INTL JOURNAL OF ELECTRONICS AND TELECOMMUNICATIONS, 2025, VOL. 71, NO. 1, PP. 87–93
Manuscript received September 18, 2024; revised March, 2025. doi: 10.24425/ijet.2025.153549

Digital image encryption with validation by ECC and embedding at low frequency region using the genetic approach

Kartikey Pandey, and Deepmala Sharma

***Abstract*—In the current internet era, the security of digital images has become increasingly important due to their numerous applications and uses. Although many researchers have proposed end-to-end security and authenticity against various attacks, achieving security, validation, and robustness together has been a challenge. This paper proposes a model called Low-Frequency Embedding and Elliptical Curve Cryptography (LFE-ECC), which provides all the necessary requirements for image security. The proposed model achieves image validation for the authentic sender by embedding a secret signature in the low-frequency region of the image. The robustness of the image is achieved by embedding a secret signature at a selected coefficient of the DWT feature. The moth flame optimization genetic algorithm is used for coefficient selection, and the additional security of embedded images is achieved using the elliptical curve cryptography technique. ECC provides encryption and validation for both parties. An experiment is conducted on real and artificial datasets under ideal and attack environments, and the results demonstrate the improved performance of the proposed LFE-ECC model against a range of attacks.**

***Keywords*—Image processing; Elliptical Curve Cryptography; Genetic Algorithm**

I. Introduction

THE development of network technology and message-merging approaches have made information and data security crucial [1]. A digital image has become an essential carrier in social relationships and information transfer due to its intuitive, vibrant, and realistic features. Therefore, photographic security is crucial. To address image security problems, a specific technology called picture encryption is employed. Traditional encryption algorithms like DES [2] and AES [3] are unable to satisfy the current needs of picture encryption due to the large amount of data, high association, and high redundancy.

The safest way to communicate images across dubious networks is the subject of the scholarly field of image cryptography, which has been the subject of in-depth study in recent years. To protect picture data, researchers have suggested several strategies and algorithms, including symmetric key cryptography and public key cryptography. Symmetric key cryptography, which uses a single encryption key for both encryption and decryption of image data, is widely used in image cryptography. Public key cryptography, which employs the usage of two keys a public key and a private key is another method utilized in image cryptography, and it is based on challenging mathematical issues such as computational complexity and discrete logarithms. [4]

Elliptic curve cryptography is a popular method for image encryption which uses elliptic curves throughout finite fields to achieve a high level of reliability with smaller key sizes. ECC is based on the problem of finding the discrete logarithm of a selected elliptic curve point. For image cryptography, ECC can be used to encrypt and decrypt images, authenticate their contents, and provide a secure shared key between the sender and the recipient. Additionally, ECC can create digital signatures for images, ensuring that they haven't been altered or tampered during transmission. [5]

ECC-based picture cryptography is extensively used in a variety of industries, such as the military, healthcare, banking, and e-commerce, where secure communication and the security of critical image files are crucial.

II. Objective

Many researchers proposed security and authentication models for digital images. But this work has proposed a combined model that provides security by use of ECC and validation by embedding secret data. In order to maintain image quality moth flame genetic algorithm has been used for the selection of embedding position. Moth flame not only maintains quality but also increases the robustness of the image as secret data is embedded at random cluster DWT coefficients. ECC, moth flame keys need to read images and secret data.

The organization of the proposed research work consists of five sections. The first section provides an overview of the research problem, objectives, and scope. The second section presents a review of past research work done by various researchers in the field. This section highlights the current state of knowledge, identifies gaps in the literature, and explains how the proposed research will address these gaps. The third

K. Pandey is with Department of Mathematics, National Institute of Techonology Raipur, Raipur Chhattisgarh, India (e-mail: nitiankartik@gmail.com).

D. Sharma is with Department of Mathematics, National Institute of Techonology Raipur, Raipur Chhattisgarh, India (e-mail: deepsha.maths@nitrr.ac.in).

section describes the research methodology used to address the research problem. This section explains the research design, data collection methods, data analysis techniques, and any ethical considerations. The fourth section presents the results of the experiments carried out. This section includes the analysis of the data collected and a discussion of the findings in relation to the research problem. The fifth and last section provides the conclusions drawn from the research work and suggests future research directions that may be pursued to further advance knowledge in the field.

III. Related Work

Amal Hafsa et al. [6] have proposed an image encryption method based on improved ECC by doing some modifications in the AES algorithm. A strong Elliptic curve-based image encryption and authentication scheme have been developed in [7] for both color and grayscale images. This model generates a shared session key using the secure Elliptic Curve Diffie-Hellman (ECDH) key exchange and the enhanced ElGamal encoding approach.

In [8], A generalized cryptosystem has been proposed to address the discovered issues and enhance the encryption strategy. To effectively defend against the exhaustive search attack, the key matrix negotiation was redefined in the improved version to a cipher that incorporates a modified EC Integrated Encryption with a generalized linear multiplication matrix.

Dawahdeh et al. [9] address the security level concern of an image encryption scheme combining ECC with Hill cipher (ECCHC). In [10], the plain text was converted into ciphertext after a distinctive key which was created using random characters. A split with a circular left and right shift strategy is used for this encryption.

C.H. Lin et al. [11] proposed an intelligent symmetric key cryptography using a chaotic map with a quantum-based key generator (KG). A self-adaptive genetic method was designed and introduced by Rongsheng Xie et al. [12] to enhance a reliable QR code watermarking scheme. In the revised scheme, authors adaptively alter the genetic algorithm process in accordance with the relationship between a population's average fitness value and maximal fitness value. Improved genetic algorithm techniques make it simpler to obtain better diversity.

Abd El-Latif et al. [13] provided the technique of image encryption using the chaotic system with the cycle of ECC. They decided to use this technique to generate the key of random by using the encryption from the original image.

Nagaraj et al. [14] suggested an algorithm that uses ECC to encrypt and decrypt images. In the suggested encryption method 4x4 magic matrix is used as a secret key, also Images are converted into 8x8 matrices and then encrypted using ECC. Singh et al. [15] proposed an algorithm that encrypts images using ECC. In order to enhance the speed of the proposed algorithm image pixels are grouped according to the prime number of ECC and converted into the big integers using the From Digits algorithm.

Laiphrakpam et al. [16] presented a new medical image encryption method based on the advanced ElGamal encryption method with ECC. This method uses a significantly improved ElGamal technique to encode a simple image into points of elliptic curve coordinates instead of using the Koblitz encoding technique. So the encryption process is done quickly and properly.

Azam et al.'s [17] suggestion of a novel Mordell elliptic curve-based picture encryption technique. The transmitter and receiver in this paper select a shared elliptic curve. The approach then uses a dynamic S-box over an elliptic curve and random values to mask and jumble pixels.

Using ECC technology, Muneeswaran et al. [18] devised an approach that uses this algorithm to encrypt images. They extracted a private key from a double line using a random integer called 'k' as well. Additionally, they multiplied each pixel value on the elliptical curve coordinates in the bitmap on the cipher image.

A. Akhavan et al. [19] suggested an image encryption technique that makes use of the Jacobian elliptic curve's map. As a result, after working with the key commence, the matrix of plain picture data will be transformed into one matrix of dimension. The elements then revert to their original dimension after being encrypted using the formula and matrix.

IV. Proposed Methodology

In this section of the paper, we present the Low-Frequency Embedding and Elliptical Curve Cryptography (LFE-ECC) model, which is designed to enhance the security and authenticity of images. The model utilizes low-frequency embedding to improve the robustness of the image against various attacks while employing the Elliptical Curve Cryptography technique to enhance the overall security of the image. The graphical flow of the LFE-ECC model is illustrated in Figure 1, and Table 1 provides the notations used to explain each block of the model.

TABLE I
Notation used in LFC-ECC

Notation	Description
I	Input Image
PI	Preprocessed Image
Ss	Secret Signature
BSs	Binary of Ss
LL	Low-Frequency Image Coefficients
Mc	Moth Coefficient Population
Mf	Moth Fitness
Cc	Cluster Center Coefficients
G	Generator Point on Curve
Ksp, keep	Sender and Receiver private keys
Ksu, Kru	Sender and Receiver public keys
EI	Embedded Image
EEI	Encrypted Embedded Image

A. Input Pre-Processing

The LFE-ECC model accepts input images of any dimension, including both two-dimensional and three-dimensional

images. For three-dimensional images, the color red is used to embed data. If the input image is in the HSV format, it is first converted to the RGB format to obtain the Processed Image (PI). Additionally, the secret signature provided, denoted as Ss, must be converted into binary format, denoted as BSs. This conversion eliminates the reliance on the type of signature, such as text, image, number, etc., and enables binary embedding.

$$BSs \leftarrow Binary(Ss) \tag{1}$$

1) DWT (Discrete Wavelet Transform): This study took advantage of the DWT frequency feature. Here, Fig. 2 illustrates the specific DWT methods used in the study that inserted a secret image at the image's LL region. This image block has been created by passing the image rows through a low pass filter and then a second layer low pass filter. This block contains flat areas of the image that lack edge information; therefore, it is referred to as an approximation of the images. [20] [21]

$$[LLLHHLHH]DWT - First\text{–}Level(PI) \tag{2}$$

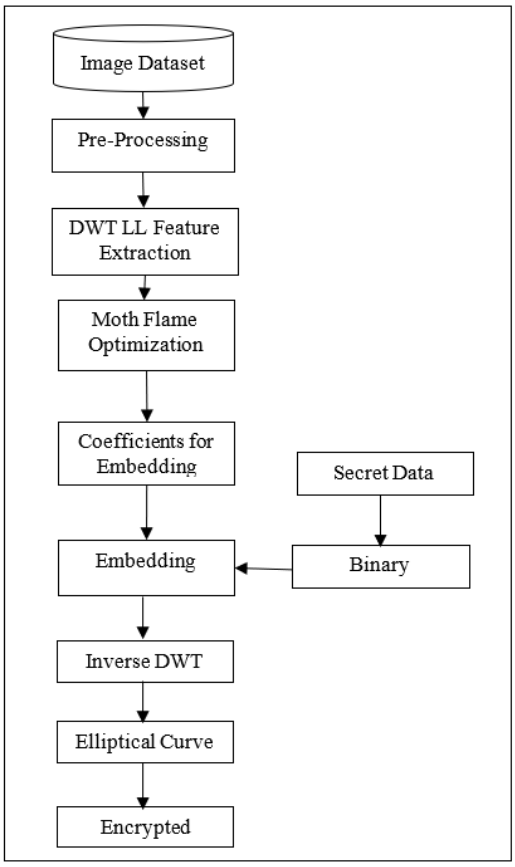

Fig. 1. Block diagram of LFE-ECC model.

B. Moth Flame Optimization Algorithm:

In this paper, the Moth Flame Optimization Algorithm has been used where each chromosome is considered as a moth.

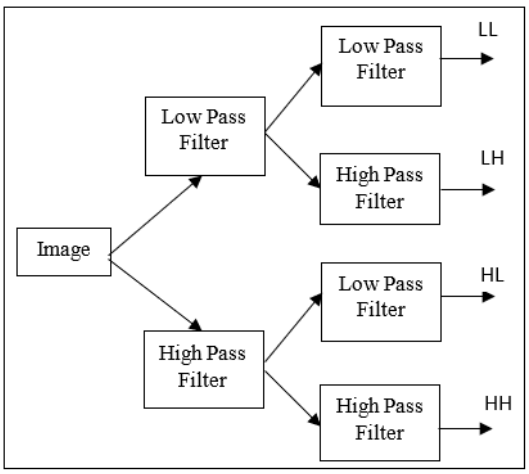

Fig. 2. DWT steps for LL image transformation.

The goal of this algorithm is to locate a moth flame that moves toward the optimal solution. In our case, the moth flame represents the cluster center coefficients [22].

1) Generate Moth Flames: A moth flame is a vector of n elements, where n is the number of cluster center coefficients. A population matrix M of p x C dimensions is created, where p is the number of moth flames generated. The K numbers of coefficients are chosen using a Gaussian random number generator function.

$$M \leftarrow MothFlamePopulation(p, C) \tag{3}$$

2) Fitness Function: Each moth flame is ranked based on the distance from the image coefficients. The entire cost of the image coefficient's distance from the cluster center coefficients of moth flames is taken into account while calculating the fitness value.
3) Moth Flame Position updated: Once the fitness value (F) has been determined by the fitness function, it should be sorted in decreasing order to identify the best Moth Flame among all the chromosomes present in the population.
4) Crossover: To improve the performance of the Crossover Genetic method, the parameter x, which determines the number of random position values to be modified, is adjusted for each Moth Flame. In this process, the best local Moth Flame set of features is used to modify each Moth Flame at x random positions. The fitness of the resulting moths is compared to their parents, and if the child moth performs better, the parent moth is replaced; otherwise, the parent moth is retained. If the maximum number of iterations is reached, the model proceeds to the cluster coefficient step; otherwise, the fitness of each Moth Flame in the updated population is evaluated.
5) Cognitive: This stage involves replacing random values from the cluster center set with a set of coefficient values ranging from 0 to 255. All of the population's food supplies are used for this activity.
6) Final Solution: The genetic algorithm's fitness value and crossover procedure are repeated T times. Using the

T operations technique, the coefficients are separated into embedded and non-embedded sets based on the population optimum parameter estimate and the best-fitting cluster center source. [23]

C. Data Embedding

The selected coefficient values are transformed into bits, and the last three bits are replaced by the model. Once the secret bits are embedded, the image is reassembled back into the embedded image. Finally, the image is inverse-transformed. [24]

D. Encryption and decryption using ECC

In this method, a Generator point G of the curve is shared between the sender and receiver for encryption and decryption of image it is done by following algorithm.

Algorithm: Suppose Alice and Bob are two communicating entities and Alice want to share any image to Bob. They reach a consensus on the equation of the elliptic curve and select a generator point (G) for their communication.

$$y^2 = x^3 + ax + bmodp$$

If Alice intends to encrypt a message (P_m) to transmit it to Bob, the resulting ciphertext (P_c) is obtained as follows:

$$P_c = (kG, P_m + kP_b)$$

where k is a randomly chosen integer, and P_b represents Bob's public key, which is calculated using Bob's private key (n_b) as $P_b = n_bG$.
Now Bob will decrypt cipher point P_c into original message P_m . So, for this decryption multiply the x-coordinate of cipher point P_c with Bob's secret key $kG \times n_B$ and now subtract $(kG \times n_B)$ from y-coordinate of cipher point P_c

$$P_m + kp_B – (kG \times n_B)$$

we know that $P_B = n_B \times G$

$$\begin{aligned} &P_m + kp_B - kp_B \\ &= P_m \end{aligned}$$

Hence Bob gets the same point P_m which is sent by Alice.

E. Proposed Work LFE-ECC Algorithm

Input: I, Ss Output: EEI

1) $PI \leftarrow Imageprocessing(I)$
2) $BSs \leftarrow Binary(Ss)$
3) $[LL\ LH\ HL\ HH] \leftarrow DWT - First - Level(PI)$
4) $Mc \leftarrow Generate - Population(LL)$
5) $Loop1 : itr$
6) $Mf \leftarrow Moth - Fitness(Mc, LL)$
7) $Mc \leftarrow Crossover(Mf, Mc)$
8) $Mc \leftarrow Cognitive(Mc)$
9) $EndLoop$
10) $Mf \leftarrow Moth - Fitness(Mc, LL)$
11) $Loop1 : Ss$
12) $LL \leftarrow Data - Embedding(Ss, LL, Cc)$
13) $EndLoop$
14) $EI \leftarrow IDWT(LL, LH, HL,\ HH)$
15) $EEI \leftarrow ECC(EI)$

F. Receiver side image extraction

In the extraction step, the receiver can extract the secret signature and the image by following the steps illustrated in Fig. 3. The ECC decryption algorithm is applied with the correct public, private, and shared keys to extract the image.

$$EI \leftarrow EEI - (K_{rp}G + Z_{SR}) \tag{4}$$

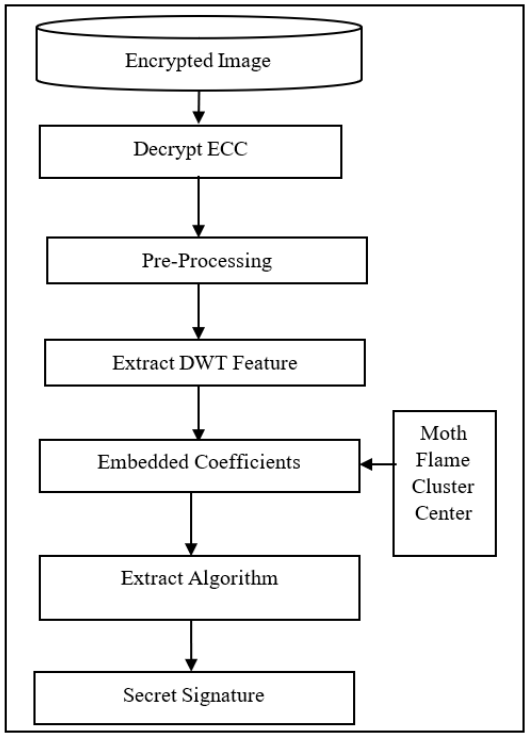

Fig. 3. Digital image watermark extraction process block diagram.

The preprocessing and DWT feature extraction are performed in the same way as in the data concealment step. Another contribution of this work is the key, which is the cluster center obtained using the moth flame optimization process. Based on the cluster center key coefficient values, the cluster coefficients are computed for data embedding and non-data embedding. The selected coefficient values are converted to bits, and the last three least significant bits are collected to create a secret signature that can be verified for authenticity.

V. Experiment and Results

This section presents the experimental evaluation of the proposed method for image protection. All calculations and utility measures are performed using the MATLAB tool. The experiments are conducted on a computer with a 2.27 GHz Intel Core i3 processor, 4 GB of RAM, and Windows 7 Professional operating system. The model construction is based on the ACM-ECC model proposed in [22].

A. Dataset

An analysis of the dataset is performed on commonly used images, such as the tree, mandrill, and Lena. These are typical images obtained from http://sipi.usc.edu/database/?volume=misc. The framework is also tested on everyday pictures.4

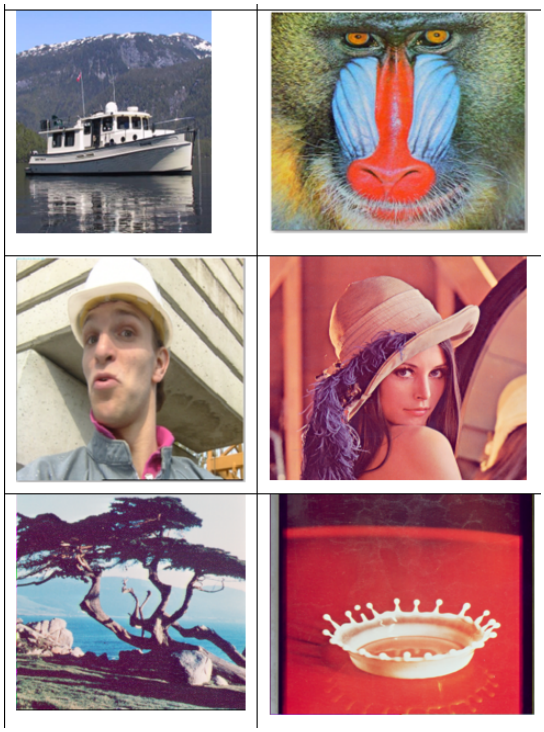

Fig. 4. Image Dataset Description

B. Results

TABLE II
IDEAL CONDITION-BASED VALUES OF LFE-ECC.

Images	PSNR	SNR	NC
Lena	55.6258	0.178034	1
Mandrill	55.836	0.16962	1
Boat	55.8099	0.170643	1
Human	55.9674	0.164567	1
Tree	55.7294	0.173837	1
Cup	55.8560.16	8842	1

Table 2 displays the evaluation parameter values of the LFE-ECC model under no attack / ideal conditions. It has been observed that the proposed model has successfully maintained the image quality during the encryption and decryption process, while also ensuring the validation of originality. The use of the moth flame optimization algorithm for secret data embedding has not had a significant impact on image quality. Moreover, the elliptical cryptography method has also not reduced the image quality during the encryption and decryption process on both the sender and receiver sides.

TABLE III
IDEAL CONDITION IMAGE SENDER TIME.

Images	LFE-ECC	ACM-ECC
Lena	0.642109	3.33925
Mandrilla	0.773766	3.78058
Boat	0.7001	3.63638
Human	0.835806	3.63638
Tree	0.676657	4.01723
Cup	0.672232	3.45752

TABLE IV
IMAGE VALIDATION (RECEIVER) TIME-BASED COMPARISON.

Images	LFE-ECC	ACM-ECC
Lena	0.566165	3.63994
Mandrill	0.604198	3.69863
Boat	0.541954	3.69863
Human	0.598673	3.69863
Tree	0.534008	3.86404
Cup	0.513104	3.68123

The encryption and decryption times of the compared models are presented in Tables 3 and 4. The results show that the use of the chaotic method in ACM-ECC has a higher execution time cost, which indirectly reflects the calculation cost. However, the use of a genetic algorithm for secret message privacy reduces the time and calculation cost. Moreover, DWT feature extraction is a less time-consuming method for security. The moth flame-based embedding position selection provides a jumbled position with high robustness against various types of attacks.

To validate the image from an authentic source, this work uses secret information matching. The proposed model extracts the secret data with 100% accuracy under ideal conditions and approximately 85% in the attacked environment, as shown in Tables 2 and 5. In contrast, the previous model uses the ACM-ECC hash key technique, which authenticates 100% under ideal conditions but fails in any type of attack environment due to different key generations at the receiver side. Therefore, the use of secret data is more efficient for data validation compared to the hash key technique.

TABLE V
COMPARISON OF LENA IMAGE AGAINST VARIOUS ATTACKS FOR NC VALUES

Attacks	Lena		Mandrill	
	LEF-ECC	ACM-ECC	LFE-ECC	ACM-ECC
Gaussian Filter	0.869	0	0.854	0
Median Filter	0.867	0	0.852	0
Poisson Noise	0.854	0	0.853	0
Salt & Pepper	0.848	0	0.894	0
Histogram	0.643	0	0.798	0
Compression	0.863	0	0.835	0

TABLE VI
COMPARISON OF LENA IMAGE AGAINST VARIOUS ATTACKS FOR PSNR VALUES

Attacks	Lena		Mandrill	
	LEF-ECC	ACM-ECC	LFE-ECC	ACM-ECC
Gaussian Filter	28.45	17.9759	20.6633	17.7029
Median Filter	35.1973	18.7065	22.501	18.2965
Poisson Noise	25.7873	24.4753	26.0668	24.4017
Salt & Pepper	28.4948	27.4839	28.83	27.9449
Histogram	14.0026	13.9774	20.9277	20.3115
Compression	35.9413	27.8669	37.9359	27.9308

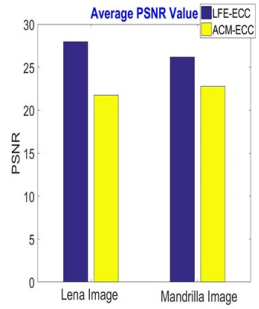

Fig. 5. Comparison of average PSNR value of different attacks

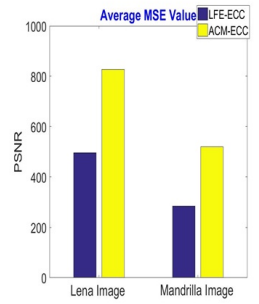

Fig. 6. Comparison of average MSE value of different attacks

Tables 6, 7, and 8 display the evaluation parameter values of the spatial attack environment for the compared models. It has been found that utilizing the moth flame optimization genetic algorithm for embedding secret data has enhanced the model's robustness against various spatial attacks. Additionally, selecting the low-frequency region of the DWT feature has improved the model's performance. As shown in Fig. 5 and 6, the average PSNR values for both testing images are high, and the MSE value is low compared to the previous model. However, the image quality parameters were greatly compromised in the ACM-ECC attacked image.

VI. CONCLUSION

This paper has proposed a model that secures images from intruders by using elliptical curve cryptography. Furthermore, the image validation has been embedded in a secret message with the help of a moth flame-based algorithm. This model

TABLE VII
COMPARISON OF LENA IMAGE AGAINST VARIOUS ATTACKS FOR PSNR VALUES

Attacks	Lena		Mandrill	
	LEF-ECC	ACM-ECC	LFE-ECC	ACM-ECC
Gaussian Filter	18.8996	18.8806	18.3293	18.1625
Median Filter	18.9006	18.8822	18.3339	18.1645
Poisson Noise	18.919	18.8806	18.3512	18.1625
Salt & Pepper	18.9137	18.898	18.3527	18.1771
Histogram	19.1914	19.1727	18.6299	18.454
Compression	18.9032	-0.37	18.342	-0.525

TABLE VIII
COMPARISON OF LENA IMAGE AGAINST VARIOUS ATTACKS FOR MSE VALUES

Attacks	Lena		Mandrill	
	LEF-ECC	ACM-ECC	LFE-ECC	ACM-ECC
Gaussian Filter	92.9149	1036.31	558.151	1103.54
Median Filter	19.6493	875.858	365.58	962.565
Poisson Noise	171.534	232.035	160.843	235.999
Salt & Pepper	91.9604	116.061	85.1292	104.373
Histogram	2587.11	2602.21	525.188	605.23
Compression	16.5557	106.264	10.459	104.714

also provides robustness for digital content with image validation. Validation of the image is achieved by embedding secret data at selected DWT coefficients. In order to cluster coefficients into selected and non-selected regions moth flame optimization genetic algorithm is used. Binary secret data is embedded at the least significant position of coefficient values of DWT. This moth flame-based embedding reduces the image data loss and maintains image quality. Embedded image security is improved by Elliptical Curve Cryptography. So ECC keys are required to decrypt images and moth flame keys are required to extract secret data for image validation. The experiment has done on real images under ideal and attack environments. It is observed that the LFE-ECC model has extracted the secret data 100% under ideal conditions and almost 85% in an attack environment. The result shows an average PSNR value of 55.804. Hence the elliptical curve cryptography method has also not reduced the image quality during the encryption and decryption process at the sender and receiver sides. In the future, scholars can apply some other validation processes that may increase the robustness of the work.

REFERENCES

[1] K. Ding, S. Chen, and F. Meng, "A novel perceptual hash algorithm for multispectral image authentication," *Algorithms*, vol. 11, no. 1, p. 6, 2018. [Online]. Available: https://doi.org/10.3390/a11010006
[2] J. Jain, A. Jain *et al.*, "Securing e-healthcare images using an efficient image encryption model," *Scientific Programming*, vol. 2022, 2022. [Online]. Available: https://doi.org/10.1155/2022/6438331
[3] C. Kumar, A. K. Singh, and P. Kumar, "A recent survey on image watermarking techniques and its application in e-governance," *Multimedia Tools and Applications*, vol. 77, pp. 3597–3622, 2018. [Online]. Available: https://doi.org/10.1007/s11042-017-5222-8

[4] Z. Zhao and X. Zhang, "Ecc-based image encryption using code computing," in *Proceedings of the 2012 International Conference on Communication, Electronics and Automation Engineering*. Springer, 2013, pp. 859–865. [Online]. Available: https://doi.org/10.1007/978-3-642-31698-2_121

[5] M. Ganavi and S. Prabhudeva, "A novel approach to enhance image security using hyperchaos with elliptic curve cryptography," *International Journal of Rough Sets and Data Analysis (IJRSDA)*, vol. 7, no. 1, pp. 1–17, 2021. [Online]. Available: https://doi.org/10.4018/IJRSDA.288520

[6] A. Hafsa, A. Sghaier, J. Malek, and M. Machhout, "Image encryption method based on improved ecc and modified aes algorithm," *Multimedia Tools and Applications*, vol. 80, pp. 19 769–19 801, 2021. [Online]. Available: https://doi.org/10.1007/s11042-021-10700-x

[7] P. Parida, C. Pradhan, X.-Z. Gao, D. S. Roy, and R. K. Barik, "Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps," *IEEE Access*, vol. 9, pp. 76 191–76 204, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3072075

[8] M. Benssalah, Y. Rhaskali, and K. Drouiche, "An efficient image encryption scheme for tmis based on elliptic curve integrated encryption and linear cryptography," *Multimedia Tools and Applications*, vol. 80, no. 2, pp. 2081–2107, 2021. [Online]. Available: https://doi.org/10.1007/s11042-020-09775-9

[9] Z. E. Dawahdeh, S. N. Yaakob, and R. R. bin Othman, "A new image encryption technique combining elliptic curve cryptosystem with hill cipher," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 349–355, 2018. [Online]. Available: https://doi.org/10.1016/j.jksuci.2017.06.004

[10] K. I. Masud, M. R. Hasan, M. M. Hoque, U. D. Nath, and M. O. Rahman, "A new approach of cryptography for data encryption and decryption," in *2022 5th International Conference on computing and Informatics (ICCI)*. IEEE, 2022, pp. 234–239.

[11] C.-H. Lin, J.-X. Wu, P.-Y. Chen, H.-Y. Lai, C.-M. Li, C.-L. Kuo, and N.-S. Pai, "Intelligent symmetric cryptography with chaotic map and quantum based key generator for medical images infosecurity," *IEEE Access*, vol. 9, pp. 118 624–118 639, 2021. [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3107608

[12] R. Xie and P. Huang, "An improved anti-counterfeiting printed qr watermarking algorithm based on self-adaptive genetic algorithm," in *IOP Conference Series: Materials Science and Engineering*, vol. 768, no. 5. IOP Publishing, 2020, p. 052002. [Online]. Available: https://doi.org/10.1088/1757-899X/768/5/052002

[13] A. A. Abd El-Latif and X. Niu, "A hybrid chaotic system and cyclic elliptic curve for image encryption," *AEU-International Journal of Electronics and Communications*, vol. 67, no. 2, pp. 136–143, 2013. [Online]. Available: https://doi.org/10.1016/j.aeue.2012.07.004

[14] S. Nagaraj, G. Raju, and K. K. Rao, "Image encryption using elliptic curve cryptograhy and matrix," *Procedia Computer Science*, vol. 48, pp. 276–281, 2015. [Online]. Available: https://doi.org/10.1016/j.procs.2015.04.182

[15] L. D. Singh and K. M. Singh, "Image encryption using elliptic curve cryptography," *Procedia Computer Science*, vol. 54, pp. 472–481, 2015.

[16] D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved elgamal encryption technique," *Optik*, vol. 147, pp. 88–102, 2017. [Online]. Available: https://doi.org/10.1016/j.ijleo.2017.08.028

[17] N. A. Azam, I. Ullah, and U. Hayat, "A fast and secure public-key image encryption scheme based on mordell elliptic curves," *Optics and Lasers in Engineering*, vol. 137, p. 106371, 2021. [Online]. Available: https://doi.org/10.1016/j.optlaseng.2020.106371

[18] S. M. C. Vigila and K. Muneeswaran, "Nonce based elliptic curve cryptosystem for text and image applications." *Int. J. Netw. Secur.*, vol. 14, no. 4, pp. 236–242, 2012.

[19] S. Behnia, A. Akhavan, A. Akhshani, and A. Samsudin, "Image encryption based on the jacobian elliptic maps," *Journal of Systems and Software*, vol. 86, no. 9, pp. 2429–2438, 2013. [Online]. Available: https://doi.org/10.1016/j.jss.2013.04.08

[20] T. Tabassum and S. M. Islam, "A digital video watermarking technique based on identical frame extraction in 3-level dwt," in *2012 15th International Conference on Computer and Information Technology (ICCIT)*. IEEE, 2012, pp. 101–106. [Online]. Available: https://doi.org/10.1109/ICCITechn.2012.6509780

[21] P. Dabas and K. Khanna, "A study on spatial and transform domain watermarking techniques," *International journal of computer applications*, vol. 71, no. 14, 2013.

[22] Z. E. Dawahdeh, S. N. Yaakob, and R. R. bin Othman, "A new image encryption technique combining elliptic curve cryptosystem with hill cipher," *Journal of King Saud University-Computer and Information Sciences*, vol. 30, no. 3, pp. 349–355, 2018. [Online]. Available: https://doi.org/10.1016/j.jksuci.2017.06.004

[23] X. Zhou, C. Cao, J. Ma, and L. Wang, "Adaptive digital watermarking scheme based on support vector machines and optimized genetic algorithm," *Mathematical Problems in Engineering*, vol. 2018, 2018. [Online]. Available: https://doi.org/10.1155/2018/2685739

[24] A. K. Sahu and G. Swain, "An optimal information hiding approach based on pixel value differencing and modulus function," *Wireless Personal Communications*, vol. 108, pp. 159–174, 2019. [Online]. Available: https://doi.org/10.1007/s11277-019-06393-z