International Journal of Mathematical, Engineering and Management Sciences
Vol. 10, No. 1, 76-91, 2025
https://doi.org/10.33889/IJMEMS.2025.10.1.005

Ram Arti
Publishers

Digital Content Security by Butterfly and Elliptic Curve Cryptography with Channel Optimization

Kartikey Pandey
Department of Mathematics,
National Institute of Technology Raipur, Raipur, Chhattisgarh, India.
E-mail: nitiankartik@gmail.com

Deepmala Sharma
Department of Mathematics,
National Institute of Technology Raipur, Raipur, Chhattisgarh, India.
Corresponding author: deepsha.maths@nitrr.ac.in

(Received May 21, 2024; Revised on August 9, 2024 & September 13, 2024; Accepted on September 18, 2024)

Abstract

As more and more services and solutions are utilizing digital data, it becomes imperative to provide strong security mechanisms to safeguard sensitive content with a rapidly growing number of users. This is especially important for users who are not as techie, and thus do not have the knowledge or skill to implement their own protections. To this effect, the present paper proposes a new model for image validation at the receiver side. This model works on low bandwidth channel and provides same level of security as end-to-end encryption. The security of the images is realized by using elliptic curve cryptography (ECC), while the segmentation and discrete wavelet transform (DWT) cooperate for achieving both transmission efficiency and preservation of individual pixel data. The model utilizes watermark embedding and a butterfly selection method for image authentication. This involves a cognitive decision step thereby ensuring the highest possible effectiveness for integrity verification. Experiments on a standard image dataset show that the proposed model is able to be much more robust under different attack vectors.

Keywords- Elliptic curve cryptography, Embedding, Encryption, Image processing, Genetic algorithm.

1. Introduction

In today digital era, it is almost ubiquitous the preference to use digital images instead of classical paper. These digital images are considered valuable for contracts and agreements. For official components in contracts (Al-Gindy et al., 2009; Chang et al., 2018), the authenticity of these digital images is extremely important. As with any document, digital data integrity and authenticity must be maintained. Thus, many digital signature models and cryptic algorithms have been introduced to ensure the protection of digital documents, however, some cryptographic signing techniques are more secure than others.

With a range of services and solutions adopting digital principles, the rapid growth in the use of digital data demonstrates that it is crucial that robust security measures are implemented to safeguard contesting information. Especially for non-technical users, they may not even know how to protect their own data properly and become the target in a major data breach. Digital images pass from being a tool to an indispensable source of information that requires identification and protection. In the last decade, we have explored that high demand of strong cryptographic techniques because of sophisticated cyber-attacks faced by digital health records. Here the ubiquitous cloud-based solutions and isolation-triggered remote communication have added up to already existing cases, causing acceleration in demand of efficient but extremely secure cryptographic techniques (Daoui et al., 2022; Singh et al., 2022a; Xu et al., 2022).

The purpose of this work is to offer a novel end-to-end solution that not only secures digital images, but also to optimize communication channels and also one secure and efficient means for digital content security. The deficiencies comprise less effective data encryption, stronger resistance attack capacities, and denoised communication standard over the network and integrity loss in image validation. We address this by using Elliptic Curve Cryptography (ECC) for efficiency, a hybrid DWT and watermarking approach for robustness, optimizing channels to reduce packet size and include a cognitive decision step for improved image integrity verification.

Digital content safety is partially secured via cryptography, a method of protecting information and communication through codes that are only intelligible to the intended receiver (Chang et al, 2018; Mohammadet al., 2019). Cryptography is a practice of secure communication in which they use mathematical techniques to encode messages into the cipher text, which is difficult to read (Chang et al., 2020; Benssalah et al., 2021; Kumar and Sharma, 2023). Such algorithms are required to generate keys, digital signatures and assurances that our online activities such as web browsing, private communications, credit card transactions, email uses etc. are safe for both users and the data from any potential hacker or virus attacks so that no unauthorized user access confidential information.

There are three main objectives when it comes to data hiding in terms of what data hiding methods try to achieve: 1) establishing a secret message delivery channel between the sender and receiver using an image as cover media; 2) inserting a message into an image when the image is transmitted so that upon receiving, it can be extracted by the recipient to confirm that the received image's integrity is unimpaired; and 3) binding a message with an user selected image so that the owner of that image can make use of this embedded message for proving his ownership. In transform domain like DCT (Zhou et al., 2017), DFT (Hernandez et al., 2015), DWT (Dharwadkar and Amberker, 2010; Zhang et al., 2019; Gao et al., 2013), EPF, and SVD (Vaishnavi and Subashini, 2015) that are widely used to transform the input image into the frequency domain. Therefore, these images are inverted after watermarking is completed. In the meantime, in comparison with spatial domain techniques, transform domain methods will permit more information to be embedded into the original image without changing its value. Still, one transforms domain can be fragile to standard as well as geometric attacks. To deal with this limitation, researchers proposed hybrid domain methods (Hernandez et al., 2015; Zhang et al., 2019) which are based on the transform domain. In recent watermarking algorithms, watermarking methods (Das and Kundu, 2012) based on hybrid domains are mainly utilized to improve the anti-attack and robustness overall performance of the algorithm, but at the cost of increased computational complexity. This paper has the following set of objectives-

(i) To provide security for digital content, by encrypting information.
(ii) To provide authenticity by embedding secret information.
(iii) To optimize the communication channel by reducing packet size, with low overheads.

This paper introduces a new model to combine Elliptic Curve Cryptography (ECC) Model with QIM Embedder & Global Selection strategy along with channel optimization for secure digital images. This research contributes to security aspects of digital images through robust encryption of images with smaller sized keys using ECC as compared to traditional approaches. The model further includes watermark embedding with butterfly selection and cognitive decision, which greatly boosts the performance of image validation and integrity verification. Furthermore, whereas the conventional algorithms may lead to working with packet sequencing for improving channel optimization, this model uses the discrete wavelet transform technique that reduces a size of packets which in turn decreases overhead and maintains a high level of security. Extensive testing on the common image dataset indicates that this model is more robust to multiple attack vectors, in addition to being an upgrade with respect to PSNR and MSE metrics over recent methods. The state-of-the-art requirements as well as suggested model make a very good part of secure digital image transmission and authentication in this paper for such applications.

The proposed research work is composed to five sections. Section one is an introduction, where we briefly mention research problem, objectives, and scope. The second section includes the literature review of various authors who have also carried out research work in the proposed 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 section describes the research methodology used to address the research problem. This section provides an explanation of the research design, data gathering strategies, data analysis approaches, and any ethical issues. The experiments' findings are shown in the fourth section. The data analysis and a discussion of the problem's findings are included in this part. The research findings and potential future research directions are presented in the fifth and final section, which also offers suggestions for how to further develop the field's understanding.

2. Related Work

With the digital revolution in full swing, it is no wonder that security of digital content has become a major concern for our society. Several techniques have been experimented to secure the trust worthiness and veracity of digital images. All across the globe, depending on traditional digital signature algorithms and cryptographic techniques have provided ground rules for maintaining a security base for our digital documents. But as technology grew, more sophisticated ways came out. Some of the notable works are as follows:

Singh et al. (2022a) used Otsu’s image segmentation technique to identify the slice that has been used for watermark embedding that has the least amount of medical information. Their suggested method used the affine transform to encrypt the watermarks itself, and used Schur decomposition, Lifting Wavelet Transform (LWT), Discrete Shearlet Transform (DST), and LWT to insert the encrypted watermark.

Singh et al. (2022b) provided a technique for dividing medical image data into two areas: the Region of Interest (RoI) and the Region of Non-Interest (RoNI), to ensure ROI integrity, tamper detection and recovery bits were encoded. ROI was watermarked using adaptive least significant bit (LSB) replacement, which took into account the concealing capacity map for improved tamper detection and recovery accuracy as well as increased imperceptibility of ROI. Electronic Patient Records (EPR) are encrypted with a pseudo-random key, sometimes referred to as a secret key, and compressed using Huffman compression to increase payload and confidentiality. The hospital logo QR code, encrypted EPR, and ROI recovery bits are interleaved in RoNI using Discrete Wavelet Transform-Singular Value Decomposition (DWT-SVD) hybrid transforms, creating a powerful watermark.

Singh et al. (2022c) proposed a watermarking technique which uses a smart block selection algorithm picking the blocks with highest entropy. The watermark and cover images are first shuffled via the Arnold transformation. The encrypted images are then subjected to additional processing, which includes singular value decomposition and a 2-level discrete wavelet transform.

Devi et al. (2016) centered on using visual cryptography to generate ownership and identity shares of an image. The low-frequency sub-band is extracted into fixed-size after shuffling and spliting the image in high- and low-frequency sub-bands. The singular value decomposition is used to compare the components in orthogonal matrices associated with different elements from each randomly chosen block to provide shares.

For the correct theory of visual cryptography in audio copyright protection, Ciptasari et al. (2014) used Naor and Shamir's notion. They provide a method for building a robust audio ownership protection system that combines digital timestamps, discrete wavelet transforms, discrete cosine transforms, and visual cryptography. In this method, the watermark is obtained by performing an OR operation between the secret and public images, rather than being encoded in the original audio. This creates a hidden image and a public picture.

Daoui et al. (2022) introduced a novel two-dimensional chaotic system namely the FrMPs map in which authors depicted chaos properties of fractional order Meixner polynomials (FrMPs).

Kumar and Sharma (2024), in the same sequence introduced new chaotic map with elliptic curve cryptography and genetic algorithm to improve image encryption. The algorithm can realize key high optical secrecy and robustness, mean while it combines the image point permutation using Arnold Cat map, pixel intensities encryption using Elliptic curve cryptography and using genetic algorithm for optimizing the keys generation.

Hanayong et al. (2021) proposed a system that implemented an encryption process based on the LSB and ECC-RSA algorithms, i.e., embedding both COVER into STGO image by being encrypted with LSB and stored in CHECK with generation of checksum using ECC-RSA. It is based on the original image and the image extracting from it.

The implementation system can encrypt, embed and decrypt a message in the research done by Hernandez et al (2015). To secure this process, ECC-RSA and LSB algorithms were used.

Al-Husainy (2006) in another study suggested a technique of image hiding with the combined effect of chaos and a special math technique. An object is created from chaos and a hash beginning with a secret key provided by the user, to get the image's secret code. The resulting code encrypted using the elliptic curve algorithm and sent to a 3rd party, who can use it to reveal the hidden image.

Chen et al. (2023) introduced a method that hide images with invisible waves and curves. Using mathematical methods, they created wave formations and changed the picture. Some numbers and one special box confused the image even more, so that it was tough to grasp.

Liang at el. (2021) Introduced a novel key-embedded hiding image technique maintain privacy and efficiency, they use bits to partition the image and disrupt it using chaotic sequences so that all pixels are made into a secret code.

Das and Kundu (2012) proposed a solution that is a blind Medical Image Watermarking (MIW) scheme using Contourlet Transform (CNT), which is robust against high JPEG and JPEG2000 compression. This technique addresses MDM challenges, including information security, content authentication, and controlled access retrieval. Hospital logo QR code, encrypted EPR and ROI recovery bits are embedded in RoNI by means of DWT-SVD hybrid trans-forms to produce a robust watermark.

Benssalah et al. (2021) presented a paper that evaluates the ECC-Hill cipher (ECCHC) technique, highlighting vulnerabilities to various attacks and the inadequacy of its key length. This is followed by a more efficient variant, that employs a generalized key matrix along with an improved EC Integrated Encryption Scheme (ECIES). Extensive testing reveals the reinvented crypto-system is more secure and more resistant to collision than existing practices. While many of the papers dealt with data security

(Hanayong et al., 2021; Daoui et al., 2022) that must be followed by authentication solutions (Daoui et al., 2022; Chen et al., 2023; Liang et al., 2021), the key issues remain to verify, identity (Liang et al., 2021; Chen et al., 2023) and finally prove secure communication channels. Hence a single model is highly desired that resolves all issues. Further few models optimize channel utilization but do not focus on data security. Hence Data security with channel optimization is desired.

The proposed research aims to fill these gaps by integrating ECC with advanced data hiding techniques and channel optimization. This research utilizes hybrid domain methods and genetic algorithms in embedding position selection, to improve security, robustness and efficiency of digital content protection. A similar type of analysis helps a review to consolidate all the already published work on the given topic. Alongside its major conclusions and results, this plays as benchmarks for the research in relation to what may have been recorded before it.

3. Proposed Methodology

In this section, paper proposed Butterfly Elliptical Curve Cryptography based Data Security (BECC-DS) model. Embedding in the image validates the authenticity of the image, while low-frequency regions improve the robustness against various attacks. To improve the security of the image, the Elliptic Curve Cryptography technique has been used. The graphical flow of work is shown in **Figure 1**. Notations used for the explanation of each block of **Figure 1** are listed in **Table 1**.

Table 1. Notation used in BECC-DS.

Notations	Description
I	Input Image
PI	Pre processed Image
S_S	Secret Signature
BS_S	Binary of S_S
L_L	Low-Frequency Image Coefficients
C_c	Cluster Center Coefficients
G	Generator Point on Curve
K_{su}, K_{ru}	Sender and Receiver public keys
K_{sp}, K_{rp}	Sender and Receiver private keys
EI	Embedded Image
EEI	Encrypted Embedded Image
S	Sensitivity
r	Genetic algorithm Iteration
M_r	Maximum iterations
C_r	Current iteration
C_1	Cognitive parameters
C_2	Social parameters
C_{eq}	Constriction Factor
N	Number of Iteration
W_t	Inertia Weight
V	Velocity
X	Position
L_{Best}	Local Best solution
G_{Best}	Global Best solution
P	Probability of Nectar Selection

3.1 Input Pre-Processing

Any input image is accepted for the work, regardless of its dimension. Both two- dimensional and three-dimensional images can be used with this piece. For a three-dimensional matrix, the color red is used to hide data (Sahu and Swain, 2019; Singh et al., 2022b). In this case, an image in HSV format would first be converted to RGB format. To obtain PI, we pre-process the input image I in the working environment. Moreover, the provided secret signature S_s must be converted into binary format BS_S. The reliance on the type of signature, such as text, image, number, etc., was eliminated by this binary embedding.

$$BS_S \leftarrow Binary\ (S_S) \quad (1)$$

$$PI \leftarrow\ Image\ processing\ (I) \quad (2)$$

3.2 DWT (Discrete Wavelet Transform)

This study takes advantage of the DWT frequency feature. Here, **Figure 2** illustrates the specific DWT methods used in the study that inserted a watermark in the image’s LL region (Tabassum and Islam, 2003; Xie and Huang, 2020). This image block is created by passing the image rows through a low pass filter and then another low pass filter, but in this case, the columns are filtered for the analysis. This block contains flat areas of the image that lack edge information; therefore, it is referred to as an approximation of the images.

$$[LL\ LH\ HL\ HH] \leftarrow DWT - First - Level\ (PI) \quad (3)$$

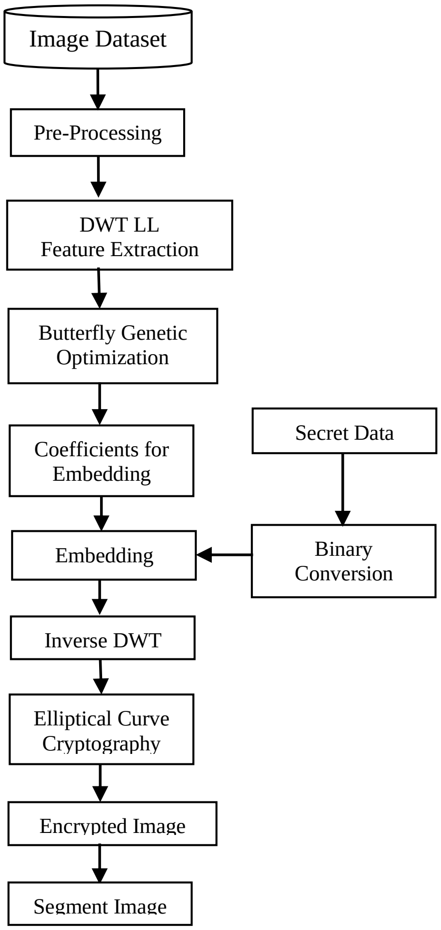


Figure 1. Block diagram of BECC-DS- model.

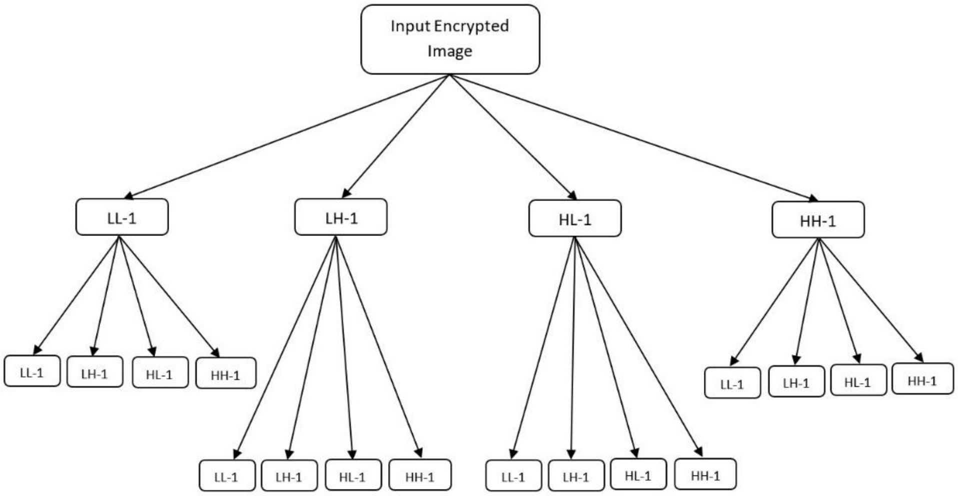


Figure 2. Image block for channel optimization.

3.3 Butterfly Algorithm

The approach used in this paper called the butterfly algorithm, treats each chromosome like a butterfly. This algorithm's goal is to get best portion of image where secrete signature will be hided. For this, at the sender side DWT LL feature extracted (Equation (3)) on preprocessed image and then apply following steps of butterfly genetic optimization for getting the best portion of image where secrete signature is hided (Zhou et al., 2021).

3.3.1 Generate Butterfly

A chromosome is a feasible solution for the set of optimum cluster center coefficients. As a result, a butterfly is a vector with n elements, where n is the number of cluster center coefficients. Hence, B is a butterfly population matrix of $p \times C$ dimensions, if p butterfly is generated. Gaussian random number generator function is used to choose the k number of coefficients.

$$B \leftarrow Butterfly\ Flame\ Population(p, C) \tag{4}$$

3.3.2 Evaluate L-Best and G-Best

In this step, the population's best chromosome is identified, and its fitness value serves as both the local and global best values. In this case, the fitness value of each likely solution in the population has been assessed to determine it. By the following algorithmic iteration, L_{Best} and G_{Best} begin to update regularly.

$$L_{Best} \leftarrow Min\ (Butterfly\ Fitness(B_C, LL)) \tag{5}$$

$$L_{Best} \leftarrow G_{Best}(Random) L_{Best} \ \leftarrow \ L_{Best}\, L_{Best} < G_{Best} \tag{6}$$

3.3.3 Fitness Function

Every butterfly is ranked according to distance. As a result, fitness value is used to evaluate distance. Coefficients based on butterflies are grouped into an image. The entire cost of the image coefficient's distance from the cluster center coefficients of the butterfly is taken into account while calculating fitness.

$$B_f \leftarrow Butterfly\ Fitness(B_C, LL) \tag{7}$$

3.3.4 Iteration Steps

In order to do this, the sensitivity of the butterfly is determined using Equation (8), while cognitive values including the constriction factor and inertia weight are assessed using Equations (9) to (11). Here, the butterfly's characteristics, including position and velocity, are also updated. Therefore, crossover is performed in accordance with the position matrix to update the population that is shown in Equations (12 and 13) (Zhou et al., 2021).

3.3.5 Sensitivity of Butterfly

$$S = e^{-M_r - \frac{C_r}{M_r}} \tag{8}$$

where, S is the sensitivity of r^{th} iteration where M_r is the maximum number of iterations that take place and C_r is the current iteration of this BA-PSO algorithm.

Cognitive and Social parameters

$$C_1 = y * \left(\frac{C_r}{M_r} + x\right) \tag{9}$$

$$C_2 = x * \left(\frac{C_r}{M_r}\right) \tag{10}$$

where, $x \; and \; y$ are constants ranging between 0 and 1.

Constriction Factor C_{eq}

$$\alpha = C_1 + C_2,$$
$$C_{eq} = 1 - \alpha - \sqrt{a^2 - 4a} \tag{11}$$

3.3.6 Inertia Weight W_t

$$W_t = y + \frac{(M_r - C_r)}{M_r}.$$

3.3.7 Update velocity V and position X of each probable solution

$$V_{i+1} = C_{eq} * \left(W_t * V_i + S * (1 - P) * R * C_1 * (G_{best} - C_r) + P * R' * C_2 * (L_{best} - C_r)\right) \tag{12}$$

$$X = R * P * V_{i+1} \tag{13}$$

In the above equation, V is velocity, X is position while R and R' are random numbers whose values range between 0 to 1. P is the probability of nectar for the butterfly selection. So as per X and V values crossover operations are performed.

3.3.8 Crossover

Because the success of the crossover genetic method depends on chromosome modification, the butterfly' number of random position values is altered by following modifying parameter x. The local Butterfly used in this operation is not the greatest. In this stage, the best local Butterfly set of features is used to modify each Butterfly x number of places at random. This butterfly is also tested for path length and their fitness level is compared to that of their parents; if the child butterfly performed better, the parent butterfly is removed; otherwise, the parent butterfly continued. After this phase, if the maximum number of iterations is completed, move on to the cluster coefficient step of the model; otherwise, assess each

Butterfly’s fitness value in the updated population.

3.3.9 Cognitive

This stage involves replacing random values from the food source cluster center set with a set of coefficient values ranging from 0 to 255. All the population’s food supplies are used for this activity.

$$L_{Best} \leftarrow Min\ (Butterfly - Fitness\ (B_c, L_L\ )) \tag{14}$$

$$B_C \leftarrow Crossover\ (L_{Best} - B_c) \tag{15}$$

3.3.10 Final Solution

Repeat the genetic algorithm’s fitness value and crossover procedure T times. Using the T operations technique, separate the coefficients into embedded and non-embedding sets based on the population optimum parameter estimate and the best-fitting cluster center source.

3.4 Data Embedding

Selected coefficient values are transformed into bits and the last three bits are replaced by the model. Once secret bits are embedded then the image is reassembled back into the embedded image. This image is inverse-transformed.

3.5 Encryption and Decryption using ECC

In this method, a Generator point G of the curve is shared between the sender and receiver. The sender encrypts the embedded image by Equation (2) (Xie and Huang, 2020).

$$EEI \leftarrow EI + (K_{sp}\, G\ + Z_{SR}) \tag{16}$$

where, K_{sp} is the sender's private key and Z_{SR} is the common number shared between the sender and receiver i.e.

$$Z_{SR} = K_{sp} * K_{ru} = K_{rp} * K_{su} \tag{17}$$

where, $\mathrm{K_{su}}$, $\mathrm{K_{ru}}$ is the sender and receiver public key, obtained from the below steps.

$$\mathrm{K_{su}} = K_{sp} * G \tag{18}$$

$$\mathrm{K_{ru}} = K_{rp} * G \tag{19}$$

3.6 Image Segmentation

DWT operation is applied for the segmentation of the image into fixed-size packets. For this, two two-level DWT operations are applied. The first input encrypted image was passed in the DWT. The output of the first DWT operation was passed into the further DWT. Hence total of 16 packets are generated by this second DWT operation. **Figure 2** shows two levels of image segmentation, for further size reduction of packets levels can be increased. This operation is expandable and lossless.

3.7 Receiver Side Image Extraction

In this extraction step receiver can extract secret signatures and images by applying the steps shown in **Figure 3**. Segmented packets are collected and unit at the receiver side. ECC decryption algorithm with correct public, private, and shared keys image got extracted.

Preprocessing and DWT-extracted features are carried out in the same manner as in the data concealment step. Key, the cluster center found using the butterfly optimization process, is another contribution to the effort. Data embedding and non-data embedding cluster coefficients are computed based on cluster center key coefficient values. Chosen coefficient values are converted to bits, and the last three least significant bits are collected to create a secret signature that could be verified as genuine.

$$EI \leftarrow EEI - (K_{rp}G + Z_{SR}) \tag{20}$$

Algorithm 1. Proposed Work BECC-DS Algorithm

```
$PI \leftarrow Image\ Processing(I)$
$BS_S \leftarrow Binary(S_S)$
$[LL\ LH\ HL\ HH] \leftarrow DW - First - Level\ (PI)$
$B_C \leftarrow Generate\ Population(LL)$
for1: itdo
        $B_f \leftarrow Butterfly\ fitness(B_C, LL)$
        $B_C \leftarrow Cognative\ (B_C)$
        $B_C \leftarrow Crossover\ (B_f,\ B_C)$
endfor
$B_f \leftarrow Butterfly\ fitness(B_C, LL)$
$C_C \leftarrow Best(B_f)$
for1:$S_S$do
        $LL \leftarrow Data\ Embedding\ (S_S[],\ LL,\ C_C)$
endfor
$EI \leftarrow IDWT\ (LL\ LH\ HL\ HH)$
$E\ EI \leftarrow ECC(EI)$
$SP \leftarrow DWT\ (EEI,\ level)$//levellike2,3,...
```

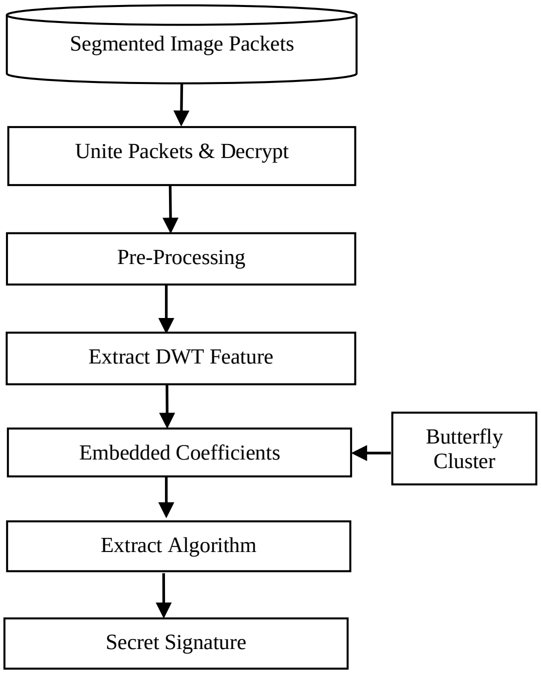


Figure 3. Secret data extraction process at the receiver side.

4. Experiments and Results

This section outlines the experimental evaluation conducted to gauge the efficacy of the suggested method for protecting images. All computations and utility measurements are carried out using the MATLAB tool. The experiments are executed on a computer with a 2.27 GHz Intel Core i3 processor, 4 GB of RAM, and Windows 7 Professional as the operating system. The proposed model is compared with the existing works ACM-ECC (Zhou et al., 2018; Parida et al., 2021).

Dataset analysis was performed on the common images, such as the tree, mandrilla, and Lena. These are typical images that are obtained from: http://sipi.usc.edu/database/?volume=misc. Framework is tried on everyday pictures also.

Table 2. Experimental Lena images of comparing models.

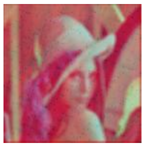
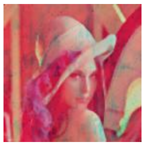
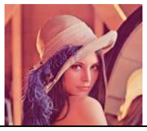
Image	BECC-DS	ACM-ECC
Embedded		
Ideal Extraction		
Gaussian Filter		
Median Filter		
Poisson Noise		
Salt & Pepper		
Histogram		
Compression		

Table 2 shows the comparison between existing model and proposed model under the different filter and noise attacks like gaussian filter, median filter. We performed these attacks on Lena image.

Table 3 shows the PSNR, and SNR values of different images after inverse cryptography at the receiver side. It is found that the use of the butterfly algorithm for embedding position selection has increased the PSNR by 9.49% as compared to the previous approach (Zhou et al., 2018). Cluster center selection is improved by the cognitive decision of the butterfly.

Tables 4 and **5** show the average execution of the comparing algorithm at the sender and receiver side. It has been found that the use of the packet clustering approach has increased the time as compared to the existing method BECC-DS.

Table 6 shows that the proposed model BECC-DS has improved the NC values by the use of a butterfly genetic algorithm for secret data embedding. It has been found that cluster-based data transfer has not made any impact during any of the attacks. This packet delivery reduces the channel dependency limit.

PSNR values of different attack images are shown in **Table 7**. It is found that in all sets of geometric, spatial attacks proposed the BECC-DS model has performed well. ECC-based encryption protects data under all attacks and maintains the PSNR value. Further, it is found that the butterfly genetic algorithm works efficiently to extract the original secret message.

Table 8 shows that the proposed model BECC-DS has improved the SNR values by the use of a butterfly genetic algorithm for secret data embedding. It has been discovered that cluster-based data transfer does not affect at on any given attack. The channel dependency limit is lowered by this packet delivery.

MSE values of different attack images are shown in **Table 9**. It is found that in all sets of geometric, spatial attacks proposed model BECC-DS model has performed well. ECC-based encryption protects data under all attacks and reduces the MSE value. Further, it is found that the butterfly genetic algorithm works efficiently to extract the original secret message.

Table 3. Ideal condition-based values of BECC-DS.

	PSNR (DB)		**SNR (DB)**	
Images	**BECC-DS**	**Das and Kundu (2012)**	**BECC-DS**	**Das and Kundu (2012)**
Lena	61.6544	55.6258	0.0332201	0.178034
Mandrilla	61.7929	55.836	0.0430323	0.16962
Boat	61.6144	55.8099	0.0448369	0.170643
Human	61.6144	55.9674	0.0448369	0.164567
Tree	61.79	55.7294	0.0430605	0.173837
Cup	61.4911	55.856	0.0461287	0.168842

Table 4. Ideal condition image sender time.

Images	**BECC-DS**	**ACM-ECC** **Parida et al. (2021)**
Lena	1.302	3.33925
Mandrilla	2.36301	3.78058
Boat	2.54611	3.63638
Human	2.07625	3.63638
Tree	3.0449	4.01723
Cup	2.76102	3.45752

Table 5. Image validation (receiver) time-based comparison.

Images	**BECC-DS**	**ACM-ECC** **Parida et al. (2021)**
Lena	2.85567	3.63994
Mandrilla	2.04175	3.69863
Boat	1.48145	3.69863
Human	2.953355	3.69863
Tree	3.55554	3.86404
Cup	1.67214	3.68123

Table 6. Comparison of various attacks for NC values.

Attacks			Lena Mandrilla					
	BECC-DS	Li and Miao (2013)	Golshan and Mohammdi (2011)	ACM-ECC Parida et al. (2021)	ACM-ECC Parida et al. (2021)	BECC-DS	Li and Miao (2013)	ACM-ECC Parida et al. (2021)
Gaussian Filter	0.878	-	0.9051	0.9603	0	0.858	-	0
Median Filter	0.877	0.9787	0.9726	0.9549	0	0.86	-	0
Poisson Noise	0.855	-	-		0	0.867	-	0
Salt & Pepper	0.859	0.9914	0.9193	0.9424	0	0.894	-	0
Histogram	0.696	-	-		0	0.757	-	0
Compression	0.879	-	-		0	0.817	-	0

Table 7. Comparison of various attacks for PSNR(DB) values.

Attacks	Lena			Mandrilla		
	BECC-DS	Li and Miao (2013)	ACM-ECC Parida et al. (2021)	BECC-DS	Li and Miao (2013)	ACM-ECC Parida et al. (2021)
Gaussian Filter	31.5413	-	17.9759	25.7588	-	17.7029
Median Filter	36.0472	30.3797	18.7065	31.8971	-	18.2965
Poisson Noise	25.7915	-	24.4753	26.0765	-	24.4017
Salt& Pepper	28.534	46.5169	27.4839	28.8719	-	27.9449
Histogram	13.988	-	13.9774	20.8508	-	20.3115
Compression	36.046	-	27.8669	38.0996	-	27.9308

Table 8. Comparison of various attacks for SNR (DB) values.

Attacks	Lena			Mandrilla		
	BECC-DS	Li and Miao (2013)	ACM-ECC Parida et al. (2021)	BECC-DS	Li and Miao (2013)	ACM-ECC Parida et al. (2021)
Gaussian Filter	18.9016	18.8996	18.8806	18.3036	18.3293	18.1625
Median Filter	18.9022	18.9006	18.8822	18.3068	18.3339	18.1645
Poisson Noise	18.9187	18.919	18.8806	18.3188	18.3512	18.1625
Salt& Pepper	18.9137	18.9137	18.898	18.3209	18.3527	18.1771
Histogram	19.1917	19.1914	19.1727	18.5953	18.6299	18.454
Compression	18.9029	18.9032	-0.37	18.3099	18.342	-0.525

Table 9. Comparison of various attacks for MSE(DB) values.

Attacks	Lena			Mandrilla		
	BECC-DS	Li and Miao (2013)	ACM-ECC Parida et al. (2021)	BECC-DS	Li and Miao (2013)	ACM-ECC Parida et al. (2021)
Gaussian Filter	45.5983	92.9149	1036.31	172.665	558.151	1103.54
Median Filter	16.1568	19.6493	875.858	42.012	365.58	962.565
Poisson Noise	171.369	171.534	232.035	160.475	160.843	235.999
Salt& Pepper	90.0478	91.9604	116.061	84.3126	85.1292	104.373
Histogram	2595.83	2587.11	2602.21	534.559	525.188	605.238
Compression	16.1613	16.5557	106.264	10.0722	10.459	104.714

5. Conclusions

As images are significant components in many applications, like today they have to be secure and validated with real-time properties. Here, this paper presents a new model which is the mixture of Elliptic Curve Cryptography (ECC) and thought to be advanced data hiding techniques for securing digital images. ECC is a strong and efficient encryption system which can be tricky to configure properly, and it may be vulnerable to side-channel attacks. DWT has the potential to produce a large amount of data reduction and enhancement of image compression due to its features using low computation cost and a lower distortion in the image stream. The butterfly algorithm improves watermark robustness and image quality, but it adds complexity and is vulnerable to more advanced attacks. The model exploits the image-based butterfly algorithm for watermark broadcasting and NEEP channels optimization using discrete wavelet transforms (DWT) to enhance security, data compression, and overhead reduction in communication by minimizing packet size. This reduces the processing power, makes it more flexible and able to provide better validation accuracy but greatly increases training data quality. Each approach offers its own security and efficiency benefits but also brings its own problems. Experimental results show a significant increase in the Peak Signal-to-Noise Ratio (PSNR) and reducing of Mean Squared Error (MSE) values, while butterfly approach improves PSNR up to 9.28% compared to previous method (Zhou et al., 2018), as well as MSE decreases at a ratio of 18.93% against various attacks. Moreover, the model demonstrates outperforming robustness on attacked database PSNR values (N = 1120721) by increasing it to 22.2%. These findings conclusively support the saliency and performance of the model as a defense against image order attacks in real life requirements, which can be employed for secure digital image transmission.

6. Future Scope

The proposed work can be further extended by the research community for future application in newly emerging areas like cognitive radio networks and IoT environments that demand a robust yet lightweight encryption techniques. Adapting the model for higher-dimensional media (video and 3D images) could open new application-areas. Moreover, more diversified and sophisticated cyber-attacks could also be used to conduct the robustness testing of the model (e.g., attacking by machine learning-based approach). Last but not the least, minor tweaking in real-time processing and reducing computational complexity surely can enhance its acceptance in resource-constrained environments.

Conflict of Interest

There are no conflicts of interest to disclose for this publication, according to the authors.

Acknowledgments

No specific grant was given for this research by public, private, or non-profit funding organizations. The editors and anonymous reviewers are appreciated by the writers for their insightful feedback, which helped to elevate the calibre of this work.

References

Al-Gindy, A., Al-Ahmad, H., Qahwaji, R., & Tawfik, A. (2009). A high capacity digital watermarking technique for the authentication of colour images. In *2009 IEEE International Symposium on Signal Processing and Information Technology* (pp. 37-42). IEEE. Ajman, United Arab Emirates.

Al-Husainy, M.A. (2006). Image encryption using genetic algorithm. *Information Technology Journal*, *5*(3), 516-519.

Benssalah, M., Rhaskali, Y., & Drouiche, K. (2021). An efficient image encryption scheme for TMIS based on elliptic curve integrated encryption and linear cryptography. *Multimedia Tools and Applications*, *80*(2), 2081-2107.

Chang, C.C., Chen, J.Y., Chen, Y.H., & Liu, Y. (2020). A reversible data hiding method for smvq indices based on improved locally adaptive coding. *International Journal of Network Security*, *22*(4), 575-583.

Chang, C.C., Li, C.T., & Shi, Y.Q. (2018). Privacy-aware reversible watermarking in cloud computing environments. *IEEE Access*, *6*, 70720-70733.

Chen, W.H., Zhou, X.F., Li, M.J., & Hu, M. (2023). Image encryption algorithm based on optical chaos and elliptic curve. *The European Physical Journal D*, *77*(11), 197. https://doi.org/10.1140/epjd/s10053-023-00774-7.

Ciptasari, R.W., Rhee, K.H., & Sakurai, K. (2014). An enhanced audio ownership protection scheme based on visual cryptography. *EURASIP Journal on Information Security*, *2014*, 1-12.

Daoui, A., Yamni, M., Karmouni, H., Sayyouri, M., Qjidaa, H., Ahmad, M., & Abd El-Latif, A.A. (2022). Biomedical Multimedia encryption by fractional-order Meixner polynomials map and quaternion fractional-order Meixner moments. *IEEE Access*, *10*, 102599-102617.

Das, S., & Kundu, M.K. (2012). Effective management of medical information through a novel blind watermarking technique. *Journal of Medical Systems*, *36*, 3339-3351.

Devi, B.P., Singh, K.M., & Roy, S. (2016). A copyright protection scheme for digital images based on shuffled singular value decomposition and visual cryptography. *SpringerPlus*, *5*, 1-22.

Dharwadkar, N.V., & Amberker, B.B. (2010). An efficient and secured non blind watermarking scheme for color images using DWT and Arnold transform. *International Journal of Computing*, *9*(2), 183-191.

Gao, H., Jia, L., & Liu, M. (2013). A digital watermarking algorithm for color image based on DWT. *TELKOMNIKA Indonesian Journal of Electrical Engineering*, *11*(6), 3271-3278.

Golshan, F., & Mohammdi, K. (2011). Evolutionary-generated watermark for robust digital image watermarking in DCT_SVD domain. *International Review on Computers and Software*, *6*(2), 155-161.

Hanayong, J., Zarlis, M., & Sihombing, P. (2021). Implementation of image security using elliptic curve cryptography RSA algorithm and least significant bit algorithm. In *5th International Conference on Computing and Applied Informatics* (Vol. 1898, No. 1, p. 012016). IOP Publishing. Medan, Indonesia.

Hernandez, M.C., Ugalde, F.G., Miyatake, M.N., & Meana, H.P. (2015). Robust watermarking method in DFT domain for effective management of medical imaging. *Signal, Image and Video Processing*, *9*, 1163-1178.

Kumar, S., & Sharma, D. (2023). Key generation in cryptography using elliptic-curve cryptography and genetic algorithm. *Engineering Proceedings*, *59*(1), 59. https://doi.org/10.3390/engproc2023059059.

Kumar, S., & Sharma, D. (2024). A chaotic based image encryption scheme using elliptic curve cryptography and genetic algorithm. *Artificial Intelligence Review*, *57*(4), 87. https://doi.org/10.1007/s10462-024-10719-0.

Li, J., & Miao, S. (2013). The medical image watermarking using arnold scrambling and DFT. In *Conference of the 2nd International Conference on Computer Science and Electronics Engineering* (pp. 192-195). Atlantis Press. Hangzhou, China. https://doi.org/10.2991/iccsee.2013.51.

Liang, H., Zhang, G., Hou, W., Huang, P., Liu, B., & Li, S. (2021). A novel asymmetric hyperchaotic image encryption scheme based on elliptic curve cryptography. *Applied Sciences*, *11*(12), 5691. https://doi.org/10.3390/app11125691.

Mohammad, A.A., Al-Haj, A., & Farfoura, M. (2019). An improved capacity data hiding technique based on image interpolation. *Multimedia Tools and Applications*, *78*, 7181-7205.

Parida, P., Pradhan, C., Gao, X.Z., Roy, D.S., & Barik, R.K. (2021). Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps. *IEEE Access*, *9*, 76191-76204.

Sahu, A.K., & Swain, G. (2019). An optimal information hiding approach based on pixel value differencing and modulus function. *Wireless Personal Communications*, *108*, 159-174.

Singh, K.U., Bhatia, S., Kumar, A., Kautish, S., Kumar, A., Basheer, S., & Hameed, A.A. (2022a). A robust NIfTI Image authentication framework based on DST and multi-scale otsu thresholding. *IEEE Access*, *10*, 132608-132620.

Singh, P., Devi, K.J., Thakkar, H.K., & Kotecha, K. (2022b). Region-based hybrid medical image watermarking scheme for robust and secured transmission in IoMT. *IEEE Access*, *10*, 8974-8993.

Singh, R., Izhar, L.I., Elamvazuthi, I., Ashok, A., Aole, S., & Sharma, N. (2022c). Efficient watermarking method based on maximum entropy blocks selection in frequency domain for color images. *IEEE Access*, *10*, 52712-52723.

Tabassum, T., & Islam, M. (2003). SM: A digital image data hiding technique based on identical frame extraction in 3-level DWT. *International Journal of Advanced Research in Computer Engineering & Technology*, *13*(7), 560-576.

Vaishnavi, D., & Subashini, T.S. (2015). Robust and invisible image watermarking in RGB color space using SVD. *Procedia Computer Science*, *46*, 1770-1777.

Xie, R., & Huang, P. (2020). 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, p. 052002). IOP Publishing. https://doi.org/10.1088/1757-899X/768/5/052002.

Xu, H., Lu, Y., & Guo, Q. (2022). Application of improved butterfly optimization algorithm combined with black widow optimization in feature selection of network intrusion detection. *Electronics*, *11*(21), 3531.

Zhang, Y., Li, Y., & Sun, Y. (2019). Digital watermarking based on joint DWT–DCT and OMP reconstruction. *Circuits, Systems, and Signal Processing*, *38*, 5135-5148.

Zhou, H., Cheng, H.Y., Wei, Z.L., Zhao, X., Tang, A.D., & Xie, L. (2021). A hybrid butterfly optimization algorithm for numerical optimization problems. *Computational Intelligence and Neuroscience*, *2021*(1), 7981670.

Zhou, X., Cao, C., Ma, J., & Wang, L. (2018). Adaptive digital watermarking scheme based on support vector machines and optimized genetic algorithm. *Mathematical Problems in Engineering*, *2018*(1), 2685739.

Zhou, Z., Chen, S., Wang, G. (2017). A robust digital image watermarking algorithm based on dct domain for copyright protection. In: Chen, Y., Christie, M., Tan, W. (eds) *Smart Graphics. SG 2015*. *Lecture Notes in Computer Science* (Vol. 9317, pp. 132-142), Springer, Cham. https://doi.org/10.1007/978-3-319-53838-9_11.

Publisher's Note- Ram Arti Publishers remains neutral regarding jurisdictional claims in published maps and institutional affiliations.