A SECURED LSB IMAGE STEGANOGRAPHY SYSTEM USING EDGE DETECTION, LZW COMPRESSION AND HYBRID ENCRYPTION METHODS

S. N. Rekha[1], Y. Manjula[2], M.Z. Kurian[3]

[1]PG Student (DE), [2]Assistant Professor, [3]HOD, Dept. of Electronics & Communication Engineering,
Sri Siddhartha Institute Of Technology, Tumakuru, Karnataka, (India)

ABSTRACT

Rapid growth of steganographic and cryptographic techniques has a great attention in digital era. Every one need privacy in this internet world. As number of users increases secret communication becomes more and more important. Transposal of data size and file quality through communication channel plays a major challenge for steganographic technique. Least significant bit is one of the simple and major steganography techniques in spatial domain, insertion of data at least significant bits has high visual quality but not robust against distortion hence not well secured. In the proposed method, the secret data is encrypted by using Hybrid encryption method i.e. AES[Advance Encryption Standard] and ECC[Elliptic Curve Cryptography] method to safe guard the secret communication. Then, Lempel Ziv Welch technique compresses the required amount of data to represent information quantity. Then Edge detection technique detects the sharp feature of image to hide secret data. The main feature of proposed method is to give better security by using the concepts of cryptography and Image steganography. Even though the adversaries have the knowledge of secret information fails to extract the correct information. Improvement may seen by comparing the results of base paper and proposed method. Better encryption methods are considered to provide better security along with steganography.

Keywords*: *AES encryption, ECC encryption, Edge detection, Steganography, LZW compression

I. INTRODUCTION

In this internet era, as fast as the new technology emerges number of users are increases at the same time eve droppers are also increases. Hardware attacks, software attacks are some of the threats arise during data transmission therefore data integrity becomes more important. The demand increases in the field of steganography and cryptography to provide better security for secret information. Steganography is a Greek word which means covered writing where it concentrates on existence of message secret. Image steganography is the way of hiding the secret data in digital images. Cryptography is a Greek word which means hidden writing where it concentrates on contents of message secret. Both methods provide secret communication between sender and receiver in the presence of adversaries.

Combining of two or more encryption methods is nothing but hybrid encryption. Both private key and public key cryptography is used for converting secret image from readable into unreadable format with a good lossless compression technique i.e. LZW and to embed the encrypted image into the cover file better steganography technique i.e. Canny edge detection technique is used.

After embedding large amount of data in to cover image some changes occurred like colour, sharpness, smoothness. Authentication of secret data, quality of stego image, embedding capacity of cover image, robustness is some of the factors considered to evaluate image steganography process.

II. LITERATURE SURVEY

Archana T. Chawhan, et al.,[1] presented a secure steganography technique which includes three methods. First, encryption is used to encode the secret data. Second, LZW compression is used to compress the data and Third, Knight Tour algorithm is used to generate the sequence of secret bit stream. On comparing the results ECC technique provide more performance and security than AES technique.

Nadeem Akhtar, et al.,[2] proposed two schemes of bit inversion technique. In first scheme, some lsb pixels of cover image is inverted and four patterns are checked if there is a particular bit pattern then less number of bits is modified. In second scheme, eight patterns are checked to modify less number of bits compare to plain lsb method. Bits are randomly distributed in cover and message image results small and large improvement in psnr value.

Debiprasad B, et al.,[3] presented a secure steganography method by using chaos theory in spatial domain where it is a deterministic non linear dynamic system which generates chaotic sequence to encrypt the secret data before embedding into the cover image by logistic chaotic map. Image fidelity and psnr are greatly improved for different image files.

Shrutika suri, et al.,[4] describes the different steganographic techniques some of them are spatial domain, transform domain, masking and filtering. By applying all the technique to embed the secret message in the cover image and the parameters like capacity, robustness, and security are evaluated.

P.M. Siva raja, et al., [5] presented a new scheme based on genetic algorithm. This algorithm selects the exact embedding region and optimizes the threshold value of the selected image regions to embed the secret message. Major drawback is less embedding rate in sequential and frequency domain.

K.S. Arora, et al., [6] presented a new technique using K-matrix. To reduce the time complexity K-matrix uses 2x2 matrix to encrypt the data and at each cell random number is assigned ranging from 1 to 16 to map the secret message.

Saurabh, et al.,[7] presented a new approach that contains hash function and canny edge detection method. Firstly, canny method is used for edge detection which detects optimal edge i.e. good detection, localization and minimal response of cover image. Secondly, Hash function generates a pattern that is used to embed text data in image. High quality of stego image is achieved. In future work can be extended to audio, video etc.

Y.P.Zhang, et al.,[8] proposed two algorithms to achieve high embedding capacity and embedding efficiency. First, High capacity information hiding algorithm uses (7, 4) hamming code and LSB method to improve embedding capacity. Second, High quality information hiding algorithm uses wet paper code to improve the embedding efficiency. As the value of WR increased PSNR value is also increased more than 52dB.

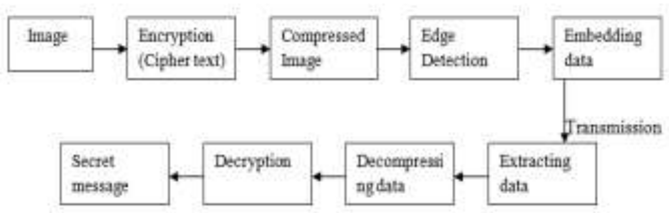
J.J. Wang, et al.,[9] presented a new data embedding technique where linear independent approximation embedding algorithm embeds the data at a specified arbitrary cover location. To avoid quantization error adaptive matrix method is used where it uses linear block codes and gives optimal solution. High probability and good speed is achieved.

Ankita Agarwal[10] presented a new model where Simplified data encryption standard is used to produce cipher text by using eight bit block of plain text and Alteration component is used to embed the encrypt data in cover image.

III. PROPOSED SYSTEM

The architecture of the proposed system is designed as shown in the Figure. It has two phases Encoding and Decoding. The Encoding process includes Encryption, Compression, Edge detection and Embedding by LSB method. Decoding process includes Extraction or de-embedding, Decompression and Decryption.

Sender



Receiver

Fig.1 Proposed system design.

In the encoding process secret image is selected. If selected secret image is colour then colour image is converted into gray scale image. Secret image is encoded by using Advanced encryption standard algorithm to obtain AES encrypted image. By taking input information of AES encrypted image secret data is again encoded by Elliptic curve cryptography technique to get ECC encrypted image. Here plain text is converted into cipher text.

To reduce the size encrypted image is compressed by Lempel Ziv Welch compression technique to get compressed image. Select the cover image, at large change in intensity of the cover image edge pixels are identified by canny edge detection technique then Compressed image is embed into the edge detected cover image by least significant bit insertion method to get stego image.

In the decoding process, stego image is extracted or de-embed by least significant bit insertion method. Extracted image is decompressed by Lempel Ziv Welch to get decompressed image. This decompressed image undergoes ECC decryption and then AES decryption to get back the secret image. Here cipher text is converted into plain text.

The sending process consists of following procedures:

3.1. Encryption

In embedding phase, the image is encrypted using different Encryption algorithms. Encryption is the process of encoding the secret message where only authorized persons can able to read even in the presence of third parties. In this process the content of secret message referred as plain text and by using different encryption algorithm cipher text is generated and after decryption the message can be read. Double encryption provides double security for secret data.

3.1.1AES (Advanced Encryption Standard) Algorithm: is based on the principle of substitution permutation network. AES is a combination of substitution and permutation. It is used for encryption of electronic data. This algorithm is flexible and supports fixed key size of 128, 192 and 256 bits. However, AES as a fixed block size and key size with minimum of 128 bits and maximum of 256 bits. Data length of 128 bit is divided into four basic operation blocks. These blocks arranged as a 4x4 column matrix of bytes i.e. called the state. For full encryption, the data is passed through number of rounds Nr (Nr=10, 12, 14).

In AES, key size specifies the number of repititions of transformation rounds where plain text is converted in to cipher text.

128 bit keys has 10 cycles of repetition
192 bit keys has 12 cycles of repetition
256 bit keys have 14 cycles of repetition.

Each round as many steps, in that four step are similar but stages are different and encryption key depend itself on steps.

By applying the reverse rounds to transform to obtain original plain text from cipher text encryption key is used.
For each
round separate 128bit key is required in AES. Some of the round steps are
Sub byte step
Shift row step
Mix column step
Add round key step

3.1.1.1.Sub byte step: In this step, each byte in the state is replaced with its entry in a fixed 8 bit look up table. S; bij= s(aij). This operation provides non linearity from multiplicative inverse over GF S-box is derived.

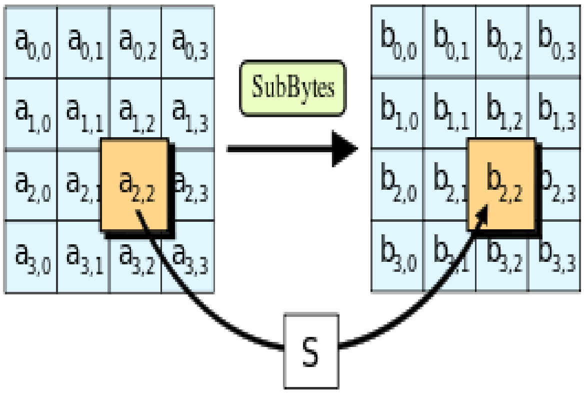

SubBytes
S
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

Fig.2 Sub byte operation

3.1.1.2. Shift row steps: In this step, each row bytes is cyclically shifted from left. Each byte places are differing from each row. By offset each row byte shifts cyclically. The main future of this step is to avoid the columns being linearly independent. Four independent block ciphers are degenerated by AES.

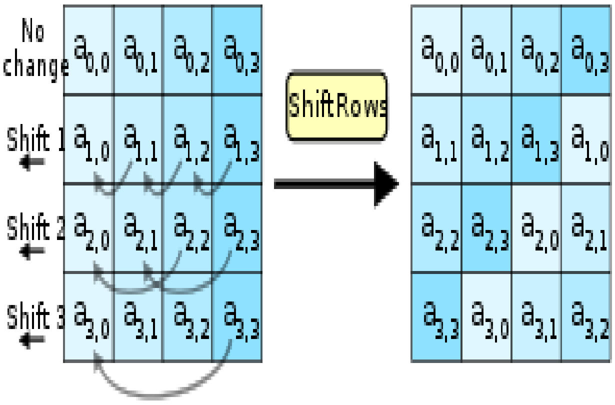

No change
Shift 1
Shift 2
Shift 3
ShiftRows
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,1}$ $a_{1,2}$ $a_{1,3}$ $a_{1,0}$
$a_{2,2}$ $a_{2,3}$ $a_{2,0}$ $a_{2,1}$
$a_{3,3}$ $a_{3,0}$ $a_{3,1}$ $a_{3,2}$

Fig.3 Shift row operation

3.1.1.3 Mix column Step: Fixed polynomial c(x) is multiplied with each column of the state. It takes 4 bytes as input and 4 bytes as output and all four bytes are affected by each input bytes. This operation provides diffusion.

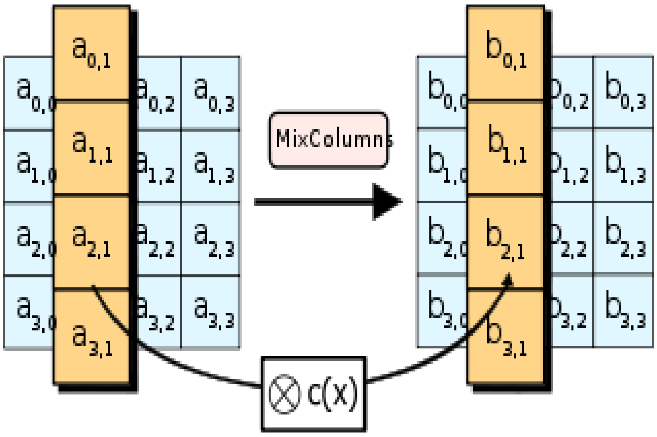

MixColumns
$\otimes c(x)$
$a_{0,0}$ $a_{0,1}$ $a_{0,2}$ $a_{0,3}$
$a_{1,0}$ $a_{1,1}$ $a_{1,2}$ $a_{1,3}$
$a_{2,0}$ $a_{2,1}$ $a_{2,2}$ $a_{2,3}$
$a_{3,0}$ $a_{3,1}$ $a_{3,2}$ $a_{3,3}$
$b_{0,0}$ $b_{0,1}$ $b_{0,2}$ $b_{0,3}$
$b_{1,0}$ $b_{1,1}$ $b_{1,2}$ $b_{1,3}$
$b_{2,0}$ $b_{2,1}$ $b_{2,2}$ $b_{2,3}$
$b_{3,0}$ $b_{3,1}$ $b_{3,2}$ $b_{3,3}$

Fig.4 Mix column operation

3.1.1.4. Add round key Step: In this step, using xor operation bytes of sub key round is combined with each byte of the state. Each state has same size as sub key.

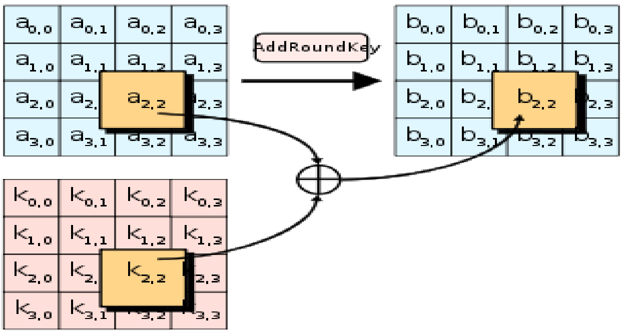


Fig 5 Add round key operation

3.2. ECC (Elliptic Curve Cryptography):

An Elliptic Curve Cryptography (ECC) technique is an algebraic structure of elliptic curves over finite fields where public key cryptography is used. In prime case, field is defined by P and binary case, field is defined by m and f. The elliptic curve is defined by the constants a and b. Then cyclic subgroup is defined by its generator point G.

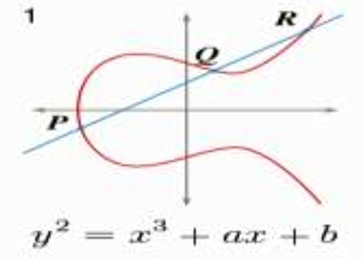


Fig.6. Elliptic curve

It is also known as public key cryptography. The equation of an elliptic curve is given as $y^2=x^3+ax+b$. Key generation of both public key and private key is very important. The sender will encrypt the message with public key receiver and private key is decrypted by receiver.

To generate public key Q=d*p equation is used where d=random number selected with on the range of 1 to n-1.

P= point on the curve

Q is the public key

d is the private key

3.3. Compression

Compression method is the process minimizing the size of the message with error free approach. LZW is the lossless data compression technique for many image file formats like GIF and TIFF. It is very fast while compressing and decompressing any type of data. LZW compressed output is identical in both big endian and little endian systems. Compressed output is stored as bytes instead of words and it does not require floating point operation. It is reffered as dictionary based or substitutional encoding algorithm. LZW coding uses fixed length code for variable sequence length. To replace the repetitive successive characters with binary code, dictionary table is created and table is sent to receiver side to extract the original secret message. Decoding of LZW data is reverse process of LZW encoding.

Amount of reducing extraneous information in an image is known as differencing. In images adjacent pixels have slight vary in value. We can replace the value of pixel by differencing the pixel and adjacent pixe,l we reduce the amount of information stored. For 8 bit gray scale images value of pixels differenced themselves. Differencing is applied across scan lines in horizontal plane then vertical plane. Using LZW method differenced image is compressed more effectively.

3.4. Edge detection

It is a fundamental tool to extract and detects the sharp feature of image at particular areas. It focuses on the detection of points at which the brightness of an image changes sharply, smoothly, formally with discontinuities. At discontinuities, set of curve line segments termed as edge. Identifying the problem of discontinuities in single dimension signals is called step detection. Identifying the problem of discontinuities overtime is called change detection. Different types of edge detectors are: Sobles Edge Detector, Prewitt Edge Detector, Canny Edge Detector and Zero crossing Detectors[13].

Canny edge detector is an operator that use multistage algorithm to identify wide range of edges in images. These techniques extract structural information which reduces the amount of data to be processed. Some criteria includes in this method are

1. It detects the edges with very low error rate.
2. Operator which detects the edge point must localize on edge center accurately.
3. Only once edge can be marked in the given image to avoid false edges.

These needs can be achieved by using calculus of variations where it optimizes the given function. It provide good and reliable detection.

3.5. Embedding Process:- In this step encoding of image is carried out to hide and protect the secret image inside the cover image. The sender uses some techniques to encode and compress the data and at large change in intensity of the cover image edge pixels are identified by canny edge detection technique. By least significant bit insertion method secret image is embed into the cover image.

The receiving process consists of following procedures:

3.6. Extraction Process:- In this step decoding of image is carried out to retrieve the secret image from the stego image. Therefore, procedure is required to extract the content of the message. As same as the sender side first extract the content of image by least significant bit de-embedding then decompress the data with LZW technique. Then decrypt the secret data by different extracting algorithms i.e. ECC decryption and AES decryption. At the end cipher text is converted into plain text.

3.7. Decompression:- Extracted image is decompressed by using Lempel Ziv Welch technique. It is the exact reverse process of LZW compression.

3.8. Decryption:-To revealed secret image decompressed image is decrypted by Elliptic Curve Cryptography decryption algorithm again the ECC decrypted image is decrypted by Advance encryption standard decryption algorithm. AES and ECC Decryption is the exact reverse process of ECC and AES Encryption. By this extracting algorithm cipher text is converted in to plain text.

IV. SYSTEM IMPLEMENTATION

4.1. AES Encryption: is one of the cryptographic techniques. It is also known as symmetric key algorithm. Private key is used to encode and decode the secret image. AES operates on state with fixed Size of 128 bits and different key length.. Depending on size of key number of repetition of transformation rounds are decided to convert plain into cipher text.

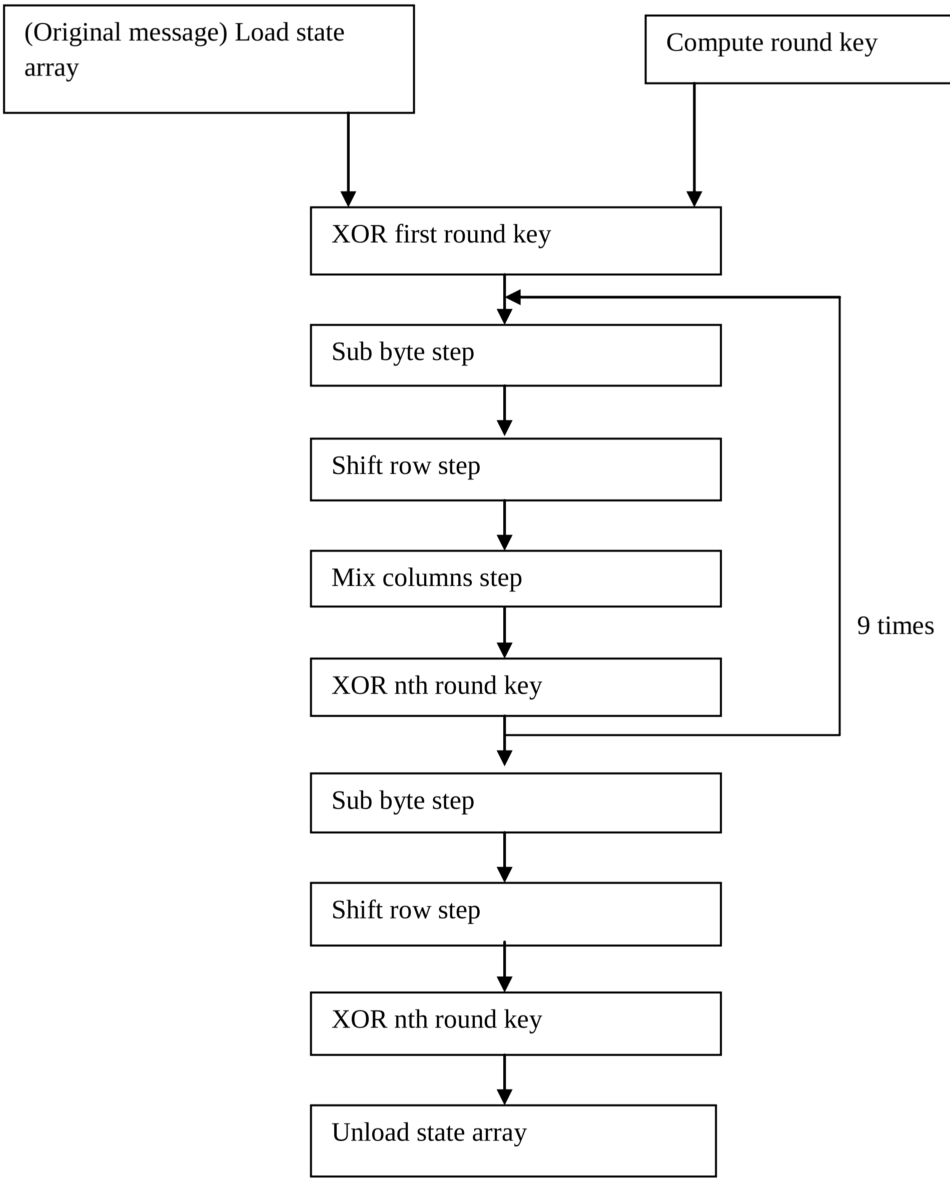


Fig.7. Flow Chart of AES Encryption

4.2 ECC Encryption: is also known as asymmetric key algorithm. In finite fields ECC is based on elliptic curves of algebraic structure. Key size is small when compare to other techniques. It can able to compute point multiplication. Input image information is entered to encrypt the secret data.

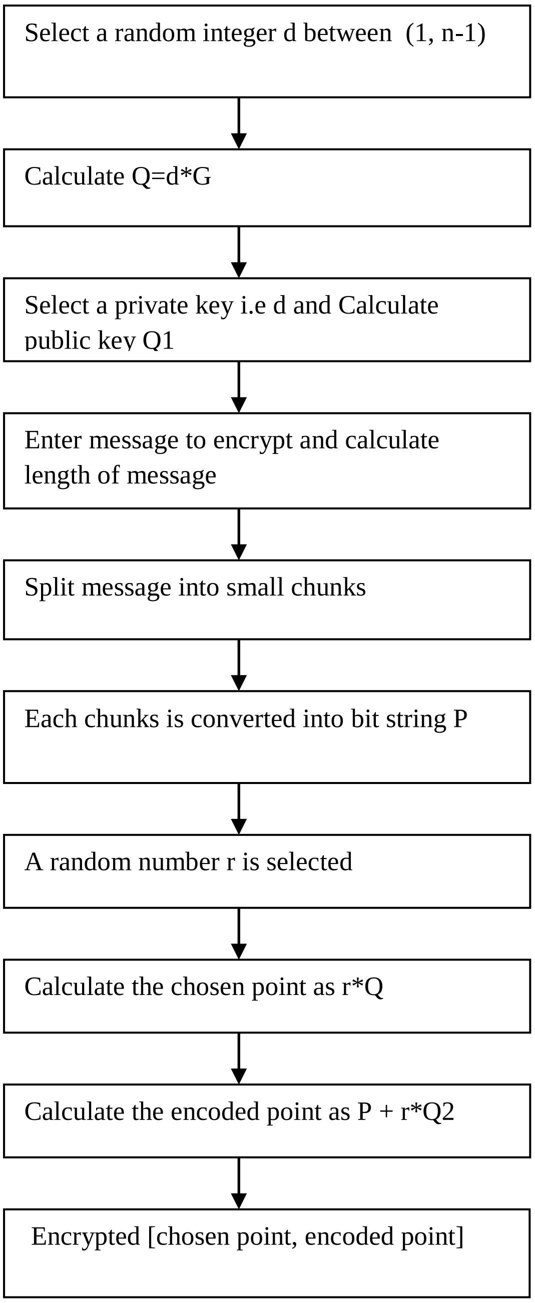

Select a random integer d between (1, n-1)
Calculate Q=d*G
Select a private key i.e d and Calculate public key Q1
Enter message to encrypt and calculate length of message
Split message into small chunks
Each chunks is converted into bit string P
A random number r is selected
Calculate the chosen point as r*Q
Calculate the encoded point as P + r*Q2
Encrypted [chosen point, encoded point]

Fig.8. Flow Chart of ECC Encryption

4.3 Compression using Lempel Ziv Welch Technique: It is one of the best loss less compression technique. It is very simple and fast to apply. If the message contains more repetitive data file size is reduced. No loss of data during or after compression. LZW is more advantageous than Huffman coding i.e. it does not requires prior information of input data stream. LZW technique compress the input data stream in a single step and it allows fast execution[1].

4.4 Edge detection using Canny edge detector: It is one of the most popular algorithm for edge detection[7].

The process for canny edge detection is as follows

1. Gaussian filter is applied to image for smoothing so as to remove the noise.
2. Intensity gradients are calculated using different operators.
3. To get rid of spurious response applies non maximum suppression to edge detection.
4. To determine the potential edges apply double threshold by using hysteresis, weak edges are suppressed.
5. The detection of edges are finalized.

Below figure shows the example of edge detection.

4.5 Embedding using LSB Insertion technique: The least significant bit (in other words, the 8th bit) of some or all of the bytes inside an image is changed to a bit of the secret message[3][11]. Digital images are mainly of two types 24 bit images and 8 bit images. In 8 bit images, one bit of information can be embedding in each pixel. In 24 bit images three bits of information is embed in each pixel, one in each LSB position of the three eight bit values. Each pixel bytes contains either 1 or 0. Increasing or decreasing the value by changing the LSB does not change the appearance of the image much so the resultant stego image looks almost same as the cover image.

The changes that are made to the least significant bits are too small to be recognized by the human eye, so the message is effectively hidden. The advantage of LSB embedding is its simplicity and many techniques use these methods LSB embedding also allows high perceptual transparency.

V. CONCLUSION

The system is designed by Hybrid encryption, LZW compression and steganography techniques. Secret image is encoded by AES encryption again encoded by ECC Encryption technique then it is compressed by LZW compression technique. Cover image edges are detected by canny Edge detector to embed the secret image. The proposed system blocks are discussed. Hybrid encryption i.e AES and ECC methods, LZW compression and Canny edge detection techniques are implemented. Least significant bit method is used to embed the secret image into the edge detected cover image to get better PSNR values.

REFERENCES

[1] Archana T Chawan, et al., "A high secure and robust lsb image steganography using Hybrid Encryption, LZW compression and Knight tour algorithm" *Proceeding of International Conference on Research Methods in Engineering and Technology*, ISSN: 978-151-1885-033, June 2015.

[2] Nadeem Akhtar, et al., "Inverted LSB Steganography", *International Conference on Issue and Challenges in Intelligent Computing Techniques(ICICT)*, 978-1-4799-2900-9/14@2014 IEEE.

[3] B.Debiprasad, et al., "A Novel secure image steganography method based on chaos theory in spatial domain*" International Journal of Security Privacy and Trust Management (IJSPTM)* Volume 3, No 1, February 2014.

[4] Shrutika suri, et al., "Comparative analysis of steganography for Coloured images" *International Journal of Computer Science and Engineering (IJCSE)*, Volume 2, Issue 4, E-ISSN 2347-2693, April 2014.

[5] P.M.Sivaraja and E.Baburaj, "Information hiding scheme for digital images based on Genetic algorithm" *Indian journal of applied research*, Volume 4, Issue 6, ISSN:2249-555X, June 2014.

[6] K.S.Arora and G.Gandhi, "Enhanced steganography using K-matrix*" Research Paper International Journal of Computer Science and Engineering (IJCSE)*, Volume 2, Issue 6, E-ISSN:2347-2693, June 2014.

[7] Saurabh Singh and Ashutosh Datar, "Improved hash based approach for secure color image steganography using canny edge detection method" by, *International Journal of Computer Science and Network Security(IJCSNS)*, Volume.14 no.7, July 2014.

[8] Y.P.Zhang, et al., "Research on embedding capacity and embedding efficiency of information hiding based on digital images" *International Journal of Intelligence science*, 2013,3,77-85 April 2013.

[9] J.J.Wang, et al., "An Adaptive matrix embedding technique for binary hiding with an efficient LIAE algorithm" *WSEAS Transaction on Signal Processing*, ISSN: 2224-3488, Issue 2, Volume 8, April 2012.

[10] Ankita Agarwal, "Security enhancement scheme for image steganography using S-DES technique" *Research paper*, Volume 2, Issue 4, ISSN:2277 128X, April 2012.

[11] Mrs. Kavitha, et al., "Steganography using lsb Algorithm" *International Journal of Engineering and Application (IJERA)*, ISSN: 22448-9622, Volume 2, Issue 3,pp. 338-341, June 2012.

[12] Shailender gupta, et al., "Information Hiding using LSB steganography and cryptography*" IJ Modern Education and Computer Science(MECS)*, June 2012 ,6,27-34.

[13] Nitin Jain, et al., "Image Steganography using LSB and Edge Detection Technique" *International Journal of Soft Computing and Engineering(IJSCE)*, ISSN:2231-2307, Volume-2, Issue-3, July 2012.

[14] Obaida Mohammad Awad Al-Hazaimeh "Hiding data in images using new Random Technique" *International Journal of Computer Science Issue (IJCSI)*, Volume 9, issue 4, No 2, july 2012, ISSN:1694-0814.

[15] Jassim Mohmmed Ahmed and Zulkarnain Md Ali " Information hiding using LSB technique" *International journal of computer science and network security (IJCSNS)*, Volume 11, No.4, April 2011.

[16] Y.P.Zhang et al., "A new scheme for information hiding based on digital images" *Seventh International Conference on Computational Intelligence and Security*, IEEE 2011.

[17] Yogendra kumar, et al., "A novel image steganography method with Adaptive number of lsb modification based on *+Private stego-key" *International Journal of Computer science and Security,* Volume 4, Issue 1, March 2010.

[18] A.Nag, et al., "A novel technique for image steganography based on block DCT and Huffmann encoding" *International Journal of Computer science and Information Technology,* Volume 2, No 3, June 2010.