International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

A HYBRID OF CHAOTIC MAPS WITH LYREBIRD OPTIMIZATION ALGORITHM FOR ENHANCING THE IMAGE ENCRYPTION MODEL

[1]Gagandeep Kaur, [2]Neha Chaudhary, [3]Gulbir Singh, [4]Anamika Goel, [5]Amita Asthana

[1]Department of Computer Science Engineering, CTIEMT (Ct Group of Institutions), Shahpur, Jalandhar, Punjab. gagandeep.2091@ctgroup.in

[2]Department of Robotics and AI (CSE), Manav Rachna University, Faridabad, India. nehachaudhary@mru.edu, ORCID ID: 0000-0002-0160-4127

[3]Department of Computer Science and Engineering, Graphic Era Hill University, Haldwani Campus, Nainital, Uttarakhand, India. gulbir.rkgit@gmail.com, ORCID ID: 0000-0002-3113-2474

[4]Department of CSE AIML, ABES Engineering College GHAZIABAD, UP, India. anamika.goel@abes.ac.in, ORCID ID: 0000-0002-0904-7310

[5]Department of Electronics and Communication Engineering, Ajay Kumar Garg Engineering College, Ghaziabad, India, researches555@gmail.com, ORCID ID:0000-0001-6433-1077

Abstract

The main purpose of the proposed image encryption (IE) method is to enhance various security characteristics to protect sensitive images on the internet. In the literature, chaotic maps are preferred for image encryption because of their high randomness and sensitivity to initial parameter values. Therefore, metaheuristic algorithms have been utilized to fine-tune the parameters. In this research, we have employed the metaheuristic Lyrebird optimization (LO) algorithm to fine-tune the chaotic map parameters. The LO algorithm is chosen over other algorithms due to its better exploration and exploitation rate to search for the best solution. The LO algorithm searches for the best parameter value based on the objective function. This research involves the formulation of a multi-objective function that incorporates numerous security parameters, namely, entropy and correlation coefficient (CC), to improve the security attributes of the IE model. The proposed IE model has two steps. In the first step, a random key is generated to transform the pixels of the secret image, whereas in the second step, the image pixels are shuffled based on the shuffling index values to reduce the correlation among the neighboring pixels. In both steps, we have used the chaotic logistic map. The proposed IE is evaluated against statistical and differential attacks on the standard dataset by considering the various images and their different resolutions. The uniform distribution of the histogram of the encrypted images is validated using the chi-square test. Besides that, entropy analysis shows that the average entropy value is 7.9973, 7.9993, and 7.9998 for 256x256, 512x512, and 1024x1024 image resolutions. The average CC and SSIM are near zero value. The average

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

NPCR value (>0.9969) is near the 1 value. Finally, the comparative analysis based on entropy, CC, and NPCR parameters shows that the proposed IE model outperforms the existing models.

KEYWORDS Chaotic Map, Differential Attacks, Image Encryption, Statistical Attacks, Metaheuristic Algorithms, Multi-Objective, Security Analysis.

1. INTRODUCTION

In the present era, secret data in the form of images are communicated in a number of applications such as social media, military, and healthcare [1]. Therefore, a security layer needs to be added to the images in order to secure them on the internet to prevent them from various attacks, namely, statistical and differential attacks [2]. In the literature, encryption is the safest security layer added to the multimedia data. The encryption method scrambles the secret data using a random key and generates a noisy encrypted image in the output [3]. Further, we found that the image has different characteristics over the text data, such as a large number of pixels and high correlation between them. Therefore, traditional encryption methods prone to statistical and differential attacks [4]. Moreover, the encryption and decryption processes of these methods are time-consuming [4]. Thus, in the literature, chaotic maps, DNA, and ECC are the most popular algorithms for encrypting the secret images [5].

In this research, we have explored the chaotic map encryption algorithms over other algorithms due to their providing randomness, non-linearity, and being very sensitive to the input parameter values [6]. Further, its performance is enhanced using the metaheuristic algorithms by finding the best parameter values [7]. These algorithms come under the optimisation category, which finds the optimal solution by exploring the solution space of the given problem [8]. In the metaheuristic algorithm, objective function plays an important role because based on it the metaheuristic algorithm is minimize/maximize the optimal solution [8].

In the previous studies, JAYA [12], Osprey Optimization [13], whale optimization [14], grasshopper optimization [15], PSO [16, 18], and coronavirus optimization [17] algorithms are successfully deployed for the image encryption method. The algorithms used in the previous studies suffer from local optima and have low exploration and exploitation capabilities, which hinder their ability to determine the optimal solution. Furthermore, they have used the single objective functions in their work, such as entropy, correlation coefficient, and SSIM. These gaps are considered in this research to select the recent metaheuristic algorithm, which provides a global solution and quickly searches for the optimal solution due to a better exploration and exploitation rate. Additionally, we have substituted a single-objective function with a multi-objective function, thereby enhancing the encryption method's multiple security characteristics.

The main contribution of this research is summarized as follows.

1. In this paper, we have presented an image encryption model by hybridizing the chaotic map and metaheuristic algorithm in order to enhance the security of the encryption method. The benefit of the chaotic map in the proposed model is that it generates a random key and optimal shuffling index in order to encrypt the image.

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

2. We have designed a multi-objective function using entropy and correlation coefficient in the metaheuristic algorithm that enhances the multiple security parameters of the image encryption model.

3. The proposed method withstands the statistical and differential attacks and performs superior to the previous recent approaches.

The remaining paper has five sections. Section 2 shows the related work is done in the IE models. The methodology is defined in Section 3. Section 4 illustrates the proposed IE model based on chaotic map and metaheuristic LO algorithm. Section 5 shows the results and discussion. Finally, the conclusion is drawn in Section 6.

2. RELATED WORK

This section examines the chaotic map-based image encryption models that the literature has proposed because it gains popularity in the encryption models due to non-linear chaotic properties such as unpredictability/non-periodicity and sensitive to initial conditions [9]. Further, in this field, metaheuristic algorithms are gained popularity to fine-tune the encryption models by determining the best parameter values of the chaotic map [10].

Sameh et al. [11], proposed an IE model by considering the several metaheuristic algorithms and shuffling the secret image using the chaotic maps. Next, Kumar et al. [12], presented an IE model by generating a random key using the 3-D chaotic logistic map and fine-tuning of parameters of it using the JAYA algorithm. In their work, they have taken a single objective function for key generation based on entropy. Further, they have shuffled the secret image based on their row and column index value. Next, Kaur et al. [13], designed an objective function by considering the entropy and structure similarity index measure (SSIM). After that, 3-D chaotic logistic map is fined tuned using the osprey optimization (OO) algorithm. Further, they have shuffled the secret image in the horizontally and vertical direction based on their index values. In [14], authors, generates the random key using the hash function and fine-tune the chaotic map using the whale optimization (WO) by considering the entropy as the objective function. Khalaf et al. [15], used the correlation coefficient (CC) as the objective function to fine-tune the chaotic logistic map using the grasshopper optimization (GO). Ahmad et al. [16] presented an encryption model that took into account the PSO and chaotic logistic map algorithm. They determined the optimal parameter value by considering the fitness function based on the correlation coefficient. Alsahafi et al. [17] considered entropy and NPCR parameters to design a multi-objective function for random key generation by utilizing the binary coronavirus optimization algorithm. Finaly, Ferdush et al. [18], used two metaheuristic algorithm, namely, GA and PSO for data encryption purposes.

We know from the studies above that many authors are looking at various metaheuristic algorithms (such as JAYA, OO, WO, and GO) to fine-tune the chaotic map's parameters for creating random keys based on objective functions (such as entropy, NPCR, SSIM, and CC). Further, shuffle the image based on the image index value or randomly generate the shuffling index value based on the chaotic map. However, none of the authors contributed to generating

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

the optimal shuffle index value, at which there is a minimum correlation between the neighbouring pixels. Therefore, a multi-objective function is created in this study by looking at the entropy and correlation coefficient functions. This function encrypts the data using the best random key and shuffles the image using the best shuffling index that is created. The best random key and shuffling index are made by using the metaheuristic LO algorithm to fine-tune the chaotic logistic map. The LO algorithm is inspired by the natural behaviour of lyrebirds. This bird, when faced with danger, then performs two operations, either running away or hiding somewhere. These operations were studied by Dehghani et al. [19], and they proposed an optimisation algorithm. Further, they have tested the LO algorithm on the number of problems and found that the LO algorithm outperforms the existing metaheuristic algorithms.

3. METHODOLOGY

In this section, we have explained the database and algorithms utilized for designing the image encryption method.

3.1 Database: In the previous studies, standard USC SIPI Image database images are mostly utilized by various authors to validate the encryption methods [9-17]. Therefore, we have chosen this database to validate the performance of the proposed IE method. This database contains images in grayscale and color format. Furthermore, images are available in various volumes and standard resolutions such as $256 \times 256, 512 \times 512, and\ 1024 \times 1024$. The format of the image is *.tiff* [23]. In this work, grayscale images were considered, and the resolution of the images was 256×256, $512 \times 512, and\ 1024 \times 1024$.

3.2 Chaotic Logistic Map

In the proposed IE model, CLM is utilized for random key and shuffling index generation purposes. It is determined using Eq. (1).

$$x_{n+1} = \mu x_n(1 - x_n) \tag{1}$$

In Eq. (1), $x_{n,}x_{n+1}$ denotes the present and next stage of the chaotic map and its value varies in between $[0 - 1]$. On the other hand, μ denotes the bifurcation function and its value varies in between $[1 - 4]$. In the practical cases of encryption, its value varies in between $[3.57 - 3.99]$. In the proposed IE model, we have found the best parameter values of the chaotic map using the metaheuristic LO algorithm.

3.3 Metaheuristic LO Algorithm

The metaheuristic LO algorithm was proposed by Dehgani et al. [19] by analysing their behavioural characteristics. This bird, when feeling danger, then it performs two operations, either escape or hiding in their surrounding environment. The authors defined the exploration phase of this algorithm based on escaping strategy and the exploitation phase based on their hiding strategy. This algorithm has better exploration and exploitation phases over the existing metaheuristic algorithm. Therefore, it was chosen for inclusion in the proposed IE model. The metaheuristic LO algorithm has similar steps to other metaheuristic algorithms, like the

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

initialisation of the parameter, generation of random population, evaluation based on the objective function, and finding the best solution. After that, the exploration and exploitation phase are executed in order to search the solution space and compare it to the best solution and update it if required. This process is executed for a fixed number of iterations, and the best solution is determined.

4. PROPOSED IMAGE ENCRYPTION MODEL

To secure the secret images while they are being shared on the internet, this section lays out the proposed IE model for image encryption. The key novelty of the proposed IE method is that it uses the metaheuristic LO algorithm to fine-tune the parameters of the chaotic map, generating a random key and shuffling index while considering multiple security parameters. The flowchart of the proposed IE model is shown in Figure 1, and its working is given below.

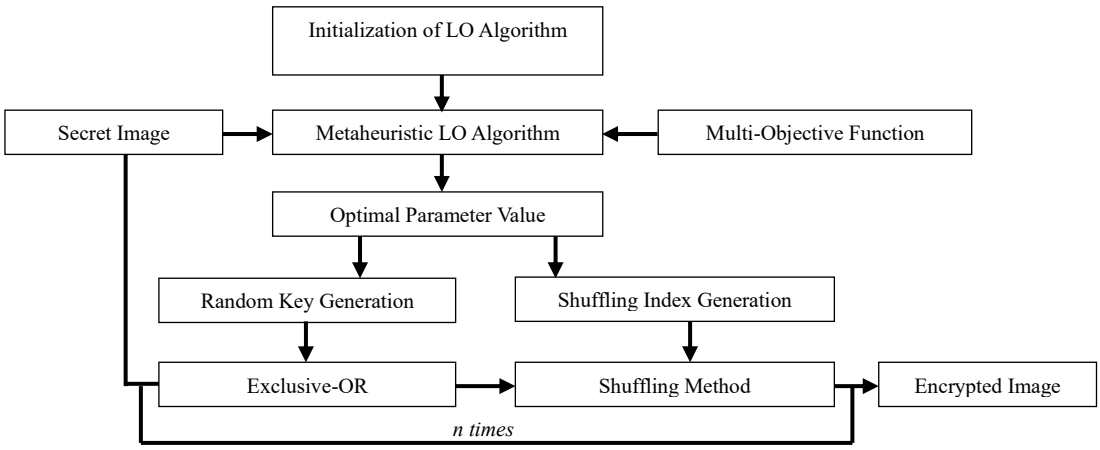


Figure 1 Flowchart of the Proposed IE Model

Initially, the secret image is read and given to the metaheuristic LO algorithm. After that, parameters of the LO algorithm are initialized according to the CLM algorithm along with the objective function. In this research, we have designed an objective function using two security parameters, namely, entropy and CC. The entropy parameter was chosen to evaluate the histogram distribution of the encryption image, whereas the correlation coefficient parameter was chosen to measure the correlation between the original and encrypted images. In a grayscale image, the entropy value varies from 0 to 8, whereas the correlation coefficient value varies between -1 and 1. In image encryption, a high value of entropy and a low value of the correlation coefficient are required (the ideal value of entropy is 8 and the correlation coefficient is 0). But when combining these parameters, one must be high and the other low. Therefore, these parameters are combined using Eq. (2) in the proposed method, and the objective function value is maximized while searching for the best parameters.

$$OF = \frac{(1-abs(CC))+\left(\frac{E}{8}\right)}{2} \quad (2)$$

In the above Eq. (2), CC, E denotes the correlation coefficient among the secret and encrypted image, whereas E denotes the entropy of the encrypted.

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

After determining the best parameter values of the chaotic map, the optimal random key and shuffling index are generated. The next step is to combine the secret image with the random key using an exclusive-OR operation. Consequently, the shuffling method receives the image and shuffles it according to the shuffling index. The exclusive-OR operation and shuffling method are performed *n* times until the desired objective function is not met. The value of *n* is also determined using the metaheuristic LO algorithm. After that operation, an encrypted image gets in the output. On the receiver side, in order to decrypt the encrypted image, the optimal parameter values of the chaotic map and parameter *n* are needed to communicate.

Next, in this section, we have explained the steps of the metaheuristic LO algorithm to find the best parameter values of chaotic map for random key and shuffling index generation.

1. In the first step, the original image was given, and LO parameters were initialized, such as population size and its dimension, total iteration, and the lower and upper bounds of the parameter.

2. In the second step, the population was generated for the chaotic map.

3. In the third step, the original image along with generated populations was given to the chaotic map to generate a random key and shuffling index. Based on the generation, the encryption was performed, and an evaluation of the encrypted image with respect to the original image was done using Eq. (2), and it was determined which population gave the best solution over others.

4. In the fourth step, new populations were generated by considering the initial populations and evaluated based on the objective function and compared with the best solution. If the new population gave a superior solution over the best solution, then the best solution was updated.

5. The previous step was iterated for a fixed number of iterations according to the total number of iterations.

6. In the sixth step, the optimal parameters were determined for generating the random key and shuffling index.

5. RESULTS AND DISCUSSION

This section presents the simulation results of the proposed IE model using the various parameters to validate its performance. In the simulation, USC SIPI image database images are considered [23]. The proposed IE model is simulated in MATLAB 2018a software in a Windows 10 environment. Further, the system is equipped with an i7 processor at 2.70 GHz and 8 GB of RAM.

5.1 Evaluation Criteria and Performance Evaluation Parameters

Table 1 displays the parameter values configured for the simulation purposes. In the proposed IE model, the metaheuristic algorithm is initialised according to these values to search for the best parameter for the chaotic logistic map algorithm.

Table 1: Simulation Setup Configuration of the Proposed IE Model

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Parameter	**Value**
Total Images	6
Image Resolution	$[256 \times 256],\ 512 \times 512, and\ 1024 \times 1024$
Image Type	.tiff
Total Population	10
Total Iteration	100
Objective Function	[E, CC]
Logistic Map Parameter r	$[3.57 - 3.99]$
Logistic Parameter x	$[0 - 1]$

Next, a detailed description of the parameters is given below that is considered to validate the performance of the proposed method.

- **Chi-Square Test:** An image's histogram shows how the values of its pixels are distributed. Histogram analysis is used in image encryption to verify that the cipher images' histograms are uniform. A cipher image is more vulnerable to statistical attacks if its histogram is consistent. To analyze the histogram, we can utilize the chi-square (χ^2) test, which is shown mathematically as [20]:

$$\chi^2 = \sum_{i=1}^{255} \frac{(f_i - \varepsilon)^2}{\varepsilon} \tag{3}$$

$$\varepsilon = \frac{H \times W}{256} \tag{4}$$

In above case, f denotes the frequency of the histogram and ε is the predicted value is determined using Eq. (3). Further, HW denotes the resolution of the image. When a ciphertext image's χ^2 score is not above 293.2478, it could qualify for the chi-square evaluation [21].

- **Entropy:** Claude Shannon developed the statistical test known as entropy in 1948 for measuring randomness and unpredictability. Communication systems' uncertainty is measured using entropy. In image encryption, a cipher image with a high entropy number masks the original image better than those with low entropy. The mathematical representation of entropy is [19,25]:

$$H(m) = -\sum_{i=1}^{2^n - 1} p(m_i) \log_2[p(m_i)] \tag{5}$$

where p(mi) indicates the probability of symbol m_i, or the likelihood that intensity i will occur for a pixel in the image, and n is the number of bits utilized to represent the symbol. In the IE

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

model, ideal value of entropy near to 8 required. Brute force attacks are less effective against cipher images with low levels of entropy.

- **CC:** Neighboring pixels in images often have a strong correlation. The goal of image encryption techniques is to reduce this correlation to better hide the image [19]. In the range [1, −1], the correlation values are as follows: 0 indicates that there is no connection between the two pixels, while 1 and −1 indicate the highest positive and negative correlations, respectively. The correlation values of an image encryption technique must be as near to 0 as feasible to be regarded secure. It is determined using Eq. (6).

$$CC = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W}(P_{ij}-\bar{P})(C_{ij}-\bar{C})}{\sqrt{\sum_{i=1}^{H}\sum_{j=1}^{W}(P_{ij}-\bar{P})^2 \sum_{i=1}^{H}\sum_{j=1}^{W}(C_{ij}-\bar{C})^2}}$$

(6)

In above Eq. (6), $PC, \bar{P}\bar{C}$ denotes the secret and encrypted image and their mean value.

- **SSIM:** The level of similarity between two images is measured by the SSIM index, which has a value between 0 and 1 [22]. Human subjectivity is quite consistent with SSIM. The whole spatial region is divided into blocks using the SSIM method. A block's quality is represented by one SSIM value, and the image's overall quality is represented by an SSIM map made up of all SSIM values. A high SSIM number means there are more white pixels in the SSIM map, showing that the source and compressed images are very close. SSIM is defined as:

$$SSIM(x,y) = \frac{(2\mu_x\mu_y+c_1)(2\sigma_{xy}+c_2)}{(\mu_x^2+\mu_y^2+c_1)+(\sigma_x^2+\sigma_y^2+c_2)}$$

(7)

$$c_1 = (K_1L)^2, c_2 = (K_2L)^2$$

(8)

The mean of x and y is represented by μ_x and μ_y, the variance of x and y is shown by σ_x and σ_y, the covariance is σ_{xy}, the dynamic range of the images is L, which defaults to 255, and two constants, K_1 and K_2. K_1 has a default value of 0.01 and K_2's default value is 0.03.

- **PSNR:** This metric calculates how much noise there is in the plain and encrypted images. The following is the mathematical representation of PSNR between the cipher image and the plaintext image [19]:

$$PSNR = 10\log_{10}\frac{I_{Max}^2}{MSE}$$

(9)

MSE stands for mean squared error, while Imax is the highest value a pixel may have (255 in 8-bit pixels). MSE measures how much the pixel values of two images vary on average by calculating the square of the differences. The MSE between an image in plaintext and an image in cipher is expressed mathematically as follows:

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

$$MSE = \frac{\sum_{i=1}^{H}\sum_{j=1}^{W}[P_{ij}-C_{ij}]^2}{HW}$$

(10)

- **Maximum Deviation (MD):** The difference between the plaintext and encrypted picture histograms is measured using this metric. A significant degree of variance between the cipher envision and the plaintext image is indicative of good encryption quality in the method [19]. The following formula may be used to determine the strongest deviation:

$$d = histogram(|P - C|)$$

(11)

$$D_{max} = \frac{d_0+d_{255}}{2} + \sum_{i=1}^{254} d_i$$

(12)

Dmax is the highest measure of difference. The histogram, represented by "d," shows the absolute differences between the original (plaintext) and encrypted (cipher) images. "di" refers to the value in the histogram at index “i,” while “d0” and “d255” are the histogram values at the very beginning (index 0) and the very end (index 255).

- **NPCR:** This measure adds up the variations between two encrypted cipher images from the identical plaintext image but with one bit changed in the plaintext [19]. This measure helps evaluate how resistant an encryption method is against differential attacks. NPCR can be computed as follows:

$$NPCR = \sum_{i-1}^{H}\sum_{j=1}^{W} D(i,j)$$

(13)

$$D(i,j) = \begin{cases} 0\ if C_1(i,j) = C_2(i,j) \\ 1\ if\ C_1(i,j) \neq C_2(i,j) \end{cases}$$

(14)

Whereas, C1 and C2 represent two cipher images that were encrypted from the identical plaintext image with a one-bit modification.

5.2 Robustness against Statistical Attack

In this section, to show the robustness of the proposed method against the statistical attack, we have measured various parameters. For example, the chi-square test is performed to evaluate the encrypted histogram distribution. Similarly, we have measured the other parameters (entropy, CC, SSIM, PSNR, and MD), which are employed to show the robustness of the proposed IE method over statistical attacks.

Table 2 (a-b) shows the visual quality of the encrypted image and its histogram. The result indicates that the encrypted image is noisy, and the proposed IE model considers different images with equally distributed histograms. Further, validation of the equally distributed histogram is done by evaluating the chi-square test.

Table 2(a): Visual Quality of the Encrypted Image and Their Histograms

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

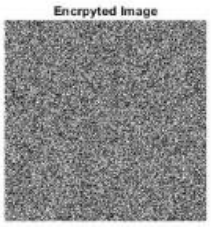
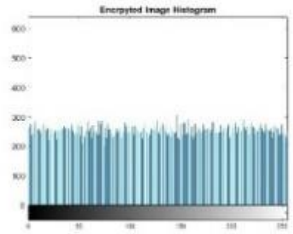
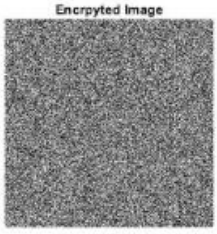
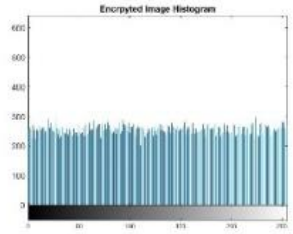
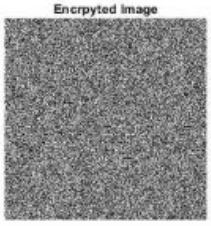
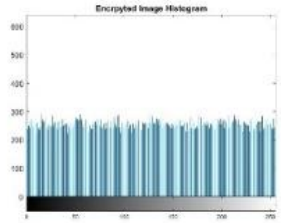
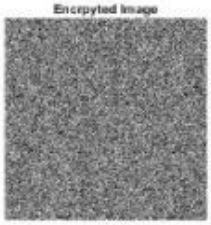
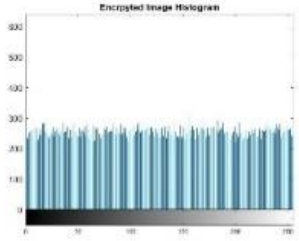
Images	Encrypted Image	Histogram
Lena		
Barbara		
Baboon		

Table 2(b): Visual Quality of the Encrypted Image and Their Histograms

Images	Encrypted Image	Histogram
Pepper		

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

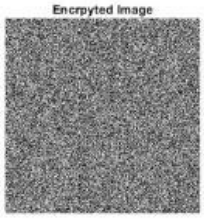
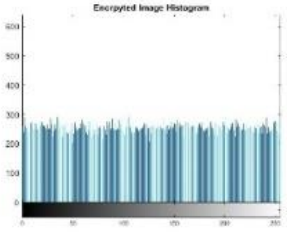
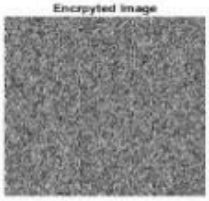
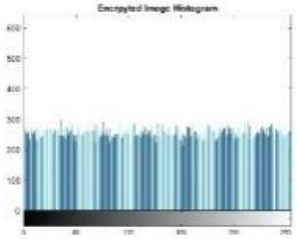
Cameraman		
Elaine		

Table 3 further evaluates the histogram distribution for the encrypted image using the chi-square test. The result shows that the proposed IE model passes the chi-square test and achieves a value less than 293.2478, which is required in the image encryption model. Table 4 shows that the proposed IE model achieves the high entropy near the ideal value of 8 for different images and their resolutions. The result indicates that the proposed method achieves the highest entropy for higher resolution images over smaller ones.

Table 3: Chi-Square Analysis for the Proposed IE Model

Images	**Chi-Square test**		
Resolution	256×256	512×512	1024×1024
Lena	240.7	237	216
Barbara	239.0	224	236
Baboon	247.7	249	224
Pepper	237.7	261	243
Cameraman	218.3	268	260
Elaine	223.3	232	290

Table 4: Entropy Analysis for the Proposed IE Model

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Images	**Entropy**		
Resolution	256×256	512×512	1024×1024
Lena	7.9972	7.9993	7.9998
Barbara	7.9972	7.9994	7.9998
Baboon	7.9972	7.9993	7.9998
Pepper	7.9973	7.9993	7.9998
Cameraman	7.9975	7.9992	7.9998
Elaine	7.9974	7.9993	7.9998

Table 5-6 presents the correlation coefficient and SSIM analysis for different images considered in the proposed IE model. The result shows that the proposed IE model achieves the CC and SSIM near to the ideal value, which is required in the image encryption model. This reflects that the proposed IE model is efficiently encrypting the secret images.

Table 5: CC Analysis for the Proposed IE Model

Images	**CC**		
Resolution	256×256	512×512	1024×1024
Lena	0.00097	0.0023	0.0001
Barbara	0.00021	0.0041	0.0002
Baboon	-0.00292	0.0029	0.0020
Pepper	-0.00023	-0.0019	0.0006
Cameraman	0.00102	0.0025	-0.0012
Elaine	-0.00107	0.0004	0.00005

Table 6: SSIM Analysis for the Proposed IE Model

Images	**SSIM**		
Resolution	256×256	512×512	1024×1024
Lena	0.0090	0.0103	0.0102

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Barbara	0.0110	0.0109	0.0099
Baboon	0.0100	0.0108	0.0105
Pepper	0.0096	0.0095	0.0099
Cameraman	0.0092	0.0094	0.0093
Elaine	0.0105	0.0106	0.0108

Table 7 presents an analysis of the PSNR parameter between the secret and encrypted images. In the encryption model, high noise in the encrypted image is required, which demands a low PSNR value. The result shows that the proposed IE model achieves a PSNR in the range of 11.635 dB to 13.831 dB, which is acceptable in the encryption model. Furthermore, Table 8 evaluates the average MD for various images. The result shows that the proposed IE model achieves high value.

Table 7: PSNR Analysis for the Proposed IE Model

Images	**PSNR (in dB)**		
Resolution	256×256	512×512	1024×1024
Lena	12.554	12.5526	12.5401
Barbara	13.831	13.7774	13.7730
Baboon	12.582	12.4010	12.4744
Pepper	12.884	12.8903	12.9094
Cameraman	12.377	12.3806	12.3760
Elaine	11.635	11.6166	12.0072

Table 8. MD Analysis for the Proposed IE Model

Images	**MD**		
Resolution	256×256	512×512	1024×1024
Lena	42880.33	168870	677016
Barbara	45733.67	175337	711710
Baboon	5.59E+04	202770	827295
Pepper	37134.33	147608	590350

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Cameraman	6.18E+04	249761	1000200
Elaine	4.22E+04	168680	672328

5.3 Robustness against Differential Attack

In this section, the robustness of the proposed IE method against different attacks is evaluated. In the differential attack, the attacker analyzes the pair of encrypted images by performing a slight change in the original image. In the literature, the NPCR parameter is evaluated to show the robustness of the encryption method over differential attacks. The proposed IE model evaluates the average NPCR for different images, as shown in Table 9. The result shows that the proposed method achieves NPCR value higher than 0.9959. Besides that, the NPCR value for the different images is near the ideal value. This reflects that a small change in the secret image changes the maximum pixels in the encrypted image. Thus, the proposed method is resistant to the differential attack.

Table 9: NPCR Analysis for the Proposed IE Model

Images	**NPCR**		
Resolution	256×256	512×512	1024×1024
Lena	0.9961	0.9963	0.9960
Barbara	0.9960	0.9961	0.9961
Baboon	0.9961	0.9962	0.9961
Pepper	0.9960	0.9961	0.9961
Cameraman	0.9962	0.9959	0.9960
Elaine	0.9966	0.9961	0.9960

5.4 Comparative Analysis

This section compares the entropy, NPCR, and CC parameters with the existing IE model to validate the performance of the proposed IE model. In order to accomplish this goal, the same images are considered, and recent existing IE models are chosen for comparative purposes. Table 10(a-b) shows the comparative analysis. Based on entropy and the CC parameter, Table 10 (a) compares the proposed IE model with Sameh et al. [11], which was proposed in 2023. The result shows that the proposed IE model achieves better entropy for the Cameraman, Elaine, and pepper images. Further, the correlation coefficient parameter is lower for different images when compared to the existing model.

Received: August 05, 2025

International Journal of Applied Mathematics

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

Table 10(a): Comparative Analysis based on Entropy and CC

Images	**Sameh et al. [11]**		**Proposed Model**	
	Entropy	**CC**	**Entropy**	**CC**
Cameraman	7.9956	−0.0039	7.9975	0.00102
Elaine	7.9951	−0.0010	7.9974	-0.00107
Lena	7.9978	−0.0032	7.9972	0.00097
Pepper	7.9961	−0.0022	7.9973	-0.00023

Table 10(b): Comparative Analysis based on Entropy and NPCR

Images	**Kumar et al. [12]**		**Ahmad et al. [16]**		**Proposed Model**	
	Entropy	**NPCR**	**Entropy**	**NPCR**	**Entropy**	**NPCR**
Lena	7.9973	99.05	7.9720	99.228	7.9972	99.61
Barbara	7.9961	99.23	7.9852	99.253	7.9972	99.60
Baboon	7.9971	99.51	7.9822	99.167	7.9972	99.61
Pepper	7.9968	99.24	7.9797	99.127	7.9973	99.60

Table 10(c): Comparative Analysis based on PSNR (in dB)

Images	**A. A. Abdallah and A. K. Farhan [24]**	**Proposed Method**
Lena	10.7931	12.554
Barbara	10.6135	13.831
Baboon	11.2825	12.582
Pepper	10.8563	12.884

Next, Table 10(b) shows how the proposed IE model compares to Kumar et al. [12] and Ahmad et al. [16] based on entropy and NPCR parameters, which was proposed in 2024 and 2018. Based on the results, the suggested IE model has higher entropy and NPCR than the current models. This means that the proposed IE model is safer. Finally, we have done the comparative analysis based on PSNR parameter with the existing method [24], which was purposed in 2022

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

in Table 10(c). The results indicates that the proposed method achieves a little bit higher PSNR due to lesser MSE over the existing method.

5.5 Discussion

The comparative analysis indicates that the proposed method achieves better entropy, CC, and NPCR over the existing methods due to enhancing the multiple security parameters by designing a multi-objective function. Besides that, the more challenging task in the proposed IE model is to set the parameter value of the metaheuristic LO algorithm. Further, we have found that the fine-tuning of the chaotic map using the metaheuristic algorithm enhances the security of the image encryption model. However, a number of parameters need to be communicated on the receiver side.

6. CONCLUSION

Regarding the security of the secret images, the previous chaotic-based IE methods enhance the single security characteristics by considering the metaheuristic algorithm. Therefore, in this article, we present an improved encryption method that enhances multiple security parameters by designing a multi-objective function. In the proposed IE method, we have incorporated the chaotic map and metaheuristic LO algorithm. We use the metaheuristic LO algorithm to fine-tune the parameters of the chaotic map, generating the optimal random key and shuffling indexes. Another good thing about the suggested IE model is that we created a multi-objective function. A metaheuristic algorithm then uses this function to find the best parameter values. Thus, it enhances the multiple security parameters of the IE model. Entropy and CC are the parameters considered in this research. We evaluate the simulation on standard dataset images by considering the several images and different resolutions, determining various parameters to ensure its robustness against various attacks. The outcome shows that the suggested IE model meets the needed level of security and does better than the current models when entropy, CC, and NPCR parameters are used for comparison. In the future, we will explore the higher-dimensional chaotic map, security parameters to design multi-objective functions, and validation on the real-time images.

DATA AVAILABILITY

The standard dataset images are used in this research are available on USC SIPI Image Database [23].

REFERENCES

[1] Y. Alghamdi and A. Munir, “Image Encryption Algorithms: A survey of design and evaluation metrics,” *Journal of Cybersecurity and Privacy*, vol. 4, no. 1, pp. 126–152, Feb. 2024, doi: 10.3390/jcp4010007. Available: https://doi.org/10.3390/jcp4010007

[2] H. Kolivand, S. F. Hamood, S. Asadianfam, and M. S. Rahim, “Image encryption techniques: A comprehensive review,” *Multimedia Tools and Applications*, vol. 83, no. 29, p. 73789, Jan. 2024, doi: 10.1007/s11042-023-17896-0. Available: https://doi.org/10.1007/s11042-023-17896-0

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[3] G. Ye, "Image scrambling encryption algorithm of pixel bit based on chaos map," *Pattern Recognition Letters*, vol. 31, no. 5, pp. 347–354, Nov. 2009, doi: 10.1016/j.patrec.2009.11.008. Available: https://doi.org/10.1016/j.patrec.2009.11.008

[4] D. Singh, S. Kaur, M. Kaur, S. Singh, M. Kaur, and H.-N. Lee, "A systematic literature review on chaotic maps-based image security techniques," *Computer Science Review*, vol. 54, p. 100659, Aug. 2024, doi: 10.1016/j.cosrev.2024.100659. Available: https://doi.org/10.1016/j.cosrev.2024.100659

[5] M. SaberiKamarposhti, A. Ghorbani, and M. Yadollahi, "A comprehensive survey on image encryption: Taxonomy, challenges, and future directions," *Chaos Solitons & Fractals*, vol. 178, p. 114361, Dec. 2023, doi: 10.1016/j.chaos.2023.114361. Available: https://doi.org/10.1016/j.chaos.2023.114361

[6] B. Zhang and L. Liu, "Chaos-Based Image Encryption: review, application, and challenges," *Mathematics*, vol. 11, no. 11, p. 2585, Jun. 2023, doi: 10.3390/math11112585. Available: https://doi.org/10.3390/math11112585

[7] M. Kaur, S. Singh, M. Kaur, A. Singh, and D. Singh, "A systematic review of metaheuristic-based image encryption techniques," *Archives of Computational Methods in Engineering*, vol. 29, no. 5, pp. 2563–2577, Oct. 2021, doi: 10.1007/s11831-021-09656-w. Available: https://doi.org/10.1007/s11831-021-09656-w

[8] M. Abdel-Basset, L. Abdel-Fatah, and A. K. Sangaiah, "Metaheuristic Algorithms: A Comprehensive Review," *Elsevier eBooks*, pp. 185–231, Jan. 2018, doi: 10.1016/b978-0-12-813314-9.00010-4. Available: https://doi.org/10.1016/b978-0-12-813314-9.00010-4

[9] J. S. Muthu and P. Murali, "Review of chaos detection techniques performed on chaotic maps and systems in image encryption," *SN Computer Science*, vol. 2, no. 5, Jul. 2021, doi: 10.1007/s42979-021-00778-3. Available: https://doi.org/10.1007/s42979-021-00778-3

[10] G. Ghosh, N. Kavita, S. Verma, N. Jhanjhi, and M. N. Talib, "Secure surveillance system using chaotic image encryption technique," *IOP Conference Series Materials Science and Engineering*, vol. 993, no. 1, p. 012062, Dec. 2020, doi: 10.1088/1757-899x/993/1/012062. Available: https://doi.org/10.1088/1757-899x/993/1/012062

[11] S. M. Sameh, H. E.-D. Moustafa, E. H. AbdelHay, and M. M. Ata, "An effective chaotic maps image encryption based on metaheuristic optimizers," *The Journal of Supercomputing*, vol. 80, no. 1, pp. 141–201, Jun. 2023, doi: 10.1007/s11227-023-05413-x. Available: https://doi.org/10.1007/s11227-023-05413-x

[12] N. Kumar, S. Saini, and D. Garg, "Color image encryption model based on 3-D Chaotic Logistic Map and JAYA algorithm," *IETE Journal of Research*, pp. 1–11, Sep. 2024, doi: 10.1080/03772063.2024.2390667. Available: https://doi.org/10.1080/03772063.2024.2390667

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[13] G. Kaur, Y. Singh, P. Bhadauria, A. Kumar, and J. P. Singh, "Color Image Encryption Method based on Three-Dimensional Chaotic Map and Nature-Inspired Osprey Optimization Algorithm," *Power System Technology*, vol. 48, no. 1, pp. 306–321, Apr. 2024, doi: https://doi.org/10.52783/pst.277.

[14] S. Saravanan and M. Sivabalakrishnan, "A hybrid chaotic map with coefficient improved whale optimization-based parameter tuning for enhanced image encryption," *Soft Computing*, vol. 25, no. 7, pp. 5299–5322, Jan. 2021, doi: https://doi.org/10.1007/s00500-020-05528-w.

[15] K. S. Khalaf, M. A. Sharif, and M. S. Wahhab, "Digital Communication Based on Image Security using Grasshopper Optimization and Chaotic Map," *International Journal of Engineering*, vol. 35, no. 10, pp. 1981–1988, Jan. 2022, doi: 10.5829/ije.2022.35.10a.16. Available: https://doi.org/10.5829/ije.2022.35.10a.16

[16] M. Ahmad, M. Z. Alam, Z. Umayya, S. Khan, and F. Ahmad, "An image encryption approach using particle swarm optimization and chaotic map," *International Journal of Information Technology*, vol. 10, no. 3, pp. 247–255, Jan. 2018, doi: 10.1007/s41870-018-0099-y. Available: https://doi.org/10.1007/s41870-018-0099-y

[17] Y. S. Alsahafi, A. M. Khalid, H. M. Hamza, and K. M. Hosny, "New optimized chaotic encryption with BCOVIDOA for efficient security of medical images in IoMT systems," *Neural Computing and Applications*, vol. 36, no. 14, pp. 7705–7723, Feb. 2024, doi: 10.1007/s00521-024-09508-1. Available: https://doi.org/10.1007/s00521-024-09508-1

[18] J. Ferdush, G. Mondol, A. P. Prapti, M. Begum, M. N. A. Sheikh, and S. Md. Galib, "An enhanced image encryption technique combining genetic algorithm and particle swarm optimization with chaotic function," *International Journal of Computers and Applications*, vol. 43, no. 9, pp. 960–967, Sep. 2019, doi: 10.1080/1206212x.2019.1662170. Available: https://doi.org/10.1080/1206212x.2019.1662170

[19] M. Dehghani, G. Bektemyssova, Z. Montazeri, G. Shaikemelev, O. P. Malik, and G. Dhiman, "Lyrebird Optimization Algorithm: A new Bio-Inspired metaheuristic algorithm for solving optimization problems," *Biomimetics*, vol. 8, no. 6, p. 507, Oct. 2023, doi: 10.3390/biomimetics8060507. Available: https://doi.org/10.3390/biomimetics8060507

[20] Y. Alghamdi, A. Munir, and J. Ahmad, "A Lightweight Image Encryption Algorithm Based on Chaotic Map and Random Substitution," *Entropy*, vol. 24, no. 10, p. 1344, Sep. 2022, doi: https://doi.org/10.3390/e24101344.

[21] Y. Zhang, W. Dong, J. Zhang, and Q. Ding, "An Image Encryption Transmission Scheme Based on a Polynomial Chaotic Map," *Entropy*, vol. 25, no. 7, pp. 1005–1005, Jun. 2023, doi: https://doi.org/10.3390/e25071005.

[22] J. Chen, X.-W. Li, and Q.-H. Wang, "Deep Learning for Improving the Robustness of Image Encryption," *IEEE Access*, vol. 7, pp. 181083–181091, 2019, doi: https://doi.org/10.1109/access.2019.2959031.

Received: August 05, 2025

Volume 38 No. 9s, 2025

ISSN: 1311-1728 (printed version); ISSN: 1314-8060 (on-line version)

[23] "SIPI Image Database." Available: https://sipi.usc.edu/database/

[24] A. A. Abdallah and A. K. Farhan, "A new image encryption algorithm based on multi chaotic system," *Iraqi Journal of Science*, pp. 324–337, Jan. 2022, doi: 10.24996/ijs.2022.63.1.31. Available: https://doi.org/10.24996/ijs.2022.63.1.31

[25] W. Feng *et al.*, "Integrating Fractional-Order Hopfield Neural Network with Differentiated Encryption: Achieving High-Performance Privacy Protection for Medical Images," *Fractal and Fractional*, vol. 9, no. 7, p. 426, Jun. 2025, doi: 10.3390/fractalfract9070426. Available: https://doi.org/10.3390/fractalfract9070426

Received: August 05, 2025