International Journal of Engineering Science Invention (IJESI)
ISSN (Online): 2319 – 6734, ISSN (Print): 2319 – 6726
www.ijesi.org ||Volume 7 Issue 8 Ver IV || Aug 2018 || PP 22-31

A Steganocryptographic Algorithm Using 3 Level Dwt Steganography And Eacc Encryption

Manjula.Y[1], Dr.K.B.Shiva Kumar[2]
[1](Department of ECE, SSIT,SSAHE, India)
[2](DepartmentTCE, SSIT,SSAHE, India)
Corresponding Author: Manjula.Y

Abstract: *Now a days comprehensive investigation of data hiding techniques is gaining huge importance .The internet has become a unreliable communication medium which enables people to communicate in unsecured network. So securing the communication medium became the important factor. There are different data hiding techniques elaborated by different authors. Glancing through the new emerging techniques and approaches on data hiding, improvisation in the techniques may enhance the security in open channel network .The confidential and integral data requires protection from unauthorised access. In the proposed paper, ECC technique is used for encryption of data with the help mapping technique and steganography uses 3 level DWT technique which are unpredictable to outside observers. Visual Cryptography (VC) is also applied which is a special technique in visual objects like images to hide data in which decryption is done by Human Visual System (HVS) only .The proposed method's performance is checked for the robustness to different types of attacks . Simulation results enhanced the security of data with low time complexity.*

Keywords *-ECC encryption,DWT steganography, Mapping technique ,Visual cryptography*.

Date of Submission: 09-08-2018 Date of acceptance: 23-08-2018

I. Introduction

Data security is one of the most major concerns in today's world. The misuse of information in the Internet requires high data security in the process of exchanging information through open channels. The confidentiality and integrity of data requires protection from unauthorized access has led to tremendous growth in the field of data hiding. Cryptography is used widely for converting the information into cipher and steganography is widely used technique that hides information existence itself. Image, audio and video are digital data which are used as cover in technical steganography. Information hiding via image is the most popular technique due to large exchange of information on the Internet is through the images, also it looks common and unsuspicious after the embedding process. The social media is the one that deal with the secrecy of information over open channel network. Cryptography is the science of writing the secret code. The secret information is identified and processed only by the intended person. Generally, the cryptographic techniques are classified into two categories: symmetric ciphers and asymmetric ciphers. Symmetric ciphers is based on the size of the key and the same key is used to encrypt and decrypt data .Asymmetric ciphers consist of two different keys which are used for encryption and decryption ,one is the public key and private key. The science of hiding the secret code in other data without knowing about its existence is called steganography. The hacker cannot identify presence of secret message in an image.

II. Literature Survey

K.S. Seethalaxmi et al,[1] proposed the combination of visual cryptography and image steganography techniques for data security enhancement. During encryption visual cryptography technique is used and decryption uses human visual system. The parameters considered are PSNR, MSE and size.

DipanwitaDebnath et al, [2] proposed the steganography method for spatial domain which includes mapping technique and algorithm converts all kind of message to text using bit manipulation tables. The parameters considered are MSE, SC, AD, MD, NAE and histogram.

Ahmed.MElshamy et al, [3] proposed the optical image encryption based on chaotic baker map and Double Random Phase Encoding (DRPE) techniques. These techniques are implemented in two layers. The parameters considered are MSE, PSNR and timing analysis.

MoreshMukhedkar et al, [4] proposed the combination of image encryption and image hiding. The image encryption uses blowfish algorithm and for image hiding LSB technique is used and the parameters considered are PSNR and MSE.

Xinyi Zhou et al, [5] proposed the combination of steganography and cryptography techniques. The LSB technique is used for data hiding and human eye visual features, digital signature for personal identity authentication, encryption techniques are used to enhance the security of the hidden data. The parameters considered are PSNR and MSE.

PunamBedi et al, [6] proposed a 2L-DWT steganography technique. The image is embedded in the higher frequency components and low frequency components are left untouched. The images used in this techniques are monochrome, colored BMP and JPEG images with high capacity. The parameters considered are MSE, PSNR, NC, NCC, NAE and IF.

Palak Mahajan et al, [7] proposed a steganography technique. The cover image is transformed from spatial domain to frequency domain using 2 DWT. The Huffman encoding technique is used to compress the secret image. The secret image massage bits are randomized using RC4 algorithm. The parameters considered are PSNR and MSF.

Palak Patel et al, [8] proposed the combined cryptography, steganography and digital watermarking techniques. During encryption RSA technique is used and the encrypted watermark logo hidden inside secrete image using DCT technique. The stego image is hidden inside cover image using DWT and SVD techniques. The parameters considered are efficiency and hiding capacity.

Khalid. A. Al- Afandy et al, [9] proposed the LSB steganography and image cropping techniques. The secret co-ordinate crops are extracted from cover image. The secret massage is embedded into image crop using LSB technique. The parameters considered are PSNR, MSE and CPU time.

SuchiGoyal et al, [10] proposed an 1-2-4 LSB steganography and RSA cryptography techniques. Image encryption used RSA technique and1-2-4 LSB is applied on the RGB image. For gray image LSB technique is applied to detect edges. The parameters considered are PSNR and MSE.

Dalia Baughali et al, [11] proposed the combination of stochastic local search meta-heuristic (SLS) and LSB techniques. Meta-heuristic approach is added to LSB technique with hybridized local search (LS) technique. The LSB technique is improved by combining with SLS which is implemented on JPEG image. AES algorithm is used to generate key and for image encryption. The parameters considered are MSE and PSNR.

Jakuboravec et al, [12] proposed the mojette transform to modify the binary image containing secret code. The modified image is embedded into cover image using LSB technique. The parameters considered are PSNR and MSE.

Truptipatel et al, [13] proposed the hierarchical visual cryptography technique. Where grayscale image is converted to binary image and encrypted to form shares. At the decryption side all shares are superimposed to reveal the secret image. The generated shares are in grayscale format not in binary format and the decrypted image has same size as original image.

R. Tavares et al, [14] proposed the LSB word-hunt (LSB WH) technique. The LSB WH technique reduces the Expected Number of Modifications Per pixel (ENMPP) and operates in the spatial domain of digital image. The parameters considered are PSNR, NMPP and MSE.

Md. Rashedul Islam et al, [15] proposed bitmap image to implement LSB steganography method. The AES cryptography technique is used for image encryption. The bitmap image uses filter based algorithm which uses MSB bit for filtering. The parameters considered are PSNR and MSE.

Sabyasachi Kamila at el, [16] proposed the steganography technique in frequency domain, where DWT technique is used to differentiate between high and low frequency components of each pixel of the image and the secret data is hidden in three higher frequency components. The parameters considered are MSE, PSNR and Structural Similarity (SSIM).

Hamad A. Al-Korbi et al [17] proposed steganography technique where binary image, color image and large text files are embedded in the single cover image using Haar wavelet transform. The parameters considered are MSE, PSNR, efficiency, performance and capacity.

Rupendra Kumar Pathak et al, [18] proposed the LSB steganography technique, where LSB bit of the cover image pixels are replaced by the MSB bit of data image pixels. Pseudo Number (PN) sequence is generated based on key used. The GCD (Gaussion convolution and deconvolution) transform is used for conversion of image into fixed point image. The parameters considered are PSNR and MSE.

Ayushiverma et al,[19] proposed an algorithm on hiding the secret image bits to the 2 level DWT based LL2 block of cover image. The drawback of this algorithm is the quality of reconstructed image is very low.

III. System Design

Elliptical curve cryptography (ECC) is a public key encryption technique based on elliptic curve theory which is used to create faster, smaller, and methodical cryptographic keys. ECC produce keys via properties of the elliptic curve equation behalf of traditional method production as the product of very large prime numbers. Research says that, ECC can yield the level of security with a 164-bit key compared to other systems which require a 1,024-bit key to achieve. ECC establishes counterpart security with lower computing power and

battery resource usage, it is customary in mobile applications. ECC is a public key cryptosystem; it is having a public key and a private key in pair. Public key is shared between the groups of users who participate in the communication, while the private key is kept confidential.

Discrete Wavelet transform (DWT) is used in decomposing an image. Wavelet transform imparts both frequency and spatial description of an image. The areas in the cover image are discerned by Discrete Wavelet Transformation in which secret image is embedded successfully. The DWT bifurcate the signal into low and high frequency parts which contain coarse information of signal and information about the edge component respectively. In case of two dimensional applications, during each level of decomposition DWT is first performed in the vertical direction followed by horizontal direction. After the first level of decomposition, there are 4 sub-bands: LL1, LH1, HL1, and HH1. In each sequential level of decomposition, the LL sub band of foregoing level is used as input. To perform DWT decomposition LL1 and LL2 is applied as input on 2 levels and 3 level respectively. At the end, 4 sub bands of 3 levels are LL3, LH3, HH3, and HL3.

The proposed method is shown in figure 3.1 ,Encryption uses ECC technique to encrypt secret message. 3 level DWT steganography is applied on cover image. High frequency coefficients embed secret encrypted message with the preferred pseudo random numbers. Stego image is obtained by performing 3 level inverse DWT. The visual cryptography technique is used to split stego image into two shares i,e. stego share1 and stego share 2

The cover image is delivered at the receiver end. The visual cryptography technique is applied by integrating the stego share 1 and stego share 2, then the stego image is decrypted to obtain secret image. The mean correlation values of DWT coefficients of both images are compared and the encrypted secret image is reconstructed. ECC technique is used on encrypted data and the secret image is recovered.

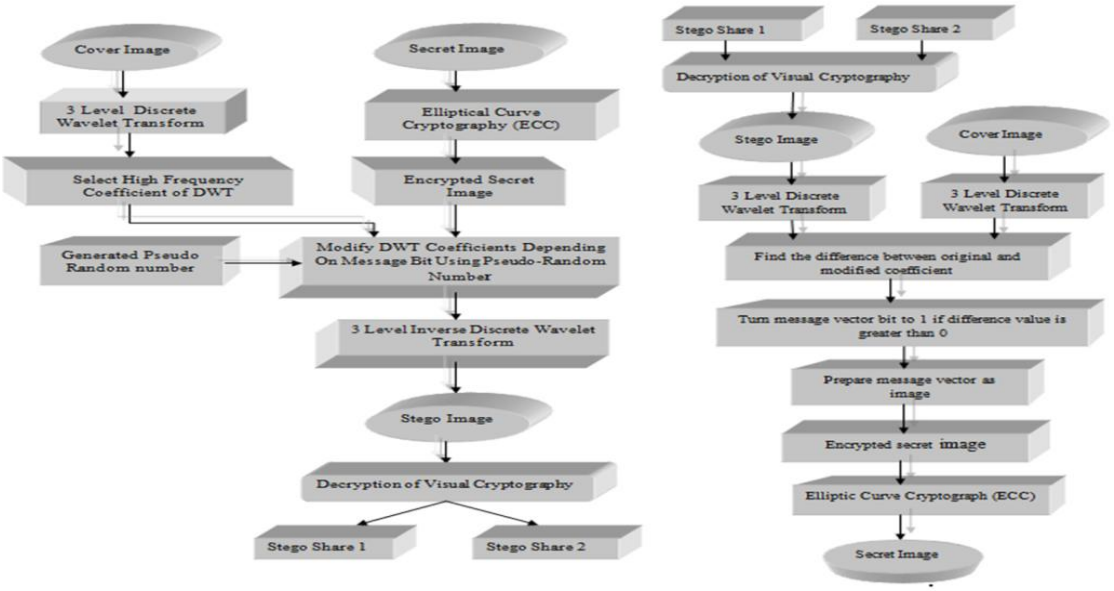

Fig 3.1. Block diagram of proposed method, Sender end and Receiver end

IV. System Implementation

4.1 Elliptic Curve Cryptography (ECC)

The cubical equation of the elliptical curve is obtained by (1):

$$y^2 = x^3 + ax + b \quad (1)$$

*a*and *b* are integers which satisfy (2) and *p* is a large prime number. Fig. 4.1 shows an elliptic curve over the real field **R** and how to add points on an elliptic curve:

$$4a^3 + 27b^2 \neq 0 \ (\text{mod } p) \quad (2)$$

Alice and Bob encrypt a message by deciding on an elliptic curve and take an affine point (G) that lies on the curve. The point P_M is encoded by plain text M. Alice and Bob chooses a random prime integer *x* and *y* respectively. Alice's private key is *x* and Bob's private key is *y*.

To generate the public key,Alice computes (3):$P_A = xG$ **(3)**

Bob Computes (4): $P_B = yG$**(4)**

Alice chooses a random integer named *k* to encrypt the message point P_M for Bob. It uses Bob's Public key (P_B) to compute the encrypted message P_C. P_C is a pair of points :

$P_C = [(kG), (P_M + kP_B)]$ **(5)**

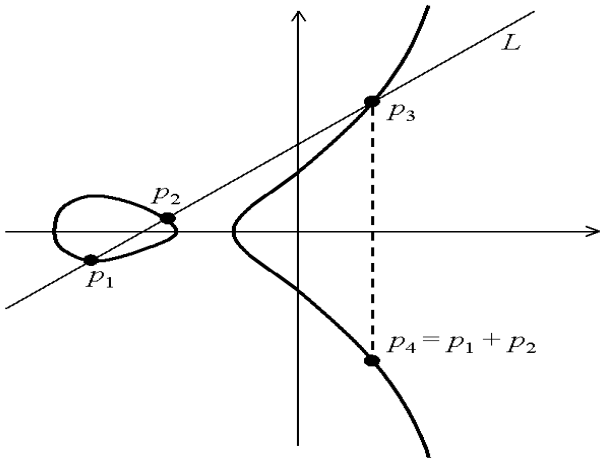

Fig.4.1 Graph of an elliptic curve

Bob receives P_C as a cipher message from Alice. Bob, receives the encrypted message P_C and uses his private key *y* to multiply with *kG*and adds the second point in the encrypted message to compute P_M, which corresponds to the plaintext message M:

$P_M = (P_M + kP_B) - [y(kG)$ **(6)**

For two points *P* and *Q* over an elliptic group the addition operation, if $P+Q = (X_3, Y_3)$ is given by (7) and (8)and the parameter λ is calculated by (9):

$X_3 = \lambda^2 - X_P - X_Q \bmod p$ **(7)** $Y_3 = \lambda (X_P - X_3) - Y_P \bmod p$ **(8)**

$$\text{where } \lambda = \begin{cases} \frac{Y_Q - Y_P}{X_Q - X_P} \; if \; P = Q \\ \frac{3X_P^2 + a}{2Y_P} \; if \; P \neq Q \end{cases} \quad \textbf{(9)}$$

Multiplication of *k P*ower an elliptic group is computed by repeating the addition operation *k* times by (7) and (8). The difficulty of finding the number of times that G is added to itself to get P_A decides the strength of an ECC-based cryptosystem. The reverse operation known as Elliptic Curve Discrete Logarithm Problem (ECDLP) is exploited in cryptography.

4.2 Mapping Methodology

Each image is composed of pixels. Each pixel of grey scale image has an 8-bit value between 0 and 255 and each pixel of color images are elucidated by three 8-bit values separately which signifies the Red, Green and Blue intensities .The pixel is considered as a message and mapped to a point on predefined elliptical curve during encryption of an image. Map table uses mapping method. From the Fig 4.1 , construct map table, the elliptic group E_p *(a, b)* which consists of all possible points on the finite field are generated and then these points are grouped into 256 groups. Each group has $N = \#(f_p)/256$ members. The row indexes start from 0 and end with 255. There are multiple points for same value and each row stands for pixel intensity. The extra rows in the last column are filled with zero if N is not a multiple of 256 and the last column will be interpreted for mapping. The corresponding point with the intensity value in the table is mapped to the first pixel in a plain image and continues to the last pixel. The next point in the corresponded row will be selected for repetitive intensity values. If all *N-1* points are selected for any of the intensities then the following one again starts from the first point. Encryption is done using receiver's public key after mapping all pixels to associated points on the table. Encryption of a point results into set of two points. In which one point is same for all pixels and the other point is different for each pixel. Result can be demonstrated as an image after encrypting all pixels .The encrypted point is viewed as an image by referring to the mapping table which finds the current index according to each point and replaces with the related value.Let both the sender and receiver decide on elliptic curve $E_{751}(-1,188)$ that is represented by:

$y^2 \bmod 751 = x^3 - x + 188 \bmod 751$ **(10)**

The generated points are also shown in Fig.4.2 The mapping table is created by placing the first point in row1 which is associated to pixel with intensity value of 0, and then it is continued with next point for next values. The first 256 points will be placed in first column of the table and next 256 points will be place in second column and here after continues to do the same for next points till the last. There are 727 points on the curve in this example. The 2nd column and 214 rows of 3rdcolumn are completely filled by these points. The last rows of the remaining columns are filled with zero. According to (1) and (2), some parameters should be defined to encrypt this image. A random integer is defined via sender by choosing G = (0, 376) as a generator point, $y=85$ as receiver private key and $k=6$. After having these values, according to (4), the receiver's public key is calculated and the result is: P_B= (671,558).

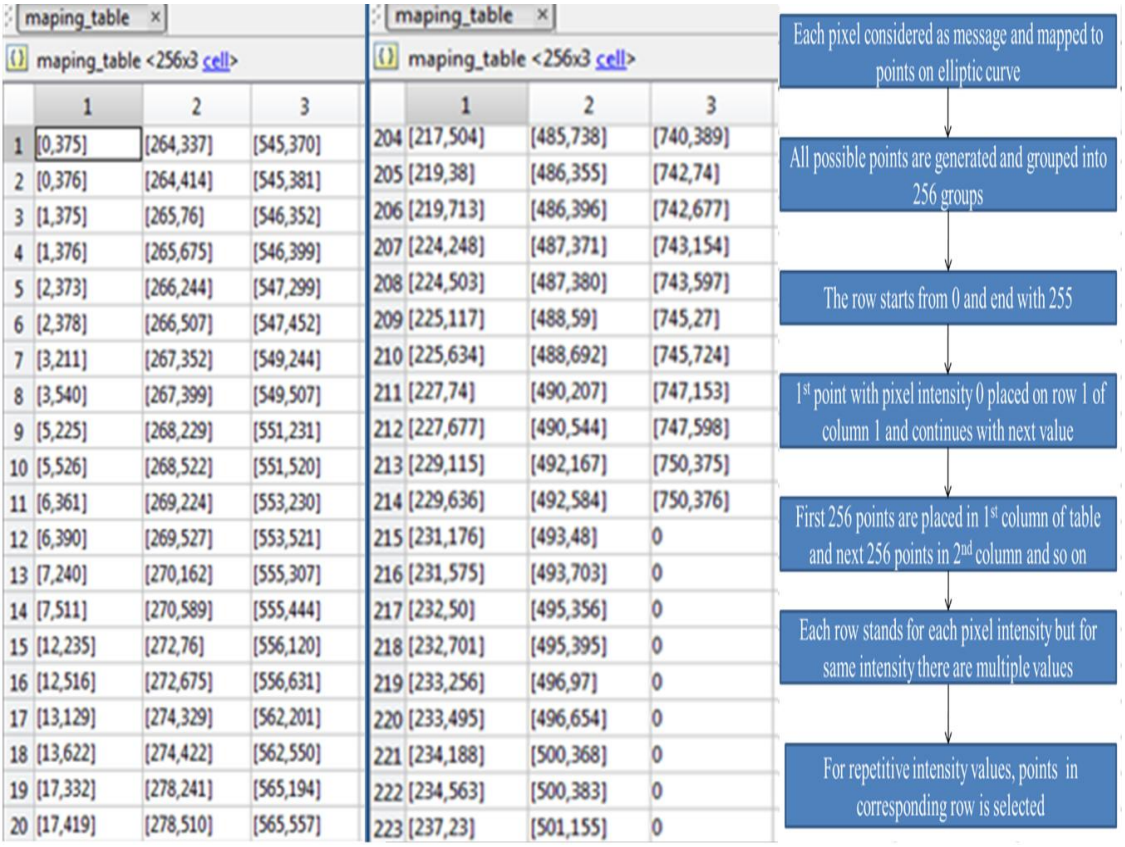

Fig.4.2points generated by using the mapping methodology

4.3 Discrete Wavelet Transforms (DWT)

The applications of Wavelet Transform (WT) include signal processing due to its discrete and multi-resolution nature. The signal is decomposed into a set of basic functions by wavelet transform. The wavelets are basic functions.

The "mother wavelet" is most elementary waveform which is denoted by ψ (t). Each high frequency sub-band is explained by translating the specific scaling parameter into a set of versions. The "father wavelet" (or scaling function) is another elementary waveform denoted by φ (t) which explains each low frequency sub-band by translating set of versions.

Continuous Wavelet Transform (CWT) and Discrete Wavelet Transforms (DWT) are the two ways in which wavelet transform is carried out. In CWT, mother wavelet creates wavelets by dilations and shifting which is also known as single prototype wavelet. The filter bank is used to analyze and rebuilt signals in discrete wavelet transform. Multi-resolution analysis (MRA) is the main feature of DWT which analyzes the signal at different frequencies giving different resolutions.

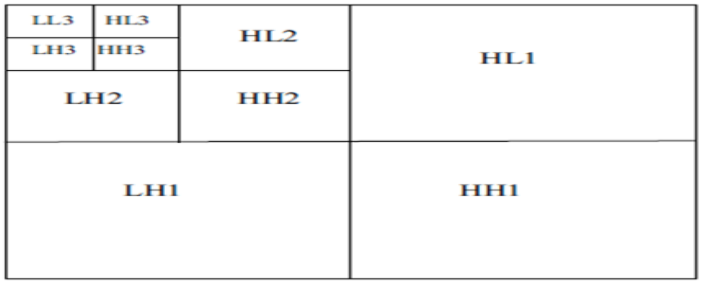

Fig.4.3 3 level discrete wavelet transform

Haar, Daubechies, Coiflet, and Legendre are the different types of wavelet transforms. Haar wavelet transform is applied here which is the oldest form of wavelet transform. Haar wavelet is the compact, dyadic and orthonormal wavelet transform. The high-pass decomposition filter which is dilated and reflected from mother wavelet by scaling function is used for Haar Wavelet Transform and is given by:

$$\varphi(x) = \begin{cases} 1, \text{ if } 0 \le x < 1 \\ 0, \text{ otherwise} \end{cases} \quad (11)$$

The Haar wavelet's mother function is defined by: $\psi(x) = \varphi(2x) - \varphi(2x - 1)$ (12)

The Haar wavelet transform can be decomposed into two stages. First step and next step is along the x-axis and y-axis respectively. We can apply fast wavelet transform for each axis. The 2D signal (here image) is divided into four bands as shown in fig 2: LL (left-top), HL (right-top), LH (left-bottom) and HH (right bottom) .The HL band and LH band signifies variation along the x-axis and y-axis respectively. The LL band is more condensed and consist more approximation details of the signal.

4.4 Visual Cryptography

Visual Cryptography (VC) is a special technique used in visual objects like images to hide data in which decryption is done by Human Visual System (HVS) only. The decoding doesn't require any computing machine. In the proposed system, an image can be sliced into n shares which demonstrate a visual secret sharing technique. The decoding of secret message is done by some predefined set of participants who bag all the n shares. This scheme was modelled as ,k out of n secret sharing problem or (k, n) problem. The working of this technique is demonstrated as follows: Each single pixel is split into sub-pixels. If a monochrome image is taken as a source image, the pixels of the image are either black or white when a monochrome image is taken as source image. Each pixel can be subdivided into 4 sub-pixels in '2 out of 2' scheme.

Fig 4.4 horizontal shares, vertical shares and diagonal shares of visual cryptography

V. Results

5.1 Encryption technique results

The inputs for the encryption technique is cover image and secret image. The secret image can be of any size which is converted into gray scale image and resized to 80x80. The image is encrypted using ECC technique. The secret image and the encrypted imageis shown fig 5.1

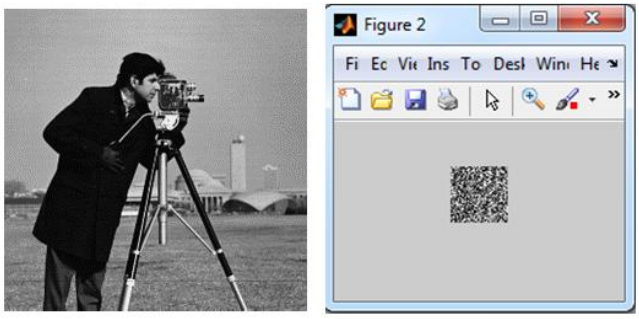

Fig 5.1 The Secret image and Encrypted image

The cover image is also a color image of any size, which is converted into gray scale image and resized in 2048*2048. The cover image is the carrier image which undergoes 3 level Discrete Wavelet Transformation (DWT) . The higher frequency coefficient HH2 of DWT is selected for embedding of encrypted secrete image. It is done by modifying the DWT coefficients depending on the message bit using pseudo random numbers. Then 3 level inverse DWT technique is applied to reconstruct the carrier image . The stego image is obtained. The visual cryptography technique is applied to the stego image and the stego image split into stego share1 and stego share2 respectively, which are transmitted through open channel network.

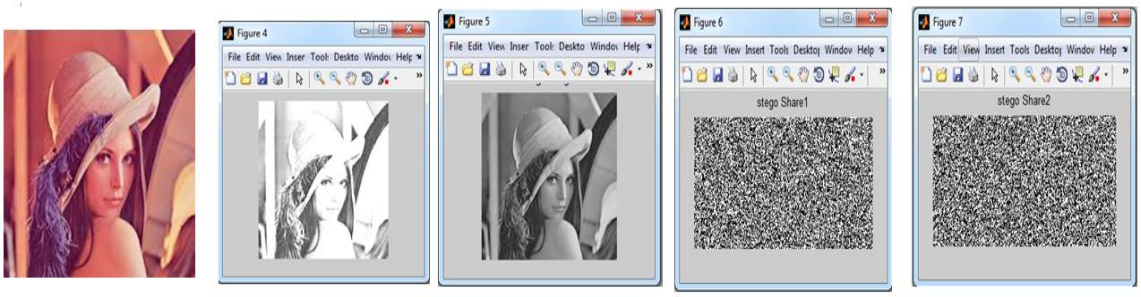

Fig 5.2 Coverimage, 3 level IDWT output, stego image, stegoshare 1and stegoshare 2.

5.2 Decryption technique results

During decryption technique both stego share1 and stego share2 are combined and visual cryptography technique is applied to obtain the stego image.

3 level DWT technique is applied to stego and cover image. The difference between original and modified coefficients are funded out. If the difference value is greater the zero then message vector bits are turned to one. Message vector bits are prepared to form encrypted image and ECC technique is applied to recover the secret image.Figure 5.3 shows the visual cryptography output, recovered encrypted image and recovered secret image.

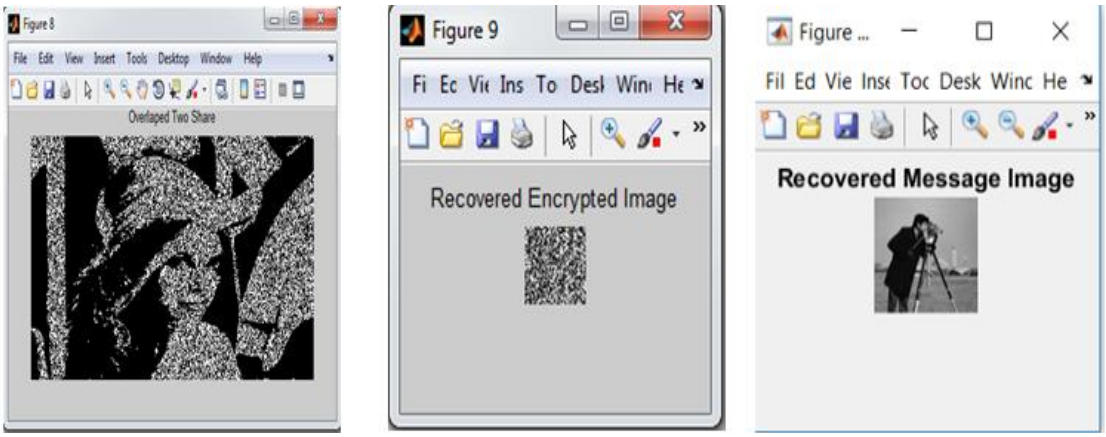

Fig.5.3 visual cryptography output, recovered encrypted image and recovered secret image.

VI. Security Parameters

Security analysis of combined hybrid steganocryptographic process is an essential processes to ensure the strength of the technique. The analysis is done through evaluating various parameters in this section.

6.1 Mean Square Error (MSE)

Poor quality Stego image is produced if embeded secret message has MSE has higher value. The MSE can be calculated as :

$$\textbf{MSE} = \frac{1}{M*N}\sum_{Y=1}^{M} \sum_{Y=1}^{N})][\boldsymbol{x(m,n)} - \boldsymbol{y(m,n)}]^2 \qquad \textbf{(13)}$$

6.2 Peak Signal to Noise Ratio (PSNR)

Higher PSNR value indicates the proposed algorithm produced good quality stego image. The PSNR can be calculated as :$\textbf{PSNR= 20log}_{10}\textbf{[MAXPIX/RMSE]} \qquad \textbf{(14)RMSE=}\sqrt{\boldsymbol{MSE}} \qquad \textbf{(15)}$

6.3 Entropy

Entropy gives uncertainty present in the cipher image .If the entropy of the cipher image is high, image has high randomness and high confidentiality.

The entropy can be calculated as: $$H(K) = \sum_{i=1}^{n} p_r(K_i) \log p_r(k_i) \quad (16)$$

Where k is the collection of pixels, $k_i$is the i^{th} value of k ,$P_r(k_i)$ is the probability of k_i,.
Ideal value of entropy is 8, which means that the probability of accidental information leakage is very small .If the entropy of the cipher image is high, image has randomness and high confidentiality.

VII. Experimental Summary

Based on above discussed formulae, various pair of images are compared. PSNR values and correlation valuesare compared for the five cases with varied set of sizes of cover and payloads in Table . The proposed method has two techniques, one is stenographic technique andsecond, cryptographic technique and that is the reason PSNR is calculated twice.

7.1 Analysis of proposed method

The PSNRs and correlation between stego and carrier images for different images are shown in Table 7.1
Table shows the values of PSNRs presenting the comparison between

A. Original cover image and stegoimage
B. Payload and retrieved payload

TABLE7.1 PSNRS OF DIFFERENT IMAGES

THE SECRET IMAGE IS OF SIZE 80*80 AND COVER BLOCK SIZE 256*256				
		PSNR BETWEEN		
SECRET IMAGE	COVERIMAGE	A.STEGO AND CARRIER	B. PAYLOAD AND RETREIVED	CORRELATION
BOAT	BABOON	46.5492	54.278207	0.99607
EINSTEIN	CAMARAMAN	54.675359	49.922944	0.999971
BARBARA	LENA	46.29	45.877	0.999739
GIRL FACE	PEPPER	46.1898	INFINITY	0.99976
SUN	EINSTEIN	61.5084	38.6289	0.9985

First part of the table results the quality stego image compared to original cover image with good PSNR values, whereas the second part ,results fair enough PSNR values for recovered payload compared to original payload after going through ECC encryption, steganography and visual cryptography. Also the structural content of the payload image is preserved with the recovered which is main objective of the hiding techniques.
In paper [19] the author hides the secret image in carrier image 2 level DWT coefficients. He has taken the similar size images as discussed the proposed method figure 7.2. From Table 7.2, when compared to the proposed method PSNR values the drawback of the paper was PSNR values are very small which reduce the quality of recovered message from original pay load image,

	Cover block size	Payload size
case1	256*256*8	32*32*8
case2	256*256*8	40*40*8
case3	512*512*8	64*64*8
case4	512*512*8	80*80*8
case5	512*512*8	90*90*8

Fig .7.2 five cases for various set of sizes of cover and payload

Table 7.2 Psnr Values For Those Set Of Five Cases

Comparision between cover and stego image

PSNRS FOR STEGO AND COVER IMAGE FOR THE ABOVE CASES

Cover Image	case1	case2	case3	case 4	case5
lena	41.75	41.71	47.496	47.429	47.388
areo	42.06	42.04	46.7959	45.848	46.1328
pepper	43.17	43.135	46.259	46.1898	46.1328
einstein	49.9236	48.839	61.912785	61.50602	61.2132

Comparision between payload and retrieved pay load

PSNRS FOR PALOAD AND RETREIVED IMAGE

Cover image	case1	case2	case3	case 4	case5
lena	46.917	48.302	45.8427	47.66864	47.3887
areo	37.984	34.405	45.84	47.86	46.94
pepper	48.302	48.302	48.84	47.66	46.94
einstein	48.302	48.302	48.84	47.66	46.94

7.2 Analysis of proposed method by comparison with existing technique

In paper [21] the algorithm is applied on bmp image of Lena with 256 colors which is resized to 20*20 block size to evaluate the impact of algorithm on entropy and correlation and the values are shown in figure 7.3.

chniques	**rrelation**	**tropy**	**ne elapse**
lcipher	**437**	**129**	**58**
ine Hillcipher	**242**	**003**	**93**
Hillcipher	**052**	**415**	**7.53**
Hill Cipher	**98**	**825**	**52**
Hill Cipher	**976**	**935**	**89**
pposed Method	**163**	**75397**	**27206**

Fig 7.3 Results of correlation and entropy values.

Considering the same image of Lena, the effect of impact factor on entropy and correlation factor is evaluated by the proposed algorithm. In figure 7.3, Entropy comparison for encrypted image using different algorithms are shown. Entropy is maximum for proposed method which shows the randomness of encryption algorithms.

Also for lena image which has the correlation coefficient of value 0.6136, calculated by using the standard formula[21] :r $= \dfrac{n\sum xy - \sum x \sum y}{\sqrt{\{[n\sum x^2 - (\sum x)^2][n\sum y^2 - (\sum y)^2]\}}}$ (17)where n is the number of pair of image ,x and y are values of two adjacent pixels in the grey image.

when correlation values are compared to paper[21] values in figure 7.3, the proposed algorithm is having the lowest value which indicates the high randomness with in the pixels in the cipher image .

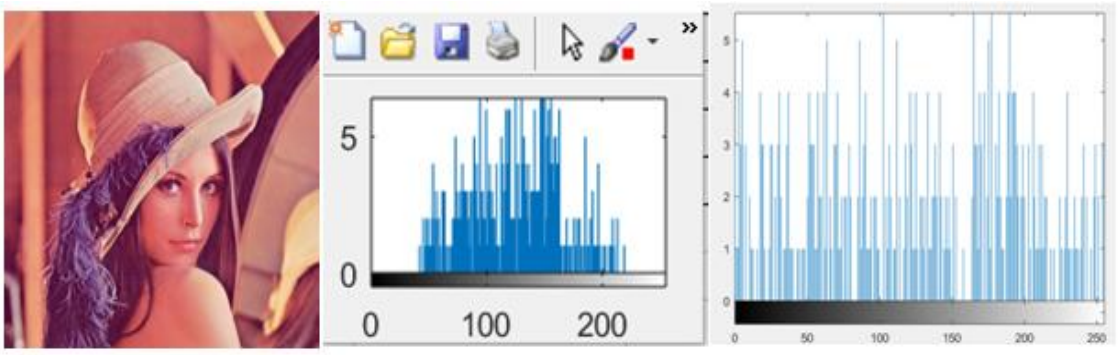

Fig 7.4 Lena image, its histogram, histogram of encrypted lena image

The above figure 7.4 shows the histograms of same Lena image and encrypted image which clearly has Uniform distribution .The Uniform distribution of histogram resists statistical attack. The leakage of the data is less. **8**Both cryptographic and steganography techniques are effectively combined and implemented with the help of new steganocyptographic algorithm. The impact of algorithm on standard parameters of both the techniques are analyzed. The visual cryptography technique split stego image into two shares. Hence the data is secured during transmission over the open channel network. The proposed system provides a fine balance between complexity of algorithm and security of data. Experimental results confirm that the combination of 3 level DWT steganography, ECC encryption, and visual cryptography methods are successful in obtaining the stego image also retrieved secret image of higher quality.

In order to analyse the strength of the system,cryptanalysis on key may be considered for the proposed system as a future work.

References

[1]. K.S.Seethalakshmi, Usha B A, Sangeetha K N, "Security Enhancement in Image Steganography Using Neural Networks and Visual Cryptography". IEEE issue 2016.

[2]. DipanwitaDebnath, Suman Deb, NirmalyaKar "An Advanced Image Encryption Standard Providing Dual Security: encryption using Hill Cipher & RGB image steganography" IEEE issue 2015.

[3]. Ahmed M. Elshamy, Ahmed N. Z. Rashed, Abd El-Naser A. Mohamed, Osama S. Faragalla, Yi Mu,Saleh A. Alshebeili, F. E. Abd El-Samie, " Optical Image Encryption Based on Chaotic Baker Map and Double Random Phase Encoding " IEEE vol 31. No 15. issue Aug 2013.

[4]. MoreshMukhedkar, PrajktaPowar, Peter Gaikwad " Secure non real time image encryption algorithm development using cryptography &Steganography" IEEE issue 2015.

[5]. Xinyi Zhou, Wei Gong, WenLong Fu, LianJing Jin, " An Improved Method for LSB Based Color Image steganography Combined with Cryptography " IEEE issue 2016.

[6]. PunamBedi, VeenuBhasi, Tarunyadav," 2L - DWT steganography technique based on second level DWT ". issue 24 sept 2016.

[7]. Palakmahajan, Heena Gupta "Improvsation of security in image stegnography using DWT, Huffman encoding and RCH based LSB embedding IEEE issue 2016

[8]. Palak Patel, Yask Patel "secure and authentic DCI image stegnography through DWI SVD

[9]. based digital water marking with RSA encryption issue 2015

[10]. Khalid A. Al-Afandy, El- security data M.EL-Rabaie, Osama S.Faragallah,AhmedElmhalaway, Gh.M.El. Bandy "High security data hiding using image cropping an LSB least significant bit steganography" IEEE issue 2016

[11]. SuchiGoyal, Manoj Ramaiya, DeepikaDubey "Improved detection of 1-2-4 LSB steganogrphy and RSA cryptography in color and grayscale imags "IEEE issue 2015

[12]. Dalilabaughaci, AbdelhafidKemauche and HocineLachibi, "Stochastic local search combined with LSB technique for image steganography" IEEE issue 2016

[13]. JakubOravec, Jan Turan,LubasOvsenik, "LSB steganography with usage of mojette transform for secret image scrambling"IEEE issue 25 May 2016.

[14]. Triphipatel,"Hierarchical visual cryptography for grayscale image". IEEE nov issue2016.

[15]. R .Tavares, F. Madeiro, " Word - Hunt : A LSB steganography method with low expected number of modifications per pixel". IEEE vol 14, No. 2 feb 2016.

[16]. Md. Rashedul Islam, Ayashasiddique, Md. Palashuddin, Ashiskumarmandal, Md. Delawarhossain " An efficient filtering based approach improving LSB image steganography using status bit along with AES cryptography" IEEE issue 2014.

[17]. Sabyasachikamila, Ratnakirtiroy, Suvamoychangder," A DWT based stegonagraphy scheme with image block partitioning ". IEEE issue 2015.

[18]. HamadA Al- korbi, Ali Al- Ataby, Majid A Al- Taee, Waleed Al. Nuaimy. " High- capacity image steganography based on haar DWT for hiding miscellanous data". IEEE issue 2016.

[19]. Rupendrakumarpathak, Shwethameena, " LSB based image steganography using PN sequence and GCD transform". IEEE issue 2015.

[20]. AayushiVerma, RajshreeNolkha, Aishwarya Singh and GarimaJaiswal , "Implementation of Image Steganography Using 2-Level DWT Technique"., International Journal of Computer Science and Business Informatics. ISSN: 1694-2108 | Vol. 1, No. 1. MAY 2013.

[21]. KBShivaKumar,KBRaja,RKChhotaray,SabyasachiPattnaik ,"Performance ComparisonOfRobustSteganography BasedOnMultipleTransformation Techniques," InternationalJournalofComp.Tech.App.,Vol.2(4),July-Aug2011,1035-1047.

[22]. Rakeshkumar,Noorahmed ,"Hybrid Approach Of Image Encryption Using DNA Cryptography And Tiff Cipher Algorithm",IEEE issue 2014.

Manjula.Y "A Steganocryptographic Algorithm Using 3 Level Dwt Steganography And Eacc Encryption." International Journal of Engineering Science Invention(IJESI), vol. 7, no. 8, 2018, pp. 22-31