Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

Color Image Encryption Method based on Three-Dimensional Chaotic Map and Nature-Inspired Osprey Optimization Algorithm

[1]Dr. Gagandeep Kaur, [2]Yeshpal Singh, [3]Prateek Bhadauria, [4]Ajay Kumar, [5]Jatinder Pal Singh

[1]Assistant Professor, Department of Computer Science Engineering, CTIEMT (CT Group of Institutions), Shahpur, Jalandhar, India. gagandeep.2091@ctgroup.in

[2]Lecturer, Department of Computer Science, Government Polytechnic, Roorkee, Baheri, Bareilly, Uttar Pradesh, India. softwareknowler33@gmail.com

[3]Assistant Professor, Department of Electronics Engineering, MITS, Gwalior, India. bhadauria.prateek@mitsgwalior.in

[4]Research Scholar, Department of Electronics and Communication Engineering, Thapar Institute of Engineering and Technology, Patiala, India. ajay.kumar@thapar.edu

[5]Research Scholar, Department of Electrical Engineering, Sant Baba Bhag Singh University, Jalandhar, India. jatindersingh20012002@gmail.com

Abstract: In this research, an encryption method is designed to secure multimedia images from various threats on the internet. In the proposed method, color images are taken as secret data, and random key generation is done using the three-dimensional (3-D) chaotic logistic map. In the 3-D chaotic logistic map, several input parameters are involved, and if their optimal parameter value is determined, it generates a completely random key to encrypt the secret images. In this research, the metaheuristic osprey optimisation algorithm is utilised to determine the best parameter value of the 3-D chaotic logistic map. The osprey optimisation algorithm is based on hunting the fish and carrying the fish to a suitable position to eat. This algorithm requires minimum internal parameters and provides a better exploration and exploitation rate to find the best solution for a given problem. Besides that, in this research, a multi-objective function is designed with the help of entropy and structure similarity index measures (SSIM) to find the parameter value of the chaotic map. After determining the parameter value, the exclusive-OR operation is performed. After that, each row and column of the color image is circularly rotated according to their row and column index to achieve the permutation in the secret image. The standard dataset of the USC-SIPI Image database is taken for evaluation purposes, and its subjective and objective analysis is done. The result shows that the proposed method achieves better performance when compared with the existing methods.

Keywords: Chaotic Map, Color Images, Encryption, Metaheuristic, Osprey Optimization, Security.

1. Introduction

In today's era, the internet is the most used network to communicate personal or work-related data from one place to another. Further, due to the adoption of smart devices, a large amount of multimedia data is uploaded and downloaded. The multimedia data is available in various

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

forms, such as text, image, audio, and video. Out of these data forms, in this research, we have focused on image multimedia data. In the present scenario, every hour, approximately 38,66,400 and 81,60,000 images are uploaded on Instagram and Facebook. However, in order to secure these images from illegal access and to provide copyright and privacy protection, cryptography is utilized [1].

Cryptology is a combination of the Greek terms Cruptos and Logos, which imply password science. Cryptography and cryptanalysis are the two categories that are examined. Cryptography is the process of transforming publicly available information into an unreadable format using private keys and then making it readable again using private keys for trustworthy individuals. Cryptanalysis refers to the processes used to make encrypted data readable [2]. Cryptography addresses information security issues like confidentiality, integrity, authentication, and non-repudiation. Confidentiality in this context refers to the information not being understood by other parties. Integrity implies that information does not alter during transmission. When two parties authenticate one another, it's called authentication. Non-repudiation implies that neither the sender nor the recipient can dispute that they transmitted or received the information. When someone sends information to someone else over an open network, that information could be changed or read by people who are not connected to the sender. The information under consideration is referred to as plain text in this context, and the method used to secure it is known as encryption. We may combine modern encryption algorithms under symmetric and asymmetric encryption methods after dividing these algorithms into two categories: classic and modern. Examples of symmetric algorithms include Data Encryption Standard (DES), Advanced Encryption Standard (AES), Triple DES (3DES); examples of asymmetric algorithms are Rivest–Shamir–Adleman (RSA) and Digital Signature Algorithm (DSA) [3].

Symmetric encryption techniques require that the secret key comprising the encrypted text be supplied to the recipient in addition to encrypting and decrypting data using the same key. With asymmetric encryption methods, the encryption key and the decryption key are distinct, and the self-specific key of every receiver is accessible. When one of these techniques is used to encrypt the plain text, the encryption process is complete. Information security is offered by this method. The secure information transmission is then finished when the recipient side uses either private or public keys to translate the ciphertext back to plain text. This describes the fundamental reasoning behind encryption and decryption. Using this fundamental reasoning, encryption and decryption procedures are carried out using the aforementioned techniques. The primary method of encrypting an image is to modify the values or positions of the individual pixels. When encrypting a text, an algorithm and a key are used to accomplish this. To decode a text message, the recipient must be aware of the encryption key and algorithm. Image encryption may be considered using this reasoning. By combining several algorithms with pixel location or value information, the original image may be encrypted using a key or keys. Using chaotic structures, encryption may be made more complicated and harder to decipher. The encryption techniques and keys used at the start of the decryption process should be known by the people who receive the encrypted picture. Text message encryption using traditional techniques works well. For images, on the other hand, chaotic encryption techniques are

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

recommended. The most essential reason why chaotic systems are chosen in encryption processes is because even little changes in the encryption keys have a significant impact on the outcome of the decoding process [4]. However, the chaotic map is highly sensitive to input parameters. Therefore, in the research, metaheuristic algorithms are utilized to fine tune the input parameter of the chaotic map. In this research, an effective image encryption method is designed by using the three-dimensional chaotic logistic map and metaheuristic osprey optimization algorithm.

Below is a summary of this research's primary contribution.

- In the proposed method, different planes of colour images are encrypted using different keys instead of a single key. The 3-D chaotic logistic map guides the determination of these keys.
- In the proposed method, the optimal parameter values of the 3-D chaotic logistic map are determined using the osprey optimisation algorithm to generate the random key.
- In this research, a multi-objective function is designed in place of a single objective function for encryption purposes.
- The evaluation of the proposed method shows that the histograms are equally distributed for encrypted images, and it achieves better performance metrics than the existing image encryption methods.

The remaining paper has six sub-sections. Section 2 shows the study of various encryption methods designed to secure multimedia images. Section 3 provides an explanation of the methodology, detailing the various components of the proposed method. Section 4 explains the proposed image encryption method. Sections 5–6 present the results, discussion, conclusions, and future work.

2. Related Work

In this section, we have studied and analysed the existing image encryption method, which is based on the chaotic map and metaheuristic algorithms. Naveen Kumar and Satish Saini [5] used the two-dimensional chaotic henon map to encrypt the grey-scale images. Further, they have used termite alate optimisation to determine the best input parameter values of the henon map based on the entropy objective function. Kumar et al. [6] used the black widow optimisation algorithm to determine the optimal parameter of the one-dimensional chaotic logistic map algorithm. Besides that, in their work, a single objective function (entropy) is taken as the objective function. Abedzadeh et al. [7] used the SHA-512, standard chaotic map, and teaching learning-based optimisation (TLBO) algorithm to design an efficient image encryption method. The TLBO searches for the best shuffled image based on the entropy parameter. Further, Sameh et al. [8] utilised various metaheuristic algorithms to fine-tune the chaotic maps to design the confusion and diffusion layers of image encryption. Khan et al. [9] utilised the three-dimensional chaotic map and grey-wolf optimisation algorithm to design the s-box for image encryption.

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

The current study reveals that image encryption methods use the chaotic map to design the confusion and diffusion matrixes. Further, metaheuristic algorithms are used in the image encryption method to fine-tune the parameter values of the chaotic map. However, in the existing work, very complex metaheuristic algorithms are utilised, in which a number of parameters need to be set to search for the best parameter value of the chaotic map. Besides that, in most of the research, a single objective function is taken into consideration. In this research, to overcome these issues, a low-complex metaheuristic algorithm is chosen, which requires a minimum parameter to be initialised to search the parameter values. Besides that, in place of a single objective function, a multi-objective function is designed.

3. Methodology

3.1 Secret Image Database: In this research, colour images are taken into consideration as secret data. In the literature, USC-SIPI-Image database images are utilised in image encryption. In this database, images are available in various volumes [10]. The encryption method uses a variety of images from these volumes. The images taken into consideration are shown in Figure 1. The resolution of the image is 256×256.

Figure 1: Database Images

3.2 3-D Chaotic Logistic Map: Chaotic logistic map is utilized in this research for key generation. In this process, the initial value of the key is constructed by initializing the chaotic parameters. However, initializing the parameter value using the best value generates a completely pseudorandom key [11]. In this research, 3-D chaotic logistic map is taken into consideration to generate the three keys to encrypt the color images. It is determined using Eq. (1-3) [12].

$$x_{n+1} = \alpha x_n(1 - x_n) + \beta y_n^2 x_n + \gamma z_n^3 \quad (1)$$

$$y_{n+1} = \alpha y_n(1 - y_n) + \beta z_n^2 y_n + \gamma x_n^3 \quad (2)$$

$$z_{n+1} = \alpha z_n(1 - z_n) + \beta x_n^2 z_n + \gamma y_n^3 \quad (3)$$

In contrast, Eq. (1-3), x= {0-1}, α= {3.68-3.99}, β= {0-0.022}, γ= {0-0.015}. In this research, the best parameter value of these equations is determined using the metaheuristic osprey optimization algorithm. To understand how osprey optimization algorithm works, its detailed description is given below.

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

3.3 Osprey Optimization Algorithm: As discussed in the previous section, the output of the chaotic logistic map is highly dependent on the input parameter values. Therefore, in this research, metaheuristic osprey optimization algorithm (OOA) is utilized for determine the parameter values based on the objective function. In this section, a detailed description of osprey optimization algorithm is given [13].

The primary source of inspiration for OOA is the technique used by Ospreys for catching fish in the ocean. Using this hunting tactic, the osprey locates its prey, hunts it, and then transports it to an ideal eating location. Below is the mathematical modeling for the Osprey optimization technique.

Through a repetition-based procedure, the proposed OOA is a population-based technique that may provide an appropriate solution based on the search capacity of its population members in the problem-solving space. Each osprey in the OOA population assigns values to the problem variables according on its location in the search space. As a result, each osprey represents a potential solution to the issue, mathematically represented as a vector. The OOA population is made up of all ospreys, and it may be described using a matrix as per (4). The initialization of osprey positions in the search space is done at random using (5) at the start of OOA implementation.

$$X = \begin{bmatrix} X_1 \\ X_2 \\ . \\ . \\ X_N \end{bmatrix}_{N\times m} = \begin{bmatrix} X_{11}X_{12} \dots \dots . X_{1m} \\ X_{21}X_{22} \dots \dots . X_{2m} \\ . \\ . \\ X_{N1}X_{N2} \dots \dots . X_{Nm} \end{bmatrix}_{N\times m} \tag{4}$$

$$x_{ij} = lb_j + r_{ij}\left(ub_j - lb_j\right), i = 1,2, \dots N, j = 1,2, \dots m \tag{5}$$

where m is the number of problem variables, N is the number of ospreys, r_{ij} are randomized numbers in the interval [0 , 1] , lb_j, and ub_j are the lower and upper bounds of the jth problem variable, respectively, and X is the population matrix of the locations of the ospreys. The objective function may be assessed because every osprey represents a potential solution to the issue that corresponds to each osprey. According to (6), a vector may be used to represent the evaluated values for the problem's objective function.

$$F = \begin{bmatrix} F_1 \\ F_2 \\ . \\ . \\ F_N \end{bmatrix}_{N\times 1} = \begin{bmatrix} F(X_1) \\ F(X_2) \\ . \\ . \\ F(X_N) \end{bmatrix}_{N\times 1} \tag{6}$$

Where F_i is the objective function value obtained for the ith osprey and F is the vector containing the objective function values. The primary criterion for assessing the level of quality of the candidate solutions is the assessed values for the objective function. Thus, the optimal candidate solution, or the best member, is represented by the best value found for the objective function, and the optimal candidate solution, or the worst member, is represented by the worst

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

value obtained for the objective function. The best candidate solution has to be changed every iteration because the ospreys' positions in the search space are modified.

3.2.2 Phase 1: Position identification and hunting the fish (exploration)

Ospreys are powerful hunters who can determine the location of fish underwater due to their ability to see clearly. Once they've located the fish, they dive under the surface to attack and hunt it. A simulation of ospreys' natural behavior serves as the basis for the first phase of the OOA population update model. By simulating the osprey's attack on fish, the location of the bird of prey in the search space is significantly altered, enhancing OOA's ability to find the best region and avoid local optima. Underwater fishes in OOA design are defined as the placements of other ospreys in the search space with a higher objective function value than each individual osprey. Each osprey's fish set is specified using (7).

$$FP_i = \{X_k | k \in \{1,2, \ldots \ldots, N\} \wedge F_k < F_i\} \cup \{X_{best}\} \quad (7)$$

where Xbest is the best viable solution (the best osprey) and FP_i is the collection of fish locations for the ith osprey. One of these fish is randomly located by the osprey, which then hits it. A new location for the corresponding osprey is determined using (8) based on the simulation of the osprey's movement towards the fish. As per (9), the osprey's original location is replaced by this new one if it enhances the value of the goal function.

$$x_i^{p1} = x_{ij} + r_{ij}.(SF_{ij} - I_{ij}.x_{ij}) \quad (8\text{-a})$$

$$x_i^{p1} = \begin{cases} x_{ij}^{p1}, lb_j \le x_{ij}^{p1} \le ub_j \\ lb_j, x_{ij}^{p1} < lb_j \\ ub_j, x_i^{p1} > ub_j \end{cases} \quad 8(b)$$

$$x_i = \begin{cases} x_i^{p1}, F_{ij}^{p1} < F_i \\ x_i, else \end{cases} \quad (9)$$

where x_i^{p1} represents the ith osprey's new position based on the OOA's first phase. Furthermore, x_{ij}^{p1} represents its jth dimension, r_{ij} are random numbers in the interval [0 , 1], SF_i is the selected fish for ith osprey, F_i^{p1} is its objective function value, SF_{ij} is the its jth dimension, and I_{ij} are random numbers from the set{1-2 }.

3.2.3 Phase 2: Transporting the fish to its ideal spot (exploitation) The osprey hunts fish and then transports it to a safe spot for him to eat it. The modeling of this osprey's natural behavior serves as the basis for the second phase of the OOA population update model. The process of carrying the fish to the appropriate location through modeling causes the osprey's position in the search space to vary slightly. This leads to an increase in the OOA's ability to exploit the local search and convergence regarding better solutions that are close to the solutions that are found.

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

In order to imitate the ospreys' natural behavior, OOA's design first generates a new random location for each member of the population that is considered a "suitable position for eating fish" (10). Then, in accordance with (11), it takes the place of the related osprey's old position if the objective function's value is increased in this new location.

$$x_i^{p2} = x_{ij} + \frac{lb_j + r(ub_j - lb_j)}{t}, i = 1,2 \ldots N, j = 1,2..m, t = 1,2 \ldots T \quad (10\text{-a})$$

$$x_i^{p2} = \begin{cases} x_{ij}^{p2}, lb_j \le x_{ij}^{p2} \le ub_j \\ lb_j, x_{ij}^{p2} < lb_j \\ ub_j, x_i^{p2} > ub_j \end{cases} \quad (10\text{-b})$$

$$x_i = \begin{cases} x_i^{p2}, F_{ij}^{p2} < F_i \\ x_i, else \end{cases} \quad (11)$$

In the above equation, x_i^{p2} represents the new position of the ith osprey. This is based on the second phase of OOA. Furthermore, F_i^{p2} is its objective function value, x_{ij}^{p2} is its jth dimension, r_{ij} are random numbers in the interval [0, 1], t is the iteration counter of the algorithm, and T represents the total iterations.

3.4 Objective Function: In this research, multiple parameters are taken into consideration to design the objective function that enhances the multiple security characteristics of image encryption. In this research, structure similarity index measure (SSIM) and correlation coefficient (CC) are the parameters taken into consideration.

3.5 Performance Metrics: In this section, the performance metrics are defined which are taken into consideration to evaluate the proposed method [5,14-15].

- Mean Square Error (MSE): The mean square error (MSE) measures the error in the encrypted image with respect to the plain image. It is determined using Eq. (12).

$$MSE = \frac{1}{JK}\sum_{m=1}^{J}\sum_{n=1}^{K}|P(mn) - E(mn)|^2 \quad (12)$$

  The plain image is represented by $P(mn)$, the encrypted image by $E(mn)$, and the sizes of both images are represented by JK.
- Peak Signal to Noise Ratio (PSNR): The PSNR provides the difference in error between the encrypted and plain images. The mean squared error (MSE) is used to calculate the PSNR.

$$PSNR = 10\log_{10}\left(\frac{255^2}{MSE}\right) \quad (13)$$

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

- Correlation Coefficient (CC): The degree of relationship between two neighboring pixels in an image is measured by the correlation coefficient. It's a term used to characterize how similar two adjacent pixels are to one another in the diagonal, horizontal, and vertical axes. A strong image encryption technique reduces the correlation between adjacent pixels in the encrypted image. The correlation coefficient may be determined using the following formulas:

$$cc_{xy} = \frac{cov(x,y)}{\sqrt{D(x)}\sqrt{D(y)}} \quad (14)$$

$$cov(x,y) = \frac{1}{L}\sum_{i=1}^{L}(x_i - E(x))(y_i - E(y)) \quad (15)$$

$$E(x) = \frac{1}{L}\sum_{i=1}^{L} x_i \quad (16)$$

$$E(y) = \frac{1}{L}\sum_{i=1}^{L} y_i \quad (17)$$

$$D(x) = \frac{1}{L}\sum_{i=1}^{L}(x_i - E(x))^2 \quad (18)$$

$$D(y) = \frac{1}{L}\sum_{i=1}^{L}(y_i - E(y))^2 \quad (19)$$

  where L is the amount of pixels, y represents the cipher image, and x represents the original image.
- Structure Similarity Index Measure (SSIM): To extract statistical image characteristics for image similarity purposes, a structural similarity measure is based on statistical measures such the mean (μ) and standard deviation (σ). Using the SSIM, the following formula may be used to define a distance function between two photos and determine how similar the reference and test images are to each other:

$$S(mn) = \frac{(2\mu_m\mu_n + c_1)(2\sigma_{mn} + c_2)}{(\mu_m^2 + \mu_n^2 + c_1)(\sigma_m^2 + \sigma_n^2 + c_2)} \quad (20)$$

  where the structural similarity measure, $S(mn)$, indicates the statistical similarity between the training image (n) and the test image (m). In the picture mn, the number $\mu_m\mu_n$ represents the statistical mean of the pixels. On the other hand, $\sigma_m^2\sigma_n^2$ represents the statistical variance of the pixels. Both c1 and c2 are constant numbers.

- Entropy: The randomization of the pixel intensities of an encrypted image is measured by entropy. A robust encryption scheme has an entropy value of around 8. The following formulae are used to compute the entropy:

$$E(X) = \sum_{j=0}^{L-1} p(x_j) \log_2 \frac{1}{p(x_j)} \quad (21)$$

  where L is the total number of investigated pixels, $p(x_j)$ is the occurrence probability, and $E(X)$ is the entropy of the plain image X.
- Time Complexity: This parameter measures how much time spent in image encryption.
- Histogram Analysis: It displays the frequency of the pixel distribution in an image. The main image has non-uniform histograms. On the other hand, in order to survive statistical attacks, the encrypted image histograms have to be consistent.

4. Proposed Image Encryption Method

The main motive of the proposed image encryption method is to secure the multimedia images on the internet. Further, the main benefit of the proposed image encryption method is that

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

different planes of the color image is encrypted using the different keys because optimal parameter of the 3-D chaotic logistic map is determined using osprey optimization algorithm based on the objective function. The flowchart of the proposed image encryption method is shown in Figure 2.

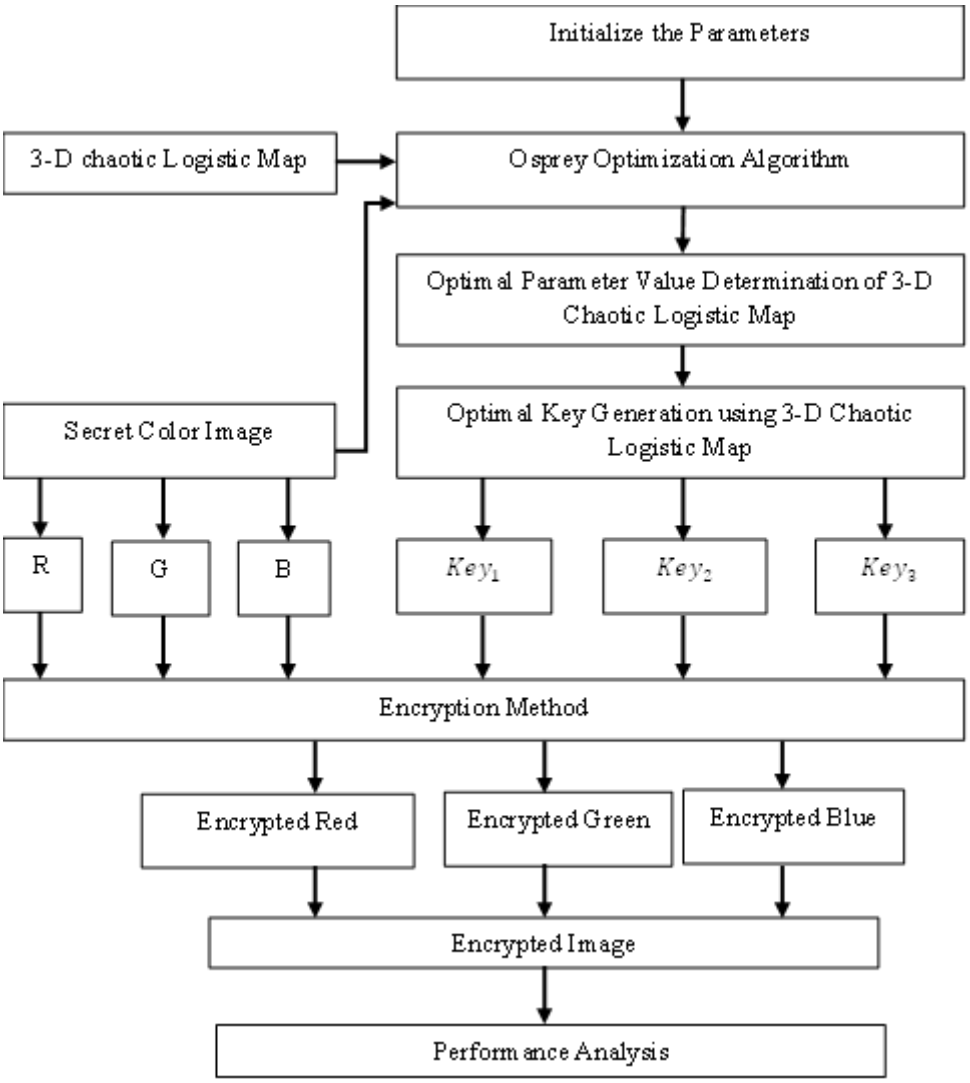


Figure 2: Flowchart of the Proposed Image Encryption Method

In the proposed method, initially, a secret image and 3-D logistic map algorithm are given to the osprey optimisation algorithm. After that, input parameters of the osprey optimisation algorithm are initialised, such as population, iterations, objective function, random number, and lower and upper bounds of the logistic parameters, along with the dimension of each parameter. After that, OOA generates the random population for the 3-D logistic map algorithm in the lower and upper limits of the parameter values. Next, each population parameter value is input to a 3-D logistic map algorithm for key generation. After key generation, the encryption process is performed using the exclusive-OR operation and permutation of the image matrix in

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

the horizontal and vertical directions. After that, the objective function is evaluated, and the fitness function of each population is determined. Based on the fitness function, the best population is determined. After that, phases 1 and 2 of the OOA are performed to explore new populations in the lower and upper limits. Besides that, each population is evaluated to determine whether it is generated in the lower and upper limits or not. If the generated solution is outside the limits, then it is assigned a lower or upper limit value, as shown in Eqs. 8–11. Next, which population gives the superior performance is chosen as the best parameter value of the chaotic logistic map. Further, based on these optimal parameter values, the best key is generated. The best key, along with different planes of the secret image, is given to the encryption method. Finally, all planes are encrypted, images are concatenated, and performance analysis is done using subjective and objective analysis.

5. Results and Discussion

This section explains the simulation evaluation of the proposed image encryption method, which is designed to secure colour images. MATLAB 2018a software simulates the proposed method. In the evaluation, five standard dataset images ("house," "female," "couple," "airplane," and "lena") are taken into consideration, and the resolution of the images is in.jpg format. Further, in the proposed method, the osprey optimisation algorithm is utilised to determine the parameter values of the chaotic map. Therefore, the osprey optimisation algorithm needs to be initialised to search for the best parameter values in the lower and upper bounds based on the objective function. Table 1 shows the osprey optimization algorithm's simulation setup configuration.

Table 1: Simulation Setup Configuration of the Osprey Optimization Algorithm for the Proposed Method

Parameter	Value
Population	20
Iterations	30
Objective Function	{SSIM, CC}
Lower and Upper Limit of x	{0-1}
Lower and Upper Limit of α	{3.68-3.99}
Lower and Upper Limit of β	{0-0.022}
Lower and Upper Limit of γ	{0-0.015}
r	{0-1}

In the proposed method, the security analysis is done based on the subjective and objective analysis. The detailed description of these analysis is given below.

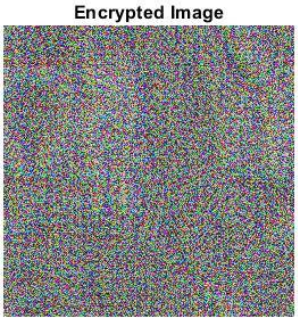
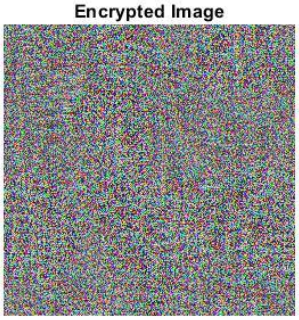
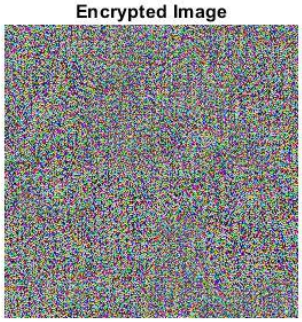
5.1 Subjective Analysis

In the subjective analysis, the visual quality of the encryption image along with its histogram is compared with respect to the original image. In the ideal case, the encryption method

Power System Technology
ISSN:1000-3673
Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

provides a completely noisy encrypted image, and their histogram should be equally distributed. Table 2-3 shows the subjective analysis by comparing the secret image and their histogram with their encrypted image and their histogram. The result shows that the images taken into consideration for evaluation purposes are completely noisy, and their histograms are equally distributed.

Table 2: Subjective Analysis by Comparing the Secret Image with Encrypted Image

Images	Secret Image	Encrypted Image
House		
Female		
Couple		

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

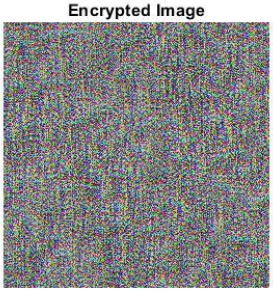
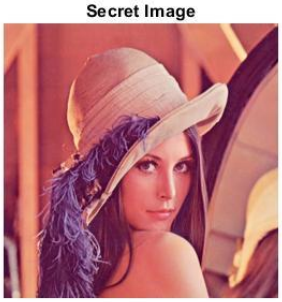
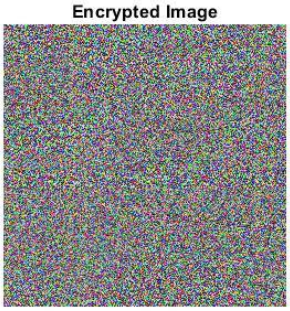
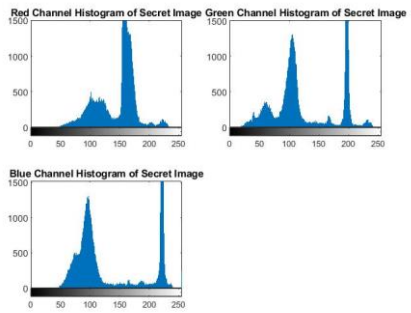
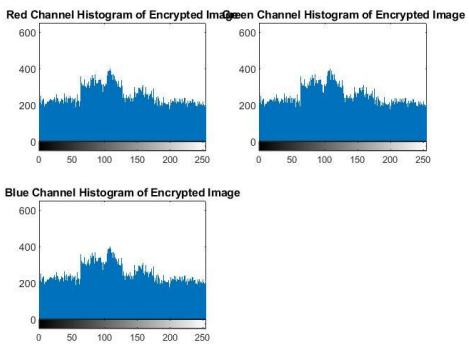
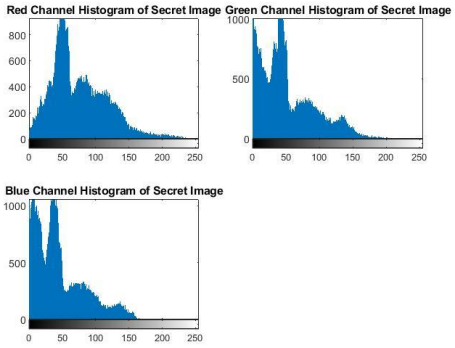
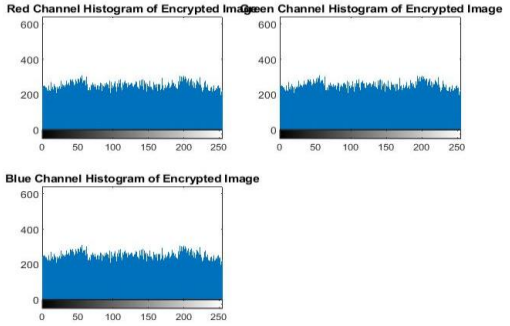
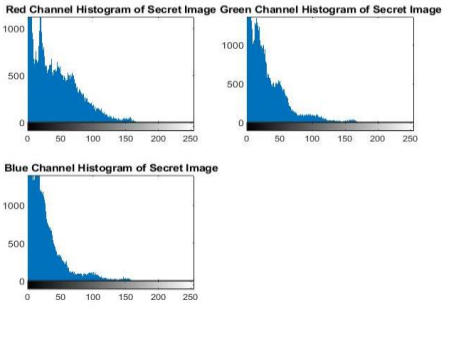
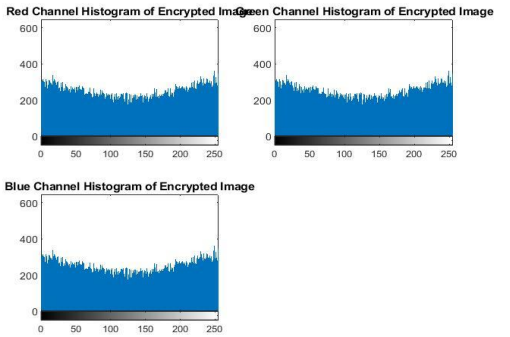
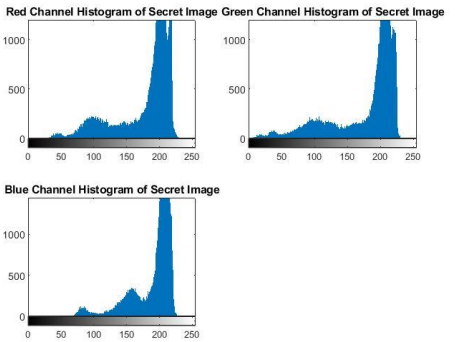
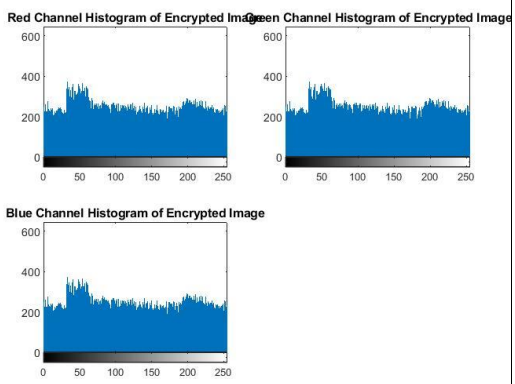
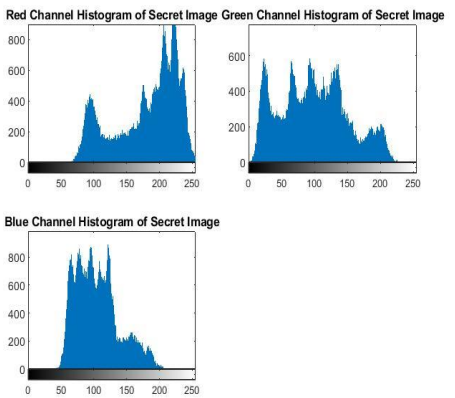
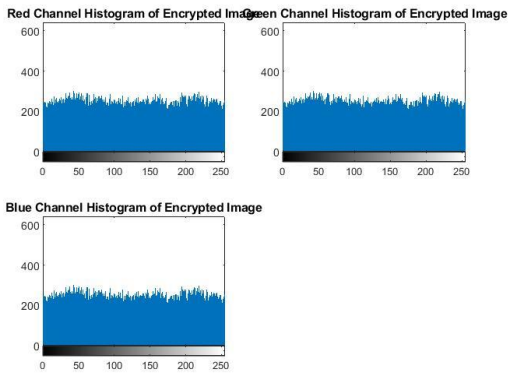
Airplane	Secret Image 	Encrypted Image 
Lena	Secret Image 	Encrypted Image 

Table 3: Subjective Analysis by Comparing the Secret Image Histogram with Encrypted Image Histogram

Images	Secret Image Histogram	Encrypted Image Histogram
House		

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

Female		
Couple		
Airplane		
Lena		

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

5.2 Objective Analysis

In this analysis, the encrypted image characteristics are studied and analysed using the various parameters with respect to the original image. Table 4 shows the parameters are taken into consideration for objective analysis of the proposed method. The result shows that the proposed method achieve low value of PSNR, CC, and SSIM and high value of MSE and entropy which is requried in the image encryption approach.

Table 4: Objective Analysis

Images	Planes	MSE	RMSE	PSNR	CC	SSIM	Entropy
House	R	4.5770e+03	67.6537	11.5250	-0.00006	0.0109	7.9730
	G	4.6388e+03	68.1089	11.4667	-0.00032	0.0112	7.9730
	B	6.0284e+03	77.6427	10.3288	0.00150	0.0124	7.9730
Female	R	1.2078e+03	34.7530	17.3109	0.00440	0.0094	7.9951
	G	648.8632	25.4728	20.0093	-0.00220	0.0058	7.9951
	B	463.2582	21.5234	21.4726	-0.00450	0.0057	7.9951
Couple	R	383.2237	19.5761	22.2963	0.00420	0.0063	7.9864
	G	231.7107	15.2220	24.4813	0.00140	0.0038	7.9864
	B	190.5071	13.8024	25.3317	0.00025	0.0046	7.9864
Airplane	R	8.8647e+03	94.1527	8.6541	0.00680	0.0106	7.9870
	G	9.2466e+03	96.1591	8.4710	0.00390	0.0099	7.9870
	B	1.0122e+04	100.6063	8.0783	0.00099	0.0104	7.9870
Lena	R	9.4032e+03	96.9703	8.3980	-0.00860	0.0097	7.9963
	G	2.4572e+03	49.5698	14.2265	-0.00770	0.0077	7.9963
	B	2.0489e+03	45.2643	15.0157	0.00130	0.0111	7.9963

5.3 Comparative Analysis

In this section, the proposed image encryption method is evaluated with the existing image encryption method based on entropy parameter. The result shows that the proposed method achieves high entropy value near to 8 values.

Tale 5: Comparative Analysis based on Entropy Parameter

Images	Encryption with 3-D Logistic Map without Optimal Parameter Values	Proposed Method
House	7.8663	7.9730
Female	7.5174	7.9951
Couple	7.9562	7.9864
Airplane	7.8868	7.9870
Lena	7.8068	7.9963

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

6. Conclusion and Future Work

This paper presents an image encryption method using the 3-D chaotic logistic map and metaheuristic osprey optimization algorithm. The 3-D logistic map is utilized for generate different keys to encrypt the different planes of color image. On the other hand, metaheuristic osprey optimization algorithm is utilized to determine the parameter values of the 3-D logistic map based on the multi-objective function. The multi-objective is designed with the help of correlation coefficient and SSIM parameter. Further, encryption process has two phases. In the first phase, exclusive-OR operation with random key is done. In the second phase, circular shifting of color image is done row-wise and column-wise based on index values of the row and column. In the simulation evaluation, the subjective analysis shows that the encrypted images are looks completely noisy and their histograms are equally distributed. Further, objective analysis shows that the proposed method achieves low value of PSNR, CC, and SSIM and high value of MSE and entropy. In the future, higher dimensional chaotic map is explored to design the encryption method. We also consider additional parameters when designing the multi-objective function.

References

[1] M. Singh and A. K. Singh, "A comprehensive survey on encryption techniques for digital images," *Multimedia Tools and Applications*, vol. 82, no. 8, pp. 11155–11187, Mar. 2022, doi: 10.1007/s11042-022-12791-6.

[2] M. Kaur, S. Singh, and M. Kaur, "Computational Image Encryption Techniques: A Comprehensive Review," *Mathematical Problems in Engineering*, vol. 2021, pp. 1–17, Jul. 2021, doi: 10.1155/2021/5012496.

[3] M. Kaur and V. Kumar, "A Comprehensive Review on Image Encryption Techniques," *Archives of Computational Methods in Engineering*, vol. 27, no. 1, pp. 15–43, Nov. 2018, doi: 10.1007/s11831-018-9298-8.

[4] H. Çelik and N. Doğan, "A hybrid color image encryption method based on extended logistic map," *Multimedia Tools and Applications*, vol. 83, no. 5, pp. 12627–12650, Jul. 2023, doi: 10.1007/s11042-023-16215-x.

[5] Naveen Kumar and Satish Saini, "Image Encryption Model based on Chaotic Henon Map and Termite Alate Optimization Algorithm," International Journal of Intelligent Systems and Applications in Engineering, vol. 12, no. 18, pp. 428-236, Feb. 2024.

[6] Ajay Kumar, Abhijit Karmakar, and Alpana Agarwal, "Improved Chaotic Logistic Map Algorithm based on Bio-Inspired Algorithm for Image Encryption," Tobacco Regulatory Science (TRS), pp, 1915-1928, 2022.

[7] M. Abedzadeh, M. J. Rostami, and M. Shariatzadeh, "Image encryption using a standard map and a teaching-learning based optimization algorithm," *Multimedia Tools and Applications*, vol. 82, no. 19, pp. 29199–29225, Feb. 2023, doi: 10.1007/s11042-023-14379-0.

[8] 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*

Power System Technology
ISSN:1000-3673

Received: 16-01-2024 Revised: 12-02-2024 Accepted: 17-03-2024

Supercomputing, vol. 80, no. 1, pp. 141–201, Jun. 2023, doi: 10.1007/s11227-023-05413-x.

[9] H. Khan, M. M. Hazzazi, S. S. Jamal, I. Hussain, and M. Khan, "New color image encryption technique based on three-dimensional logistic map and Grey wolf optimization based generated substitution boxes," *Multimedia Tools and Applications*, vol. 82, no. 5, pp. 6943–6964, Aug. 2022, doi: 10.1007/s11042-022-13612-6.

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

[11] W. Song, C. Fu, Y. Zheng, M. Tie, J. Liu, and J. Chen, "A parallel image encryption algorithm using intra bitplane scrambling," *Mathematics and Computers in Simulation*, vol. 204, pp. 71–88, Feb. 2023, doi: 10.1016/j.matcom.2022.07.029.

[12] Ramakrishna CJ, Reddy DB, Bharadwaj BV, Agrawal S, Hegde G., "A Novel Image Encryption using 3D Logistic Map and Improved Chirikov Map," *In2022 International Conference on Advances in Computing, Communication and Materials (ICACCM) 2022 Nov 10*, pp. 1-7, 2022.

[13] M. Dehghani and P. Trojovský, "Osprey optimization algorithm: A new bio-inspired metaheuristic algorithm for solving engineering optimization problems," *Frontiers in Mechanical Engineering*, vol. 8, Jan. 2023, doi: 10.3389/fmech.2022.1126450.

[14] Z. Zhang, J. Tang, H. Ni, and T. Huang, "Image adaptive encryption algorithm using a novel 2D chaotic system," *Nonlinear Dynamics*, vol. 111, no. 11, pp. 10629–10652, Mar. 2023, doi: 10.1007/s11071-023-08397-8.

[15] M. T. Elkandoz and W. Alexan, "Image encryption based on a combination of multiple chaotic maps," *Multimedia Tools and Applications*, vol. 81, no. 18, pp. 25497–25518, Mar. 2022, doi: 10.1007/s11042-022-12595-8.