Enhanced Colour Image Security and Data Hiding Using ECC Encryption and DWT-SVD Transforms

Afshan taj
M.Tech Student, Digital electronics
,Dept. of ECE,SSIT, Tumakuru, India, 572105.

Anitadevi M.D
Assistant Professor, Dept. of ECE, SSIT,
Tumakuru, India, 572105.

***Abstract*—Two types of data hiding techniques are most popular in today's world, they are cryptography and steganography. Where cryptography is science of writing secret code and steganography is art and science of hiding the secret code. In cryptography data is converted to unreadable form, so that unauthorized users cannot access the secret data. Where in steganography the secret data is hidden into digital media like image, audio and video. The combination of cryptography and steganography techniques will provide the higher security while communicating on the open channel. In the proposed system Elliptic curve cryptography (ECC) technique is used for data encryption and steganography uses DWT-SVD method to hide the encrypted data. These two techniques will provide higher security and the system yields high quality image, less memory utilization, more complexity and higher embedded capacity.**

Keywords*— *Cryptography, Steganography, ECC, DWT-SVD.

I. INTRODUCTION

The data security over communication is one of the most major concerns in today's world. Transferring the information via the Internet requires high security, hence process of exchanging information secretly through open channels become valuable due to increase in the data exchanged over internet. The confidentiality and integrity of data requires protection of unauthorized access and increased wanton has led to tremendous growth in the field of data hiding. Cryptography and steganography are well-known and widely used techniques that handle information in order to cipher or hide their existence respectively. The digital data like image, audio and video are used as cover in technical steganography. Hiding information in an image is the most popular type because of the large exchange on the Internet; it looks common and unsuspicious after the embedding process. The social media's are the one that deal with the confidentiality of information over open channel network. Cryptography and steganography both techniques are used to provide the authenticity to the data which has to be sent over the network and to hide it from its misuse. As a society, humans have continually sought new and efficient ways to communicate. Advancements of civilization introduced written language, telegraph, radio/television, and most recently electronic mail. As more and more communication is conducted electronically, new needs, issues, and opportunities are born at times when all of us communicate; The intended recipient have the ability to decipher the contents of the communication. The message has been kept secret. A common solution to this problem is the use of encryption. Steganography can be used to hide or cover the existence of communication. A major drawback to encryption is that the existence of data is not hidden. Data that has been encrypted, although unreadable, still exists as data. If given enough time, someone could eventually decrypt the data. A solution to this problem is steganography. The main aim of steganography is to keep the message undetectable from any unauthorized access. The concept of cryptography is not always as sufficient to provide the secure communication. But, the combination of both the scheme results in the secure and confidential form of data which can be kept secret easily and prevents it from any unauthorized access. The primary goal of cryptography is entirely based on the capability to hide the message from any insecurity. Essentially, the principle of cryptography and steganography is to offer secret and secure communication. Steganography can be implemented to wrap hidden messages in the form of audio, video or image and also text files cryptographic techniques are classified into two categories: symmetric ciphers and asymmetric ciphers.

A. Symmetric cipher

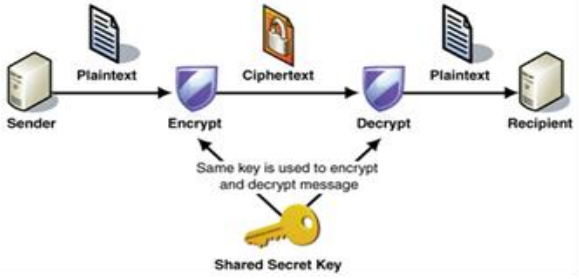

Fig. 1. Symmetric cryptographic technique

Symmetric ciphers is based on the size of the key and the same keys are used to encrypt and decrypt data.

B. Asymmetric cipher

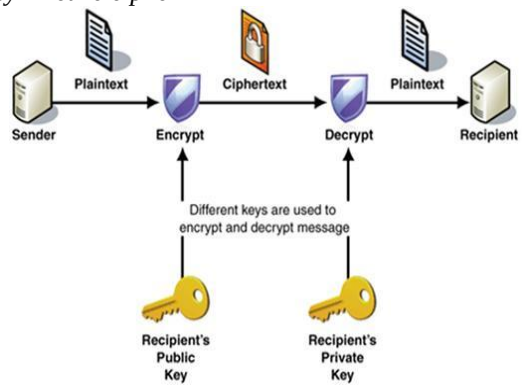

Fig. 2. Asymmetric cryptographic technique

Asymmetric ciphers consist of two different keys are used for encryption and decryption, one is the public key and private key.

C. Steganography

The word steganography is derived from the Greek words "stegos" meaning "cover" and "grafia" meaning "writing". Steganography is the science of hiding the secret message, image, or file within another message, image, or file, video. Steganography is used to reveal the information which is hidden in an audio or video file. To control the hiding process a stego-key is used so as to limit the detection or recovery of fixed data. The hacker cannot identify presence of secret message in an image without proper key.

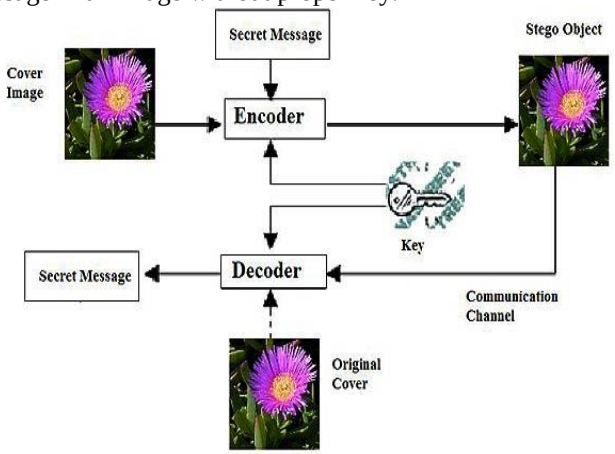

Fig. 3. Steganography technique with secret key

II. LITERATURE SURVEY

Hayfaa Abdulzahra Atee et al,[1] proposed the combination of cryptography and steganography techniques. A dynamic encryption method is used for cryptography and simple LSB and Color Image Based Data Hiding (CIBDH) are the steganograpic methods used. To hide the secret messages into image, the sequential concealment technique is used by simple LSB and the concealment technique is used by CIBDH. Parameters such as PSNR, capacity and MSE values for robustness are considered.

Pye Pye Aung et al, [2] proposed the combination of cryptography and steganography techniques . To encrypt secrete message cryptographic technique uses advanced encryption standard (AES) algorithm. which have separate keys to hide in cover image. Steganography technique used here is Discrete Cosine Transform (DCT) which uses a part of encrypted message as a key to hide in an image. Parameters such as security and robustness, image quality are considered.

Shaikh Shoaib et al, [3] proposed the digital video watermarking using 3 level DWT algorithm for securing data with a secret key. The key generated with watermarking image is considered during encryption process and during decryption process the same key is used. The parameters considered are MSE and PSNR.

Mohamed A. Seif At el [4] proposed the ECC based DES algorithm. The DES is a symmetric key Cipher algorithm. The ECC technique is used to generate the required key. The ECC based DES method is applied for different image files for both encryption and decryption with large key space to resist brute force attack. The parameters considered are histogram analysis, correlation, PSNR, MSE and key sensitivity analysis.

Blessy Joy A et al, [5] proposed the cryptographic technique, ECC technique is used to encrypt the RGB image to protect the data from unauthorized access. The image undergoes pixel wise xor operation and encrypted by ECC. Required number of bit planes are encrypted to achieve different levels of security. Parameters like processing power, energy, bandwidth limited for ECC are considered. It is used in multimedia communication.

Chuanmu Li et al, [6] proposed the image watermarking in DWT domain. The binary watermark is generated by a Chaotic map using secret key. The sub bands of 3 level DWT are selected to embedding the watermark by adjusting the coefficients order in different orientation. Parameter such as PSNR, MSE are considered.

Aayushi Verma et al , [7] proposed steganography technique, that is Discrete Wavelet Transform (DWT). The complexity of hidden image has been decreased through DWT technique. The DWT algorithm is used for embedding and extracting the secret image embedded behind the cover gray scale image. Parameters such as Peak signal to noise ratio (PSNR) and Mean square error (MSE), secure, robust and embedding capacity, less distortion are considered.

Nikita Gupta et al, [8] proposed the ECC technique for color image. NIST curves are used for ciphering the color images. The ECC technique key size is compared with RSA method depending on the strength and speed .Parameters such as timing analysis, size are considered.

Pallavi H. Dixit et al, [9] proposed the cryptography and steganography techniques for data security on open network. BLOWFISH method is used for data encryption and Steganography uses List significant Bit (LSB) for hiding the encrypted data. Iris image of authorized person is used to hide encrypted data for the security purpose. The secret key is generated from same iris image which is required for encryption using BLOWFISH algorithm. On 32 bit ARM 7 the algorithms are implemented. Parameters such as memory utilization, processing time for encryption and decryption, security for embedded systems are considered. it is used in mobile, smart card, ATM etc.

Melad J. Saeed et al, [10] proposed the cryptography and steganography techniques in which chaotic method is used for data encryption and Discrete Cosine Transform (DCT)

domain to hide encrypted color image. The original image in spatial domain is transformed to frequency domain using DCT. The cover image is embedded in DCT. Parameters such as MSE, PSNR and normalized correlation (NC), to phase and capacity are considered.

Pratibha Sharma et al [11] proposed the steganographic technique, in which 3 level discrete wavelet transform (DWT) is a steganographic method uses for digital image watermarking is presented and it is compared with 1 and 2 levels DWT. In the low frequency sub-band of a cover image multi-bit watermark is embedded by using alpha blending technique. During embedding, depending upon the scaling factor of alpha blending technique watermark image is dispersed within the original image. The watermark image is extracted by same scaling factor as for embedding. Parameters such as peak-signal-to-noise-ratio (PSNR) and mean square error (MSE) are considered.

Chandra Prakash Shukla et al, [12] proposed the combination of cryptography and steganography to protect the confidential messages on any network. Where Rivest Shamir Adleman (RSA) algorithm is used to secure the message from the hacker. The RSA algorithm converts the text message to cipher text. It is used in FBI, RAW and in security agencies to transfer the secret message.

K.S.Abitha et al, [13] proposed the cryptographic technique in which Elliptic Curve Cryptography (ECC) used to secured data transmission, which increases network security using Ad Hoc on Demand Distance Vector Routing (AODV) algorithm for transfer of data and also increment the efficiency of AODV algorithm using ECC. Parameters such as efficiency and reliability are considered. ECC algorithm is used to encrypt and decrypt the data that is to be transferred

Lei Lei, Chao Wang et al, [14] proposed the steganographic technique in which Discrete wavelet transform (DWT) technique is used for data hiding. Selecting a suitable Decomposition Level (DL) in DWT is of paramount importance to its performance. Sparseness of the transformed signals will determine the appropriate DL. The sparseness of transformed signals after DWT increases with the increasing DLs. it is effective, and widely adopted in biomedical signal processing for de-noising, compression and so on.

Mahmoud F. Abd Elzaher et al [15] proposed the cryptographic technique, which is used for communication of voice on secure channel. The voice samples undergo permutation and substitution using transform domains and secret keys in time. To increase the security chaotic maps are used. For permutation of the samples Arnold cat map is applied, in the substitution process Henon map is used for key generation to generate mask keys. Parameters considered are key sensitivity and high quality recovered signal, larger key space.

III. SYSTEM DESIGN

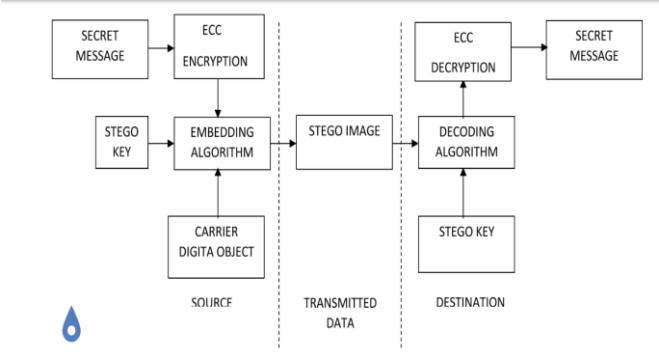

Fig. 4. Encryption and decryption using ECC.

Figure.4 shows the basic model of proposed system contains a Carrier, Message encryption and Password. cover-object is also known as Carrier, in which the message or data is embedded and serves to hide the presence of the message or data. Basically, the model of system is shown on Fig.1. Message is the data that the sender wishes to remain it dern. The message data is an image which encrypted using (Elliptical Curve Cryptography ECC) which is a Public key encryption technique. Stego-key is known as Password, which ensures that message from a cover-object can be extracted only by the recipient who knows the corresponding decoding key. The cover-object with the derned embedded message using DWT-SVD technique is then defined as the stego object. Restoring message from a stego-object needs the cover-object itself and a similar decoding key if a stego-key was used during the encoding process. The original image may or may not be required in most applications to extract the message.

IV. SYSTEM IMPLEMENTATION

An Elliptic curve is a cubic with the form of (1):

$$y2 = x3+ax+b \quad (1)$$

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

$$4a3+27b2 \neq 0 \pmod p \quad (2)$$

To encrypt a message, Alice and Bob decide on an elliptic curve and take a affine point (G) that lies on the curve. Plaintext M is encoded into a point PM. Alice chooses a random prime integer x and Bob chooses a random prime integer y. x and y are Alice and Bob's private key respectively. To generate the public key, Alice computes (3),

$$PA=xG \quad (3)$$

and Bob Computes (4).

$$PB=yG \quad (4)$$

To encrypt a message point PM for Bob, Alice choose another random integer named k and computes the encrypted message PC using Bob's Public key (PB). PC is a pair of points (5):

$$PC= [(kG), (PM+kPB)] \quad (5)$$

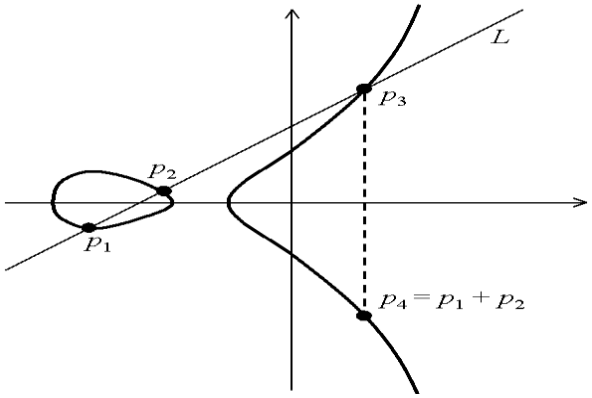

Fig. 5. Graph of an elliptic curve

Alice Sends PC to Bob as a cipher message. Bob, receiving the encrypted message PC and using his private key, y, multiplying with kG and add with second point in the encrypted message to compute PM, which is corresponding to the plaintext message M (6),

PM= (PM+kPB) - [y (kG)] (6)

Addition operation for two points P and Q over an elliptic group if P+Q= (X3, Y3) is given by (7) and (8) and the parameter λ is calculated by (9):

X3 = λ2- XP – XQ mod p (7)

Y3= λ (XP-X3) – YP mod p (8)

$$\lambda = \begin{cases} \frac{Y_Q - Y_P}{X_Q - X_P} & if\ P \neq Q \\ \frac{3X_P^2 + a}{2Y_P} & if\ P = Q \end{cases}$$

Multiplication kP over an elliptic group is computed by repeating the addition operation k times by (7) and (8). The strength of an ECC-based cryptosystem is depends on difficulty of finding the number of times that G is added to itself to get PA. Reverse operation known as Elliptic Curve Discrete Logarithm Problem (ECDLP) and exploit in cryptography.

IV. MAPPING METHODOLOGY

Every image consists of pixels. In gray scale images each pixel has an 8-bit value between 0 and 255. In color images each pixels defined by three 8-bit values separately demonstrate the Red, Green and Blue intensity. To encrypt an image using ECC, each pixel is considered as a message and should be mapped to a point on predefined elliptic curve. The Proposed mapping method is based on a map table. To create this table, the elliptic group Ep (a, b) which is all possible points on the finite field are generated first and then these points are grouping in 256 groups. Each group has $N = \#(fp)/256$ members. The row indexes are start from 0 and end with 255. Each row stands for a pixel intensity value but for same values there are multiple points. If N is not a multiple of 256, then extra rows in the last column are filled with zero and the last column will consider for mapping. Starting from the first pixel in plain image, the corresponded point with the intensity value in the table is mapped to this pixel and continue to the last pixel. For repetitive intensity values the next point in the corresponded row will be selected. For any of intensities, if all N-1 points are selected then for next one again starts from the first point. After mapping all pixels to related points on the table, encryption is done using receiver's public key. Encrypting a point results a set of two points. In this case, one point is same for all pixels, but the other point is different for each pixel. After encrypting all pixels, also result can be demonstrated as an image. To view the encrypted points as an image, refer to the mapping table and find the current index according to each point and replace with the related value.

Let both the sender and receiver decide on elliptic curve E751 (-1,188) that represented by:

$$y2\ mod\ 751 = x3 - x + 188\ mod\ 751$$

Table 4.2 shows a part of generated points. To create the mapping table, the first point will place in the row 1 which is corresponded to pixel with intensity value of 0, and then continue next point with next value. After placing first 256 points in first column of the table, next 256 points will place in second column and hereafter will do the same for next points to the last. In this example, there are 727 points on the curve. These points completely fill 2 columns and 214 rows of 3rd column. Rest rows of the last column fill with zero. According to (1) and (2), to encrypt this image, some parameters should be defined. Choosing G=(0, 376) as a generator point, y=85 as receiver private key and k=6, a random integer defined by sender. Having these values, according to (4), receiver's public key is calculated and the result is: PB=(671,558).

Index	1st Mapping	2nd Mapping	3rd Mapping	4th Mapping	5th Mapping	482nd Mapping
0	(42908,0)	(512,47183)	(1033,54418)	(1533,9490)	(2093,30783)	(122949,83868)
1	(95914,0)	(513,33718)	(1035,9194)	(1534,56042)	(2095,41465)	(122951,74372)
2	(108092,0)	(515,24882)	(1039,3322)	(1535,33470)	(2096,16779)	(122953,121769
3	(3,31443)	(516,49743)	(1041,8203)	(1543,36384)	(2097,9443)	(122954,66970)
4	(5,11660)	(519, 6902)	(1043,46883)	(1544,10278)	(2098,19721)	(122958,73556)
5	(6,2174)	(520,20390)	(1044,52089)	(1546,38337)	(2099,57887)	(122959,84424)
6	(7,58403)	(521,20390)	(1046,3610)	(1548,55400)	(2100,39297)	(122961,71950)
7	(8,29200)	(524,59065)	(1049,55356)	(1550,3312)	(2102,15631)	(122962,91690)
154	(305, 46853)	(824,9038)	(1339,50036)	(1896,22466)	(2412,59464)	(123276,99876)
155	(306, 33458)	(825,50433)	(1340,25625)	(1897,20281)	(2413,4124)	(123277,107283
156	(307, 29631)	(831,5746)	(1341,37870)	(1898,37575)	(2414,49935)	(123279,104846
157	(312, 43431)	(832,39441)	(1342,48041)	(1899,60234)	(2417,26883)	(123280,82736)
158	(314, 37257)	(834,26653)	(1344,60034)	(1902,7652)	(2418,11842)	(123285,119446
159	(315, 58283)	(835,23727)	(1346,20117)	(1905,19609)	(2420,6170)	(123287,87751)
160	(317, 57467)	(836,30492)	(1351,35977)	(1906,43788)	(2422,33537)	(123288,84108)
161	(318,23904)	(840,29931)	(1355,30658)	(1908,59509)	(2426,272)	(123289,81841)
250	(501,10872)	(1020,25923)	(1511,61516)	(2076,24517)	(2596,8145)	(123456,95491)
251	(504,34198)	(1021,52191)	(1514,18629)	(2079,52447)	(2597,20182)	0
252	(508, 56806)	(1022,35175)	(1515,52722	(2082,51701)	(2602,1137)	0

TABLE II. RESULTS OF MAPPING PIXELS TO POINTS, ENCRYPTION AND MAPPING ENCRYPTED POINTS TO PIXELS

161	159	157	158	161	159	156	157	159	158
(318, 23904)	(315, 58283)	(312, 43431)	(314, 37257)	(840, 29931)	(835, 25727)	(307, 29831)	(832, 39441)	(304, 9557)	(834, 26653)
(117616, 24017)	(117616, 24017)	(117616, 24017)	(117616, 24017)	(117616, 24017)	(117616, 24017)	(117616, 24017)	(117616, 24017)	(117616, 24017)	(117616, 24017)
(122358, 40144)	(60803, 3943)	(11960, 81566)	(99326, 59783)	(8435, 79086)	(24718, 3745)	(63094, 28246)	(102540, 105454)	(109441, 89040)	(111938, 83952)
205	222	82	77	107	88	82	91	169	120

Table 4.2: Mapping table

4.3 Discrete Wavelet Transforms (DWT):

The DWT in one dimensional signal is divided in two parts one is low frequency part and another is high frequency part. Next the low frequency part is split into two parts and the similar process will continue until the desired level. The high frequency part of the signal is contained by the edge components information of the signal. Now DWT (Discrete Wavelet Transform) decomposition on an image separates into four parts these are approximation Image (LL) as well as horizontal (HL), vertical (LH) and diagonal (HH) for detail components. In the DWT decomposition input signal must be multiple of 2n. Where, n represents the number of level. To analysis and synthesis of the original signal DWT provides the sufficient information and requires less computation time. Watermarks data are embedded in these regions that help to increase the robustness of the watermark. A one level DWT decomposition process is shown in Figure 4.3.1.

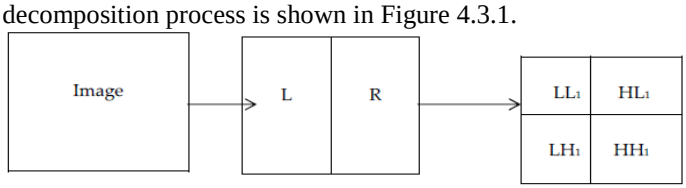

Fig 4.3.1 Single level decomposition using DWT

DWT is a new technique which is used to represent image in a new time and frequency scale in recent years. The basic function of DWT is decomposing the input signal to multi-resolutions. If input signal is an image DWT decompose it into low frequency(LL) and high frequency(HL,LH and HH). HL represents the horizontal detail, LH represents the vertical detail and HH represents the diagonal part. The low frequency and is the optimal approximation of the original image, which is determined by the DWT decomposition progressions that represents the maximum scale and distinguishing degree.

Wavelet Transform has become an important method for image compression. Wavelet based coding provides substantial improvement in picture quality compression ratio mainly due to better energy compaction property of wavelet transforms. Wavelets are functions which allow data analysis of signals or images, according to scales or resolutions. The DWT represents an image as a sum of wavelet functions, known as wavelets, with different location and scale. It represents the data into a set of high pass(detail) and low pass(approximate) coefficients. The input data is passed through set of low pass and high pass filters. The output of high pass and low pass filters are down sampled by 2. The output from low pass filter is an approximate coefficient and the output from the high pass filter is a detail coefficient. This procedure is one dimensional(1-D)DWT. But in this research work we are using two dimensional(2-D) DWT. In case of two directions, both rows and columns, the outputs are the n down sampled by 2 in each direction as in case of 1-DDWT[8].Output is obtained in set of our coefficients LL,HL,LH2-DDWT,the input data is passed through set of both low pass and high pass filter and HH. The first alphabet represents the transform in row where as the second alphabet represents transform in column. The alphabet L means low pass signal and H means high pass signal. LH signal is a low pass signal in row and a high pass in column. Hence, LH signal contain horizontal elements. Similarly, HL and HH contains vertical and diagonal elements, respectively.

The Forward DWT Eq.:-

$(JO,) = 1\ M\quad (n)\quad o, k\ (n)$

$W\Psi\ (j, k) = 1\ Mfnn\Psi\ J, K\ (n)\qquad for\ j \geq j0$

The complementary inverse DWT eq. is:-

$F\ (n) = 1\quad (JO,)\ \varphi j\ o, k\ (n) + 1\quad \Sigma\ W\Psi\ (j, k)\quad J, K\ (n)$

V. RESULTS

The cover image and secret image are the inputs for encryption technique.

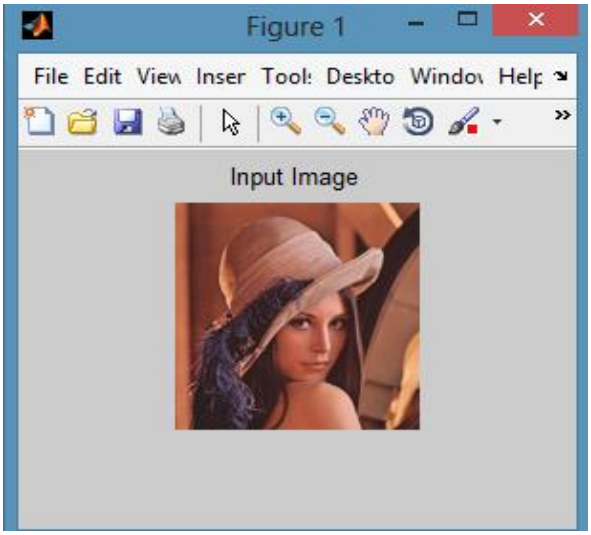

Figure 6.1: Secret image

The secret image is a colour image as shown in figure 6.1.

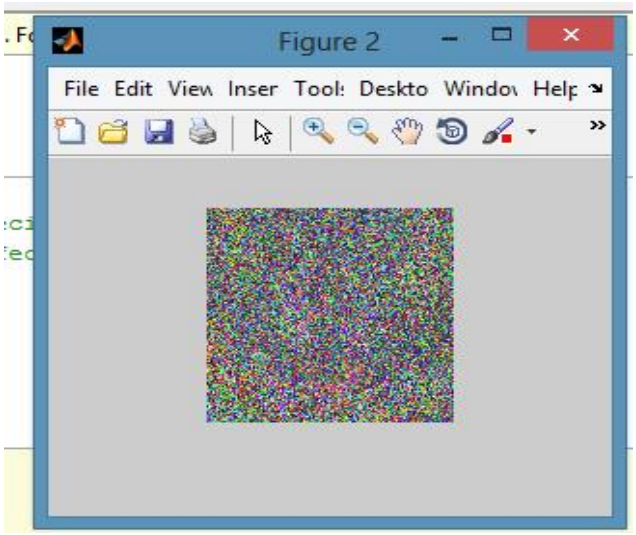

Figure 6.2: Encrypted image

The image is encrypted using ECC technique, figure 6.2 shows the encrypted image.

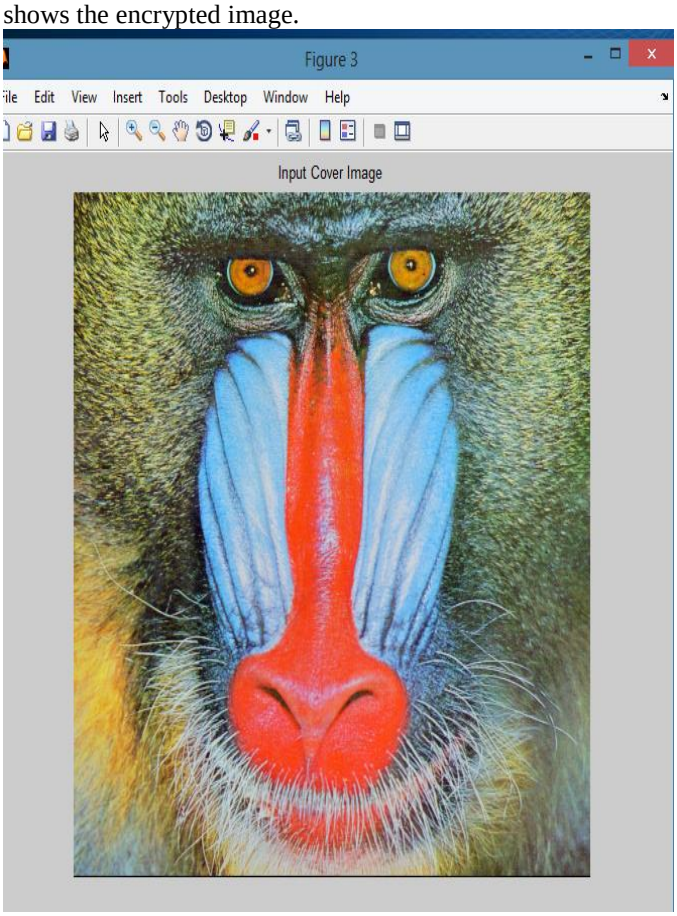

Figure 6.4: Input Cover image

The Input cover image is also a color image of any size shown in figure 6.4. cover image is of greater size than that of input image.

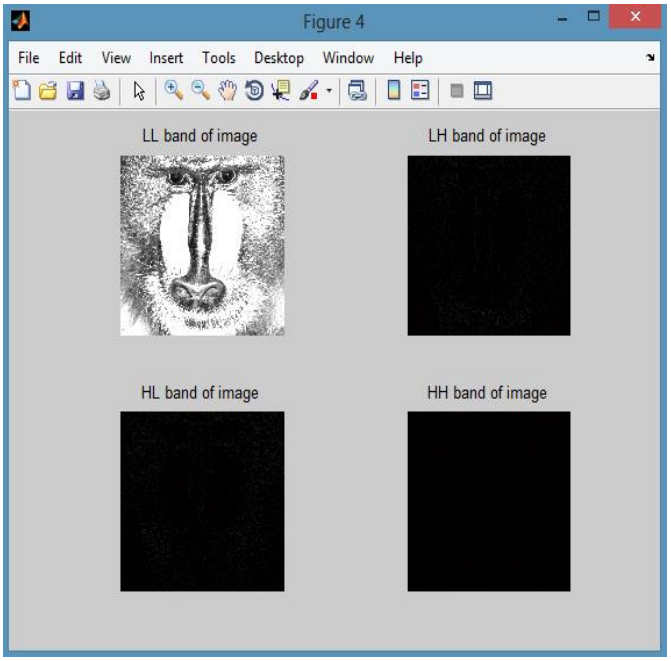

Figure 6.4: DWT transformation

The cover image is the carrier image which undergoes Discrete Wavelet Transformation (DWT) as shown in figure 6.4. and the size of cover image is more than that of secret data which has to be hidden inside the cover image.

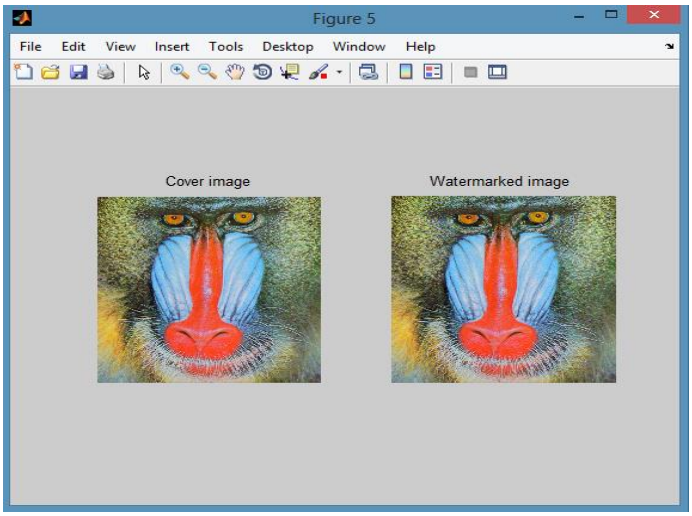

Figure 6.5: cover image and water marked image.

The higher frequency coefficient HH of DWT is selected for embedding of encrypted secrete image. Then inverse DWT technique is applied to reconstruct the carrier image as shown in figure 6.5.

Decryption technique results

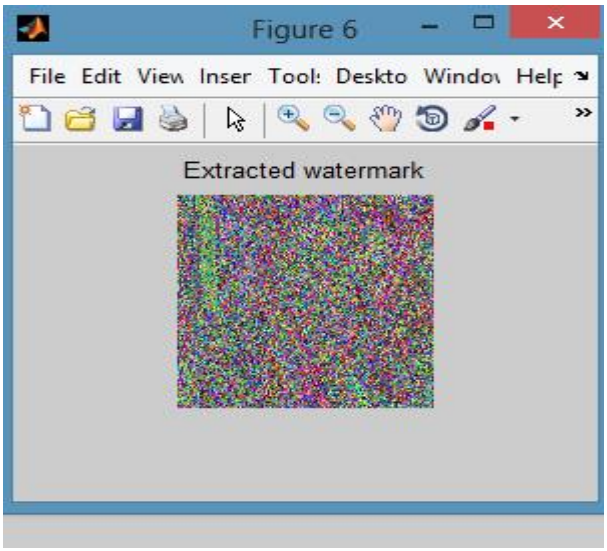

Figure 6.6: Extracted water marked image

The Extracted water marked image obtained is shown in figure 6.6. from the cover image the secret data is extracted.

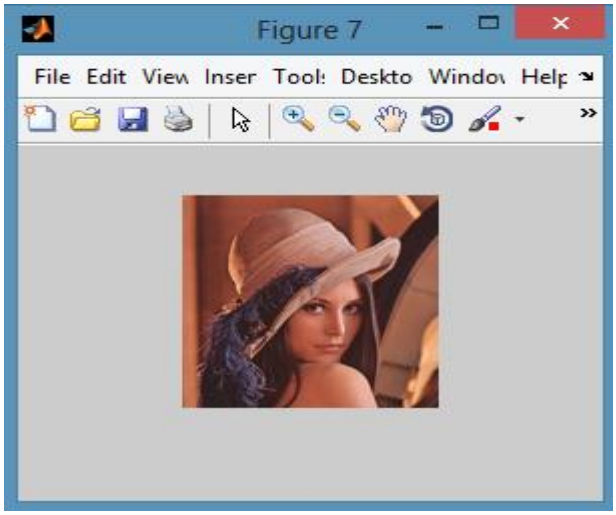

Figure 6.7: Recovered secret image

The DWT technique is applied to stego and cover image. The difference between original and modified coefficients are finded out. Message vector bits are prepared to form an image and encrypted image is as shown in figure 6.7. The ECC technique is applied to recover the secret image as shown in figure 6.7.

VI. CONCLUSION

The combination of cryptography and steganography features provides satisfying factors for better performance. The ECC technique and DWT-SVD technique is designed and implemented. The ECC method is used for encryption of the secret data and steganography uses DWT technique to hide the encrypted data. Hence the data is secured during transmission over the open channel network. The proposed system provides high complexity and security. Hence hacker face difficulty while accessing the secret data.

VII. FUTURE WORK

Elliptic curves are believed to provide good security with smaller key sizes, something that is very useful in many applications. Smaller key sizes may result in faster execution timings for the schemes, which is beneficial to systems where real time performance is a critical factor. The market for Personal Digital Assistants (PDA) is growing rapidly and PDAs are becoming increasingly interesting for commercial transactions. One requirement for further growing of E-commerce with mobile devices is the provision of security. We can implement elliptic curves over binary fields on Palm OS device.

VIII. REFERENCES

[1] Hayfaa Abdulzahra Atee, Robiah Ahma and Norliza Mohd Noor," Cryptography and image Steganography usin dynamic encryption on LSB and color image based data hiding", publication 2015.
[2] Pye Pye Aung and Tun Min Naing, "A novel secure combination technique of Steganography and cryptography", vol. 2, No. 1, February 2014.
[3] Shaikh Shoaib, Prof. R. C. Mahajan, "Authenticating using secret key in digital video watermarking using 3 level DWT",IEEE Issue 17, January 2015.
[4] Moamed A. Seif Eldeen, Adbellatif A. Elkouny, Salwa Elramly "DES algorithm security fortification using elliptic curve cryptography", IEEE issue 2 Dec 2015
[5] Blessy Joy A,R. Girish, "RGB image encryption based on bitplanes using Elliptic Curve Cryptography", vol. 5, Issue 2, February 2015.
[6] Chuannu li, Haiming sing," A novel watermarking scheme for image authenticaton in DWT domian", vol 61, issue 20 Oct 2013.
[7] Aayushi Verma, Rajshree Nolkha, Aishwarya Singh and Garima Jaiswal, "Implementation of Image Steganography Using 2-Level DWT Technique".
[8] Nikita Gupta, Vikas Kundu, Neha Kurra, Shivani Sharma, Bhagyashree Pal, "Elliptic curve cryptography for ciphering image", IEEE issue 25 Jan 2015
[9] Pallavi H. Dixit, Kamalesh B. Waskar, Uttam L. Bombale, "Multilevel Network Security Combining Cryptography and Steganography on ARM Platform", Vol. 3, No. 1, 2015
[10] Melad J. Saeed, "A new technique based on Chaotic Steganography and Encryption text in DCT domain for color image", Vol. 8, No. 5, 2013.
[11] Pratibha Sharma, Shanti Swami, "Digital Image Watermarking Using 3 level Discrete Wavelet Transform", 2013
[12] Chandra Prakash Shukla, Ramneet S Chadha, Abhishek Kumar, "Enhance security in stegnography with cryptography", Vol. 3, Issue 3, March 2014.
[13] K.S.Abitha, Anjalipandey, DR.K.P.Kaliyamurthie, "Secured Data Transmission Using Elliptic Curve Cryptography", Vol. 3, Issue 3, March 2015.
[14] Lei Lei, Chao Wang, and Xin Liu, "Discrete Wavelet Transform Decomposition Level Determination Exploiting Sparseness Measurement", Vol:7, No:9, 2013.
[15] Mahmoud F. Abd Elzaher, Mohamed Shalaby, Salwa H. El Ramly, "Securing Modern Voice Communication Systems using Multilevel Chaotic Approach", Volume 135 – No.9, February