMT), Fractal Transform, etc. Then the message is hidden inside the transformed cover image by applying embedding techniques. But in spatial-domain Steganography, the secret message is hidden inside the image by applying some manipulation over the different pixels of the image. In this paper, chaos-based data hiding scheme is implemented to achieve high level security. First level of security is achieved by using chaotic based encryption as a part of cryptography. The reason behind using chaotic maps is that the properties of chaotic map comprise dynamic behaviour, ergodicity, sensitive towards initial conditions and non-linear deterministic nature that provides good confusion and diffusion in encryption methods. Second level of security is achieved by imposing a transformation on cover image before embedding by

implementing image steganography. In order to increase the level of security, frequency domain steganography method namely Discrete Wavelet Transform (DWT) is employed in this paper. Least significant bit (LSB) insertion is used to embed the secret image inside transformed cover image. The LSB algorithm is employed in spatial domain in which the payload bits are embedded into the least significant bits of cover image to obtain the stego-image. The present scheme implements a blend of two methods – confusion and diffusion by making use of 2D Henon map and 3D Lorenz map in encryption stage. Chaotic systems possess randomness, highly sensitive to initial conditions and ergodicity. These properties are very much suitable for implementation of cipher images. The following sub sections gives the details of Henon map, Lorenz map, DWT and LSB that are implemented in the present paper.

A. Henon Map

Henon Mapping system is discovered by Henon in 1978. Henon map is an instance of discrete time dynamical frameworks that prove chaotic behaviours. It takes a point (x_n, y_n) in the plane and maps it to another point, (x_{n+1}, y_{n+1}). It is characterized by accompanying arrangement of distinction conditions. Henon layout is a clear two-dimensional guide with quadratic non-linearity and Henon map chaotic system is defined in equation 1 and equation 2 as below.

$$x_{n+1} = y_n - 1 + a \times x_n^2 \quad (1)$$

$$y_{n+1} = b \times x_n \quad (2)$$

The Henon map is dependent on two parameters, a and b, and the values for a and b are chosen as 1.4 and 0.3 respectively for which the Henon map is chaotic. For other values the behavior is periodic or convergence to a constant value. The initial values and the values of parameters is important to make Henon strange attractor, or diverge to infinity. Figure 1 shows the 3-D view of Henon mapping system.

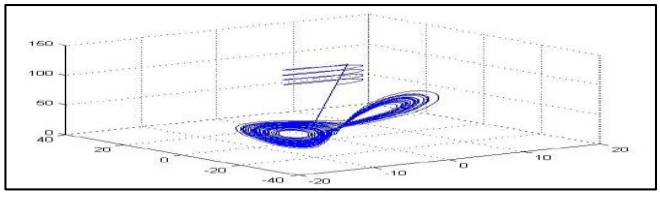


Fig. 1: 3D view of Henon Mapping system

B. Lorenz Map

The Lorenz system is a system of ordinary differential equations developed by Edward Lorenz in 1963. Lorenz structure have varying bifurcation parameter to improve the complex behaviour of chaotic system. Three factors of system (X, Y, Z) are used as the initial keys of chaotic encryption system. The Lorenz differential condition is defined in the equations 3, 4 and 5.

$$\frac{dX}{dt} = s \times (X - Y) \quad (3)$$

$$\frac{dY}{dt} = Y \times (r - Z) - Y \quad (4)$$

$$\frac{dZ}{dt} = X \times Y - b \times Z \quad (5)$$

Here X, Y and Z are the state variables, t is the time. Real numbers, s, r and b are control parameters and left-hand side of the equations (3), (4) and (5) stands for time derivatives of the state variables. The chaotic behaviour is observed only when the system parameters are chosen as s = 10, r = 28 and b = (8/3). Moreover, the values of control parameters guarantees that the system has chaotic attractors, which is important in terms of cryptography and any change in initial conditions will cause trajectories to be in the same attractor set, hence making it difficult to predict any outcomes without knowing the exact initial conditions of the system. Figure 2 shows the 3D view of Lorenz chaotic system.

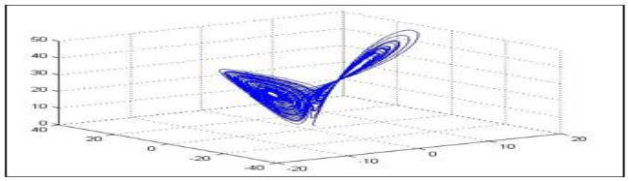


Fig. 2: 3D view of Lorenz system

C. LSB(Least Significant Bit)

Least Significant Bit Substitution is the most popular stenographic technique deployed in spatial domain. The basic concept of LSB is to embed the secret data at the bit level such that the embedding process will not affect the original pixel value. It exploits the fact that the level of precision in many image formats is more than that perceivable by human vision. The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is altered to a bit of the secret

message. After embedding, the difference between the cover image and the stego image will be hardly noticeable to the human eye. This embedding LSB approach has become the basis of many techniques to hide the messages within multimedia carrier data. It can be employed in data domains, like embedding a hidden message onto the color values of RGB bitmap data, the frequency coefficients of a JPEG image and also be applied to a variety of data formats and types. Therefore, LSB is one of the most important steganography techniques which is in use today. This paper implements LSB Steganography in the embedding process as a basis to achieve more robustness in the system. The secret message is converted to stream of bits and each bit of the message is embedded into the LSB of the pixels of the transformed cover image which does not result in a significant change in the image quality perceptually.

D. DWT(Discrete Wavelet Transform)

DWT is one of the frequency domain transformation widely used in image steganography. It has many advantages, one of which is its superior character in decomposing the image and address robustness of the Information-Hiding system. DWT is a domain transformation that has good multiresolution characters in human vision systems and also works well in spatial localization. In DWT based steganography approach, the wavelet coefficients of the cover image are modified to embed the secret message. In wavelet analysis, DWT decomposes a signal into a set of mutually orthogonal wavelet basis functions and these functions differ from sinusoidal basis functions such that they are spatially localized. The aim of using DWT is to decompose original signal into low frequency and high frequency sub-bands in frequency subdomain. DWT transformation separates the high frequency and low frequency components while preserving information the signal. It divides the image into the following sub bands such as LL (Approximation Coefficient), LH (Horizontal Coefficient), HL (Vertical Coefficient) and HH (Diagonal Coefficient) Where, H stands for high pass filtering and L stands for low pass filtering. LL consists of the Blur features, low-frequency signals, that are approximations. LH consists the horizontal features. HL contains the vertical features and HH contains the diagonal features. Figure 3 shows one level, two dimensional DWT.

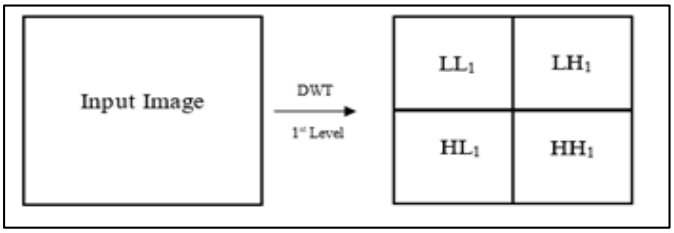


Fig. 3 : 1-level, two dimensional DWT

II. LITERATURE SURVEY

A novel method has been implemented to hide the encrypted secret image in two distinct cover images using hybrid DWT-DCT steganography technique [1]. The implementation is on two colour cover images. To achieve better imperceptibility with robustness and to have a higher PSNR value, applied a combined DWT – DCT steganography technique in the proposed work. DWT is applied on two distinct cover images to obtain Coefficients of HH sub band. Before embedding an encrypted secret image in it, the DCT is applied on these sub band DWT coefficients and results show PSNR of 49.23dB. A new double layer information security by combining encryption and hiding methods is proposed. [2] The secret data is encrypted by using a zigzag matrix transformation and the cover image is encrypted using two dimensional (2D) logistic map. Encrypted data are randomly embedded in encrypted cover image and the decrypted stego image is transformed to the receiver. Simulation results show PSNR of 43dB. [3] A gray image is hidden into another gray scale image. Firstly, the secret image is encrypted using logistic chaotic map to achieve high security. Then the encrypted secret image embedded into the HH sub band of the wavelet transformed cover image. Favourable results obtained peak signal to noise ratio (PSNR) of 37dB and correlation criteria. [4] Proposes hiding gray images in a colour image based on Least Significant Bits method (LSB) with shuffling by using two types of 4-D chaotic systems namely Lu and Liu. 4-D chaotic system provide an efficient security key and more difficult to forecast attack and achieved PSNR of 46.27dB. [5] This research proposes a simple and safe way to hide messages in LSB techniques. Three times the XOR operation is done to encrypt the message before it is embedded on the LSB and results in PSNR value of 54.3 dB. A graph wavelet transform-based steganography using graph signal processing (GSP) is presented in [6], which results in better visual quality stego image as well as extracted secret image. In the proposed

scheme, graph wavelet transforms of both the cover and transformed secret image (using Arnold cat map) are used. The GSP-based inverse wavelet transform is performed on the resulting image to obtain the stego image with PSNR of 52.2dB. [7] proposed a modified secure and high capacity based steganography scheme of hiding a large-size secret image into a small-size cover image. Arnold transformation is employed to scramble the secret image. Discrete Wavelet Transform (DWT) is performed in both images and using Alpha blending. Then the Inverse Discrete Wavelet Transformation (IDWT) is used to get the stego image. The results show that the proposed algorithm is highly secured to good perceptual invisibility with PSNR of 49.5dB. [8] A hybrid technique is introduced by combining the cryptography and Steganography properties. Also for data encryption vary the block size in place of fixed block. The proposed image steganography algorithm works on spatial domain. LSB method is used for data hiding in different ways and PSNR value shows 64.5dB. A new method of image steganography is blended with cryptography that is present in [9]. First encrypted using Vernam cipher algorithm and then the ciphered message is embedded in an image using LSB with Shifting (LSB-S) with PSNR of 56.9dB. [10] The proposed method of Least Significant bit (LSB) for secret message insertion is made on the basis of sensitivity of human eyes to various colour wavelengths. This selective approach induces lower noise and high security for transferring images and results in PSNR of 55.9dB.The researchers [11] examined on simplification of traditional Fourier transform, established years before in arithmetic survey. As a result of superior calculation related to this, discrete FrFT comes into picture. The PSNR result in frequency and time domain gives equal value and DFrFT provides an advantage in terms of having added secret key. The results achieved with the PSNR value of 32.46. [12] Employ a variety of plain LSB calculation. Bit-reversal system applied to improve stego picture quality. The exhibited strategy indicates great improvement to Least significant bit system in thought to safety and picture quality. The outcome gives PSNR value of 54.34. In [13] proposed a feasible steganography technique utilizing Integer Wavelet Transform to ensure the MRI therapeutic picture into a single partition picture. The observed results are not better with adequate PSNR contrasted with the current calculations and value is 50.48 based on block-DCT with Huffman coding. [14] Introduced the novel plan inserts data in integer wavelet transform coefficients by utilizing an extra memory of 8×8 square on broaden image. The best pixel transform practice linked subsequent to implanting the message. Results demonstrates that the strategy beats versatile steganography system dependent on integer wavelet change as far as PSNR reach upto 43.23. [15] Gives novel method to picture steganography dependent on Huffman Encoding. Two 8 bit dimension picture of size M x N and P x Q are utilized as cover picture and secret picture individually. Results demonstrate that the calculation has a high limit and a decent imperceptibility with PSNR value is 46.86dB for wavelet families such as Db1. [16] Introduced whole number Wavelet Transform (IWT) that is utilized in steganography. [17] Secure Steganography utilizing Hybrid Domain Technique (SSHDT) is implemented using Daubechies Lifting Wavelet Transforms (LWT) that is connected on wrap picture to produce 4 sub groups XA, XH, XV and XD. The XD band included and isolated into two equivalent squares state upper and lower for load inserting. Daubechies Inverse LWT (ILWT) is connected on XA, XH, XV and XD stego items to acquire stego picture in spatial area. It has been seen that PSNR with value of 48.27. [18] Given data hiding scheme using DWT and get the stego image using IDWT. The method tried to improve data hiding capacity on steganographic scheme and provides modified approach established towards security. In order to scramble the secret image, Arnold transformation is used. DWT operates on all types of images followed by alpha blending process. The result shows a PSNR value of 49.32dB. [19] The specific picture encryption method secures just the area of interest for the picture. The Gaussian Mixture Model based Expectation and Maximization (GMM-EM) bunching procedure is connected here. The chaos bunched locale is exposed to both the disarray and dispersion, Confusion utilizing 2D-Ikeda clamorous map and Diffusion utilizing 1D-Quadratic map. The appraisal parameters are Peak-Signal to Noise Ratio, Mean Square Error, Entropy, Correlation, Pixel change rate, Average change in force, Encryption time and Percentage of encryption. Results are then contrasted and existing strategies guaranteeing a higher level of security against static and dynamic assaults by the interceptor. [20] A Novel steganographic scheme dependent on disorderly emphases was proposed. Steganographic

calculations takes an interest in the advancement of a semantic web. [21] proposed to plan multi-bits steganography security framework for concealing touchy information on PCs with client security need. The examination utilized distinctive picture based stego frameworks (1-LSB, 2-LSB, 3LSB, 4-LSB) that are completely subject to the PC information accessible to guarantee full control of the security of the framework to be given to the client. [22] Security in pictures represents a genuine test like robustness, attacks and conveyed refusal of administration assaults. Henon and Lorenz are the chaotic mapping used to assess the pictures free from the security.

III. OVERVIEW OF THE PROPOSED WORK

The proposed work is divided into 2 phases namely, (a) Embedding Framework with Encryption and (b) Extracting Framework with Decryption. In Image Embedding framework approach, a chaotic image encryption is proposed to change secret image into encrypted by using two chaotic maps namely, Henon and Lorenz map. Next, a cover image is transformed into four sub-bands using Discrete Wavelet Transform (DWT). Later the scrambled secret image is hidden into the selected high frequency band of transformed cover image using Least Significant Bit (LSB) method to obtain final stego image as shown in figure 4.

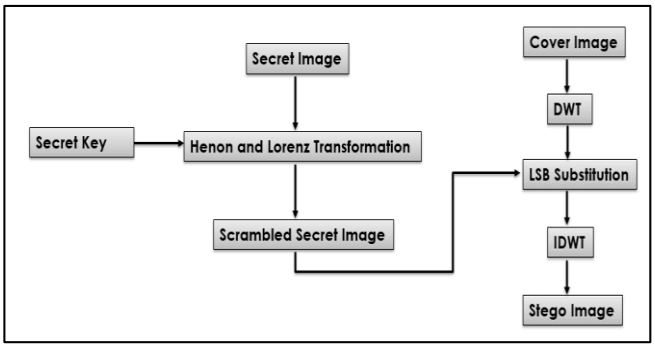


Fig. 4 : Embedding Framework with Encryption

In Image Extracting framework approach, DWT is applied to the stego image for extracting bits from HH band to get the scrambled secret image. Finally, inverse Henon and Lorenz map transformation is applied to get the original secret image as shown in figure 5.

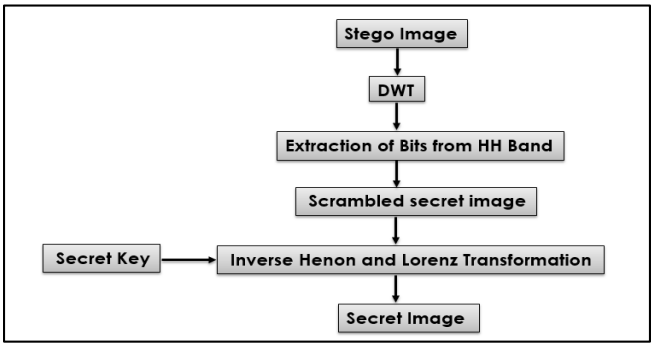


Fig. 5 : Extracting Framework with Decryption

IV. PROPOSED ALGORITHM

To evaluate the performance of the proposed method, the proposed method is implemented in Matlab of version 2013a. In this simulation, 60 general sample images have been tested by using this proposed algorithm. For representation purpose, variety of images been shown. In Encryption stage secret images namely, bird, boy, plane, cameraman, MR_cervical vertibra, CT_knee and lena images are shown. In stego image formation, cover images namely, bird, cameraman, CT_kneee, lena, flower, man, MR_cervical vertibra are considered and respective secret images are plane, insect, baboon, boy, peppers, bird and Barbara images. The process of getting encrypted image from the secret image follows two mapping techniques such as Henon and Lorenz map to generate chaotic sequences, by the way to get confused and diffused images. The proposed scheme combines two chaotic maps namely 2D henon map and 3D Lorenz map to scramble the secret image. The secret keys used in the algorithm are the initial conditions X_0, Y_0 of the Henon map, the initial conditions X_0, Y_0, Z_0 and the step size h of the Lorenz equation.

The Proposed algorithm comprises of encryption process namely, confusion-diffusion followed by stego image formation and extraction of decrypted (original) secret image from the stego image which is explained in the below sub-sections.

A. Confusion process -

The input plain image I (i, j) having size of M x N is divided into R squares of size A x B such that A x B x R=M x N. These squares are then placed on top of the other to obtain matrix J of height R.

1. For the Henon map, the initial values selected are 0.6315477 for X_0 and 0.18906343 for Y_0. The values of

system parameters considered are 1.4 for a and 0.3 for b to obtain the successive R values.

2. The values of X and Y are magnified to an appropriate natural number.
3. Modulus is calculated between the obtained natural number and the height R to obtain the matrix J having length 1 x R.
4. The R elements of J along the height are then filled up into another same sized matrix K (permutation matrix).
5. The Permutation matrix K is used to change the position of the R squares taken from the input image to form confused matrix S.
6. Confusion process is depicted in figure 6 and the stages in the confusion stage is shown in figure 6(a), 6(b), 6(c) and 6(d)

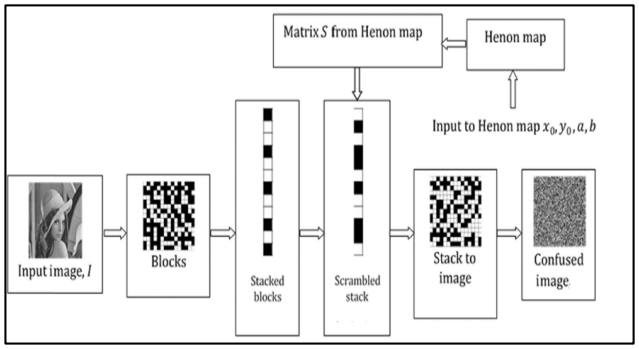


Fig. 6 : Confusion process in Encryption

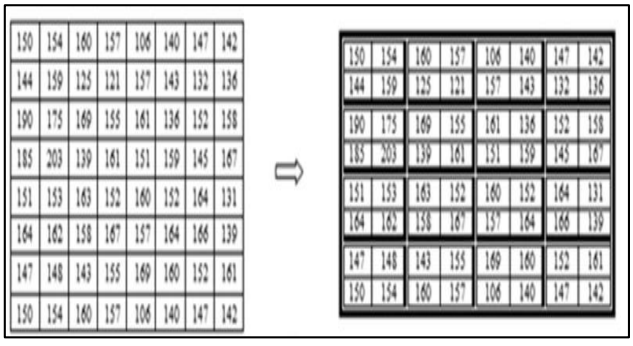


Fig. 6(a) Original matrix (M × N = 8 × 8) divided into (2 × 2) blocks

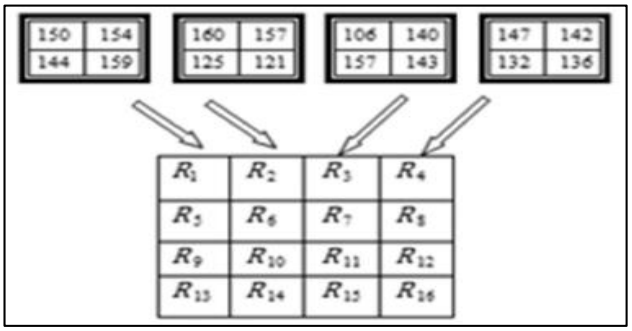


Fig. 6(b) R(= 16) blocks of size A× B(2 × 2)

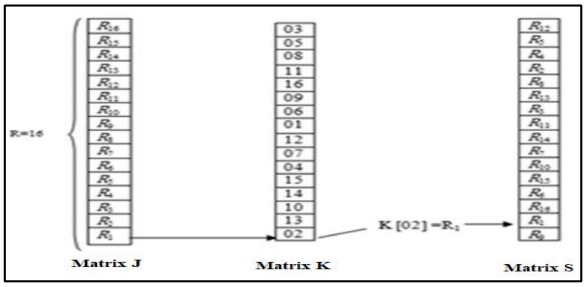


Fig. 6(c) Stacked matrix J, matrix K, matrix S generated from Henon map

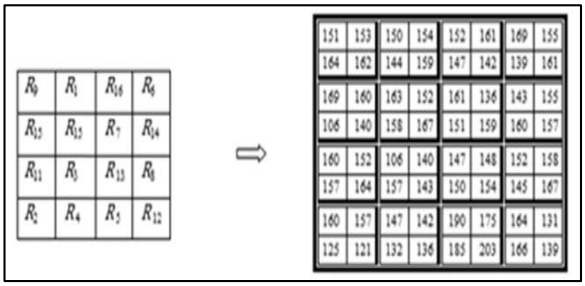


Fig. 6(d) Confused matrix L from confused blocks

B. Diffusion Process –

The confused matrix is further XORed with the matrix obtained using Lorenz equations to obtain final encrypted image.

1. For the Lorenz map, the initial values selected are 0.0000000000778899 for X_0, 0.0000000000123654 for Y_0 and 0.00000000000657789 for Z_0. The values of system parameters considered are s = 10, r = 28 and b = (8/3) to generate a chaotic sequence.
2. Using a large number (10^{15}), the obtained chaotic sequence is transformed into a large integer and modulus is performed with M.
3. From the obtained integer stream, the pixel values of the plain image I (i, j) is modified by performing bit-wise XOR with the confused matrix to get the ciphered image I' (i, j). The diffusion process is depicted in figure 7.

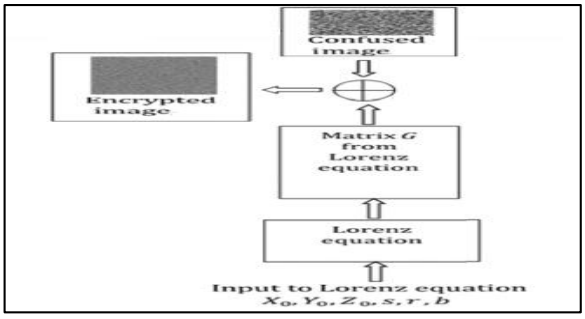


Fig. 7 : Diffusion process in Encryption

C. The process of stego image formation is explained in following steps.

1. A logical array is constructed to hold the binary equivalent pixel values of encrypted message image of size R2*C2*8, where R2 and C2 is the number of rows and columns of encrypted message image respectively.
2. A cover image of size R1*C1 is transformed to one dimensional DWT which results in 4 sub bands namely, LL, LH, HL and HH bands, where, LL is the low frequency band in which maximum information is available and visible to human eye. LH represent the pixel intensity in horizontal direction.HL represent the pixel intensity in vertical direction and HH is pixel intensity in diagonal direction.
3. Embedding process is done using 1 – bit lsb technique by replacing each lsb value of pixel of HH band of cover image with lsb value of encrypted message image.
4. The embedding process is repeated till all the pixel values of message image is embedded in the transformed cover image. Inverse DWT is applied to obtain the required Stego Image.

D. Extraction of secret image from the stego image is explained in following steps.

1. DWT is applied to the stego image and HH band is selected.
2. Extracted message bits from selected HH band to get encrypted image. The obtained image is scrambled secret image.
3. This Recovered image is XORed with the random numbers generated in encryption stage since XOR is reversible operation.
4. The Matrix wise arrangement is changed to stack arrangement and Shuffled blocks stored in stack is reshuffled to get the original arrangement of blocks.
5. The final matrix is converted to image format to get the original secret image.

V. Performance Analysis and Simulation Results

Analysis is done in 3 phases namely, (1) Encryption stage (2) Stego image formation stage (3) Secret image extraction stage

1. Encryption

A. Performance Analysis

To evaluate the performance of the proposed method, the algorithm is implemented in Matlab of 2013a version. In this experiment, 60 general sample images is tested. For representation purpose, few test images are shown namely bird, baby, plane, cameraman, MR_cervical vertibra, CT_knee and lena. Encryption results are depicted in figure 8.

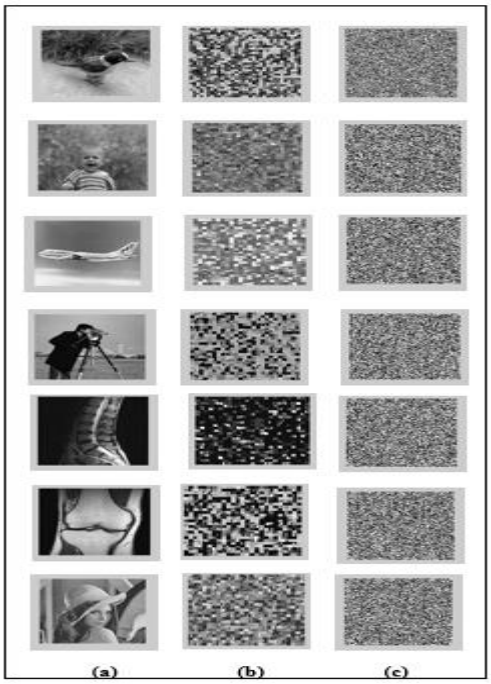


Fig. 8 : (a) Secret images (b) Images after confusion (c) Images after diffusion.

1. MSE(Mean Square Error)

MSE (Mean Square Error) is the parameter that calculates the magnitude of average error between the original image and stego image. The differences between plain and encrypted images is detected using this parameter. More the difference proves the efficacy and security of the proposed method.

Mean Square Error (MSE) is given by the equation,

$$MSE = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}[plain(i,j)-cipher(i,j)]^2}{M*N} \quad (6)$$

plain(i,j) represent pixel location of ith row and jth column of plain image, cipher(i,j) represent pixel location of ith row and

jth column of cipher image and M*N is the pixel size. It is observed that MSE is more for a small change in initial conditions. A small value of MSE enables the intruder to visualize the original image. More the MSE, better is the encryption algorithm.

2. PSNR(Peak Signal to Noise Ratio)

The good visual quality of stego is the most important property of steganography system as it is difficult to detect by detectors. Peak Signal to Noise Ratio (PSNR) is used to measure the distortion between an original cover image and stego image.

The equation for PSNR is,

$$PSNR = 10\frac{\log_{10}(255)^2}{MSE}\ dB \quad (7)$$

The experimental results in the encryption stage is shown in table 1 for different images. It is observed that the low peak signal to noise ratio shows that the intelligent information cannot be extracted from the ciphered image.

Secret Image	PSNR (dB)	MSE
1. Lena	8.618	7654.66
2. Baboon	8.075	6609.24
3. Plane	8.954	8014.50
4. Peppers	8.054	8135.59
5. Cow	9.059	8074.60
6. Cameraman	8.249	9276.83
7. Baby	9.596	6586.76
8. MR-Spine	6.535	14438.85
9. CT-Knee	7.381	11606.06
10. Bird	7.591	10368.56

Table 1: PSNR and MSE results in Encryption stage

3. SSIM(Structural Similarity Index Measure)

SSIM is one of the best approach for evaluation of image quality. It measures the similarities between the two images. This compares the contrast, luminance and structural information between equal sized gray level images. The range of value for SSIM is between 0 and 1. The value 1 says that the two images are exactly the same and value 0 denotes they are dissimilar. It is an indicator of the homogeneity between the two images, and can be gauged using the below mentioned formulae, defined in the equations 8, 9 10, 11, 12 and 13.

The equation for SSIM is given by,

$$SSIM = \frac{(2*\bar{x}*\bar{y}+c1)*(2\sigma_{x,y}+c2)}{(\bar{x}^2+\bar{y}^2+c1)*(\sigma_x^2+\sigma_y^2+c2)} \quad (8)$$

Where, c1 and c2 are the two variables to stabilize the division with weak denominator, given by,

$$c_1=(k_1 L)^2,\ c_2=(k_2 L)^2 \quad (9)$$

$$\mathbf{L} = \mathbf{2}^{\text{No. of bits per pixel}} - 1 \quad (10)$$

Mean of x and y is defined as ,

$$\bar{x} = \frac{1}{M*N}\sum_{i=1}^{M*N} x_i \qquad \bar{y} = \frac{1}{M*N}\sum_{i=1}^{M*N} y_i \quad (11)$$

Variance of x and y is defined by ,

$$\sigma_x^2 = \frac{1}{M*N}\sum_{i=1}^{M*N}(x_i-\bar{x})^2 \qquad \sigma_y^2 = \frac{1}{M*N}\sum_{i=1}^{M*N}(y_i-\bar{y})^2 \quad (12)$$

Covariance of x and y is given by,

$$\sigma_{x,y} = \frac{1}{M*N}\sum_{i=1}^{M*N}(x_i-\bar{x})*(y_i-\bar{y}) \quad (13)$$

B. Security Analysis

A good encryption scheme must resist all kinds of known attacks. The main attacks is aimed at the chaotic image encryption schemes based on entropy analysis, security wise.

1. Entropy Analysis

In image encryption scheme, Entropy is important as it measures the strength of the cryptosystem which also represents the randomness in the encrypted image. For a gray scale image comprising 256 different intensity levels, entropy value must be equal to eight, ideally. Its value is dependent on the probability of occurrence of varying pixels in the cipher image. When all the pixels with different gray levels are equally probable, then the entropy value is 8. It also represents the amount of leakage of information. If the value is closer to 8, it results in reduced information leakage and hence enhanced safety achieved against statistical attacks.

The entropy is calculated using equation 14.

$$ET(m) = -\sum_{i=0}^{L-1} p(m_i) \times log_2(p(m_i)) \quad (14)$$

Where ET denote entropy, L is the total gray levels and (m_i) is the probability occurrence of pixel at each gray level m_i. Table 2 shows the calculated entropies for original and cipher images.

Image	Original Image	Cipher Image
1. Bird	7.6266	7.9817
2. Lena	7.3958	7.9803
3. Baboon	7.0936	7.9809
4. Plane	7.0737	7.9807
5. Peppers	7.5623	7.902
6. Cow	6.903	7.9832
7. Cameraman	7.041	7.9815
8. Baby	6.946	7.9807
9. MR_Cervical_vertibra	5.8611	7.9839
10. CT_Knee	7.0304	7.9823

Table 2: Entropies of original and cipher images in Encryption stage

From table 2, it is observed that the entropy values of cipher images are nearly equal to 8 which show that the proposed encryption algorithm resists statistical attacks.

C. Statistical Analysis

In order to demonstrate the robustness of the proposed method, correlation analysis is done.

1. Correlation

The correlation of the adjacent pixels for encrypted cipher image is one of an important criteria to measure the performance of the cryptosystem. It measures the relationship between adjoining pixels in an image which may be horizontal, vertical or diagonal in direction. The plain image exhibits a strong relationship between its adjoining pixels. The correlation coefficients of the plain and enciphered image are calculated in multiple directions by randomly selecting a set of multiple pairs of adjoining pixels. The correlation coefficient is given by equation 15,

$$C_{xy} = \frac{COVR(x,y)}{\sqrt{V(x)}\sqrt{V(y)}} \quad (15)$$

Where $COVR$ (x,y) in equation 15 is the Covariance between x and y and can be formulated using equation 16.

$$COVR(x,y) = \frac{1}{n}\sum_{i=1}^{n} E\left(\left(x_i - \mu(x)\right)\left(y_i - \mu(y)\right)\right) \quad (16)$$

Where, x and y are two adjacent pixels values in the image, V (x) is the variance of variable x and V (y) is the variance of variable y. The results obtained using equation 15 are tabulated in table 3 and table 4.

Secret Images	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
1. Bird	0.9551	0.9509	0.9277
2. Lena	0.8677	0.9391	0.8109
3. Baboon	0.8603	0.8825	0.8113
4. Cow	0.8258	0.9217	0.8051
5. Peppers	0.8834	0.9265	0.8201
6. Plane	0.9687	0.9014	0.885
7. Cameraman	0.9045	0.9454	0.8603
8. Baby	0.8654	0.8187	0.7622
9. Spine	0.8967	0.9495	0.8998
10. Knee	0.9364	0.979	0.9167

Table 3 : Correlation coefficients of two adjacent pixels in horizontal, vertical and diagonal directions for plain secret images.

Tabulated values in table 3 shows that the adjacent pixels are highly correlated (horizontally, vertically and diagonally) for original image which is almost nearer to value 1.

Encrypted Secret Images	Horizontal Correlation	Vertical Correlation	Diagonal Correlation
1. Bird	0.0028	-0.0078	-0.0004
2. Lena	0.0172	-0.0198	-0.0181
3. Baboon	0.0008	0.0273	-0.0248
4. Cow	0.0523	-0.007	0.0236
5. Peppers	0.0335	-0.0144	0.0312
6. Plane	0.0134	-0.022	-0.0282
7. Cameraman	0.0302	0.0086	0.0182
8. Baby	0.014	-0.013	-0.0435
9. Spine	-0.0149	0.0114	0.0051
10. Knee	-0.0021	0.0089	0.0058

Table 4 : Correlation coefficients of two adjacent pixels in horizontal, vertical and diagonal directions for encrypted secret images

Readings of table 4 tends to zero which reveals the non-prevalence of any relationship between the adjoining pixels of the encrypted image. Hence the proposed encryption scheme does not convey any meaningful visual information and difficult to break the algorithm. Different Correlations are shown in figure 9 by considering lena as secret image.

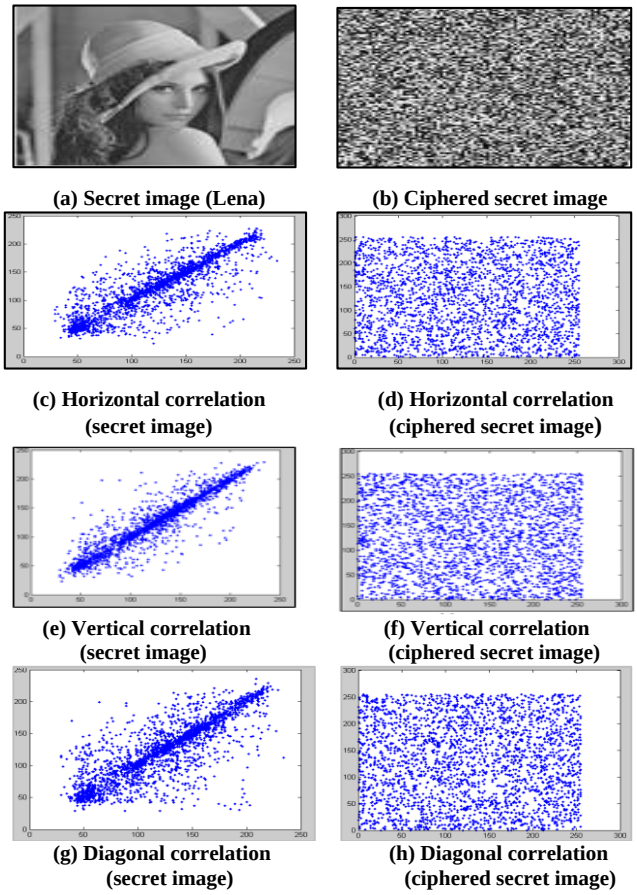
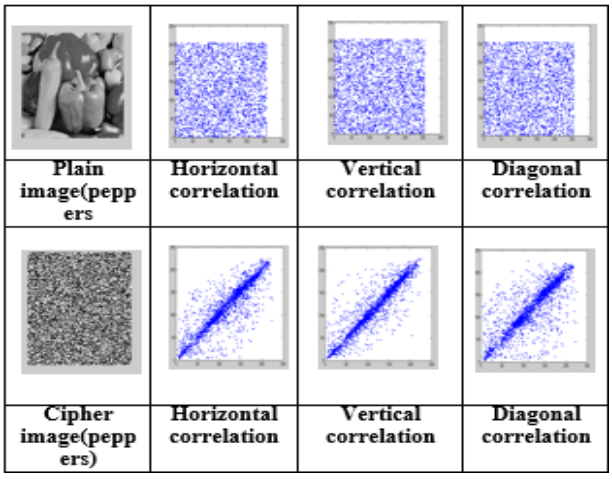


Fig. 9 : Different Correlations of secret image and ciphered image

Figure 10 shows correlations in horizontal, vertical and diagonal directions where x-axis represent correlation values and y-axis represent two adjacent pixel values in the image considering horizontally, vertically and diagonally. 60 test images are considered. For representation purpose, three images are shown namely peppers, lena and bird from top to bottom.



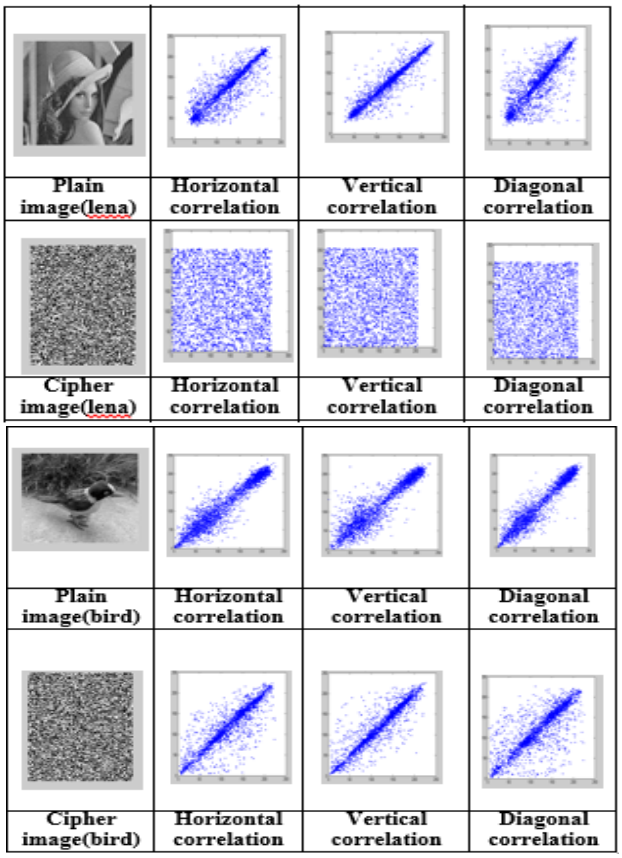


Fig. 10 : Horizontal, Vertical and Diagonal correlations for both plain and cipher images

D. Histogram Analysis

Histogram is a pictorial depiction of the pixel distribution of different intensities. A secure encryption scheme will have flat histogram and can resist statistical attack. It reveals that the significant region of the cipher image can resist statistical attacks. The plain image has spikes whereas the cipher image has no spikes in the histogram graph. All pixels are uniformly distributed. Hence the encrypted image cannot disclose the statistical information of the plain image to the intruder. Figure 11 shows the histogram of plain and encrypted images for cameraman image where x-axis denotes pixel intensity levels and y-axis represent number of pixels. Histograms of plain and cipher images (lena, plane, cameraman, MR_Cervical_vertibra and cow) are depicted in the figure 12 and figure 13. It has been observed that the pixels are uniformly distributed in figure 13(b). Therefore, it is hard to find any statistical information from these encrypted images.

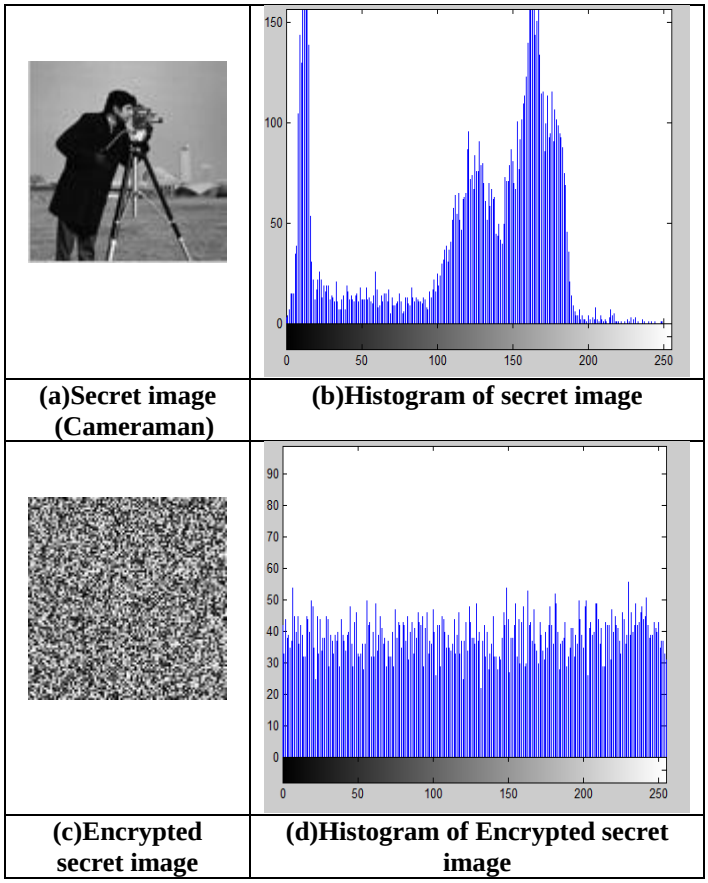


Fig. 11 : Histogram results in Encryption stage

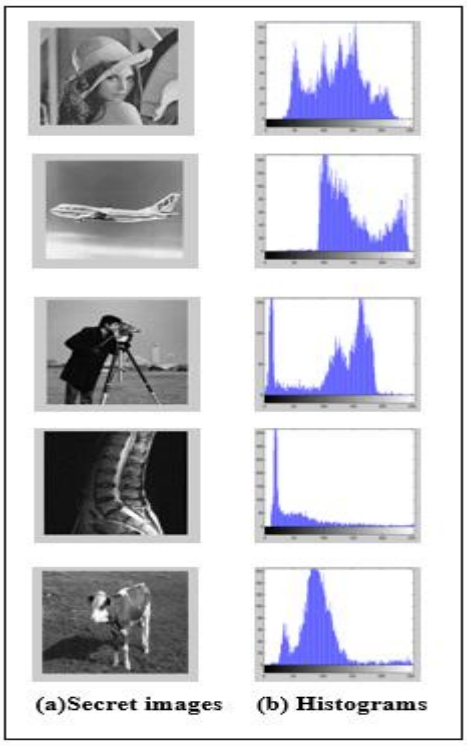


Fig. 12 : Histograms of secret images

(a) Secret images(lena, plane, cameraman, MR_Cervical_vertibra and cow)

(b) Histograms of secret images

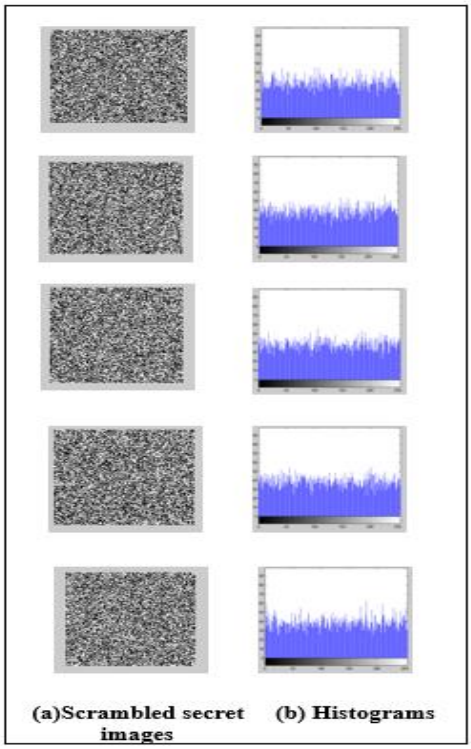


Fig. 13 : Histograms of scrambled secret images

(a) Scrambled secret images

(b) Histograms of scrambled secret images

2. Stego image formation

Stego image is obtained by embedding the encrypted secret image onto the transformed cover image. Table 5 shows the PSNR, MSE and Correlation results for variety of images with different combinations of cover and secret images.

Cover Image	Secret Image	PSNR (dB)	MSE	Correlation
Bird	Plane	64.415	0.023	0.999
Insect	cameraman	63.453	0.029	0.999
CT-Knee	Baboon	65.206	0.019	0.999
Lena	Boy	65.068	0.021	0.999
Flower	Peppers	64.585	0.022	0.999
Man	Bird	63.124	0.031	0.999
MR-Spine	Girl	64.464	0.023	0.999
Fruits	Cow	64.342	0.024	0.999
Galaxy	Mountain	64.751	0.026	0.999
Zelda	ship	64.755	0.021	0.999

Table 5 : PSNR, MSE and Correlation values in stego image formation process.

Figure 14 depicts the stages in stego image formation and secret image extraction in which scrambled secret image is embedded in transformed cover image to obtain stego image and the original secret image is been extracted by considering cover images as bird, insect, CT_knee, lena, flower, man, MR_cervical vertibra, fruits, galaxy and Zelda and corresponding secret images are Plane, cameraman, baboon, baby, peppers, bird, girl, cow, mountain and ship shown from top to bottom. The size of cover image and secret image chosen are 1024x1024 and 128x128 respectively. Table 6 shows the PSNR and MSE results for different secret images with **cover image as lena**. Table 7 shows PSNR and MSE results for different secret images with **cover image as plane**.

Cover Image = Lena			
Sl. No.	Secret Image	PSNR (dB)	MSE
1.	Galaxy	65.074	0.0202
2.	Zelda	65.083	0.0201
3.	Cameraman	65.074	0.0202
4.	Fruit	65.030	0.0204
5.	Bird	65.087	0.0201
6.	Army	65.075	0.0202
7.	Harbour	65.100	0.0200
8.	Barbara	65.095	0.0201
9.	Mountain	65.074	0.0202
10.	MR-Spine	65.046	0.0203

Table 6 : PSNR and MSE results with cover image as lena

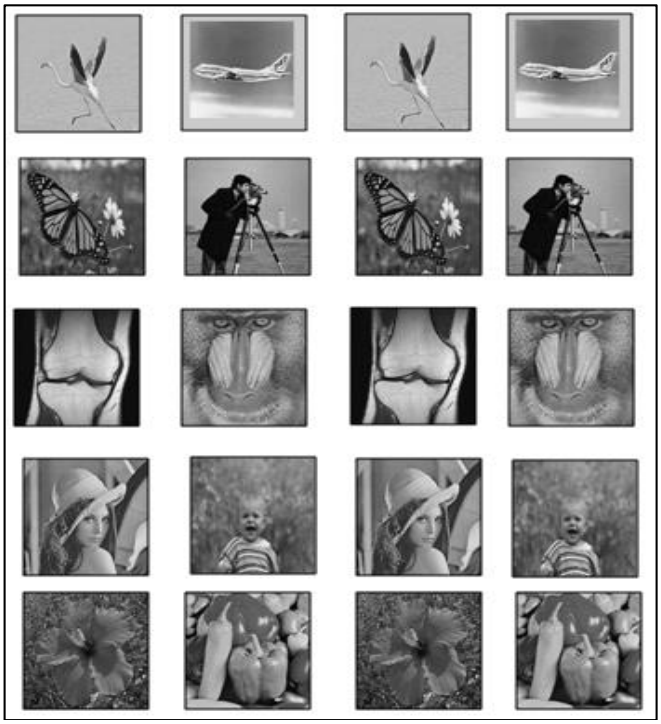


Fig. 14 : Stego image formation and extraction of secret image (a) cover images (b) secret images (c) stego images (d) Recovered secret images

Cover Image = Plane			
Sl. No.	Secret Image	PSNR (dB)	MSE
1.	Peppers	62.878	0.03351
2.	Baboon	62.868	0.03359
3.	CT-knee	62.876	0.03353
4.	Lena	62.880	0.03350
5.	Bird	62.884	0.03346
6.	Cow	62.883	0.03347
7.	Baby	62.879	0.03350
8.	Flower	62.879	0.03350
9.	Ship	62.865	0.00335
10.	Insect	62.884	0.03346

Table 7 : PSNR and MSE results with cover image as plane

3. Secret image extraction

Parameters say, PSNR, MSE, SSIM and Correlation is calculated to show the similarity between embedded secret image and extracted secret image. The values of MSE, PSNR, correlation and SSIM are shown in table 8 to justify this similarity. The test images chosen are plane, baboon, boy, peppers, barbara, bird and cameraman as shown in the figure 15 from top to bottom.

(a) **(b)**

Fig. 15 : Depicting the similarity between (a) secret image hidden inside the covered image and (b) the same secret image recovered from the stego image

MSE	PSNR	Correlation	SSIM
0	Infinity	1	1

Table 8 : Depicting the similarity between original secret image and extracted secret image

VI. Comparision Results of PSNR of proposed method with existing techniques

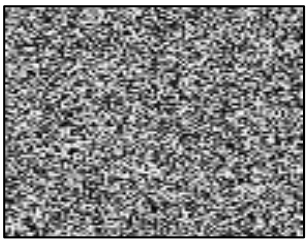
Reference of Existing Techniques	PSNR of Existing Techniques(dB)
[1]	49.23
[2]	43
[3]	37
[4]	46.27
[5]	54.3
[6]	52.2
[7]	49.5
[8]	64.5
[9]	56.9
[10]	55.9
[11]	32.46
[12]	54.34
[13]	50.48
[14]	43.23
[15]	46.86
[17]	48.27
[18]	49.32

Table 9 : PSNR results of Existing techniques

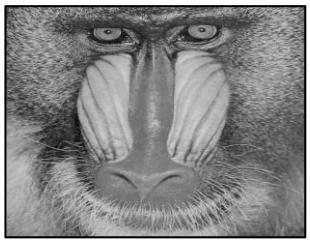
Table 9 gives the comparision results of PSNR of the proposed method with existing techniques which clearly shows that the proposed method achieves best PSNR results compared with existing techniques.

VII. The Complete stages of Encryption, Image Hiding and Decryption in the proposed system

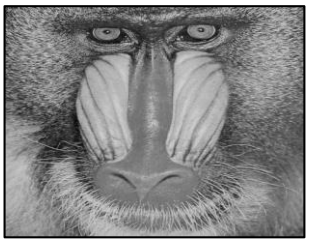
(a) Lena as Secret image



(b) Encrypted lena image



(c) Baboon as cover image



(d) Stego baboon image

(e) Decrypted lena image

Fig. 16 : Simulation results showing image encryption, hiding and decryption stages in the proposed system

Figure 16 depicts the Complete stages in the proposed algorithm employed in the proposed algorithm. (a) The secret image (b) is encrypted (c) baboon used as cover image (d) and same scrambled secret image is embedded in transformed cover image to obtain stego baboon image (e) and finally the original secret image, lena is decrypted and extracted from the stego image.

VIII. DISCUSSION AND CONCLUSION

Extensive analysis is carried out in terms of PSNR, histogram, correlations, entropy, and similarity metrics that proves the effectiveness of the proposed system in terms of high imperceptibility, robustness and security. From the simulation results and the readings tabulated, the proposed work achieves good PSNR, MSE, correlation and entropy values which is better than the existing work. It is hard to distinguish between two similar images (cover image and stego image) by human eyes when the PSNR is superior to 30 dB. From the table 5, 6 and 7, it is observed that the PSNR is above 30 dB by which the stego-image was obtained. A large PSNR value denotes that the stego image is almost similar to original image. From table 4, the correlation values for ciphered secret images is almost nearing to zero from which the interceptor can hardly make any kind of relationship between the pixels to break the algorithm. The confusion process used in encryption stage can change the histogram of the image, so it is difficult for attackers to do any statistical analysis because the histogram is changed greatly after confusion. The block diffusion method which is deployed in the encryption stage is extremely efficient and able to obtain the values of entropy nearly equal to 8. Hence the proposed algorithm can be used as a reliable data encryption approach. Also introduced good visible quality in stego image that led to the best secret image imperceptibility inside the transformed cover image by the implementation of LSB and DWT techniques in image hiding stage. The blend of chaotic image encryption with image hiding contributes to the achievement of robustness with high sensitivity. Overall the proposed system contributes to achieve high robustness with security.

IX. FUTURE WORK

Development of the proposed work can be extended to hide other forms of information such as audio and video. Also the performance can be measured using additional parameters with respect to different analysis techniques.

X. REFERENCES

[1] Giovani Ardiansyah , Christy Atika Sari,“Hybrid Method using three DES, DWT and LSB for Secure Image Steganography Algorithm”, 2017, 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE).

[2] Sujarani Rajendran, “A Chaos Based Double Layer Secure Data Hiding In Confused Image”, International Journal of Pure and Applied Mathematics, Volume 117 No. 16 2017, 517-524 ISSN: 1311-8080.

[3] Iman I. Hamid, “Image Steganography Based on Discrete Wavelet Transform and Chaotic Map”, International Journal of Science and Research (IJSR) ISSN, 2015.

[4] Jinan N. Shehab, Hussein A. Abdulkadhim, “Image Steganography Based on Least Significant Bit (LSB) and 4-

Dimensional Lu and Liu Chaotic System", 2018, International Conference on Advanced Science and Engineering (ICOASE).

[5] Yani Parti Astuti, De Rosal Ignatius Moses Setiadi, Eko Hari Rachmawanto, Christy Atika Sari, "Simple and Secure Image Steganography using LSB and Triple XOR Operation on MSB", 2018 International Conference on Information and Communications Technology (ICOIACT).

[6] Vijay Kumar Sharma, Devesh Kumar Srivastava, Pratistha Mathur, "Efficient image steganography using graph signal processing", IET Image Process., 2018, Vol. 12, Iss. 6, pp. 1065-1071.

[7] Prabakaran. G, Bhavani.R, "A Modified Secure Digital Image Steganography on Discrete Wavelet Transform", 2012 International Conference on Computing, Electronics and Electrical Technologies [ICCEET].

[8] Shivani Chauhan, Jyotsna, Janmejai Kumar, Amit Doegar, "Multiple layer Text security using Variable block size Cryptography and Image Steganography", 3rd IEEE International Conference on "Computational Intelligence and Communication Technology", 2017.

[9] Kamaldeep Joshi, Rajkumar Yadav, "A New LSB-S Image Steganography Method Blend with Cryptography for Secret Communication", 2015 Third International Conference on Image Processing.

[10] Amritpal Singh, Harpal, "An Improved LSB based Image Steganography Technique for RGB Images", IEEE, 2015.

[11] Soni, Jain, Roshan, "Image steganography using discrete fractional Fourier transform," Intelligent Systems and Signal Processing (ISSP), 2013 International Conference on image processing, 2013.

[12] Akhtar.N, Johri.P, Khan.S, "Enhancing the Security and Quality of LSB based Image Steganography", 5th International Conference on Computational Intelligence and Communication Networks (CICN), 2013.

[13] Das R., Tuithung T., "A novel steganography method for image based on Huffman Encoding", 3rd National Conference on Emerging Trends and Applications in Computer Science (NCETACS), 2012, on March 2012.

[14] Hemalatha S.; Acharya U.D.; Renuka A.; Kamath P.R., "A secure image steganography technique using Integer Wavelet Transform", World Congress on Information and Communication Technologies (WICT), 2012.

[15] Prabakaran G., Bhavani R., Rajeswari P.S., "Multi secure and robustness for medical image based steganography scheme", International Conference on Circuits, Power and Computing Technologies (ICCPCT), 2013.

[16] Thenmozhi S., Chandrasekaran M., "Novel approach for image stenography based on integer wavelet transform", IEEE International Conference on Computational Intelligence & Computing Research (ICCIC), 2012.

[17] Reddy H.S.M., Sathisha N., Kumari A., Raja K.B., "Secure steganography using hybrid domain technique", Computing Communication & Networking Technologies (ICCCNT), Third International Conference, 2012.

[18] Masud Karim, S.M. Rahman, M.S. Hossain, "A new approach for LSB based image steganography using secret key," Computer and Information Technology (ICCIT), 2011 14th International Conference on , Dec. 2011.

[19] C R Revanna, C Keshavamurthy, "A New Selective Document Image Encryption Using GMM-EM and Mixed Chaotic System", International Journal of Applied Engineering Research ISSN 0973-4562, Volume 12, (2017).

[20] Jacques M. Bahi, Jean François Couchot, Nicolas Friot, and Christophe Guyeux, "A Robust Data Hiding Process Contributing to the development of a Semantic Web", 2017.

[21] Adnan Gutub and Nouf Al-Juaid, "Multi-bits stego-system for hiding text in multimedia images based on user security priority", Journal of Computer Hardware Engineering, 2018.

[22] Anandkumar R, Kalpana R, "Analyzing of Chaos based Encryption with Lorenz and Henon Map", 2nd International conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), 2018.