Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Durga Nadarajan[1*], T. Pramananda Perumal[2]

[1]Research Scholar (PT), Dept. of Computer Science, Presidency College, Chennai-600005
[2]Principal (Retired), Presidency College, Chennai-600 005

*Corresponding author: email: <u>durga.nadan@gmail.com</u>

PUBLISHED DATE: 10-AUG-2023

Abstract

Objectives: The main objective of this study is to develop a new chaotic-based image encryption scheme with key optimization to provide enhanced security over open social networks(OSNs) since the shared informations raise a number of security and privacy concern while uploading the contents like images, audio and video. **Methods:** The image encryption is done using proposed Elliptic Curve Cryptography and Logistic 2Dimensional Map Encryption (ECC-L2DME) scheme. The images for encryption are gathered from online open source; then shuffling of rows and column is performed on each image which is represented by a matrix of rows and columns of pixels. Elliptic Curve Cryptography (ECC) is used to encrypt every shuffled image, where the key is optimized with the help of Combined Pathfinder and Falcon Optimization (CPFO) algorithm. Then every encrypted image along with optimal key is given as input to the logistic 2Dimensional map encryption. **Findings:** Performance evaluation is done with various image encryption metrics and the resultant outcome is compared with existing optimization algorithms. On comparison, the results show that the total processing time(36.84 ms) of our proposed Combined Pathfinder and Falcon Optimization ECC-L2DME-based security scheme is less than that of the Dingo Optimization(66.27 ms), Black Widow Optimization(54.13 ms), PathFinder Optimization (66.86 ms) and Falcon Optimization (76.03 ms) and the memory space for encryption (404.02 KB) of our Combined Pathfinder and Falcon Optimization ECC-L2DME-based security scheme is less than that of the Dingo Optimization(790.3 KB), Black Widow Optimization(782.07 KB), PathFinder Optimization (561 KB) and Falcon Optimization (763.04 KB). Hence, our proposed CPFO with ECC-L2DME scheme is better than other optimization algorithms with respect to security in OSNs. **Novelty:** The novelty of this study is to optimize the key and reduce the processing time using the ECC-L2DME with CPFO and thus this study has achieved an enhanced performance to provide security in OSNs.

Keywords: Open Social Networks, Chaotic Map, Pathfinder Optimization, Falcon Optimization, Elliptic Curve Cryptography, Logistic 2-Dimensional Map Encryption

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

1. Introduction

In the domain of open social networks (OSNs), there is a wide array of online platforms such as Facebook, Twitter, WhatsApp, and others are now readily accessible. One major obstacle, faced by the open social networking platforms is the task of establishing secure communication channels among users. To address this challenge, various cryptographic algorithms are employed to maintain security within open social network communication.

Cryptography encompasses both symmetric and asymmetric algorithms, which are utilized for the encryption and decryption of data. An ECC framework has been proposed in such away that the authentic users are only eligible to upload the data and for those who have authentication rights from the owner are only eligible to download the uploaded contents within a specified time after which the key expires automatically [1]. The security framework Enhanced Bennet and Brassand 84 Quantum Cryptography protocol (EBB84QCP) efficiency is demonstrated by taking into account the limited resources of the body sensor in terms of battery life, memory and computational capacity along with key distribution method [2]. Security of images is achieved by hybrid optimization with cryptographic encryption algorithms and the results are compared with various encryption algorithms [3]. In the chaotic system, the trajectory is unpredictable and its dynamic response is very much sensitive to the method's initial variables and parameters. A classical key distribution protocol based on coherence optics and randomness based key generation has been suggested and examined to overcome the constraints in cryptographic algorithms [4]. A Cryptographic Architecture for Big Data Security(Z-CABDS) is proposed by Zheng, which offers compatibility and comprehensiveness in ensuring security in big data [5].

The proposed Combined Pathfinder and Falcon Optimization -Elliptic Curve Cryptography with Logistic 2-Dimensional Map Encryption (ECC-CPFO-L2DME) security scheme in this study is as follows:

- To build an advanced encryption-based security scheme to protect the information shared by the people in OSNs.
- To provide enhanced security to OSNs, an ECC-L2DME algorithm is proposed with key optimization using CPFO algorithm.
- The output of the proposed ECC-CPFO-L2DME-based security scheme is compared with the existing optimizatiom algorithms in order to identify the effectiveness of our proposed security scheme.

A security secheme is propsed which works more effectively to improve security, authenticity and has reduced the computing complexity. A content-based double encryption algorithm using symmetric key cryptography method is proposed and this algorithm has used binary addition, circular bit shifting and the folding method [6].

A system has been suggested which addresses the security vulnerabilities of using a public key cryptosystem, based on hyper elliptic curves combining the Digital Signature method with Elgamal techniques to ensure entity authentication and safe group communication [7].

A technique has been proposed on the basis of bilinear pairing cryptography and a tri-party one-round authenticated key agreement protocol to enable safe communication [8].

An efficient scheme using an asymmetric cryptography method has been used for an effective and secure anonymous communication method via wireless networks. Performance and cost analysis have concluded that this scheme is well-suited for wireless systems with limited power and resource availability [9].

7783

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Addition Chains(Acs) have been created using Particle Swarm Optimization (PSO) and Simplified Swarm Optimization (SSO), which are applied to the RSA and ECC procedures using two android and window emulators, respectively. Analysis has been done on the processing time, power consumption, decryption procedure and security [10].

A new L-shaped approach has been suggested that depends on dynamic blocks, which is combined with a one-dimensional chaotic system (Logistic map) and a two-dimensional chaotic system (2D-LASM system) to produce chaotic sequences for picture scrambling and diffusion. The results of the security analysis have showed that this algorithm has a strong encoding effect, excellent security and the ability to withstand different attacks [11].

Numerous statistical techniques, including Correlation Coefficient, Number of Pixels Change Rate (NPCR), Unified Average Changing Intensity (UACI) and Entropy have been used to determine the effectiveness of the proposed encoding method. They have included an example to show how the suggested encryption approach might produce extremely secure encrypted images [12].

A framework has been suggested for generic medical picture encryption based on a novel combination of Dynamic Substitution Boxes (S-boxes) and Chaotic Maps. Experimental findings conclude that traditional Baker map or Henon map has been used to achieve encryption without hardware acceleration, based on speed analysis [13].

This paper is organised as follows. Section 2 decribes the proposed scheme, ECC-Chaotic map-based encryption standard to provide high security over open social networks with key optimization. In Section 3, we present the results and discussion on the performance evaluation of the proposed Elliptic Curve Cryptography with Logistic 2Dimensional Map Encryption- Combined Pathfinder and Falcon Optimization (ECC-CPFO-L2DME) -based security scheme. In Section 4, we highlight the principle outcome of the study.

2. Methodology

2.1 Proposed ECC- CPFO-L2DME -based security scheme

Three different groups of images like natural images, satellite images and medical images are gathered from https://www.kaggle.com for performing the encryption operation and the images are in PNG, JPG and JPEG formats. The MATLAB R2020a programming platform is used to implement the proposed ECC-CPFO-L2DME-based security scheme. The images for encryption are gathered from online open source. Shuffling of rows and column is performed on each image . Elliptic Curve Cryptography (ECC) is used to encrypt every shuffled image, where the optimal key is created with the help of Combined Pathfinder and Falcon Optimization (CPFO) algorithm. This study is implemented with population, chromosome length and maximum iterations viz. 10, 4 and 50 respectively. Then every encrypted image along with optimal key is given as input to the logistic 2Dimensional map encryption. The encrypted image from ECC and optimized key are given as input to the L2DME system for proper encryption. This system consists of three phases such as 2D logistic permutation, diffusion and transposition. The decryption process is carried out in L2DME in reverse order to obtain the original image. The visual illustration of the above mentioned ECC-CPFO-L2DME-based security scheme is given in Fig.1.
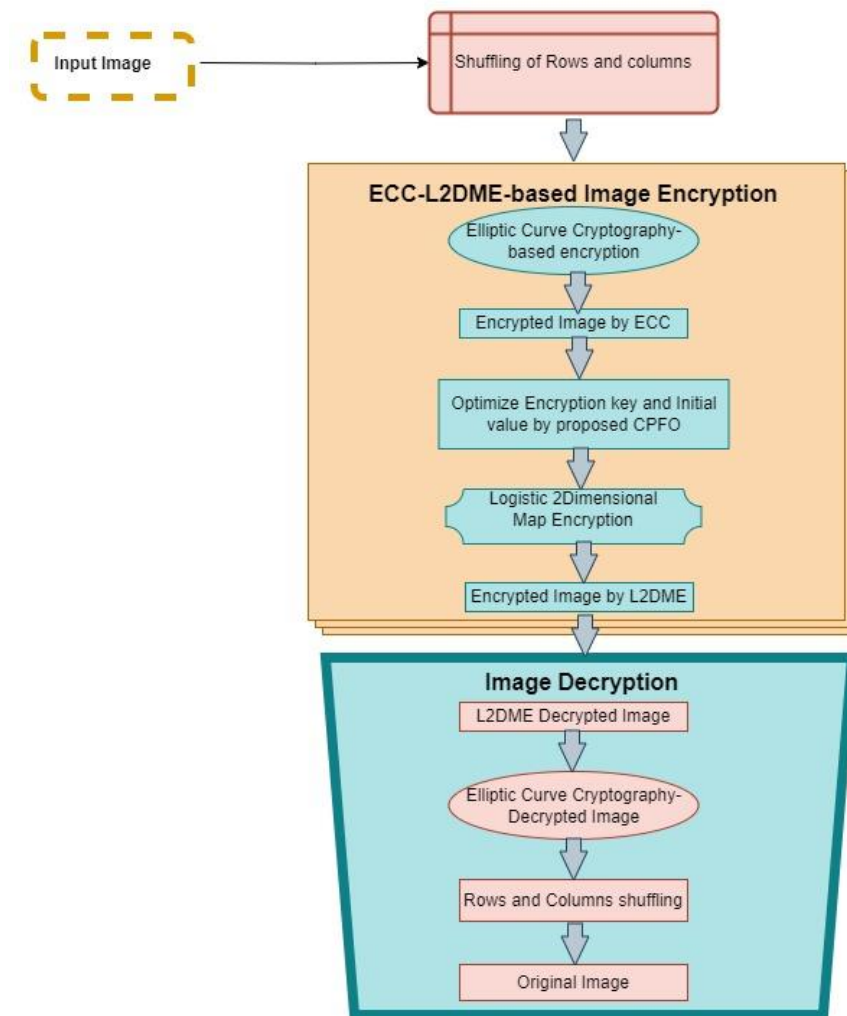
7784

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Fig. 1. Flow diagram of the proposed ECC-CPFO-L2DME-based security scheme

2.2 Shuffling of rows and columns of pixels of an image

The shuffling of rows and columns of pixels of an image can be easily done with the aid of a Pseudo-Random Number Generator (PSNG) and it is given in Eq. (1).

$$x_{i+1} = x_i^2 + x\,i + t \bmod m \quad \text{for i=0,1,2…} \tag{1}$$

Here, **t** is the random initial seed, **m** is a large number, x_i and x_{i+1} represent the pixel values in the ith and $(i+1)^{th}$ rows. The row shuffle table, T_R is defined in Eq. (2) and Eq. (3).

$$a = x_i \,(\bmod h) \tag{2}$$
$$T_R(i) = a + b \tag{3}$$

where h is the number of rows of the image and b is a non-negative integer which ensures a + b does not appear before. The sequence value at position $T_R(i)$ is obtained by adding a and b. As per the table T_R, row i is shuffled to row $T_R(i)$ for i=0,1,2,…, h-1. The column shuffle table $T_C(i)$ is defined similarly [14]. The shuffled images are given as input for image encryption using Elliptic Curve Cryptography.

7785

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

2.3 Elliptic curve cryptography (ECC)

Elliptic Curve Digital Signature Algorithm (ECDSA) public parameters consist of an elliptic curve denoted as C over a finite field Fq where q is the prime number representing the size of the field along with a fixed base point G belonging to C(Fq) which is chosen to have a large prime order n. Additionally, a one-way hash function **H** is also included in these parameters.

Key-pair creation: Here, d is the private key and is randomly generated from $[1, n-1]$ and also the value of the public key Q is calculated by using the private key and it is given in Eq. (4).

$$Q = d\,G \tag{4}$$

Signature generation: The signature value **s** is calculated using the formula, given in Eq. (5).

$$s = k^{-1}\,(H(M) + d * r) \bmod n \tag{5}$$

The signature **s** as the pair (r, s). Here, M represents the message, r is obtained as the x-component of the point resulting from the scalar multiplication of the secret key k and the base point G. i.e., r = x-component of [(kG) mod n]. The values H(M), d, n, and k are essential components in this process.

Signature verification: The value of R is calculated by Eq. (6).

$$R = vG + wQ \tag{6}$$

Here, v= H(M)w mod n, w=s x mod n and x= s^{-1} mod n

The signature is considered to be valid only if the x-coordinate of point R is equal to s mod n. The encrypted image is given as input to L2DME along with the key.

2.4 Logistic 2Dimensional Map Encryption (L2DME)

The encrypted image from the ECC process is given as input. The key generated in ECC is used as one of the parameters in L2DME system [16]. If any change occurs in the parameters of the system, then the whole system is entered into the chaos region. Image encryption in 2D logistic maps consists of three stages such as 2D logistic permutation, diffusion and transposition.

Key Generation: Generate a secret key that includes the parameters required for the logistic map. This includes the control parameters (r1, r2), the initial conditions (x_0, y_0), and the size of the image.

Initialization: Initialize the logistic map by setting the initial conditions (x_0, y_0) based on the key.

Chaotic Sequence Generation: Iterate the logistic map equations for a certain number of iterations to generate a 2D chaotic sequence. The iteration equations for the two-dimensional logistic map are given in Eq.(7) and Eq.(8).

$$x_{i+1} = r1 * x_i * (1 - x_i) + y_i \tag{7}$$
$$y_{i+1} = r2 * y_i * (1 - y_i) + x_i \tag{8}$$

where x_i represents the value of the row component (x-coordinate) at the ith iteration, y_i represents the value of the column component (y-coordinate) at the ith iteration, r1 and r2 are constants that influence the behavior of the chaotic system. By applying these, we get the 2D chaotic sequence with each point (x,y).

7786

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Image Scrambling: Map the chaotic sequence to the pixel positions of the image. Multiply the normalized chaotic sequence values by the image dimensions to obtain the new pixel positions. Swap the pixel values between the original and new positions to scramble the image.

Encryption Key Update: Update the key by applying a secure key update mechanism to ensure the security of the encryption process. This can involve changing the control parameters, initial conditions, or other components of the key.

Repeat: Depending on the desired encryption strength, steps 3 to 5 can be repeated multiple times.

The cipher text, produced from the three stages is combined together to form a permutation-substitution network. Finally, the encryption E and decryption D of the 2D logistic system are given in Eq. (9) and Eq. (10).

$$E = E(Q,K) \tag{9}$$
$$D = D(E,K) \tag{10}$$

Here, the encryption key is indicated as K. The decryption of image is done in reverse order to obtain the original image.

2.5 Pathfinder and Falcon Optimization Algorithms

a) Pathfinder Optimization Algorithm (PFOA):

The algorithm depends on the headship quality of animals for foraging their food [17].

The members of the group are positioned in two-dimensional spaces. From these members, the best one is selected as a leader based on the position of that particular member. This team leader is considered as a pathfinder for finding the position of prey, and it is expressed in Eq. (11).

$$\mathbf{x}(t + \Delta t) = \mathbf{x}(t) \cdot \mathbf{n} + \mathbf{f}_i + \mathbf{f}_p + \boldsymbol{\varepsilon} \tag{11}$$

$x(t)$ and $x(t + \Delta t)$ represent the positions of the team leader at time t and $t + \Delta t$ respectively, where Δt is a small time interval, $\mathbf{x}$ is the position vector, $\mathbf{n}$ is the unit vector without any angle, f_i is a pairwise interaction with neighbors x_i and x_j, f_p is the global force which depends on global optimum or position of pathfinder and $\boldsymbol{\varepsilon}$ is vector of vibration

The below Eq. (12) is used to find the new location of Pathfinder.

$$x_p(t + \Delta t) = x_p(t) + \Delta x + A \tag{12}$$

where, x_p is the position vector of pathfinder, Δx is the distance taken by pathfinder to move from one point to another and A is the vector of fluctuation rate.

The key purpose of optimization problem is to find the optimum. The modified eqation is given in Eq. (13).

$$x_i^{K+1} = x_i^K + R_1 \cdot (x_j^K - x_i^K) + R_2 \cdot (x_p^K - x_i^K) + \varepsilon, \quad i \geq 2 \tag{13}$$

K represents the current iteration, x_i is the position vector of ith member, x_j is the position vector of ith member, R1 and R2 are the random vectors. R1 is equal to $\alpha.r1$ and R2 is equal to $\beta.r2$, where r1 and r2 are random variable uniformly generated in the range of [0,1], α is the coefficient for interaction which defines the magnitude of movement of any member together with its neighbor and β is the coefficient of attraction which sets the random distance for keeping the herd roughly with leader. Also, r1 and r2 provide a random movement. There are two significant situations when $\alpha \to 0$, $\beta \to 0$ and $\alpha \to \infty$, $\beta \to \infty$

The second modification is given in Eq. (14).

$$x_p^{K+1} = x_p^K + 2r_3 \cdot (x_p^K - x_p^{K-1}) + A \tag{14}$$

where r_3 is a random vector uniformly generated in the range of [0,1], A is generated in each iteration using Eq. (15) and Eq. (16).

$$\varepsilon = (1 - K/Kmax) \cdot u_1 \cdot D_{ij}, \quad D_{ij} = \|x_i - x_j\| \tag{15}$$
$$A = u_2 . e^{-2K/Kmax} \tag{16}$$

7787

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

where u_1 and u_2 are random vectors range in $[-1,1]$, D_{ij} is the distance between two members and K_{max} is the maximum number of iterations. By u1 and u2 variables are set in the range $[-1,1]$, members can also move to their previous positions.

b) Falcon Optimization Algorithm (FOA):

The working of this algorithm is based on the foraging process of falcons [18].

Stage 1: Initialization of parameters
Initially, the limits, optimization difficulties and decision variables are defined by using the FOA algorithm. After that, the parameters like cognitive, following and social constants are represented as d_d, g_d and t_d, falcon quantities is indicated as OQ, BQ and EQ are specified as awareness and diving probabilities, respectively, u_{max} is represented as maximum acceptable speed.

Stage 2: Initialize the value of velocity and location of falcons
In this stage, the boundary conditions are taken into account for randomly locating the falcons in D-dimensional space.
Here, y is specified as falcon position, and it is based on the number of falcons OQ at the D-dimension. The values of maximum and minimum velocity are determined using Eq. (17) and Eq. (18).

$$u_{max} = 0.1 \; ub \tag{17}$$

$$u_{min} = -u_{max} \tag{18}$$

Here, upper bound limit range is termed as ub, and maximum and minimum acceptable velocities are represented as u_{max}, and u_{min}, respectively.

Stage 3: Finding the values of best global and individual location and determination of fitness value.
The fitness value is indicated as pg and it is determined by producing a vector.
Here, the best individual position of the falcon is represented as y_{best}. Finally, the new locations are created by using the individual best location of Falcon y_{best}, and it is based on the diving and awareness probabilities.

Stage 4: Establishment of the new location and upgrade the new location of falcons
In the beginning, the awareness and diving probabilities are contrasted by generating the two random numbers and it is specified as q_{BQ} and q_{EQ} respectively. After that, the value of q_{BQ} is contrasted with awareness probability BQ. If the value of $q_{BQ} < BQ$, the experience of the falcon is taken into consideration for identifying its prey and it is specified in Eq. (19).

$$y_{Itr} = y_{Itr-1} + u_{Itr-1} + d_d s(y_{best,Itr-1} - y_{Itr-1}) + t_d s(h_{best,Itr-1} - y_{Itr-1}) \tag{19}$$

Here, the velocity and present location of the falcon is indicated as y_{Itr-1}, u_{Itr-1}, respectively.
If the value of $q_{BQ} < BQ$ then fitness value of both falcon and prey are contrasted together. At last, the falcon follows suitable prey by diving method and it is given in Eq. (20).

$$y_{Itr} = y_{Itr-1} + u_{Itr-1} + g_d \; s(y_{cho} - y_{Itr-1}) \tag{20}$$

where y_{cho} is the chosen prey. If the above condition is not satisfied, then the displacement of falcons is based on the individual best location and it is expressed in Eq. (21).

$$y_{Itr} = y_{Itr-1} + u_{Itr-1} + d_d \; s(y_{best,Itr-1} - y_{Itr-1}) \tag{21}$$

Finally, velocity and boundary conditions are examined for the new location, and the fitness value is also computed for the new position. The new positions of y_{best} is also determined.

Stage 5: Continue the above steps until achieving the maximum number of iterations.

7788

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

2.6 Proposed model for Combining Pathfinder and Falcon Optimization Algorithms (CPFO)

The Pathfinder optimization algorithm (PFOA) is a meta-optimization algorithm. Yet, it does not give proper outcomes for large dimension problems. Since, Falcon optimization algorithm (FOA) is a meta-heuristic-based optimization algorithm and it is more comfortable for large dimensional problems. The FOA algorithm has a lower convergence rate and high oscillations. These limitations are overcome by combining these two optimization algorithms. This is the proposed model in our study. In this model, both Path Finder(PF) and Falcon Optimization(FO) algorithms are combined together in optimizing the key for encryption of data in order to maintain the secure data transfer. The proposed optimization model is hereafter named as Combined Pathfinder and Falcon optimization algorithm(CPFO).

The main objective of the proposed ECC-CPFO-L2DME-based encryption scheme is to minimize the encryption time as well as the memory space. The total time taken for execution of a single data (image) secure transfer is known as the total processing time (T) in milliseconds(ms). It is calculated by summing the encryption and decryption times of each data secure transfer. The total amount of memory space, used for a single secure data transfer is known as memory size (M) in bytes

Pseudo code for the proposed CPFO is depicted in Algorithm 1.

Algorithm 1: Proposed CPFO
Initialize the maximum number of iteration
Initialize number of population
for $t = 1$ *to* M_itr
for $i = 1\,to\,N_P$
Find the value of fitness using improved algorithm
Evaluate the value of y_j^{L+1} by Eq. (13)
Evaluate the value of y_q^{L+1} by Eq. (14)
Find the value of $u_{\max}$ by Eq. (17)
Evaluate the value of y_{ltr} using Eq. (20)
If t is an odd number
Update using PFA
Else
Update using FOA
End if
End for
End for

2.7 Key- time validity

Key-time validity is an important factor that is performed on the generated key. If the authenticated user wants to decrypt the data, the encrypted image must be decrypted within specified time duration (in seconds). If it exceeds a specified time duration, it can not be opened by the authenticated receiver.

7789

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

3. Results and Discussion

3.1 Performance evaluation of our proposed scheme (ECC-CPFO-L2DME)

3.1.1 Image Collection

The sample images, required for the encryption scheme like natural images, satellite images and medical images are gathered from https://www.kaggle.com. Sample images are shown in Fig. 2.
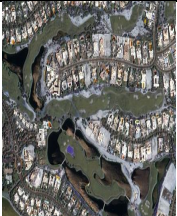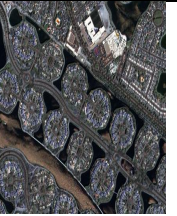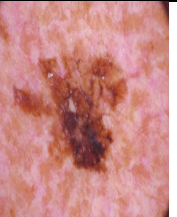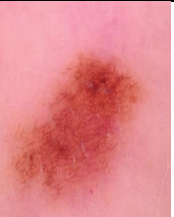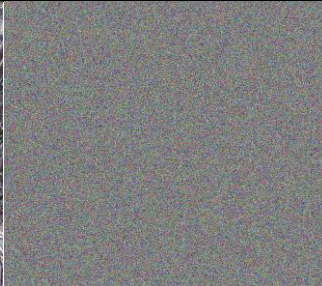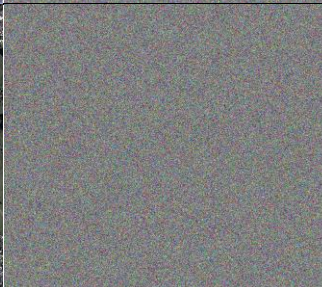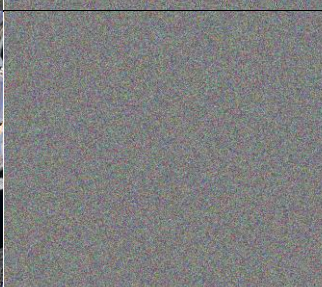
Type of image	1	2	3	4	5	6
Natural image						
Satellite image						
Medical image						

Fig. 2. The gathered Natural, Satellite and Medical images for the proposed scheme
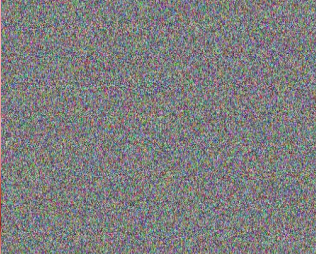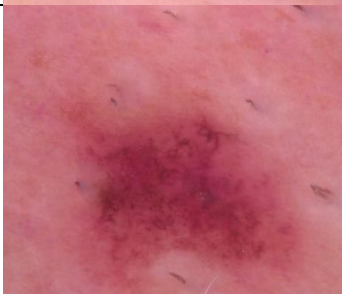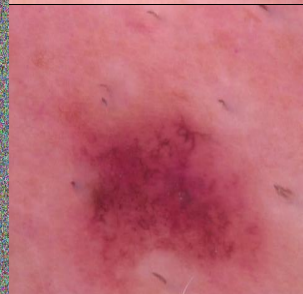
3.1.2 Images during encryption and decryption

The original, encrypted and decrypted images after the implementation of our proposed ECC-CPFO-L2DME-based security scheme are shown in Fig. 3.

7790

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Images	Natural images		
	Original image	**Encrypted image**	**Decrypted Image**
1			
2			
3			
4			
5			
6			

7791

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Imges	Satellite images		
	Original image	**Encrypted image**	**Decrypted image**
1			
2			
3			
4			
5			

7792

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Images	Medical images		
	Original image	**Encrypted image**	**Decrypted Image**
1			
2			
3			
4			

7793

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Fig. 3. Original, Encrypted and Decrypted Images

3.1.3 Performance metrics

Mean Square Error(MSE): It is calculated by Eq. (25).

$$MSE = \frac{1}{M} \sum_{j=1}^{M} (z_j - \hat{z}_j)^2 \qquad (25)$$

Here, M is the number of data points, then the observed and predicted values is marked as z_j and $\hat{z}_j$, respectively.

Number of Pixel Changing Rate(NPCR): It is determined using Eq. (26).

$$NPCR = \frac{N\_diff}{N\_width * N\_height} * 100 \qquad (26)$$

where N_diff is the total number of differing pixels between the two encrypted images and N_width is the width of the images (in pixels). N_height represents the height of the images (in pixels).

Peak Signal to Noise Ratio(PSNR): It is given in Eq. (27).

$$PSNR = 10 * log_{10} \frac{S^2}{MSE} \qquad (27)$$

where S is the maximum pixel value of the image (usually 255 for 8-bit grayscale or 255 for each color channel in a color image). MSE is the mean squared error between the original and encrypted images, calculated as the average of the squared differences between corresponding pixels.

Unified Average Changing Intensity(UACI): It is calculated as in Eq. (28).

UACI = (1 / (N_width * N_height)) * Σ|I(x, y) - E(x, y)| $\qquad$ (28)

where N_width is the width of the images (in pixels), N_height is the height of the images (in pixels), I(x, y) represents the intensity of a pixel at coordinates (x, y) in the original image, E(x, y) represents the intensity

7794

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Input Images	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
5	1.5686	0.78431	3.9216	3.5294	7.451
1	5.098	5.4902	3.5294	3.1373	6.2745
2	3.9216	1.5686	1.5686	1.9608	5.098
3	3.6216	3.8431	3.1373	3.5294	3.9216

Table 1. MSE for Natural Images

of a pixel at coordinates (x, y) in the encrypted image and Σ denotes the sum of the absolute differences in pixel intensities over all pixels in the image.

3.1.4 Performance evaluation on natural Images

The performance metrics MSE, NPCR, PSNR, UACI, encryption time, decryption time, total processing time and memory size are calculated for determining the efficiency of the proposed ECC-CPFO-L2DME-based security scheme. Table 1. Table 2, Table 3, Table 4, Table 5, Table 6, Table 7 and Table 8 show the results, obtained by calculating the above metrics for the other existing optimization algorithms such as Dingo Optimization(DO), Black Widow Optimization(BWO), Path Finder Optimization(PFO) and Falcon Optimization (FO) and our proposed ECC-CPFO-L2DME-based security scheme for natural images .

Input Images	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
5	10.016	6.516	11.809	8.463	6.124
1	11.378	11.882	10.293	10.127	6.540
2	10.628	8.106	10.952	9.478	5.118
3	9.183	7.897	8.336	6.282	5.394

Table 2. PSNR for Natural Images

Table 3. NPCR for Natural Images

Input Images	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
5	91.773	93.087	93.053	92.358	93.55
1	91.043	90.729	90.015	90.09	93.914
2	90.126	92.76	90.478	90.416	93.718
3	92.252	93.075	92.486	93.93	93.957

7795

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Table 4. UACI for Natural Images

Input Images	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
5	32.646	32.657	31.509	30.301	32.707
1	30.895	31.771	29.36	32.431	32.84
2	29.416	30.665	30.029	32.012	32.641
3	31.155	31.531	30.943	29.471	32.992

Table 5. Encryption time in milliseconds(ms) for Natural Images

Input Image Types	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
PNG	48.56	48.551	57.182	64.415	29.084
JPG	70.705	37.603	68.539	63.544	14.775
JPEG	60.977	12.126	21.84	42.425	5.315

Table 6. Decryption time in milliseconds(ms) for Natural Images

Input Image Types	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
PNG	17.715	7.7607	9.6777	11.648	6.5473
JPG	14.692	3.4061	5.9548	19.305	19.305
JPEG	17.577	19.736	19.019	10.458	10.5851

7796

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Table 7. Total Processing time in milliseconds(ms) for Natural Images

Input Image Types	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
PNG	66.274	54.133	66.86	76.063	36.844
JPG	85.398	41.009	74.494	69.943	34.08
JPEG	78.555	31.862	40.859	52.882	22.849

Table 8. Memory size in Kilobytes (KB) for Natural Images

Input Image Types	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
PNG	790.3	782.07	561	763.04	404.02
JPG	958.23	531.11	516.89	657.66	448.41
JPEG	594.02	693.54	618.5	860.2	409.49

Fig. 4. depicts the comparison of the proposed ECC-CPFO-L2DME-based security scheme with other existing optimization algorithms on natural images.

(a)
(b)

7797

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346
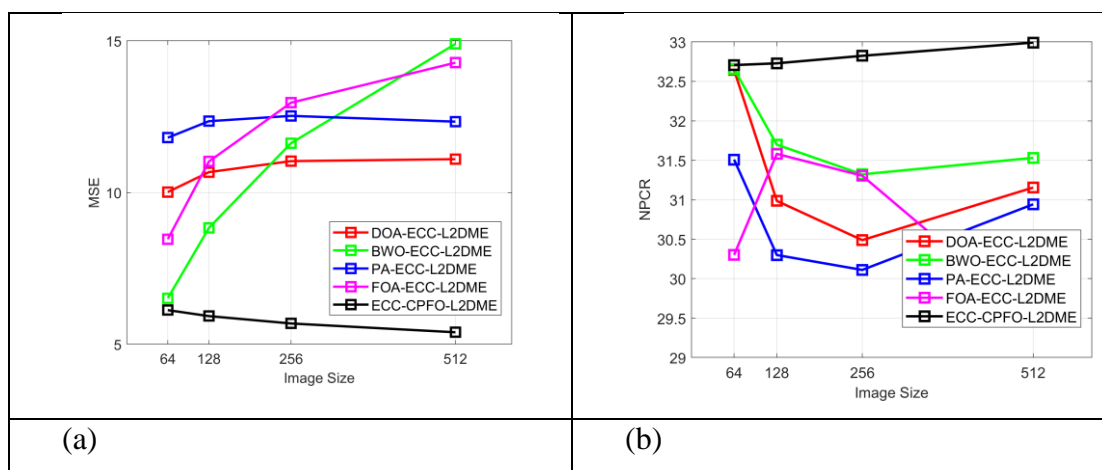
Fig. 4. Comparison of ECC-CPFO-L2DME-based security scheme with other existing optimization algorithms on natural images (a) MSE (b) NCPR (c) PSNR (d) UACI (e) Encryption time (f) Decryption time (g) Memory size (h) Total processing time

3.1.5 Performance evaluation on satellite images

Table 1. Table 2, Table 3, Table 4, Table 5, Table 6, Table 7 and Table 8 show the results, obtained by calculating the above metrics for the other existing optimization algorithms such as Dingo Optimization(DO), Black Widow Optimization(BWO), Path Finder Optimization(PFO) and Falcon Optimization (FO) and our proposed ECC-CPFO-L2DME-based security scheme for satellite images

7798

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Table 9. MSE for Satellite Images

Input Images	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
4	12.376	11.107	11.404	13.423	6.9001
1	7.8503	12.441	14.425	8.3077	7.4522
5	13.208	9.7239	9.5191	10.4	5.4115
6	7.7347	7.3451	9.84	9.432	5.1796

Table 10. PSNR for Satellite Images

Input Images	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
4	92.062	90.313	90.595	91.287	93.273
1	90.729	92.117	92.194	91.06	93.435
5	92.573	90.959	93.566	91.42	93.732
6	93.033	93.483	92.221	90.196	93.733

Table 11. NPCR for Satellite Images

Input Images	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
4	29.172	32.307	30.592	30.65	32.818
1	32.01	30.581	31.28	30.041	32.381
5	31.341	31.275	32.663	29.922	32.764
6	30.58	31.331	30.959	32.519	32.551

Table 12. UACI for Satellite Images

Input Images	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
4	17.255	17.255	14.902	9.0196	18.824
1	15.294	9.0196	14.51	13.333	18.824
5	12.549	14.118	12.549	13.725	16.863
6	15.686	14.118	14.51	12.941	18.039

7799

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Table 13. Encryption time in milliseconds(ms) for Satellite Images

Input Image Types	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
PNG	63.204	89.282	44.421	78.551	6.302
JPG	58.409	69.022	84.314	58.512	17.033
JPEG	33.754	40.95	41.525	99.57	10.491

Table 14. Decryption time in milliseconds(ms) for Satellite Images

Input Image Types	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
PNG	11.955	16.005	19.934	15.154	3.949
JPG	13.6	12.753	10.714	6.036	19.314
JPEG	12.931	6.0185	12.586	17.679	12.931

Table 15. Total Processing time in milliseconds(ms) for Satellite Images

Input Image Types	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
PNG	75.159	105.29	45.793	93.705	10.251
JPG	59.676	81.775	95.028	64.548	36.347
JPEG	39.772	42.696	54.111	117.25	23.422

Table 16. Memory size in Kilobytes(KB) for Satellite Images

Input Image Types	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
PNG	617.1	781.2	819.5	881.57	417.13
JPG	521.4	715.7	727.4	820.34	582.5
JPEG	699.3	891.74	795.7	808.6	467.24

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Fig. 5. depicts the comparison of the proposed ECC-CPFO-L2DME-based security scheme with other existing optimization algorithms on satellite images.
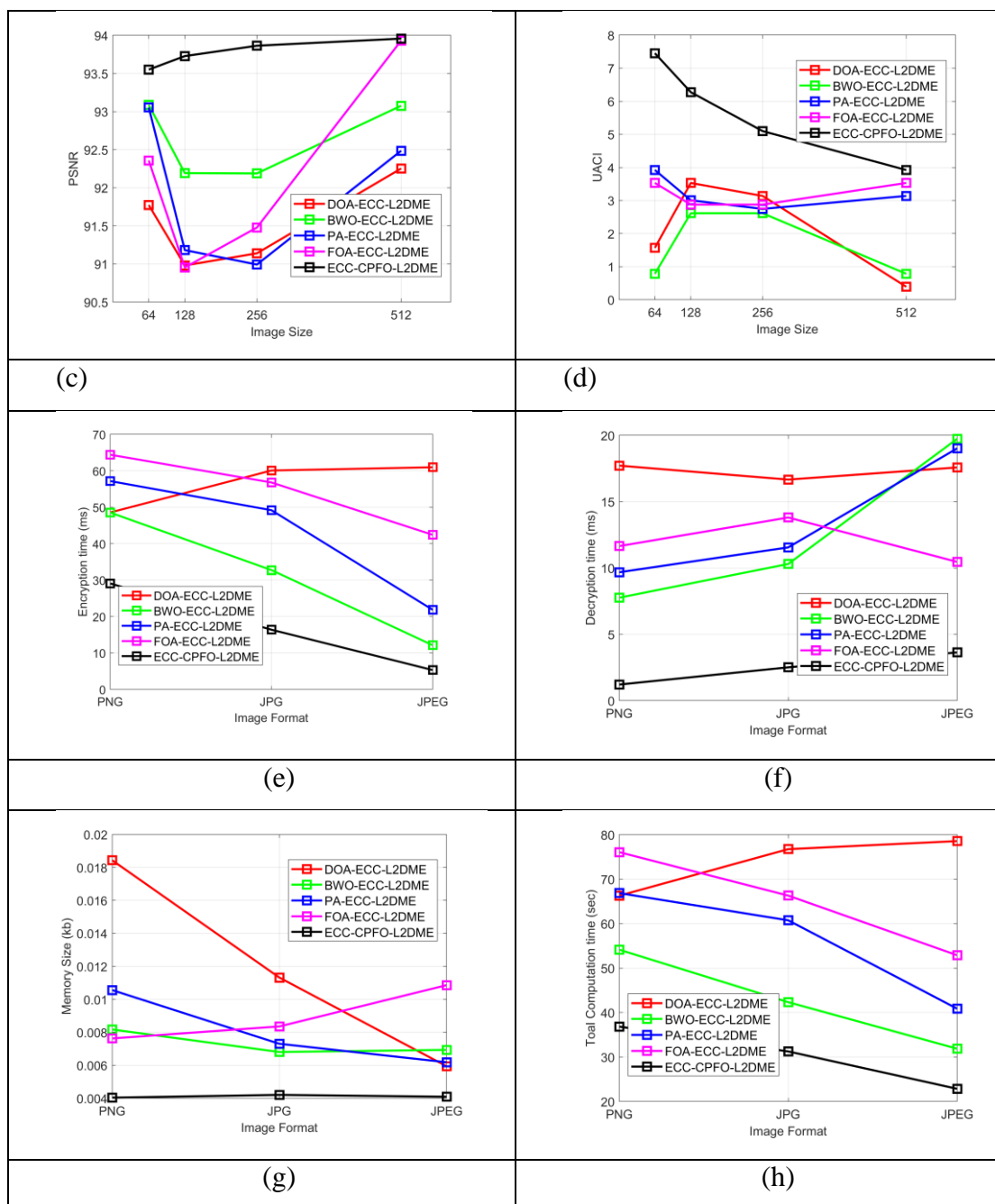

(a)　　(b)　　(c)　　(d)　　(e)　　(f)　　(g)　　(h)

7801

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

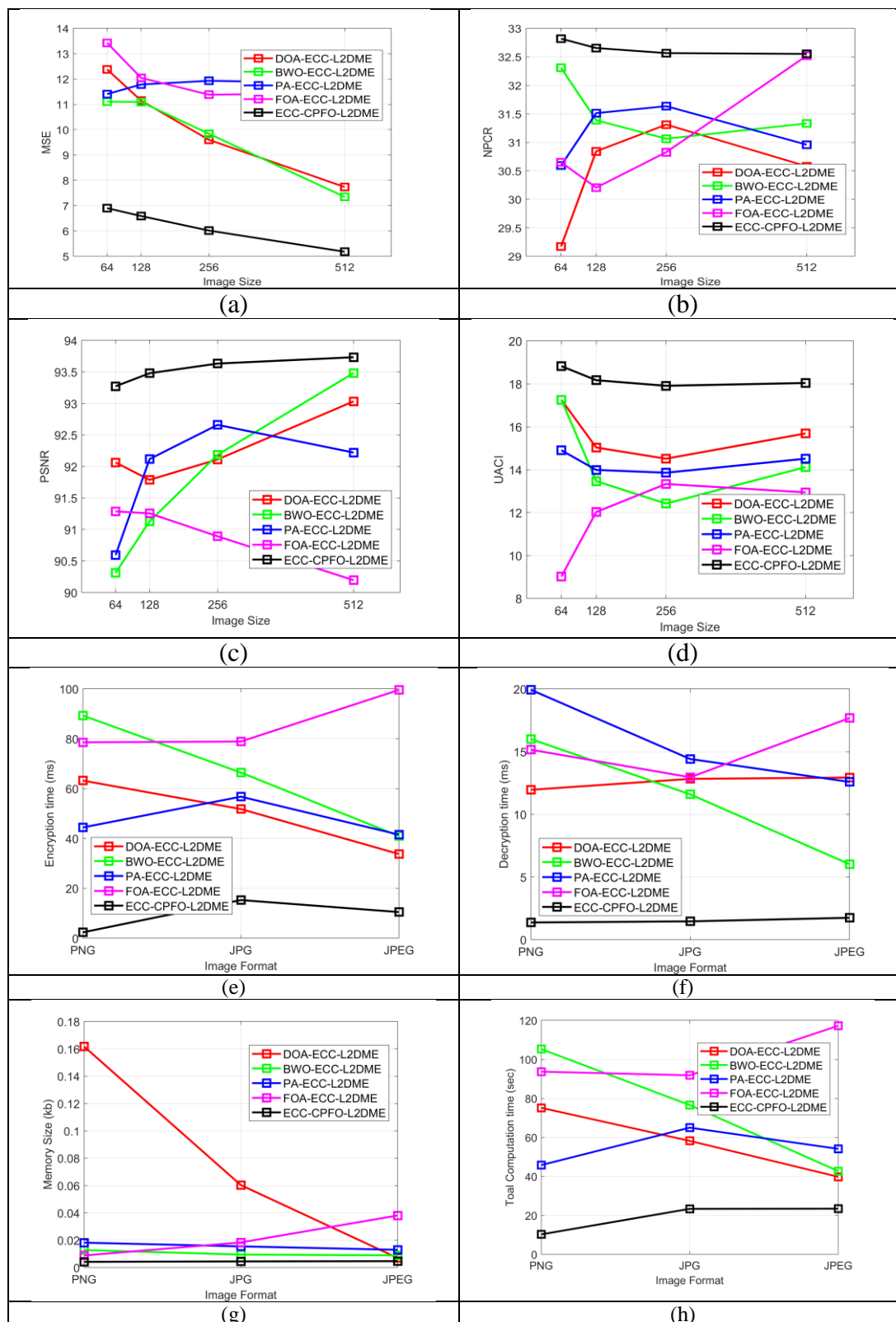*Section A-Research paper*
ISSN 2063-5346

Fig. 5. Comparison of ECC-CPFO-L2DME-based security scheme with other existing algorithms on satellite images (a) MSE (b) NCPR (c) PSNR (d) UACI (e) Encryption time (f) Decryption time (g) Memory Size (h) Total Processing time

3.1.6 Performance evaluation on medical images

The performance metrics MSE, NPCR, PSNR, UACI, encryption time, decryption time, total processing time and memory size are calculated for determining the efficiency of the proposed ECC-CPFO-L2DME-based security scheme. Table 1. Table 2, Table 3, Table 4, Table 5, Table 6, Table 7 and Table 8 show the results, obtained by calculating the above metrics for the other existing optimization algorithms such as Dingo Optimization(DO), Black Widow Optimization(BWO), Path Finder Optimization(PFO) and Falcon Optimization (FO)   and our proposed ECC-CPFO-L2DME-based security scheme for medical images .

Table 17. MSE for Medical Images

Input Image	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
6	6.5113	12.485	8.6067	8.3895	6.3773
1	10.639	13.622	14.511	12.203	7.9652
3	11.381	10.813	9.0879	14.982	6.2457
5	7.607	6.2035	6.0607	13.651	5.2473

Table 18. PSNR for Medical Images

Input Image	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
6	93.133	91.824	91.501	92.875	93.903
1	90.118	90.951	93.418	92.492	93.817
3	91.461	91.992	90.372	92.425	93.87
5	92.333	93.243	91.054	93.054	93.354

Table 19. NPCR for Medical Images

Input Image	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
6	30.522	29.287	30.364	30.052	32.885
1	29.617	32.367	30.792	30.866	32.814
3	29.755	29.616	31.44	30.808	31.587
5	31.4	32.823	29.155	32.515	32.97

7802

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Table 20. UACI for Medical Images

Input Image	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
6	3.9216	5.098	4.3137	3.5294	6.6667
1	3.5294	1.9608	4.7059	6.6667	7.0588
3	1.1765	4.3137	4.7059	4.3137	6.6667
5	2.7451	5.098	4.3137	3.9216	8.2353

Table 21. Encryption time in milliseconds(ms) for Medical Images Images

Input Image Types	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
PNG	22.008	79.367	38.866	23.115	11.263
JPG	24.209	46.936	37.119	42.363	9.094
JPEG	39.34	93.064	44.092	25.871	20.468

Table 22. Decryption time in milliseconds(ms) for medical Images

Input Image Types	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
PNG	16.376	17.719	18.444	13.623	10.230
JPG	13.395	5.2645	13.182	9.5819	7.869
JPEG	5.3907	9.4119	15.914	15.203	23.862

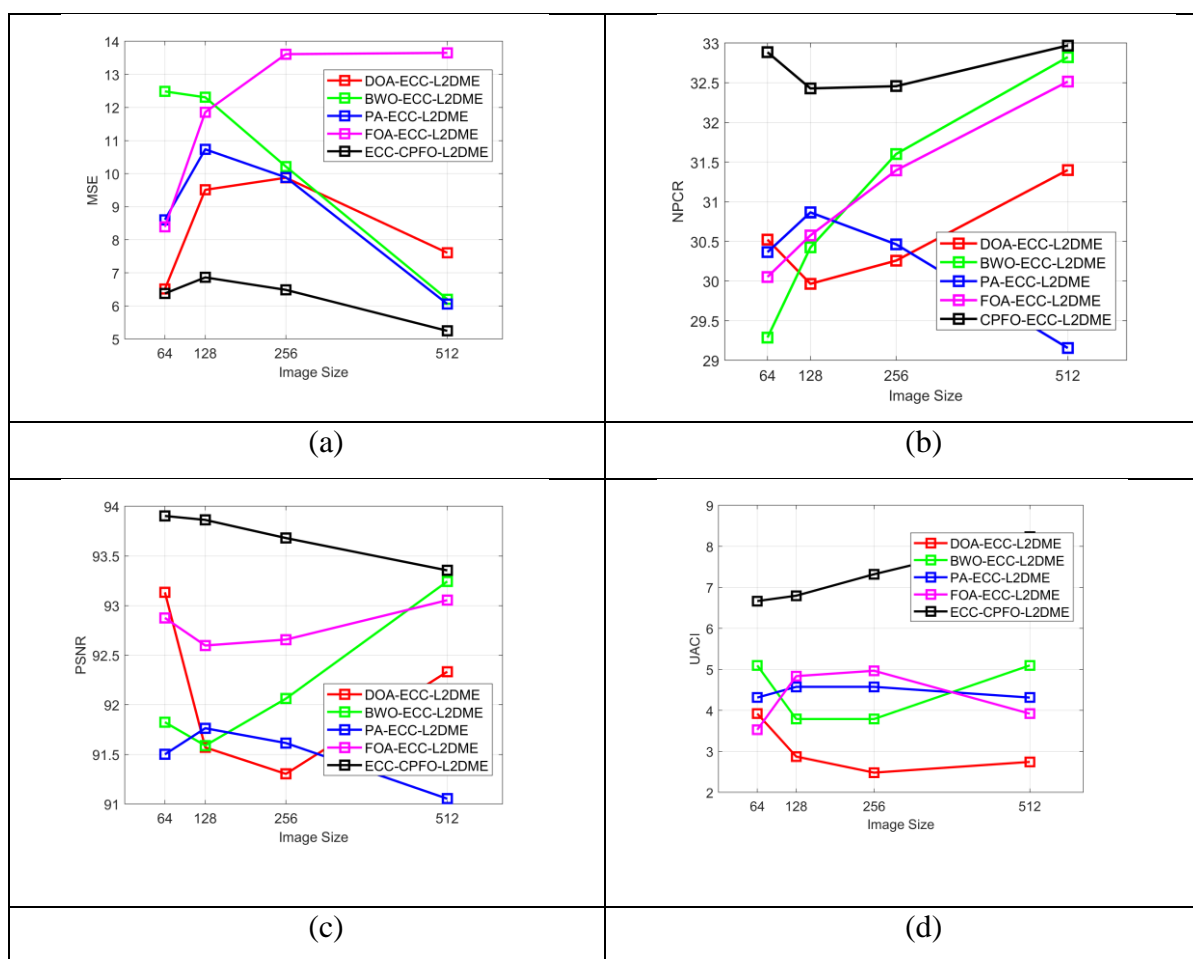Table 23. Total Processing time in milliseconds(ms) for medical Images

Input Image Types	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
PNG	38.383	97.086	57.31	30.189	21.493
JPG	33.791	52.201	50.302	44.578	16.963
JPEG	102.48	45.263	41.074	24.66	44.33

7803

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Table 24. Memory size(KB) for Medical Images

Input Image Types	DOA-ECC-L2DME	BWO-ECC-L2DME	PA-ECC-L2DME	FOA-ECC-L2DME	ECC-CPFO-L2DME
PNG	657.98	626.06	563.25	813.46	505.12
JPG	835.04	757.41	853.4	700.17	832.9
JPEG	581.6	489.45	670.6	807.02	449.5

Fig. 6. depicts the comparison of the proposed ECC-CPFO-L2DME-based security scheme with other existing optimization algorithms on medical images.

(a) (b) (c) (d)

7804

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

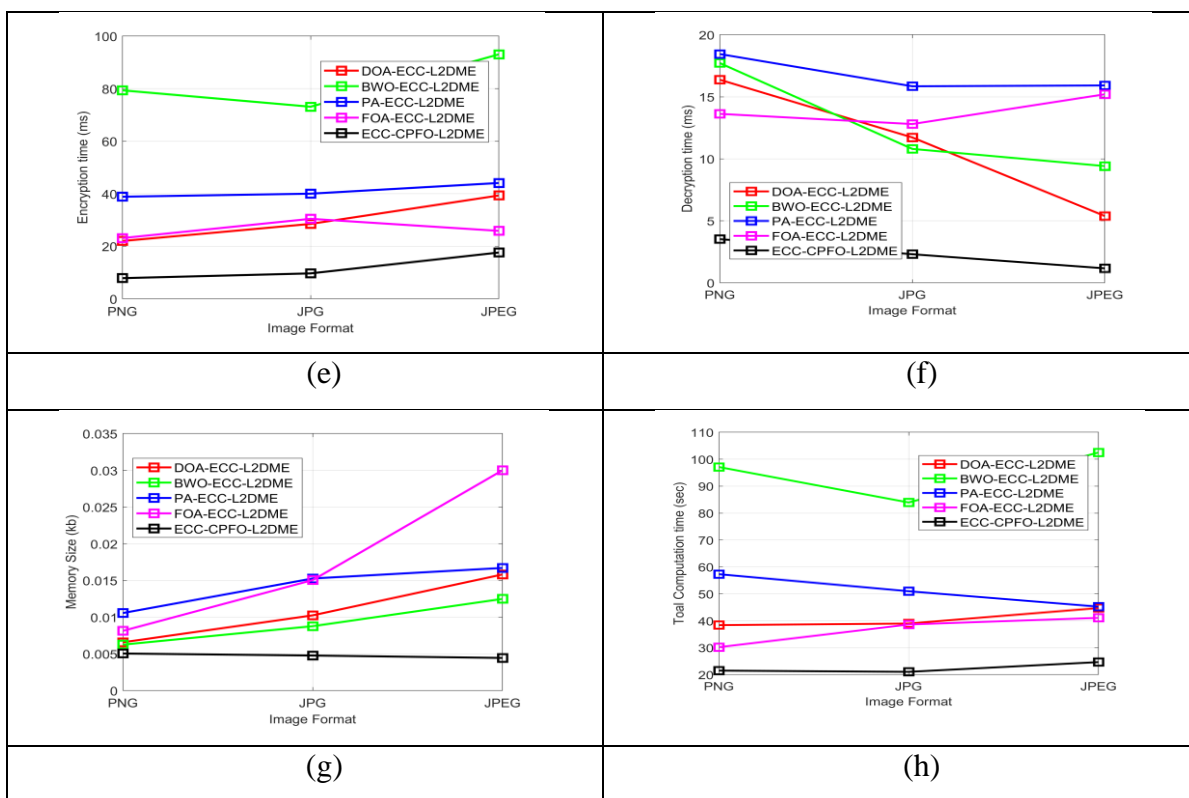*Section A-Research paper*
ISSN 2063-5346

Fig. 6. Comparison of ECC-CPFO-L2DME-based security scheme with other optimization algorithms on medical images (a) MSE (b) NCPR (c) PSNR (d) UACI (e) Encryption time (f) Decryption time (g) Memory Size (h) Total processing time

3.1.7 Convergence examination

The convergence analysis of the ECC-CPFO-L2DME-based security scheme is shown in Fig.7. The number of iterations is taken in the x-axis to get precise outcomes. The convergence analysis of the proposed ECC-CPFO-L2DME-based security scheme is better than the DOA-ECC-L2DME, BWO-ECC-L2DME, PA-ECC-L2DME and FOA-ECC-L2DME with 25%, 40%, 40% and 50% at 30th iteration.
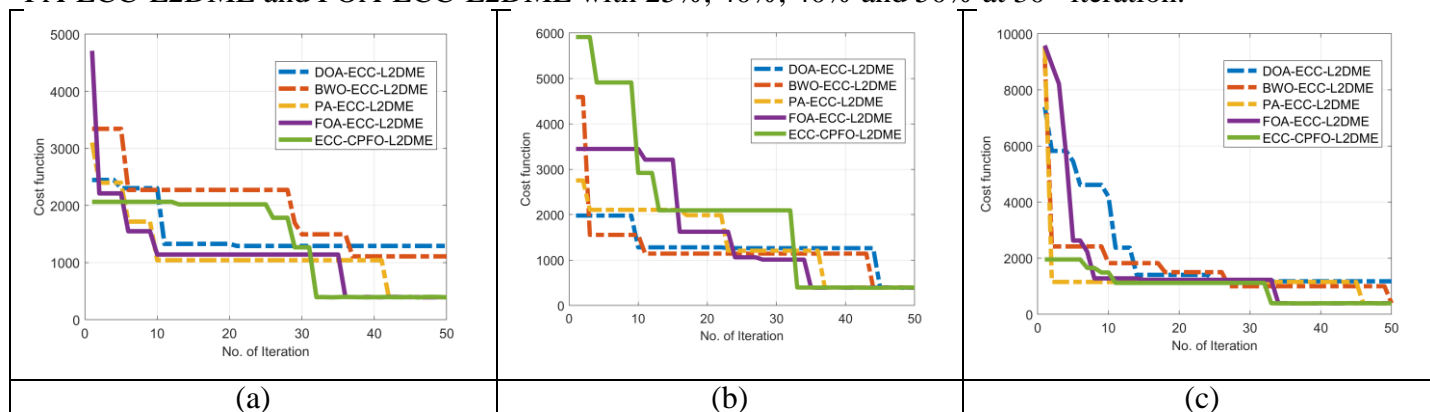

Fig. 7. Convergence examination of ECC-CPFO-L2DME-based security scheme with various algorithms (a) Natural image, (b) Satellite image and (c) Medical Image

7805

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

3.1.8 Chosen Plain Text Attack (CPA) analysis

Fig. 8. depicts the CPA analysis of the proposed ECC-CPFO-L2DME-based security scheme .
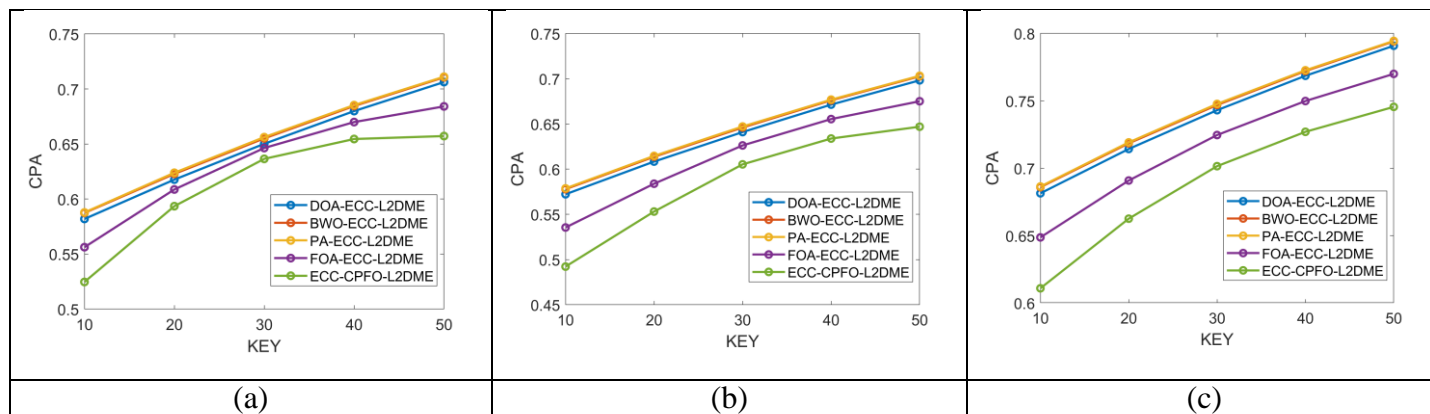

(a)   (b)   (c)

Fig. 8. CPA examination of ECC-CPFO-L2DME-based security scheme with other existing optimization algorithms (a) Natural image, (b) Satellite image and (c) Medical Image

The key values are considered in x-coordinate to get the proper encryption. The CPA value of the suggested ECC-CPFO-L2DME-based security scheme is less than the DOA-ECC-L2DME, BWO-ECC-L2DME, PAECC-L2DME and FOA-ECC-L2DME with 3.22%, 3.06%, 4.8% and 1.62% at 30th key coordinate.

3.1.9 Known Plain Text Attack (KPA) analysis

The KPA analysis of the proposed ECC-CPFO-L2DME-based security scheme is given in Fig. 9.
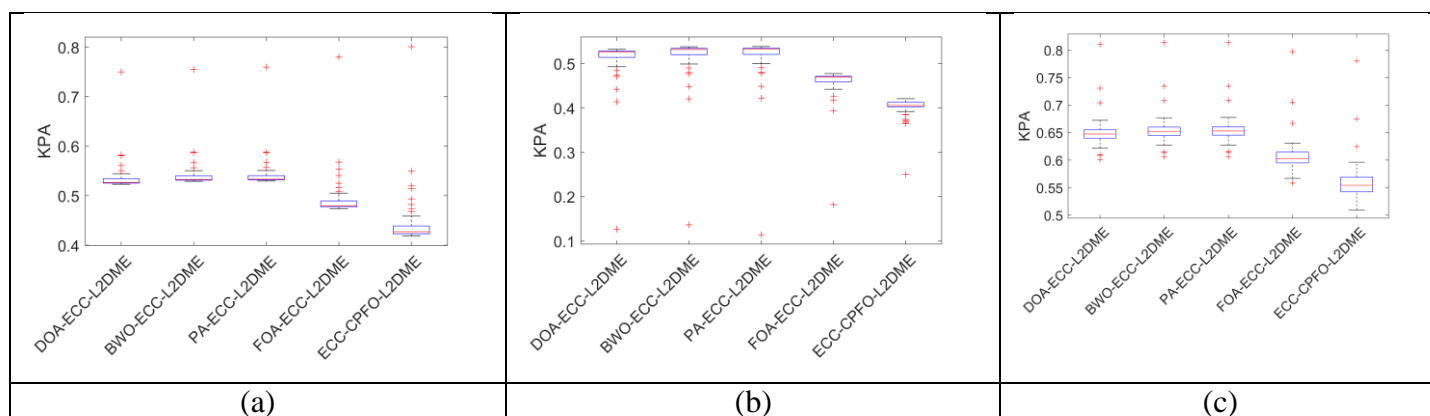

(a)   (b)   (c)

Fig 9. KPA examination of enhanced security scheme with with other existing optimization algorithms (a) Natural image, (b) Satellite image and (c) Medical Image

The comparison result shows that the KPA value of the suggested ECC-CPFO-L2DME-based security scheme is less than that of the DOA-ECC-L2DME, BWO-ECC-L2DME, PA-ECC-L2DME and FOA-ECC-L2DME with 23%, 26.19% , 26% and 7.14% .

7806

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

3.1.10 Key sensitivity examination

The following Fig. 10. shows the key sensitivity examination of the proposed ECC-CPFO-L2DME-based security scheme.
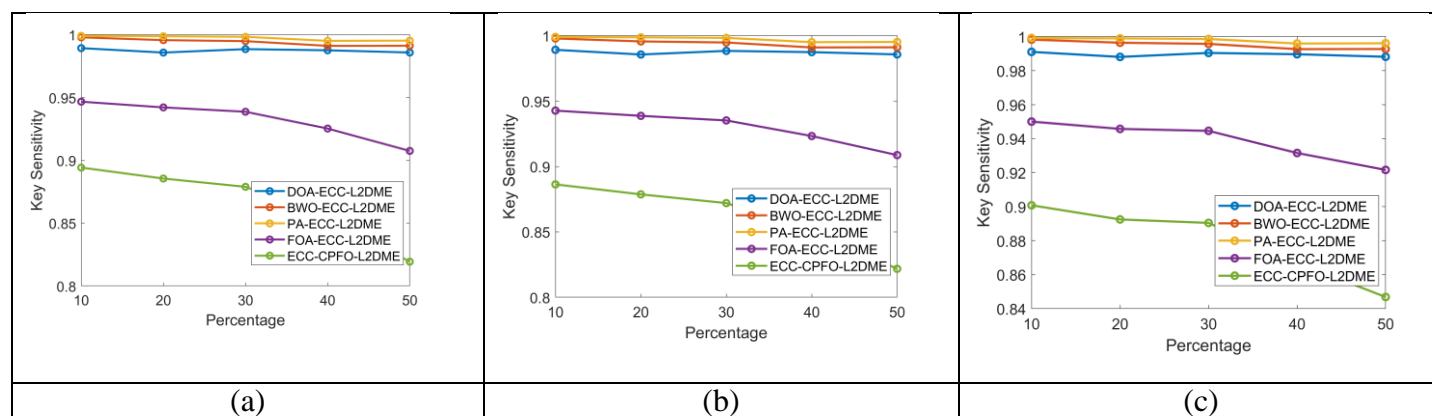

Fig. 10. Key Sensitivity examination of enhanced security scheme with various algorithms
(a) Natural image (b) Satellite image (c) Medical Image

The comparison result shows that the key sensitivity value of the suggested ECC-CPFO-L2DME-based security scheme is less than the DOA-ECC-L2DME, BWO-ECC-L2DME, PA-ECC-L2DME and FOA-ECC-L2DME with 12.64%, 13.79%, 14.9% and 8.04% at the 30th percentage of the key randomness.

4. Conclusions

Our proposed Elliptic Curve Cryptography and Logistic 2Dimensional Map Encryption with Combined Pathfinder and Falcon Optimization (ECC-CPFO-L2DME)-based security scheme is implemented to provide high security to the OSNs. The image encryption is done using proposed (ECC-L2DME) scheme. The images for encryption are gathered from online open source; then shuffling of rows and columns is performed on each image which is represented by a matrix of rows and columns of pixels. Elliptic Curve Cryptography (ECC) is used to encrypt every shuffled image, where a key is generated along with the encrypted image. This key is optimized with the help of Combined Pathfinder and Falcon Optimization (CPFO) algorithm. Then every encrypted image along with optimal key is given as input to the logistic 2Dimensional map encryption. The encrypted image from the L2DME process is then decrypted in the reverse order and thus the original image is obtained.

The comparison of the proposed ECC-CPFO-L2DME-based security scheme with other existing optimization algorithms on natural images are done. The results show that the MSE value of proposed Combined Pathfinder and Falcon Optimization + ECC-L2DME-based security scheme(5.39) is less than that of the Dingo Optimization(9.18), Black Widow Optimization(7.89), PathFinder Optimization (8.33) and Falcon Optimization (6.28). The NPCR value of the proposed Combined Pathfinder and Falcon Optimization + ECC-L2DME-based security scheme(93.95) is greater than that of the Dingo Optimization(92.25), Black Widow Optimization(93.07), PathFinder Optimization (92.48) and Falcon Optimization (93.93). The PSNR value of proposed Combined Pathfinder and Falcon Optimization + ECC-L2DME-based security scheme(3.92) is greater than that of the Dingo Optimization(3.62), Black Widow Optimization(3.84), PathFinder Optimization (3.13) and Falcon Optimization (3.52). The UACI value of proposed Combined

7807

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

Pathfinder and Falcon Optimization + ECC-L2DME-based security scheme(32.99) is greater than that of the Dingo Optimization(31.15), Black Widow Optimization(31.53), PathFinder Optimization (30.93) and Falcon Optimization (29.47).

Comparing the proposed ECC-CPFO-L2DME-based security scheme with other existing optimization algorithms on natural images, the results show that the total processing time(36.84 ms) is less than that of the Dingo Optimization(66.27 ms), Black Widow Optimization(54.13 ms), PathFinder Optimization (66.86 ms) and Falcon Optimization (76.03 ms) and the memory size (404.02 KB) of our Combined Pathfinder and Falcon Optimization ECC-L2DME-based security scheme is less than that of the Dingo Optimization(790.3 KB), Black Widow Optimization(782.07 KB), PathFinder Optimization (561 KB) and Falcon Optimization (763.04 KB).

KPA analysis, CPA analysis, key sensitivity and convergence examination are also performed and results are found to be better than the other existing optimization algorithms.

Hence it is concluded that the ECC-CPFO-L2DME-based image encryption system is more secure in open social networks(OSNs) and reduces the processing time as well as memory size than the other existing optimization algorithms. The future scope of this study may be extended to audio and video encryptions.

Acknowledgements

5. References

[1] Durga Nadarajan and T. Pramananda Perumal. Elliptic Curve Cryptography Encryption Framework for Ensuring Security in Open Social Networks. Scandinavian Journal of Information Systems. 2023;35;606–615.

[2] Anusuya Devi V, Kalaivani V. Enhanced BB84 quantum cryptography protocol for secure communication in wireless body sensor networks for medical applications. Personal and Ubiquitous Computing. 2021;27:875-885. Available from: https://doi.org/10.1007/s00779-021-01546-z

[3] Mohamed Elhoseny, K. Shankar, S. K. Lakshmanaprabu, AndinoMaseleno and N. Arunkumar. Hybrid optimization with cryptography encryption for medical image security in Internet of Things. Neural Computing and Applications.2020;32:10979–10993. Available from: https://doi.org/10.1007/s00521-018-3801-x

[4] Byoung S. Ham. Unconditionally secured classical cryptography using quantum superposition and unitary transformation. Scientific Reports. 2020;10:11687. Available from: https://doi.org/10.1038/s41598-020-68038-7

[5] Siqi Lu, Jianhua Zheng, Zhenfu Cao, Yongjuan Wang and ChunxiangGu. A survey on cryptographic techniques for protecting big data security: present and forthcoming. Science China Information Sciences. 2022;65:201301. Available from: https://doi.org/10.1007/s11432-021-3393-x

[6] Sourabh Chandra, Bidisha Mandalb, Sk. Safikul Alam and Siddhartha Bhattacharyya. Content-based double encryption algorithm using symmetric key cryptography. Procedia Computer Science. 2015;57:1228–1234. Available from: https://doi.org/10.1016/j.procs.2015.07.420

[7] S. Kavitha , P. J. A. Alphonse and Y. Venkataramana Reddy. An Improved Authentication and Security on Efficient Generalized Group Key Agreement Using Hyper Elliptic Curve Based Public Key Cryptography for IoT Health Care System. Journal of Medical Systems. 2019;43:260. Available from: https://doi.org/10.1007/s10916-019-1378-2

Logistic 2D Map based Elliptic Curve Cryptography Encryption Scheme with Key optimization using Pathfinder and Falcon Algorithms for Providing Enhanced Security in Open Social Networks

Section A-Research paper
ISSN 2063-5346

[8]   Hadeal Abdulaziz Al Hamid, Sk Md Mizanur Rahman, M. Shamim Hossain, Ahmad Almogren and Atif Alamri. A Security Model for Preserving the Privacy of Medical Big Data in a Healthcare Cloud Using a Fog Computing Facility With Pairing-Based Cryptography. IEEE Access. 2017;5:22313-22328. Available from: https://doi.org/10.1109/ACCESS.2017.2757844

[9]   Imran Memon, Ibrar Hussain, Rizwan Akhtar and Gencai Chen. Enhanced Privacy and Authentication: An Efficient and Secure Anonymous Communication for Location Based Service Using Asymmetric Cryptography Scheme. Wireless Personal Communication. 2015;84:1487–1508. Available from: https://doi.org/10.1007/s11277-015-2699-1

[10] A. Mullai and K. Mani. Enhancing the security in RSA and elliptic curve cryptography based on addition chain using simplified Swarm Optimization and Particle Swarm Optimization for mobile devices. International Journal of Information Technology. 2020; Available from: https://doi.org/10.1007/s41870-019-00413-8

[11] Xingyuan Wang and Yuxin Chen. A New Chaotic Image Encryption Algorithm Based on L‑ Shaped Method of Dynamic Block. Sensing and Imaging. 2021;22:31. Available from: https://doi.org/10.1007/s11220-021-00357-z

[12] C.K. Huang, C.W. Liao, S.L. Hsu and Y.C. Jeng. Implementation of gray image encryption with pixel shuffling and gray-level encryption by the single chaotic system. Telecommunication System. 2013;52:563–571. Available from: https://doi.org/10.1007/s11235-011-9461-0

[13] Saleh Ibrahim, Hesham Alhumyani, Mehedi Masud, Sultan S. Alshamrani, Omar Cheikhrouhou, Ghulam Muhammad, M. Shamim Hossain and Alaa M. Abbas. Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps.   IEEE Access. 2020;8:160433-160449. Available from: https://doi.org/10.1109/ACCESS.2020.3020746

[14] Weihai Li, Yupeng Yan and Nenghai Yu. Breaking Row-Column Shuffle Based Image Cipher. Conference: Proceedings of the 20th ACM international conference on Multimedia. 2012; 1097-1100. Available from https://doi.org/10.1145/2393347.2396392

[15] Omar Rafik Merad Boudia, Sidi Mohammed Senouci, and Mohammed Feham. Elliptic Curve Based Secure Multidimensional Aggregation for Smart Grid Communications. IEEE Sensors Journal. 2017;17(23):7750-7757. Available from: http://doi.org/ https://doi.org/10.1109/JSEN.2017.2720458

[16] Yue Wu, Gelan Yang Huixia Jin and Joseph P. Noonan. Image encryption using the two-dimensional logistic chaotic map. Journal of Electronic Imaging. 2012;21(1):013014. Available from https://doi.org/10.1117/1.JEI.21.1.013014

[17] Hamza Yapici and Nurettin Cetinkaya. A new meta-heuristic optimizer: Pathfinder algorithm. Applied Soft Computing.2019;78:545-568. Available from: https://doi.org/10.1016/j.asoc.2019.03.012

[18] Emerson Hochsteiner de Vasconcelos Segundo, Viviana Cocco Mariani and Leandro dos Santos Coelho. Design of heat exchangers using Falcon Optimization Algorithm. Applied Thermal Engineering. 2019;156:119-144. Available from: https://doi.org/10.1016/j.applthermaleng.2019.04.038

[19] Juan H. Almazán-Covarrubias, Hernan Peraza-Vazquez, Adrian F. Peña-Delgado and Pedro Martin García-Vite. An Improved Dingo Optimization Algorithm Applied to SHE-PWM Modulation Strategy. Applied Science.2022; 12(3):992. Available from: https://doi.org/10.3390/app12030992

[20] Vahideh Hayyolalam and Ali Asghar Pourhaji Kazem. Black Widow Optimization Algorithm: A novel meta-heuristic approach for solving engineering optimization problems. Engineering Applications of Artificial Intelligence. 2020;87:103249. Available from: https://doi.org/10.1016/j.engappai.2019.103249

7809

Eur. Chem. Bull. 2023,12(issue 8), 7782-7809