I. J. Computer Network and Information Security, 2023, 2, 31-47
Published Online on April 8, 2023 by MECS Press (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2023.02.03

Two-Layer Security of Images Using Elliptic Curve Cryptography with Discrete Wavelet Transform

Ganavi M.*
JNNCE/CSE, Shivamogga, 577204, Karnataka, India
E-mail: gaanavi4@jnnce.ac.in
ORCID iD: https://orcid.org/0000-0002-4149-0144
*Corresponding author

Prabhudeva S.
JNNCE/MCA, Shivamogga, 577204, Karnataka, India
E-mail: pdshirematt@gmail.com
ORCID iD: https://orcid.org/0000-0002-7720-3776

Received: 08 August 2021; Revised: 03 November 2021; Accepted: 17 February 2022; Published: 08 April 2023

Abstract: Information security is an important part of the current interactive world. It is very much essential for the end-user to preserve the confidentiality and integrity of their sensitive data. As such, information encoding is significant to defend against access from the non-authorized user. This paper is presented with an aim to build a system with a fusion of Cryptography and Steganography methods for scrambling the input image and embed into a carrier media by enhancing the security level. Elliptic Curve Cryptography (ECC) is helpful in achieving high security with a smaller key size. In this paper, ECC with modification is used to encrypt and decrypt the input image. Carrier media is transformed into frequency bands by utilizing Discrete Wavelet Transform (DWT). The encrypted hash of the input is hidden in high-frequency bands of carrier media by the process of Least-Significant-Bit (LSB). This approach is successful to achieve data confidentiality along with data integrity. Data integrity is verified by using SHA-256. Simulation outcomes of this method have been analyzed by measuring performance metrics. This method enhances the security of images obtained with 82.7528db of PSNR, 0.0012 of MSE, and SSIM as 1 compared to other existing scrambling methods.

Index Terms: Elliptic Curve Cryptography, DWT, Encryption, Decryption, Hiding, Extracting.

1. Introduction

The different forms of multimedia details, such as digital images, audio signals, and frames of video, have led to the speedy growth and development of communication systems and innovations. For many applications, including military, commercial and medical, digital images are more frequently used. In all these cases, the carrying and repository of images through a public domain becomes a challenging issue. Thus, the field of information security must dominate the communication world. Information security protocols must allow only authorized users to access, use, and modify the data. Information Security systems are built with three major objectives, Confidentiality, Integrity, and Availability [1]. The confidentiality of digital images can be preserved by using various types of technology such as scrambling, embedding, and watermarking.

Cryptography algorithms scramble the substantial images into unidentifiable and unreadable scrambled images, making them reach only the intended recipients. It is a technique to protect and safeguard secret information from cyber criminals [2]. Thus, scrambling techniques are classified into secret-, public-key, and hash systems. Single-key is used in the secret-key cryptosystem. But the challenging issue is the key distribution. Whereas in a public-key cryptosystem, computational complexity is a major concern even though using two different keys, one to scramble and another to descramble. Public-key innovation put forward recommended safety apart from secret-key innovation. Intensify data security is the predominant interest of asymmetric innovation. It is the most immovable scrambling procedure since end-users are not at all recommended to give away their private keys, thereby diminishing the prospect of a hacker tracking down an end user's private key during conveyance.

Rivest–Shamir–Adleman (RSA) is very methodical in scrambling nonetheless slow-going to descramble [3]. But

ECC is more methodical and steadier than RSA [4]. Smaller keys in ECC are as powerful as lengthier keys in RSA. Such an outcome produces reduced web overhead, permitting high-speed execution. The hash algorithm produces a fixed-size hash value for any arbitrary-size input. It is a one-way function. It helps computer administrators to encrypt passwords and it can be used to verify the user. SHA-256 bases are applied frequently for coding such as information substantiation, digital signatures, etc [2]. Therefore, it should be faster, quicker nonetheless to compute and confirm. It is more special and secure as it is a one-way computation, that can't be achieved in reverse order. Nonetheless, Cryptography converts information unreadable, and steganography hides the existence of a message from the intruder.

Most of the cryptographic scrambling methods furnish security to the data conveyance. Some methods restrict integrity analysis on transferred data. There is a necessity to implement a robust system so that it should analyze data integrity along with maintaining its confidentiality. In this paper, a more powerful ECC algorithm along with SHA-256 is used to get the scrambled mode of the secret image. This permits first-level security to the secret image.

After the scrambling process for any secret image, then there is a necessity of hiding the process in the cover. Embedding and extracting the information from other media can be done by the technique known as Steganography. Spatial and transform domains can be used to carry out embedding. Spatial domain methods hide secret information directly on pixels of carrier images and are easy to implement. The LSB steganography is one such method where the least significant bit is changed by another information bit [5]. This perspective has the benefit as simple to learn and effortless to encode. Whereas transform domain techniques embed data in the transformed coefficients and are complex to implement. Discrete Wavelet Transform (DWT) has decoded the issues in robustness and reliability. The reliability level in the transform discipline is greater in comparison with spatial discipline [3, 6, 7]. As DWT is a stronger transform to achieve a robust and reliable system [8], in this paper DWT is applied to the carrier image two times. Then LSB is applied to hide encrypted pixels on DWT transformed pixels. This permits second-level security to the secret image.

Independently, cryptography, steganography, and hashing algorithms contribute confidentiality and integrity to the data but with their susceptibility. Therefore, many researchers have proposed various systems by applying combinations of cryptography and steganography algorithms. Combining cryptography, steganography, and hashing algorithms can lead to a more powerful and robust system.

In this paper, an approach with two-tier protection of sensitive data is proposed by combining elliptic curve cryptography (ECC), DWT, SHA-256, and LSB. This paper is explained in order Segment 1 presents an introduction to encryption and embedding, segment 2 gives information about the motivation behind this work, and segment 3 presents the contribution of the paper. Segment 4 surveys different existing encrypting and embedding methods. Segment 5 presents the methodology of the proposed system. Segment 6 consists of results and performance analysis and segment 7 include the conclusion.

2. Motivation behind this Work

The stretching capability of current communications demands the security of data. As data being traversed on the internet increases, information security is becoming more significant. Confidentiality and data integrity are essential to safeguard from unofficial users. Such security can be obtained by utilizing good encryption and embedding algorithms. ECC is a public key algorithm based on an elliptic curve used to generate speedy, tidy, and well-ordered encryption keys [9,10]. ECC provides more security with lesser bits comparable to RSA systems. SHA-256 hashing can be applied to image data types to obtain data integrity. It is a non-reversible one-way process. DWT can be used as a stronger transform domain steganography which is applied for embedding the sensitive information in the frequency domain and it can be determined as the study of indistinguishable communication. The LSB steganography can be applied to replace the least significant bit of the pixel with secret or encrypted information [9]. As ECC consumes less memory and is faster [11] than RSA, can be combined with SHA-256 to scramble the secret image. This provides the first level of security to the secret image. DWT is a stronger transform and can be combined with LSB for embedding the scrambled image. This provides a second level of security to the secret image.

3. Contribution of Paper

The security challenge for the communication of information is Confidentiality. It is the prevention of disclosure of information to unauthorized parties. This can be achieved only by applying cryptographic scrambling algorithms on information to make it unintelligible to all but only to authorized users. The next security challenge is message integrity, maintaining information unchanged during transmission. This can be achieved by applying hash algorithms. Further next level of security can be achieved by stronger steganographic transform domain techniques to make the information undetectable. The objectives of this work are to enhance the confidentiality, message integrity, and undetectability of the input secret images. Such security is obtained by utilizing the encrypting and embedding methods. The proposed work includes:

- Scramble the input secret images using ECC.
- Find the hash of the input image, and add it to scrambled pixels.
- Convert cover image to transform domain using DWT at two levels.

- Insert scrambled image pixels at LSB of the first level of DWT.
- Added scrambled with hash is inserted at the second level of DWT.
- Security measures for the encrypted and stego are analyzed.

4. Related Works

Researchers have developed several image scrambling and steganography methods. Space- and frequency domains are the major category where steganography algorithms are designed and can be differentiated. Each of them has its advantages and disadvantages. Based on the security requirement, particular algorithms, or combinations of these can be applied for enhancing the security of the data. Major security goals of information hiding are confidentiality, undetectability, and the imperceptibility of non-disclosure data.

Transformed images are helpful to achieve confidentiality so that data is undetectable to the intruder. DCT and DWT are the two compression techniques that can be used to perform the embedding process. DCT has been used in [1] to get the frequency sub-bands of the carrier. Hiding of data is done on middle and high-frequency bands with different zigzag scanning fashions. Applied chaotic sequences for the selection of color channels, blocks, and coefficients in the hiding and scrambling stage. They applied DCT on the carrier, and examine the AC coefficients in a zigzag manner. This scan is used to identify the embedding positions in the carrier. The chaotic function is used on the secret image to get the sequence. The generated sequence is embedded using DCT in a carrier. SSIM is a measurable metric, that can be utilized to examine the visible quality of the stego. The resultant outcome is less bit error rate (BER) with more embedding capacity.

A good compression ratio can be obtained using DWT when compared to DCT. DCT uses low processing power, but it is a lossy compression technique. A variety of discrete wavelet transformations can be applied to the image to transform. A combination of DCT and DWT can also be applied to the carrier to perform steganography. So many encryption algorithms can be used to scramble sensitive data. An OTP is used for scrambling input data in [2]. Carrier is processed through DCT, followed by DWT, and then encrypted data is hidden in the low-level sub-band. A method in [3] used DCT to compress the input image and then scrambled it using RSA by taking two large prime numbers. Carrier is applied with two-level DWT and its high-frequency band is used for embedding secret data.

A method in [4] scrambled the plain text using ECC. One-level DWT is applied to carriers to embed the scrambled text. A method is proposed in [5] for hiding and extracting secret information on carrier media with DWT and LSB. The major contribution is embedding multiple images within a single carrier. They measured PSNR, MSE, and NCC. Their method resulted in better efficiency and capacity. Laplace transforms in hiding and extraction phases have been used in [6]. This approach is based on frequency domain steganography. Performance parameters are evaluated to security level. A method to scramble the information by two-level and then used two-bit inverted LSB for embedding has been proposed in [7]. First level by Arnold's transformation and then by RSA. PSNR and entropy are used as security measures. Image steganography in [8] used LSB and DWT for digital images to enhance the robustness. Performance metrics such as MSE, PSNR, BER, and total time to execute are used to evaluate the system.

A method in [9] used audio as a carrier and decomposed it into approximation and detail coefficients by applying DWT. Encrypting data before embedding give more security. So, data is encrypted with RSA. Detail coefficients are used for embedding the scrambled data. Four-level decomposition of carrier is done using DWT. A method in [10] adopted quantum cryptography with Huffman encoding to achieve two-level security. Noisy pels of the carrier are used for hiding. Noisy pels of the carrier were used for the hiding process and achieved high embedding capacity with reduced pictorial quality. Machine learning techniques have been adopted in image steganography. An approach in [11] used DCT to scramble the carrier image and later hiding capacity of DCT blocks is identified by using a quantization table. An optimized modified quantization table is suggested in this paper.

A Haar wavelet to get the frequency domain transformation of the carrier, and then a randomly generated key is used to identify the location to embed it on the carrier in the [12]. Four sub-bands of the carrier generated by using the Haar wavelet transform are used in [13]. A high-frequency sub-band is used for hiding scrambled with histogram modification data. Scrambling is done on rows and then on columns to get a strong security process. Results are measured with PSNR and correlation. An integer wavelet transforms for image embedding has been used in [14]. Classification of edge coefficients is determined by MSBs and used to embed the information. DWT can be used for hiding on a human visual system model. Watson's visual system model has been used in [15]. The utmost endurable swap in DWT coefficient in the HSV model is withdrawn to fix it to the histogram of low-precision coefficients and then the communication bits are ciphered. The SSIM is used to measure perceptual quality. In all these research papers, authors have contributed to the embedding of data using DWT. The embedding process is carried out on a high-frequency sub-band as it makes data undetectable.

OTP has been applied in [16] for scrambling of input data. The high-frequency band is selected by using a wavelet. PN generators are used in generating random binary numbers. This method is successful in improving the stego images. A combination of revised RSA and LSB has been proposed in [17]. Scrambling of message done by RSA algorithm. Edge and non-edge pixels in the carrier are segregated by Canny edge detection. LSB is used to hide secret information bits. Performance metrics are measured. This method is successful in effectiveness, security, and undetectability.

A method has been proposed in [18] where an improvement of the existing hiding methods with variable data into the required frequency band is introduced. Results are presented with varying input data lengths to generate less PSNR. But higher PSNR can be achieved by increasing DWT levels**.** Scramble and embedding secret data in the carrier are the other techniques that can be used to enhance the security of data. There is a necessity of securing the data while transmission as well as while storage. A hashing technique using SHA-256 to achieve data confidentiality and integrity in images has been proposed in [19]. The model resulted in high PSNR for various images. A bit matching embedding algorithm is presented in [20] that computes the position of matched pels and then used them to retrieve the secret bits. This method is used with the Advanced Encryption System (AES) to further enhance the security of images. The Colour channels of the cover are used for matching the bits. Blocking can be applied to images that are later used for matching the blocks. The operation is carried out on coefficients of approximation and detail on the secret and carrier, respectively.

An approach is proposed in [21] that resulted in hiding large data within a single media. The carrier and secret images are applied with DWT. Matching of a pixel in cover and secret is carried out to perform embedding. PSNR is used for the performance of the stego image. An image scrambling method is proposed in [22] which is based on Power Modulus Scrambling (PMS) and the blocking technique. Key-based permutation & combination has been adopted for hiding information. This resulted in the good imperceptibility of images. Scrambling of input information using OTP has been used in [23]. The high-frequency band at the fourth level is used for embedding the scrambled data. PSNR, MSE, and NCC are used for the comparison of results with the existing other methods. A combination of DWT with the Laplacian pyramid for steganography has been used in [24]. An edge-based image embedding has been proposed in [25]. Dual-Tree Complex Wavelet Transform (DT-CWT) has been adopted for the hiding process. A modified quantization table is used to find the location of hiding in the Laplacian pyramid. This method in [26] was achieved with high embedding capacity with better stego-quality. A hybrid model is proposed in [27]. The plaintext is scrambled using an asymmetric and the computed hash is scrambled using an asymmetric. Combining these two resulted in a cipher.

The combination of RSA, Huffman-coding, DWT, and LSB is used in [28]. Compression of input text is done by Huffman and then encrypted by RSA. Carrier is compressed by DWT and later uses LSB to place the scrambled text in DWT coefficients. Security measures are also evaluated to result in a good performance. An approach in [29] used Elliptic Curve Cryptography (ECC) and LSB Inversion. Scrambling of information has been done by ECC and later hidden on the carrier by LSB Inversion. Some steganalysis attacks like visual, histogram and chi-square are tested on the stego-results. Comparisons for improved embedding capacity with other existing methods are also presented. An adaptive method for image steganography has been proposed in [30]. This is based on the inverted LSB method. The best pattern for inverted LSB substitution is selected by calculating the error ratio for different patterns.

In this literature survey, requisite contributions in the field of encryption and embedding systems are described. The encryption of the input image before hiding it plays an important role. An encryption algorithm ECC with a less key size would provide more security in comparison with the RSA algorithm. When spatial hiding techniques are combined with transform type will be helpful to obtain a more hiding capacity with less manipulation. Therefore, encryption followed by hiding using transform type is the best-suited approach.

5. Methodology

The proposed approach contains three stages. In stage one, ECC with modifications is applied to encrypt the image. Obtain hash of image using SHA-256. This is merged with an encrypted image to prove the data integrity. In stage two, the carrier image is applied with DWT [3,7,8] to generate four sub-bands as LLs1, LHs1, HLs1, and HHs1. Apply DWT on the LLs1 sub-band to generate next-level sub-bands as LLs2, LHs2, HLs2, and HHs2. In the final stage, the encrypted and hash merged image is hidden in the HHs1 and HHs2 sub-bands accordingly. LSBs are used while obtaining the stage. The process in the reverse order is followed at the receiver. This is presented in Fig.1 and Fig.2.

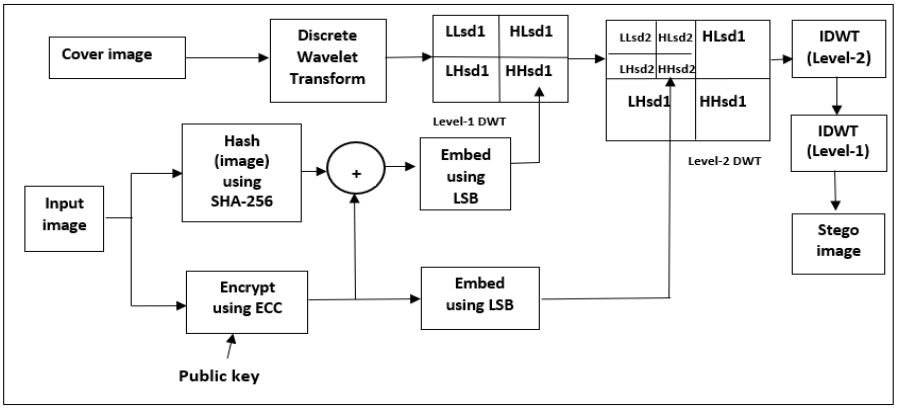


Fig.1. Encrypt and hide at source.

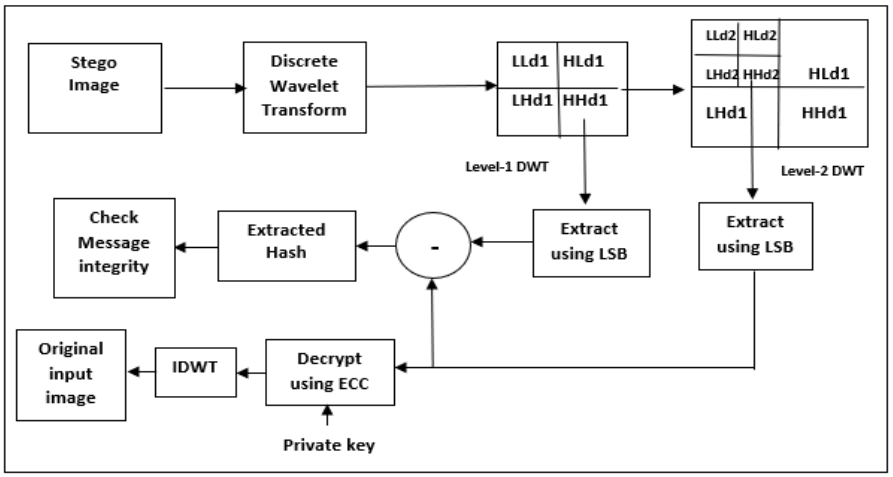


Fig.2. Extract and decrypt at destination.

5.1. Encryption and Decryption Process

Input secret images are secured by encryption using an algorithm ECC. The private key is generated using the prime number and generator point. This key varies on the prime number selected. The steps followed in the ECC algorithm are:

- Obtain all points for an elliptic curve $E_{pm}\ (a_m, b_m)$.
- Allocate every point to every pixel for the input image in the order from 0 to 255, presented in Table 1.
- Select generator $G_m\ (x_m, y_m)$ with order 'n' in $E_{pm}\ (a_m, b_m)$
- At the source**,** obtain private and public keys as

$$Src\_pr = x \tag{1}$$

$$Src\_pub = X = x * G_m\ (x_m, y_m) = (Src\_xpub,\ \mathrm{Src}\_ypub) \tag{2}$$

- Pick arbitrary number 'r' and multiply with 'G_m'

$$R_m = r * G_m\ (x_m, y_m) = (R_m\_xpub,\ R_m\_ypub) \tag{3}$$

- Take the first pel from the input and map it to a point using Table 1. Continue this procedure until all the pixels are mapped to points, as presented in Fig.3 & Fig.4.
- At the destination, obtain private and public keys as

$$Dst\_priv = y \tag{4}$$

$$Dst\_pub = Y = y * G_m\ (x_m, y_m) = (Dst\_xpub,\ B\_ypub) \tag{5}$$

- Generate cipher using '*Src_pr*' and '*Dst_pub*' for an input '$Pi\ (x_m, y_m)$' as

$$Ci\ (x_m, y_m) = Pi\ (x_m, y_m) + (Src\_pr * \mathrm{Dst}\_pub) + (R_m) \tag{6}$$

here $i =$ 0, 1, 2, …….255

- Now, the cipher '$Ci\ (x_m, y_m)$' is converted to pixels using Table 1 resulting in 'C_{enc}', as shown in Fig.5 & Fig.6.
- Transfer 'C_{enc}' by hiding using DWT in carrier media.
- At the destination, decrypt the cipher using

$$Pi\ (x_m, y_m) = Ci(x_m, y_m) - (Dst\_priv * \mathrm{Src}\_pub) - \mathrm{R} \tag{7}$$

here $i =$ 0, 1, 2, …….255

Table 1. Points generated for the elliptic curve E_{pm} (a_m, b_m).

Pixel value	Points on ECC
0	(0,32)
1	(0,219)
2	(1,5)
.	.
5	(2,6)
.	.
25	(22,28)
.	.
78	(74,210)
.	.
105	(101,118)
.	.
201	(191,49)
.	.
255	(239,1)

25	29	105	.	24
45	5	39	.	25
13	78	89	.	52
42	76	96	.	56
.	.	.	.	.
28	57	66	.	48

Fig.3. Grayscale image with pixel value.

(22, 88)	(27, 22)	(101,118)	.	(20,161)
(41,64)	(2,6)	(37,37)	.	(22,88)
(11,89)	(74,210)	(84,82)	.	(48,149)
(38,129)	(73,167)	(90,236)	.	(53,246)
.	.	.	.	.
(24,134)	(53,39)	(64,171)	.	(46,217)

Fig.4. Pixel mapped to ECC points according to Table 1.

(59,153)	(11,162)	(181,46)	.	(199,39)
(74,41)	(222,149)	(210,100)	.	(20,26)
(6,248)	(83,19)	(35,37)	.	(84,82)
(96,214)	(204,225)	(125,83)	.	(245,223)
.	.	.	.	.
(75,196)	(192,15)	(1,5)	.	(206,189)

Fig.5. Encrypted ECC points.

62	14	191	.	217
77	238	231	.	223
10	87	37	.	89
100	224	311	.	258
.	.	.	.	.
80	203	3	.	226

Fig.6. ECC points mapped to pixels.

5.2. Embed and Extract Process

The second layer of security of the encrypted image is provided by hiding in a carrier. DWT converts the carrier into sub-bands. Approximation contains information whereas details include noise. Therefore, use noisy sections to hide the secret information. Though the DWT is a complex, tedious frequency domain technique, more protected and insusceptible to noises. LSB in the carrier is replaced by an encrypted image. SHA-256 hashing is utilized to clarify the data unchanged in the sent message.

The procedure to hide the cipher in a carrier is as follows:

- Take the carrier image.
- Apply 2D DWT on the carrier to generate coefficients of approximation as *'LLsd1'* and detail as *'LHsd1', 'HLsd1', and 'HHsd1'* accordingly.

$$\left[LLsd1,\ LHsd1,\ HLsd1,\ HHsd1\right] = dwt2\ (carrier\_image,'haar') \tag{8}$$

- Compute the hash of secret image *'Isecret_image'* by using SHA-256.

$$Pi\_hash = sha256hasher.ComputeHash\left(Isecret\_image\right) \tag{9}$$

- Combine two images from equations (6) and (9).

$$Cenc\_hash = Ci\ \left(x_m,\ y_m\right)\ +\ Pi\_hash \tag{10}$$

- Use LSB to embed *'Cenc_hash'* in *'HHsd1'* detail coefficient segment.
- Apply 2D DWT on *'LLsd1'* to generate coefficients of approximation as *'LLsd2'* and detail as *'LHsd2', 'HLsd2', and 'HHsd2'* accordingly.

$$\left[LLsd2,\ LHsd2,\ HLsd2,\ HHsd2\right] = dwt2\ \left(LLsd1,\ 'haar'\right) \tag{11}$$

- Use LSB to embed cipher image *Ci* (x_m, y_m) in *'HHsd2'* detail coefficient segment.
- Use 2D Inverse DWT (IDWT) to recreate the segment *'LLsd1'* by utilizing *'LLsd2', 'LHsd2', 'HLsd2', and 'HHsd2'* as

$$LLsd1 = idwt2\ (LLsd2,\ LHsd2,\ HLsd2,\ HHsd2,'haar') \tag{12}$$

- Use 2D IDWT to generate the stego by utilizing *'LLsd1', 'LHsd1', 'HLsd1', and 'HHsd1'* as

$$Stego\_image = idwt2\ (LLsd1,\ LHsd1,\ HLsd1,\ HHsd1,'haar') \tag{13}$$

The procedure to extract the cipher from the carrier is as follows:

- Take the stego image.
- Apply 2D DWT on the stego to generate coefficients of approximation as *'LLd1'* and detail as *'LHd1', 'HLd1', and 'HHd1'* accordingly.

$$\left[LLd1,\ LHd1,\ HLd1,\ HHd1\right] = dwt2(Stego\_image,'haar') \tag{14}$$

- Use LSB to extract *'Cenc_hash'* from *'HHd1'*.
- Apply 2D DWT on *'LLd1'* to generate coefficients of approximation as *'LLd2'* and detail as *'LHd2', 'HLd2', and 'HHd2'* accordingly

$$\left[LLd2,\ LHd2,\ HLd2,\ HHd2\right] = dwt2(LLd1,'haar') \tag{15}$$

- Use LSB to extract *Ci* (x_m, y_m) from *HHd2*.
- Subtract *Ci* (x_m, y_m) *from Cenc_hash* to get *Pi_hash.*

$$Pi\_hash = Cenc\_hash - Ci\ \left(x_m, y_m\right) \tag{16}$$

- Use the ECC algorithm to decrypt *Ci* (x_m, y_m) to obtain the input secret image, *Pi* (x_m, y_m) as shown in equation (7)
- Compute the hash of an obtained image *Pi* (x_m, y_m).

$$Pi\_hash\_calc = sha256hasher.ComputeHash\left(Pi\ \left(x_m, y_m\right)\right) \tag{17}$$

- Confirm whether the hash values '*Pi_hash'* and '*Pi_hash _calc'* at equations (16) and (17) are the same or not. If remains the same, then it tells that encrypted data sent is not changed while communicating. Or else, it is modified. This step is processed to clarify the integrity of the data.

6. Results and Analysis

Some of the input secret and carrier images used are presented in Fig.7. and Fig.8. These are taken from USC-SIPI [31] and KODAK [32] databases. The points generated using ECC are depicted in Fig.9. Input, ECC encrypted, and hash added encrypted image is presented in Fig.10. Carrier, 2D DWT of the carrier and stego is presented in Fig.11. Decrypted image is presented in Fig.12 and equivalent histograms are depicted in Fig.13. Histogram of the encrypted indicates the uniform distribution of data i.e., encrypted image is more random. Histograms of the carrier & stego are the same. No one can recognize the identity of the secret in the carrier. It becomes difficult for any hacker. Hence, this system provides better safety to the input secrets.

Fig.7. Input secret images.

Fig.8. Carrier images.

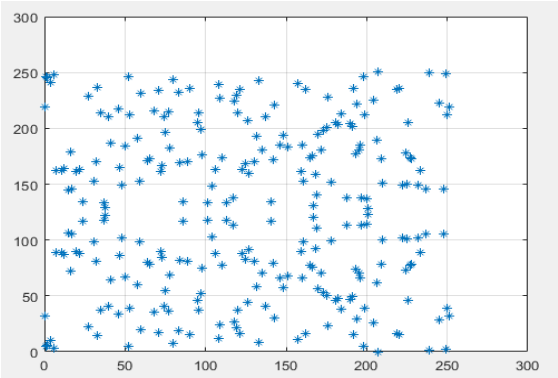


Fig.9. Generated ECC points.

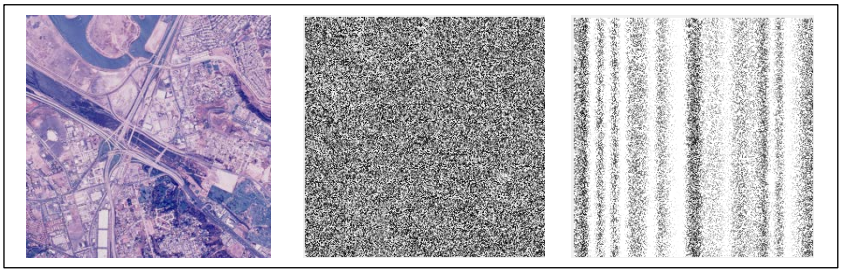


Fig.10. Input secret (San Diego.tiff), ECC encrypted, and hash added encrypted image.

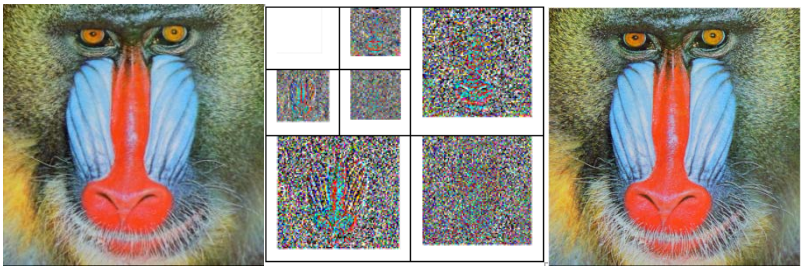
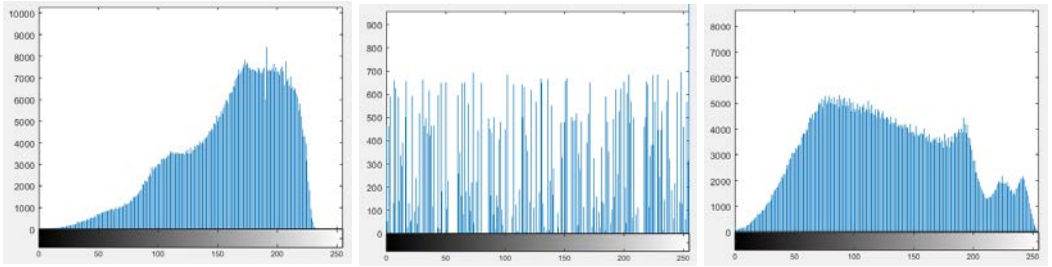
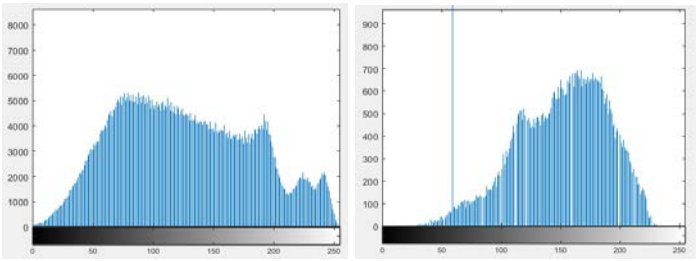


Fig.11. Carrier (Mandril.tiff), 2D DWT, and Stego.

Fig.12. Decrypted Image.



(a) (b) (c)



(d) (f)

Fig.13. Histogram of (a) Input, (b). Encrypted, (c) Carrier, (d). Stego, and (f) Decrypted Image.

6.1. Performance Analysis

The performance of this system is analyzed by measuring the security metrics. Some of the security measures used are as follows

A. Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), and Structural Similarity Index (SSIM)

MSE is practiced by evaluating the error amid estimated and actual values. Higher MSE gives better security for the encrypted and less MSE gives better picture quality in the stego.

$$MSE = \frac{1}{P1*P2}\sum_{i=1}^{P2}\sum_{j=1}^{P1}\left[J1(i,j) - J1'(i,j)\right]^2 \tag{18}$$

Where P_1, P_2 = Total rows & columns in picture, *J1(i, j)* = input picture and *J1' (i, j)* = output picture

PSNR is practiced for the computation of quality assessment among images. Lower PSNR represents more randomness in the encrypted and higher PSNR represents higher quality reconstruction from the stego.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \tag{19}$$

An SSIM measure assesses the perceptual dissimilarity among two indistinguishable images. In an encrypted, the SSIM value should be nearer to zero and it should be 1 for the stego.

$$I(x,y) = \frac{\left(2\mu_x\mu_y + c_1\right)\left(2\sigma_{xy} + c_2\right)}{\left(\mu^2{}_x + \mu^2{}_y + c_1\right)\left(\sigma^2{}_x + \sigma^2{}_y + c_2\right)} \tag{20}$$

where c_1 and c_2 are constants, *x* and *y* are carrier & stego. Then, μ & σ are the averages & standard deviation.

B. Number of Pixel Change Rate (NPCR), Unified Average Changing Intensity (UACI), and Information Entropy

NPCR is the difference in the pace of the number of pixels in cipher when just a single pixel of an input image is adjusted. NPCR should be nearer to 100 for encrypted and should be nearer to zero for stego.

$$NPCR = \frac{1}{P*Q}\sum_{w1=1}^{P}\sum_{w2=1}^{Q} A(w1,w2)*100\% \tag{21}$$

where $A(w1,w2) = \begin{cases} 1, & if\ y1(w1,w2) \neq y1'(w1,w2) \\ 0, & if\ y1(w1,w2) = y1'(w1,w2) \end{cases}$

UACI is the average level matrix change among the pixels of two images. The ideal value for UACI is 33.

$$UACI = \left(\sum_{w1=1}^{P}\sum_{w2=1}^{Q}\left(\frac{|\,y1(w1,w2) - y1'(w1,w2)\,|}{255*P*Q}\right)\right)*100\% \tag{22}$$

where P*Q is image dimension, *y1(w1, w2)* is ciphertext pixel concerning original plaintext, and *y1' (w1, w2)* is ciphertext pixel concerning changed plaintext. The values obtained for NPCR and UACI in the recommended approach are given in Table 2. This method is unsusceptible to differential attacks.

Information Entropy is helpful in the quantifiable investigation and assessment of information. The maximum entropy value for scrambled should be 8-bits.

$$E = -\sum_{k=0}^{N} pk \log_2 (pk) \tag{23}$$

where N is the number of characters, and pk is the probability of the presence of character k.

The proposed approach has encryption and hiding stages. The analysis is carried out by measuring performance metrics as shown in Table 2. Fewer PSNR & higher MSE shows more randomness in the encrypted image. This makes it tough for an attacker to identify and get the data back. Less SSIM, 100% NPCR, and UACI >33.46% in encrypted images gives good result. In the proposed approach, PSNR is 9.0534(dB), MSE is 8.46e+03, SSIM is 0.0156, NPCR is 99.63, and UACI is 33.4635 accordingly.

Table 2. The measure of performance metrics for encrypted images.

Input secret images	PSNR	MSE	SSIM	NPCR	UACI
Mandril.tiff	9.1758	7.8614e+03	0.0140	100	33.4635
CT scan.tiff	9.5351	9.3735e+03	0.0126	99.56	33.4635
lena_color_512.tif	8.8816	8.4124e+03	0.0202	100	33.4635
lena_color_256.tif	8.8576	8.4590e+03	0.0170	100	33.4635
Peppers.tiff	8.7022	8.7672e+03	0.0173	100	33.4635
San Diego.tiff	9.1683	7.8750e+03	0.0123	100	33.4635
Average	9.0534	8.46E+03	0.0156	99.93	33.4635

Table 3. The measure of performance metrics for stego1 images.

Input secret images	PSNR	MSE	SSIM	NPCR	UACI	Information Entropy	
						Carrier	Stego
Mandril.tiff	80.5941	0.0056	1	0.0567	33.4635	7.7624	7.7624
CT scan.tiff	75.5952	0.0018	1	0.1793	33.4635	7.7624	7.7624
lena_color_512.tif	75.0462	0.0020	1	0.2035	33.4635	7.7624	7.7624
lena_color_256.tif	75.2348	0.0019	1	0.1948	33.4635	7.7624	7.7624
Peppers.tiff	76.9254	0.0013	1	0.1324	33.4635	7.7624	7.7624
San Diego.tiff	76.0323	0.0016	1	0.1621	33.4635	7.7624	7.7624
Average	76.5713	0.0024	1	0.1548	33.4635	7.7624	7.7624

Carrier is applied with DWT, utilized LSB to hide, and generated with stego. Tables 3 and 4 include the measure of performance metrics for stego. More PSNR, less MSE, SSIM as 1, less NPCR, and UACI >33.46% for stego give good results. By taking Mandrill. tiff as a carrier in Table 3, stego1 PSNR is 76.5713 (dB), MSE is 0.0024, SSIM is 1, NPCR is 0.1548, UACI ss 33.4635 accordingly. By taking Peppers.tiff as the carrier, the stego2 PSNR is 75.9604(dB), MSE is 0.0014, SSIM is 1, NPCR is 0.1481, UACI is 33.4635 accordingly. Information entropy remains the same after hiding the data as shown in Tables 3. & 4.

Table 4. The measure of performance metrics for stego2 images.

Input secret images	PSNR	MSE	SSIM	NPCR	UACI	Information Entropy	
						Carrier	Stego
Mandril.tiff	76.2596	0.0004	1	0.0422	33.4635	7.6698	7.6698
CT scan.tiff	75.6386	0.0018	1	0.1775	33.4635	7.6698	7.6698
lena_color_512.tif	75.106	0.0020	1	0.1986	33.4635	7.6698	7.6698
lena_color_256.tif	75.2519	0.0019	1	0.1940	33.4635	7.6698	7.6698
Peppers.tiff	77.2466	0.0012	1	0.1226	33.4635	7.6698	7.6698
San Diego.tiff	76.2596	0.0015	1	0.1539	33.4635	7.6698	7.6698
Average	75.9604	0.0014	1	0.1481	33.4635	7.6698	7.6698

The plot of PSNR and MSE is shown in Fig.14 & Fig.15 for encrypted, stego1, and stego2 images. PSNR is less for encrypted and high for stego. MSE is high for encrypted and very less for stego.

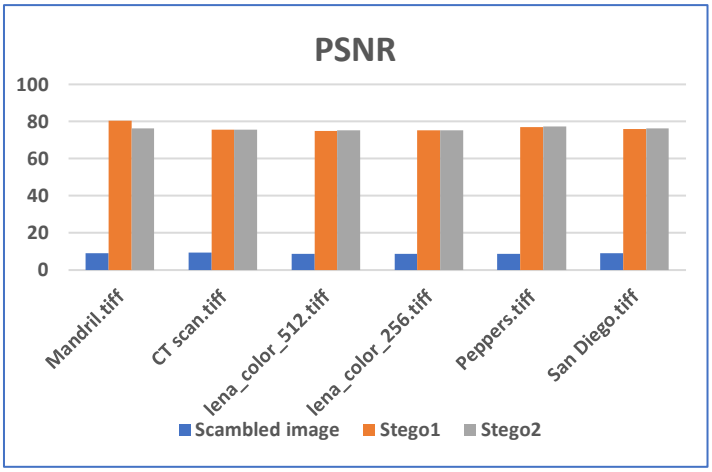


Fig.14. Graph of PSNR for encrypted, Stego1, and Stego2.

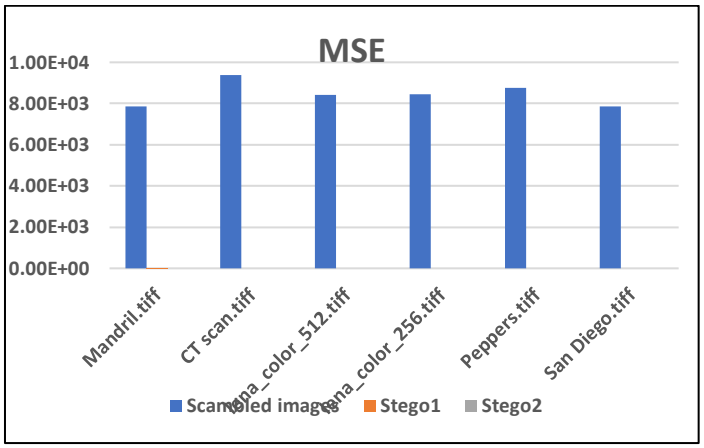


Fig.15. Graph of MSE for encrypted, Stego1, and Stego2.

The performance metrics are also computed for different databases. Generated values for encrypted are shown in Table 5. In the proposed approach, PSNR is 8.2356(dB), MSE is 1.00e+04, SSIM is 0.0129, NPCR is 100, and UACI is 33.4635 respectively. The values are matched with the ideal values.

Table 5. Measure of performance metrics for encrypted images.

Data Sets		Scrambled images				
		PSNR	MSE	SSIM	NPCR	UACI
USC-SIPI	Aerials	9.0548	8.0862e+03	0.0118	100	33.4635
	Miscellaneous	6.9518	1.3205e+04	0.0098	100	33.4635
Kodak		8.7001	8.7715e+03	0.0171	100	33.4635
Average		8.2356	1.00e+04	0.0129	100	33.4635

Encrypted images are hidden in the carrier. By taking Mandrill.tiff as a carrier in Table 6, the stego generated PSNR is 82.3495(dB), MSE is 0.0016, SSIM is 1, NPCR is 0.0808, and UACI is 33.4635, accordingly. By taking the Peppers.tiff as a carrier in Table 7, the stego-generated PSNR is 83.1562(dB), MSE is 0.0007, SSIM is 1, and NPCR is 0.0740, and UACI is 33.4635, accordingly.

Table 6. The measure of performance metrics for Stego.

Data Sets		Stego				
		PSNR	MSE	SSIM	NPCR	UACI
USC-SIPI	Aerials	75.1097	0.0021	1	0.2050	33.4635
	Miscellaneous	83.8824	0.0027	1	0.0272	33.4635
Kodak		88.0565	0.0001	1	0.0102	33.4635
Average		82.3495	0.0016	1	0.0808	33.4635

Table 7. The measure of performance metrics for Stego.

Data Sets		Stego images				
		PSNR	MSE	SSIM	NPCR	UACI
USC-SIPI	Aerials	75.2706	0.0020	1	0.1982	33.4635
	Miscellaneous	86.9527	0.0001	1	0.0137	33.4635
Kodak		87.2452	0.0001	1	0.0102	33.4635
Average		83.1562	0.0007	1	0.0740	33.4635

Table 8. The measure of performance metrics for Stego.

Existing methods	PSNR	MSE	SSIM
Wellia Shinta Sari, et al [2]	51.197	0.501	NA
Andik Setyono, et al [23]	54.213	0.247	NA
Osama Fouad Abdel Wahab, et al [28]	40.310	2.717	0.9451
Proposed method	82.7528	0.0012	1

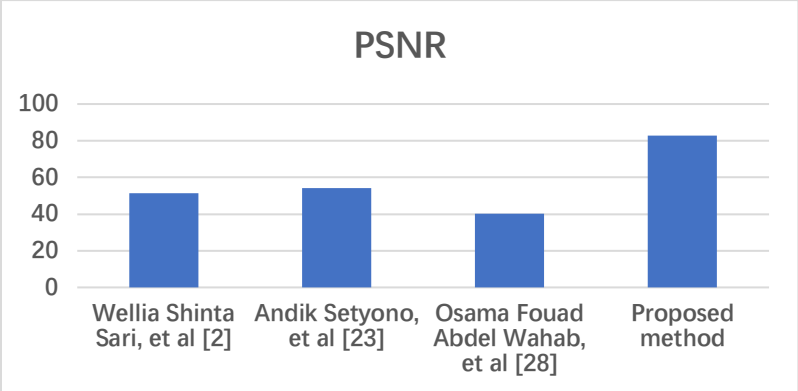


Fig.16. Graph of PSNR for this method in comparison with other existing methods [2, 23, 28].

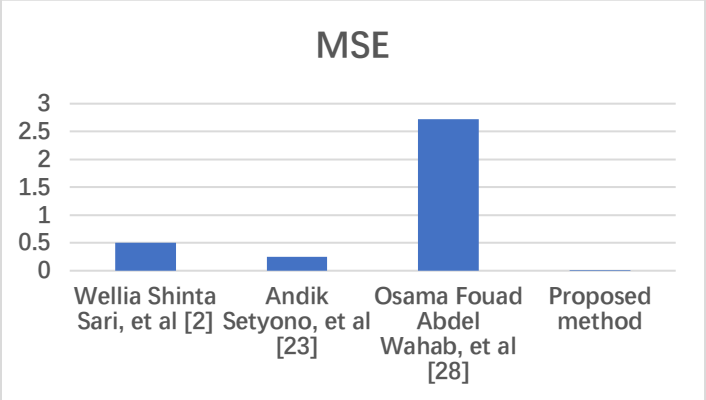


Fig.17. Graph of MSE for this method in comparison with other existing methods [2, 23, 28].

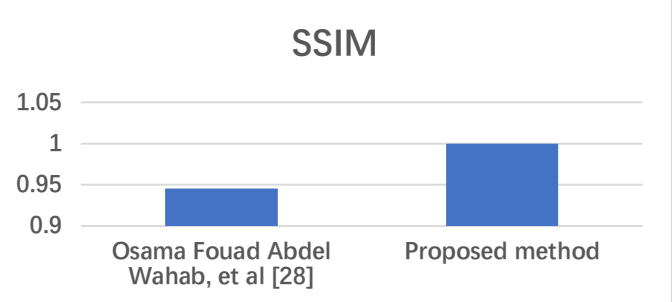


Fig.18. Graph of SSIM for this method in comparison with other existing methods [28].

This method gives high PSNR (82.7528 dB) and less MSE (0.0012) compared to existing methods [2, 23, 28,]. Also gives SSIM as 1 compared to the method [28]. These are shown in Table 8. The equivalent graphs are presented in Fig.16, Fig.17, and Fig.18.

C. Correlation Coefficient

The correlation coefficient characterizes the interrelation between any two variables. If the value of coefficient outreach to zero, then the image has been ciphered with a better system. The correlation coefficient is computed for horizontal, vertical & diagonal positions of input and cipher images. It can be calculated by the eq. (24).

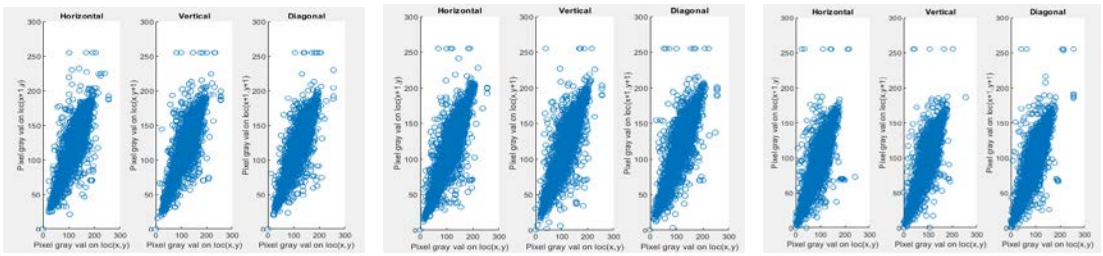
$$Cx1, x2 = \frac{1}{\sigma x1 * \sigma x2} Cov\left(x1, x2\right) \tag{24}$$

Here *Cx1, x2* is the correlation coefficient, *Cov* is the covariance of variables *x1* & *x2*, *σx1* & *σx2* are standard deviations of *x1* & *x2*, respectively.

The correlation coefficient values for input & encrypted are given in Table 9. The horizontal, vertical & diagonal correlation coefficients are calculated for R, G, & B channels. The correlation coefficient is very less for the encrypted in comparison with the input image. The correlation coefficient for input, encrypted, cover, stego, and decrypted are shown in Fig.19. (a), (b), (c), (d), & (e). The correlation coefficient for the encrypted is uniformly distributed. Carrier and stego look the same indicating that the hidden data is not recognizable. Therefore, the proposed approach generates a better encrypting and hiding effect with a higher security level.

Table 9. Correlation Coefficient values for input and encrypted images.

Input Secret images	Three channels	Input			Encrypted		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Mandril.tiff	R	0.9141	0.9239	0.9202	-0.0026	0.0290	0.0280
	G	0.8660	0.8600	0.8778	0.0001	-0.0102	0.0031
	B	0.9115	0.9066	0.9066	-0.0012	0.0010	0.0120
CT scan.tiff	R	0.9224	0.9229	0.9254	0.1793	0.1948	0.1958
	G	0.8671	0.8615	0.8672	-0.0248	0.0056	0.0026
	B	0.9050	0.9105	0.9089	0.0739	0.0248	0.1256
lena_color_512.tif	R	0.9166	0.9284	0.9260	0.0684	0.0802	0.0920
	G	0.8554	0.8639	0.8635	0.0089	0.0046	0.0201
	B	0.9310	0.9083	0.9077	0.0827	0.1024	-0.0236
lena_color_256.tif	R	0.9670	0.9176	0.9224	0.0534	0.0670	0.0718
	G	0.8693	0.8556	0.8696	-0.0043	0.0104	0.0056
	B	0.9052	0.9052	0.9087	0.0621	0.0521	0.0276
Peppers.tiff	R	0.9193	0.9225	0.9235	0.0641	0.0521	0.0467
	G	0.8609	0.8709	0.8664	0.0400	0.0257	0.0012
	B	0.9109	0.9000	0.9099	0.0532	0.0456	0.0078
San Diego.tiff	R	0.9266	0.9305	0.9230	0.0067	0.0093	0.0020
	G	0.8680	0.8673	0.8718	0.0021	0.0012	-0.0243
	B	0.9032	0.9107	0.9063	0.0027	0.0022	0.0013



(a)

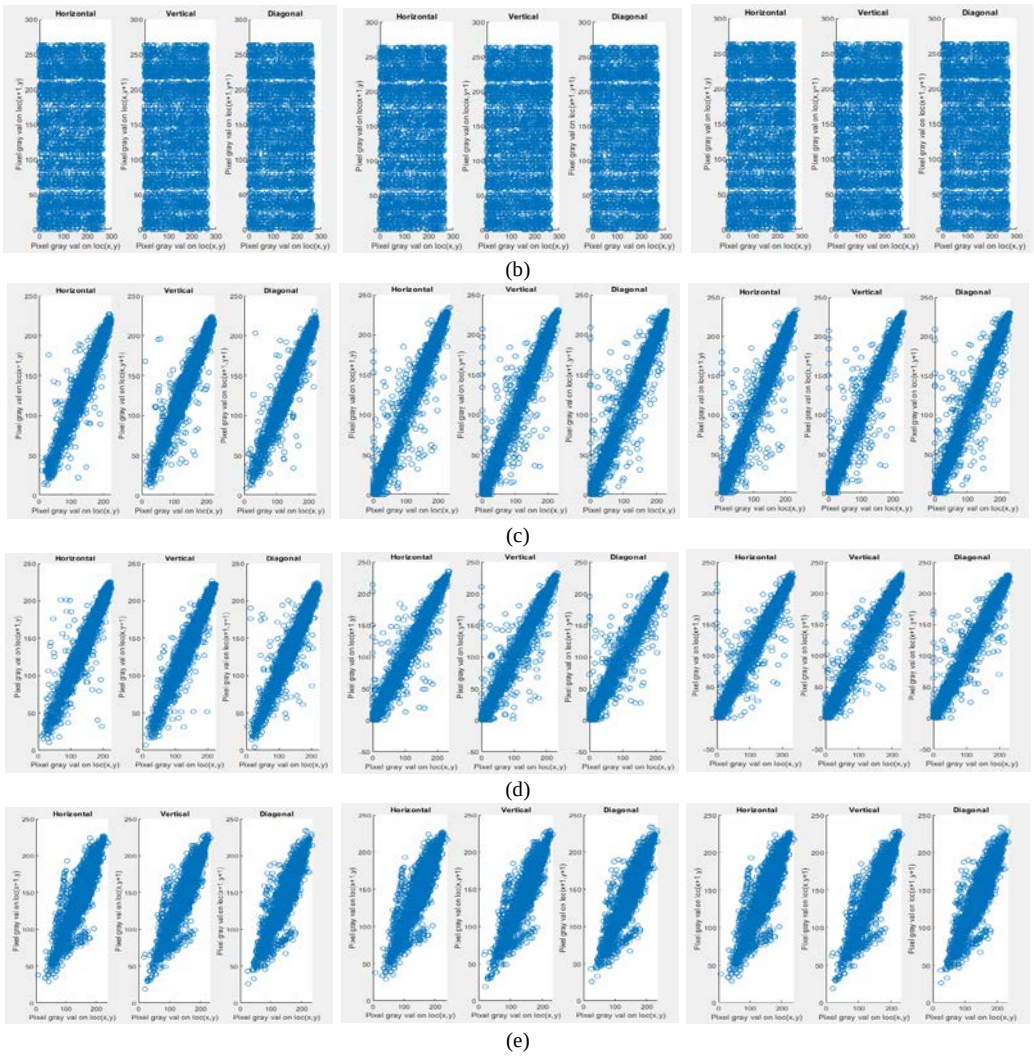


Fig.19. The correlation coefficient of (a). Input secret (b). Encrypted (c). Cover (d). Stego and (e). Decrypted image.

Table 10. Time to encrypt, embed, extract, and decrypt.

Input secret images	Encrypt (Seconds)	Embed (Seconds)	extract (Seconds)	Decrypt (Seconds)
Mandril.tiff	162.9043	4.3977	2.1919	172.6910
CT scan.tiff	150.4614	3.1826	1.8918	164.2833
lena_color_512.tif	157.3588	2.8329	1.6989	161.0113
lena_color_256.tif	153.2790	3.2068	1.9356	163.5855
Peppers.tiff	159.5519	3.0102	1.7075	169.7848
San Diego.tiff	164.5472	2.8401	2.0236	167.9522
Average	158.0171	3.24505	1.908216	166.5513

D. Total Time to Process

The time utilized to encrypt, embed, extract, and decrypt the input is given in Table 10. The time taken to encrypt, and decrypt is much higher compared to embed and extract. But this method gives better security measures. So, this method can be considered for applications to enhance the security of images.

This method generates good results in terms of performance metrics. It is successful in achieving research objectives like confidentiality and data integrity. High random encrypted images cannot be decoded by any attacker. ECC is utilized in this method acts an important role. SHA-256 hashing used cannot be reverted. A better transform domain technique like DWT with LSB generated with better unnoticeable stego.

7. Conclusions and Future Scope

In this method, the ECC, SHA-256, DWT, and LSB algorithms are put together to enhance confidentiality and message integrity. A stronger ECC makes it tough for third-party to extract the encrypted image. Mapping operations on the input image pixels for the elliptic curve points are carried out. Combining this image with the SHA-256 hash output image results in a scrambled image. DWT and LSB are utilized in the hiding and extracting stages. Encrypted and stego show that this method generates good results. Together with encrypted, the hash of input is also hidden. Two different information of an input image is hidden within a single image thereby enhancing its security level. The performance analysis for encrypted and stego is carried out by measuring PSNR, MSE, SSIM, NPCR, UACI, and information entropy. For stego, more than 75 dB of PSNR, less MSE, SSIM as 1, NPCR approximately 100%, UACI as 33.4635%, and good information entropy, indicates that this approach outputs with a good undetectable embedding system. A very less correlation coefficient indicates that the encryption method generates more randomness. This approach is progressively secure and suitable for applications of encryption & hiding of images. In the future, the work can be extended to reduce the execution time to scramble and descramble the input images.

References

[1] Mahboubeh Nazari, Iman Dorostkar Ahmadi, "A novel chaotic steganography method with three approaches for color and grayscale images based on FIS and DCT with flexible capacity", Multimedia Tools and Applications, Vol.79, No.19, pp.13693-13724, 2019. DOI: https://doi.org/10.1007/s11042-019-08415-1

[2] Wellia Shinta Sari, Eko Hari Rachmawanto, De Rosal Ignatius Moses Setiadi, Christy Atika Sari, "A good performance OTP encryption image based on DCT-DWT steganography", TELKOMNIKA Telecommunication, Computing, Electronics and Control, Vol.15, No. 4, pp.1987-1995, 2017. DOI: 10.12928/TELKOMNIKA.v15i4.5883

[3] Ali Kadhim Bermani, "High Security Steganography Model Based on DWT, DCT and RSA", Journal of Engineering and Applied Science, Vol.12, Special Issue 10, pp.8875-8881, 2017. DOI: 10.3923/jeasci.2017.8875.8881

[4] Shivanand S Gornale, Nuthan A. C, "Discrete Wavelet Transform (DWT) Based Triple-Stegging with Elliptic Curve Cryptography (ECC)", In International conference on recent trends in Signal Processing, Image Processing and VLSI [ICrtSIV], 2015. DOI: http://dx.doi.org/10.1145/2791405/2791514

[5] Adnan Gutub, Faiza Al-Shaarani, "Efficient implementation of multi-image secret hiding based on LSB and DWT steganography comparisons", Arabian Journal for Science and Engineering, Vol.45, No.4, pp.2631-2644, 2020. DOI: https://doi.org/10.1007/s13369-020-04413-w

[6] Ayan Chatterjee, Nikhilesh Barik, "A New Data Hiding Scheme Using Laplace Transformation in Frequency Domain Steganography", International Journal of Hyperconnectivity and the Internet of Things (IJHIoT), Vol.4, No.1, pp.1-12, 2020. DOI: 10.4018/IJHIoT.2020010101

[7] Edi Jaya Kusuma, Christy Atika Sari, Eko Hari Rachmawanto, De Rosal Ignatius Moses Setiadi, "A Combination of Inverted LSB, RSA, and Arnold Transformation to get Secure and Imperceptible Image Steganography", Journal of ICT Research & Applications, Vol.12, No.2, 2018. DOI: 10.5614/itbj.ict.res.appl.2018.12.2.1

[8] Kalpana Sanjay Shete, Mangal Patil, J. S. Chitode,"Least Significant Bit and Discrete Wavelet Transform Algorithm Realization for Image Steganography Employing FPGA", International Journal of Image, Graphics and Signal Processing, Vol.8, No.6, pp.48-56, 2016.

[9] Said E. El-Khamy, Noha O. Korany & Marwa H. El-Sherif, "A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption", Multimedia Tools and Applications, Vol.76, No.22, pp.24091-24106, 2017. DOI 10.1007/s11042-016-4113-8

[10] Sangeeta Dhall, Rinku Sharma, Shailender Gupta, "A multi-level steganography mechanism using quantum chaos encryption", Multimedia Tools and Applications, Vol.79, No.3, pp.1987-2012, 2020. DOI:10.1007/s11042-019-08223-7

[11] Pratik Gupta, Manoj Kumar," A Verifiable Ring Signature Scheme of Anonymous Signcryption Using ECC ", International Journal of Mathematical Sciences and Computing, Vol.7, No.2, pp. 24-30, 2021.

[12] Marwa Saidi, Houcemeddine Hermassi, Rhouma Rhouma, Safya Belghith, "A new adaptive image steganography scheme based on DCT and chaotic map", Multimedia Tools and Applications, Vol.76, No.11, pp.13493-13510, 2017. DOI 10.1007/s11042-016-3722-6

[13] Enas Muzaffer Jamel, "Image Steganography Based on Wavelet Transform and Histogram Modification", Ibn AL-Haitham Journal for Pure and Applied Science, Vol.33, No.1, pp.173-186, 2020. DOI: 10.30526/33.1.2365

[14] Aref Miri, Karim Faez, "An image steganography method based on integer wavelet transform", Multimedia Tools and Applications, Vol.77, No.11, pp.13133-13144, 2018. DOI 10.1007/s11042-017-4935-z

[15] Mohammad Fakhredanesh, Mohammad Rahmati, Reza Safabakhsh, "Steganography in discrete wavelet transform based on human visual system and cover model", Multimedia Tools and Applications, Vol.78, No.13, pp.18475-18502, 2018. DOI: https://doi.org/10.1007/s11042-019-7238-8

[16] Andik Setyono, De Rosal Ignatius Moses Setiadi, "Imperceptible Improvement of Secure Image Steganography based on Wavelet Transform and OTP Encryption using PN Generator", Journal of Physics: Conference Series, Vol. 1196, 012031, 2019. DOI:10.1088/1742-6596/1196/1/012031

[17] V. Kalaichelvi, P. Meenakshi, P. Vimala Devi, H. Manikandan, P. Venkateswari, S. Swaminathan, "A stable image steganography: a novel approach based on modified RSA algorithm and 2–4 least significant bit (LSB) technique", Journal of Ambient Intelligence and Humanized Computing, Vol.12, pp.7235–7243, 2020. DOI: https://doi.org/10.1007/s12652-020-02398-w

[18] Manal K. Oudah, Aqeela N. Abed b, Rula S. Khudhair c, Saad M. Kaleefah, "Improvement of Image Steganography Using

Discrete Wavelet Transform", Engineering and Technology Journal, Vol.38, No. 1, pp.83-87, 2020. DOI: https://doi.org/10.30684/etj.v38i1A.26620
[19] Ahmed Hambouz, Yousef Shaheen, Abdelrahman Manna, Dr. Mustafa Al-Fayoumi, Dr. Sara Tedmori, "Achieving data integrity and confidentiality using image steganography and hashing techniques", 2019 2nd International Conference on New Trends in Computing Sciences (ICTCS), pp.1-6, 2019. DOI: 10.1109/ICTCS.2019.8923060
[20] Harianto Antonio, P. W. C. Prasad, Abeer Alsadoon, "Implementation of cryptography in steganography for enhanced security", Multimedia Tools and Applications, Vol.78, No.23, pp.32721-32734, 2019. DOI: https://doi.org/10.1007/s11042-019-7559-7
[21] Vijay Kumar, Dinesh Kumar, "Performance evaluation of modified color image steganography using discrete wavelet transform", Journal of Intelligent Systems, Vol.28, No.5, pp.749-758, 2019. DOI: https://doi.org/10.1515/jisys-2017-0134
[22] Srilekha Mukherjee, Goutam Sanyal, "A multi-level image steganography methodology based on adaptive PMS and block-based pixel swapping", Multimedia Tools and Applications, Vol.78, No.13, pp.17607-17622, 2019. DOI: https://doi.org/10.1007/s11042-018-7127-6
[23] Andik Setyono, De Rosal Ignatius Moses Setiadi, Muljono, "StegoCrypt method using wavelet transform and one-time pad for secret image delivery", 2017 4th International Conference on Information Technology, Computer, and Electrical Engineering (ICITACEE), pp.203-207, 2017. DOI: 10.1109/ICITACEE.2017.8257703
[24] Tamer Rabie, Mohammed Baziyad, Ibrahim Kamel, "Enhanced high-capacity image steganography using discrete wavelet transform and the Laplacian pyramid", Multimedia Tools and Applications, Vol.77, No.18, pp.23673-23698, 2018. DOI: https://doi.org/10.1007/s11042-018-5713-2
[25] Inas Jawad Kadhim, Prashan Premaratne, Peter James Vial, "High-capacity adaptive image steganography with cover region selection using dual-tree complex wavelet transform", Cognitive Systems Research, Vol.60, pp.20-32, 2020. DOI: https://doi.org/10.1016/j.cogsys.2019.11.002.
[26] Hongzhu Dai, Jie Cheng, Yafeng Li, "A Novel Steganography Algorithm Based on Quantization Table Modification and Image Scrambling in DCT Domain", International Journal of Pattern Recognition and Artificial Intelligence, Vol.35, No.1, 2154001, 2021. DOI: 10.1142/S021800142154001X
[27] Zuhi Subedar, Ashwini Araballi. " Hybrid Cryptography: Performance Analysis of Various Cryptographic Combinations for Secure Communication ", International Journal of Mathematical Sciences and Computing, Vol.6, No.4, pp.35-41, 2020.
[28] Osama Fouad Abdel Wahab, Ashraf A. M. Khalaf, Aziza I. Hussein, and Hesham F. A. Hamed, "Hiding Data Using Efficient Combination of RSA Cryptography, and Compression Steganography Techniques", IEEE Access, Vol.9, pp.31805-31815, 2021. DOI: 10.1109/ACCESS.2021.3060317
[29] R Shanthakumari, Malliga S, "Dual layer security of data using LSB inversion image steganography with elliptic curve cryptography encryption algorithm", Multimedia Tools and Applications, Vol.79, No.5, pp.3975-3991, 2020. DOI: https://doi.org/10.1007/s11042-019-7584-6
[30] Supriadi Rustad, De Rosal Ignatius Moses Setiadi, Abdul Syukur, Pulung Nurtantio Andono, "Inverted LSB image steganography using adaptive pattern to improve imperceptibility", Journal of King Saud University-Computer and Information Sciences (2021). Article in press. DOI: https://10.1016/j.jksuci.2020.12.017
[31] USC-SIPI Image Database Website. http://sipi.usc.edu/database
[32] KODAK Image Dataset Website. http://r0k.us/graphics/kodak

Authors' Profiles

Ganavi M. is working as an Assistant Professor in the Department of Computer Science & Engineering (CSE) at Jawaharlal Nehru New College of Engineering (JNNCE), Shivamogga, Karnataka, India. She is pursuing a Ph.D. in Computer Science and Engineering from the Department of CSE, JNNCE, Shivamogga. Her research interests include Cryptography and information security.

Prof. Prabhudeva S. is working as a Professor and Director in the Department of Master of Computer Applications (MCA) at Jawaharlal Nehru New College of Engineering (JNNCE), Shivamogga, Karnataka, India. He received his Ph.D. degree in Reliability Engineering from IIT Bombay, India in 2010. Presently three research scholars are pursuing Ph.D. under his guidance. His research interests include Reliable and Security Modelling. He has published 22 papers in international journals and conferences. He has 18 years of research experience.

How to cite this paper: Ganavi M., Prabhudeva S., "Two-Layer Security of Images Using Elliptic Curve Cryptography with Discrete Wavelet Transform", International Journal of Computer Network and Information Security(IJCNIS), Vol.15, No.2, pp.31-47, 2023. DOI:10.5815/ijcnis.2023.02.03