

Image Encryption Method Based On Metaheuristic Social Group Optimization Algorithm

¹Dr. Gagandeep Kaur, ²Dr. Sachin Kumar

¹Post Doctoral Research Fellow, Institute of Computer Science and Information Science, Srinivas University, Mangalore, India. gagankaur.0813@gmail.com

²Associate Professor, Dept. of Information Technology, Management Education & Research Institute, Affiliated to GGSIP University, New Delhi, India. sachinks.78@gmail.com

Abstract: The multimedia data exchange has been raised due to rapid technological improvements in recent years. The attackers investigate how to acquire this data so they can obtain people's sensitive information. Thus, in the present scenario, security is a big concern. Therefore, we have presented a novel image encryption (IE) method based on the metaheuristic social group optimization (SGO) algorithm that explores the best parameter value of the chaotic maps for better security. In the proposed method, the 1-D chaotic logistic map (CLM) is employed for optimal key generation and substitution box (s-box), whereas the 1-D chaotic tent map (CTM) is employed to generate an optimal shuffling index to achieve permutation in the encryption method. In the proposed method, there are a total four stages to achieve the encryption. In the first and last stages, the optimal random key is employed to perform an exclusive-OR operation, whereas in the second and third stages, s-box and permutation are performed. Next, the demonstration of the presented IE method is done for the standard dataset images by analyzing the various security parameters. Lastly, the effectiveness of the proposed approach is compared to existing IE methods using these parameters. The result indicates that the proposed method achieves an average entropy value of **7.9971**, an NPCR value of **99.607**, and a PSNR value of **14.026dB**.

Keywords: Chaotic, Encryption, Image, Metaheuristic, Optimization, Security, SGO.

1. INTRODUCTION

In the present scenario, the people used the open networks and internet to communicate the multimedia data from one place to another. This necessitates the addition of a security layer to safeguard the multimedia data from potential attackers. In the previous studies, encryption is the most preferred approach in which multimedia data is transformed into coded form, which is decrypted by only the intended recipient [1-2]. In this paper, the focus is on image-based multimedia data due to its huge demand in several applications: medical, military, and social media. The image-based multimedia data has different characteristics as compared to the text-based data, such as larger size and high correlation between the pixels [3]. Therefore, the standard encryption methods, namely, DES, 3DES, and AES, take longer for encryption due to multiple rounds being performed in them for encryption purposes. Besides that, these methods are prone to differential attack because the data is processed in blocks form, and a slight change in the input data only changes the pixel value of that block [4]. Consequently, the chaotic map is employed in the IE methods to transform the secret image into an encrypted image. The chaotic map is a non-linear function that provides chaotic behavior, such as highly complex and unpredictable behavior [5]. This behavior is highly sensitive to the input parameter. This implies that a small change in the input parameter value changes a majority value of data in the output. Thus, it is difficult for the attacker to forecast the output data value based on the input parameter [6]. Further, the previous studies show that in the chaotic map, finding the best input parameter value to achieve the chaotic behavior is a challenging task [7]. Therefore, metaheuristic algorithms are employed in this field to search the parameter value based on the objective function at which desired chaotic behavior is achieved for better security in the IE method. In the literature, chaotic maps are successfully used for random key generation purposes, and these keys are employed to achieve confusion and diffusion in the IE methods [8]. In this paper, we have enhanced the security of the IE method by combining the chaotic maps with metaheuristic algorithms for random key, S-box, and shuffling index matrix generation purposes. The main contribution of this article is as follows.

- We have designed an IE method using the metaheuristic SGO algorithm that hyper-tuned the parameters of the 1-D chaotic maps to secure the secret image. This hyper-tuning of the parameters is done to generate a random key, substitution box, and shuffling index matrix to achieve encryption.
- The result demonstrates that the suggested IE method accomplishes superior performance in terms of entropy (7.9971), NPCR (99.607), and PSNR (14.026dB) as compared to the previous methods.

The remaining structure of the research article as follows. Section 2 provides the related work done in the IE method. Section 3 gives an overview of the metaheuristic SGO algorithm. Section 4 provides the detailed description of the proposed IE method. The results and discussion is presented in Section 5. Finally, Section 6 draws the conclusion and future scope of the work.

2. Related Work

This section investigates and analyzes IE methods that rely on metaheuristic and chaotic maps. Al-Hyari et al. [9] employed two chaotic maps, such as the Henon map and the logistic map. They employed the logistic map for permutation and the Henon map for key generation in their work. S. A. Gebereselassie and B. K. Roy [10] analyzed whether 1-D chaotic maps or an integrated approach based on them are suitable for encryption purposes. In their work, the sine, tent, logistic, and cubic maps were considered. Their analysis shows that 1-D chaotic maps outperform the integrated approaches. H. Çelik and N. Doğan [11] proposed an approach in which initially affine transformation was performed on the secret image. The chaotic map is then used to generate the s-box for encryption purposes. Hosny et al. [12] performed scrambling and diffusion of the secret color image by considering the three chaotic maps: Lorenz, Hénon, and logistic. These chaotic maps generate the scrambling and diffusion matrices for RGB planes of the color image. Wen et al. [13] performed the permutation, diffusion, and linear transformation process at the bit level to achieve encryption. The chaotic map generated the random keys for these processes. Sameh et al. [14] considered the eight chaotic maps for key generation purposes. In their work, they performed hyperparameter tuning by taking into account the metaheuristic algorithms. Their findings show that the Gauss chaotic map outperforms in terms of computational complexity, while the circle map outperforms in random key generation. Kumar et al. [15] used the JAYA algorithm to adjust the settings of the 3D-CLM algorithm, focusing on entropy for creating random keys. The image matrix is then shuffled both row-wise and column-wise. A. Srivastava and S. Solanki [16] used the OBO algorithm to adjust the parameters of chaotic maps for creating random keys and rearranging the pixels based on a multi-objective function that includes entropy and correlation coefficient. Agarwal et al. [17] used the moth-flame optimization algorithm for key generation and applied chaotic logistics for encryption, using the objective function of the correlation coefficient. Krishnamoorthi et al. [18] employed the chaotic map for pseudorandom key generation purposes to secure the secret data.

From the previous studies, we found that most of the authors used the chaotic map to generate keys and for shuffling index purposes. Further, metaheuristic algorithms are used with chaotic maps for fine-tuning the parameters based on the objective function. However, in the encryption method, the substitution box plays an important role in exploiting the linear relationship between the secret and the encrypted image. Therefore, in this paper, we have designed an enhanced encryption method that generates optimal random keys, S-boxes, and shuffling indexes using the chaotic maps and metaheuristic SGO algorithm security enhancement.

3. Metaheuristic SGO Algorithm

In 2016, Suresh Satapathy and Anima Naik presented SGO, an optimization algorithm motivated by population-based human behavior. SGO draws inspiration from how people behave in social situations while working together to address a variety of challenging issues. In SGO, everyone contributes to finding a single solution, and the group works together to make that solution “fitter” by using random numbers repeatedly [19-20]. The two stages of SGO implementation are the acquiring phase and the improving phase. Both stages use basic evolutionary computation to modify the solutions that are chosen at random at the start using a technique called “greedy selection.” The search procedure starts with choosing the “leader” or “gbest” from the group of people who were chosen at random.

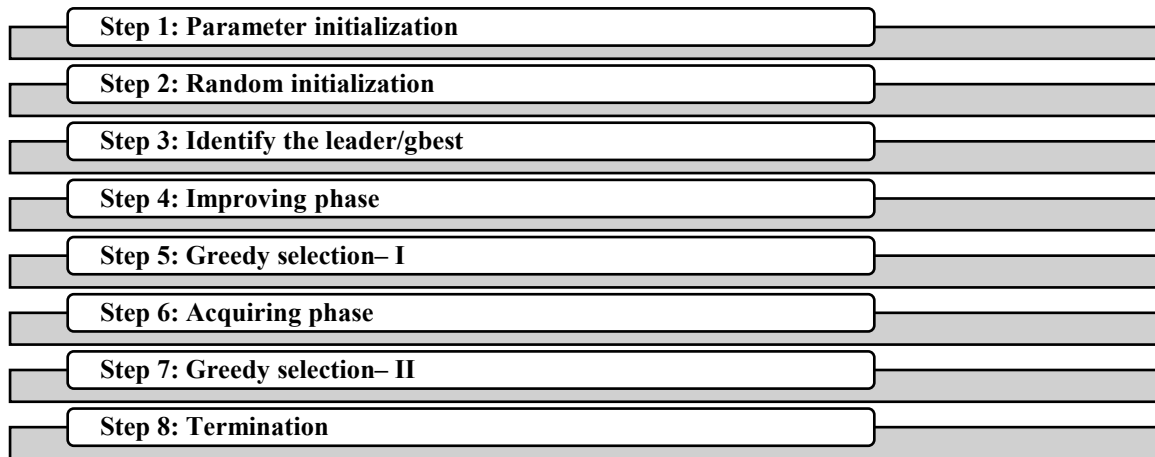


Figure 1 Steps of SGO Algorithm [20]

Step 1: Initialization of Parameters: Some of the most important parameters are the population size (P), the fitness function (F) that should be maximized or minimized, the number of iterations (N), the number of dimensions or decision variables (d), the constraint functions (G), and the decision variables' upper and lower bounds (Lb, Ub).

Step 2: Randomized Initialization: The initial population set is kept in an initialization vector and is initialized at random within the upper and lower bounds. The solution set is shown in each row of this vector, and each member in a row is a decision variable. The vector's size is determined by $P \times d$.

Step 3: Leader/gbest Identification: To find the appropriate fitness function value, the values of the decision factors in each row of the Initialization vector are loaded into the fitness function. It is done to check its feasibility. Every group member follows this process, and the person with the lowest level of fitness is selected as the leader or gbest. If two members have the same fitness value but different requirements, the one that meets the most constraints (the most viable solution) will be given priority.

Step 4: Improving Phase: The goal of this stage is to encourage algorithm exploration while maintaining connections to the leader's role. As one searches the area between the leader and the ideal candidate, it relates to an individual learning from the leader.

Step 5: Greedy Selection- I: After the improvement phase is over, the solution vector is substituted in the fitness function to verify each new solution for its matching fitness values.

Step 6: Acquiring Phase: Similar to the exploitation phase, the acquiring phase guarantees accuracy and convergence to the best solution in the world. The goal of this phase is to change the search group's population's positions about the best or the leader. For example, someone with less knowledge can learn from someone with more knowledge and teach someone with less knowledge.

Step 7: Greedy Selection - II - The solution vector is replaced in the fitness function to verify that the new solutions produced during the acquiring phase have the appropriate fitness values.

Step 8: Termination: In each iteration, the algorithm keeps looking for an improved option. Until the last iteration, the method continually displays the same solution. This serves as the fundamental termination criterion if no better solution can be found or if the global optimum is obtained. Other ways to end an algorithm include limiting the amount of function evaluations or establishing a goal solution that the algorithm will stop running when reached.

4. Proposed Image Encryption Method

This section presents the IE method is designed to protect the confidential images on the internet. The suggested IE method's primary innovation is that optimal random key, s-box, and shuffling index is generated by hyper-tune the parameters of the chaotic maps using the metaheuristic SGO algorithm. Thus, it is not possible for the attacker to reveal the confidential image without the information of optimal parameter values. Furthermore, the parameter value is not same for different images. Figure 2 depicts the flow diagram of the IE approach that has been suggested.

The recommended method entrusts the metaheuristic SGO algorithm with the secret image and chaotic maps. The SGO algorithm's primary goal is to find the optimum key generation, s-box, and shuffle index

by searching the solution space of the upper and lower limits of the 1-D CLM and CTM algorithms' parameters.

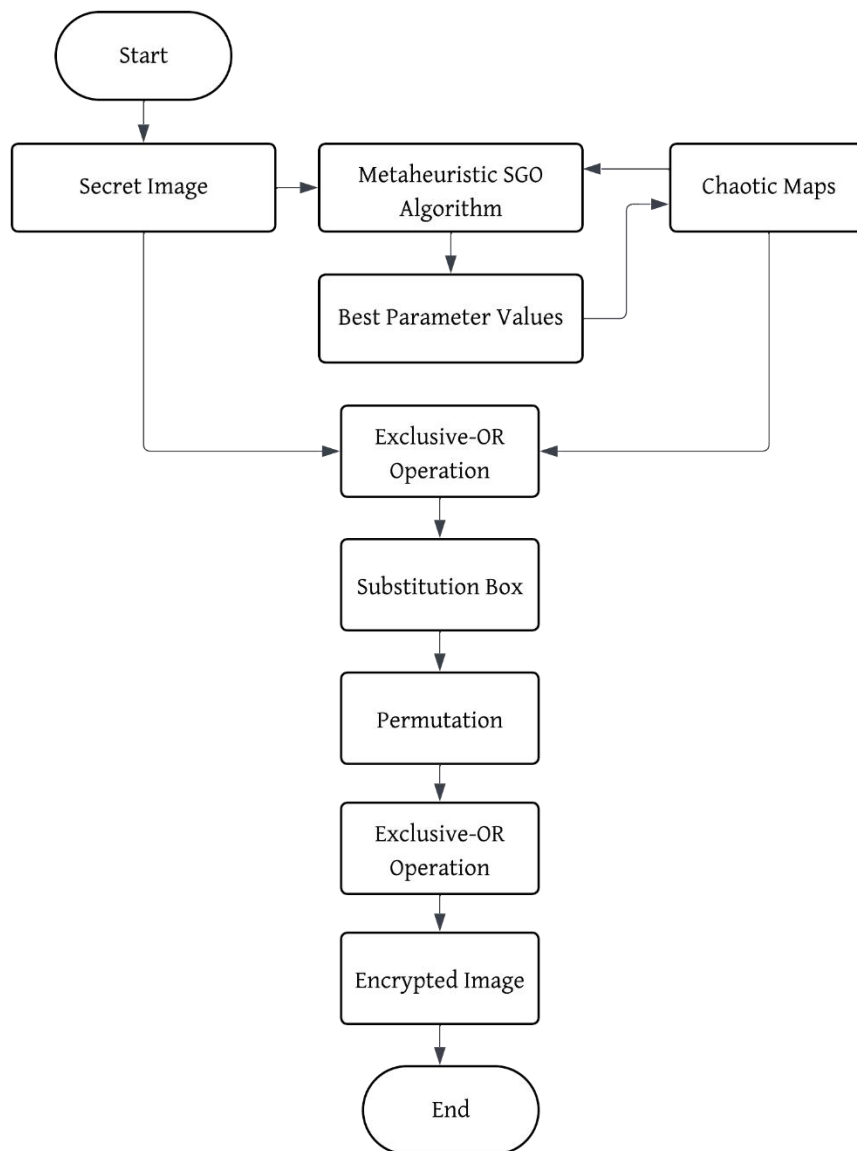


Figure 2 Proposed IE Method

First, the CLM algorithm's ideal parameter value is determined to produce the S-box. This takes into consideration the bijective function. This function helps to achieve the one-to-one mapping between input and output. After that, the population of the SGO algorithm is randomly initialized in the lower and upper bounds of the parameters of CLM and CTM. In this work, the dimension of each population is two. The first value of the population searches the CLM parameter value, whereas the second value searches the CTM. Afterwards, the objective function receives these values. The objective function generates a random key using the CLM algorithm. Followed by performing the exclusive-OR operation and substitution of the image pixels based on the S-box. Later on, an optimal shuffling index value is generated using the CTM algorithm to shuffle the image, and an exclusive-OR operation is performed for final encryption. Finally, objective function based on entropy, CC, and SSIM is evaluated between the secret image and the encrypted image using Eq. (1). This procedure is repeated a certain number of times to search the solutions space of the CLM and CTM algorithms, and optimal parameter values are determined. Based on these parameter values, the exclusive-OR, substitution based on s-box, shuffling the image based on shuffling index value, and exclusive-OR operation are performed to achieve the

encryption. The ideal parameter and the encrypted image values of the chaotic maps is communicated to the receiver for decryption purposes. On the receiver end, an inverse S-box, a random key, and a reverse shuffling index matrix are generated based on the optimal parameter value. After that, in the reverse order, exclusive-OR with a random key, rearrangement of the image pixel based on the reverse shuffling index matrix, passing through the inverse s-box, and exclusive-OR operation with a random key are performed to get the secret image.

$$OF = \left[\frac{E}{8} + (1 - |CC|) + (1 - SSIM) \right] / 3 \quad (1)$$

5. RESULTS AND DISCUSSION

This section provides the simulation results for the standard dataset by evaluating the various security parameters for the presented method [21]. These security parameters are considered to show the effectiveness of the suggested IE method over the recent existing methods. In this work, ten grayscale images were considered, and MATLAB 2018a software was used. Next, the proposed IE method was coded and simulated on an Intel Core i7-7500 CPU with 8GB memory. The detailed description of the simulation setup configuration, security analysis, comparative analysis, and discussion is given in this section.

5.1 Setup Configuration for Metaheuristic SGO Algorithm

This section shows the setup configuration for the SGO algorithm is considered to find the best parameter value of CLM and CTM algorithm for random key, s-box, and shuffling index generation purposes. Table 1 shows the parameter related to SGO, objective function, and lower and upper bound value of the CLM and CTM algorithm.

Table 1 Simulation Setup Configuration of SGO Algorithm

Parameter	Values
S-Box Value	[0-255]
CLM	[0-1], [3.90-3.99]
CTM	[1.9-2]
SGO _{Pop}	10
SGO _{dim}	2
SGO _{iteration}	50
SGO _{Objectivefunction}	E, CC, SSIM

5.2 Security Analysis

In this section, several performance parameters are evaluated to measure the security of the proposed method. The parameters considered in this article are the chi-square test, entropy, CC, SSIM, MSE, PSNR, maximum deviation, and NPCR.

- **Chi-Square Test Analysis:** This analysis is performed to measure the uniformity of the encrypted image histogram to secure the encryption method against statistical attacks performed by attackers [22]. The chi-square value is determined using Eq. (2-3). In the encryption method, a low value of chi-square indicates a uniform distribution of the histogram [23]. Table 2 shows the histogram distribution analysis based on the chi-square test. The result indicates that the proposed IE method achieves the chi-square value in the range of 227-277, which is less than the reference value (293.83) of the encryption method.

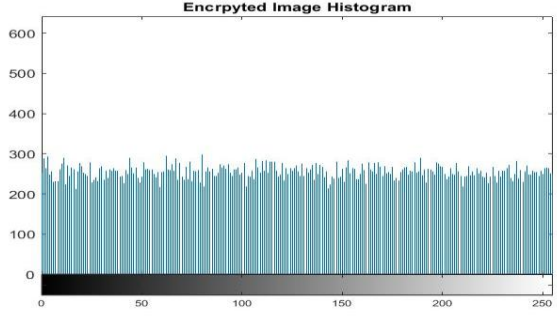
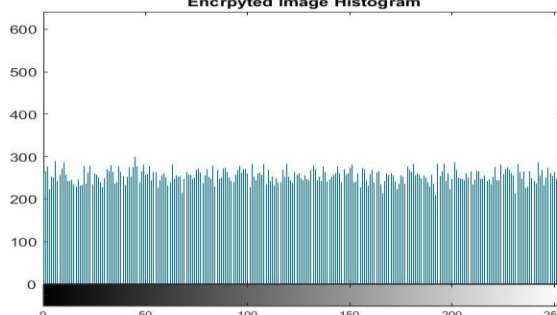
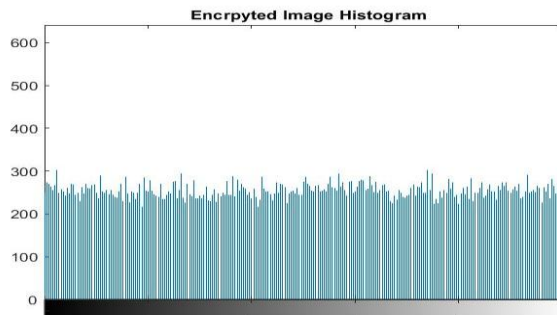
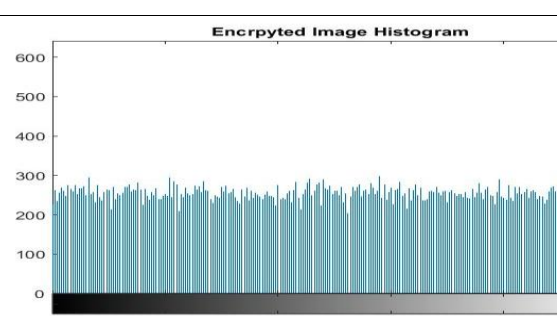
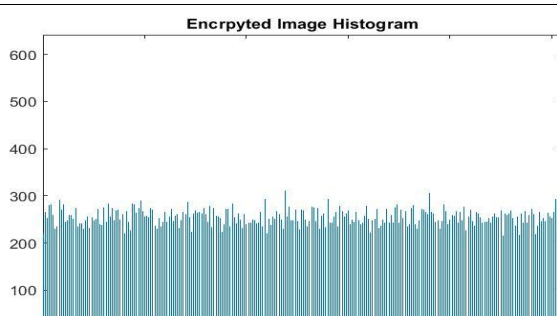
$$\chi^2 = \sum_{i=1}^{255} \frac{(f_i - \varepsilon)^2}{\varepsilon} \quad (2)$$

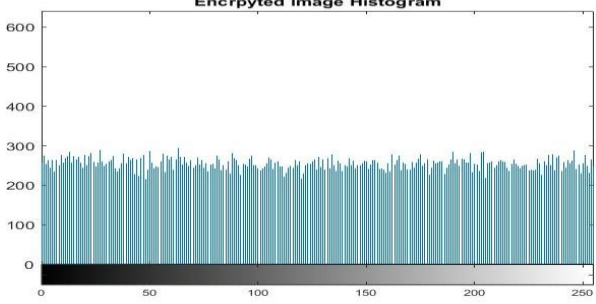
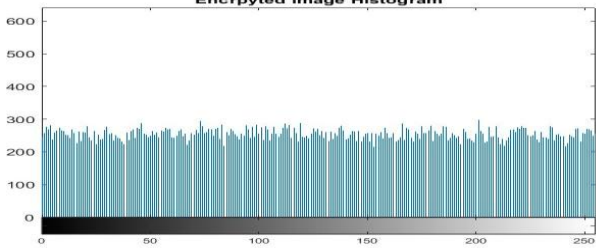
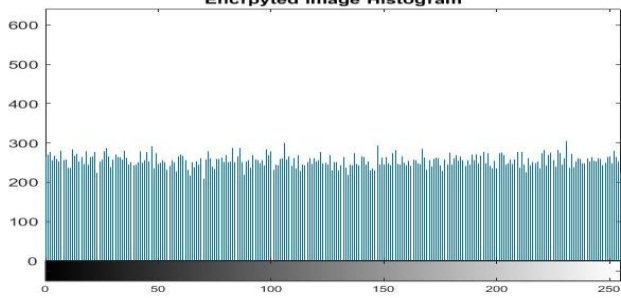
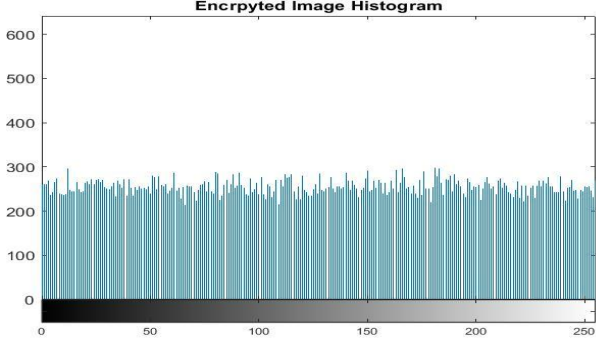
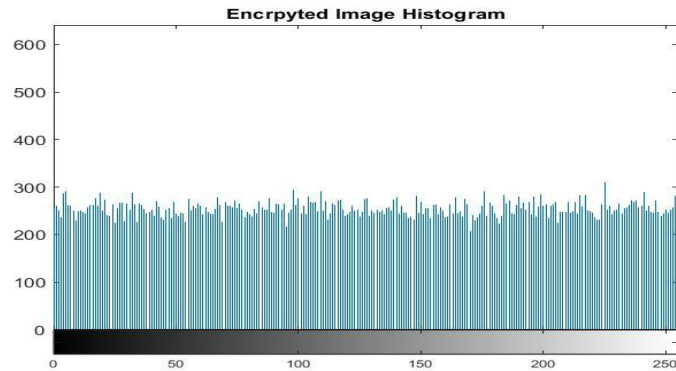
$$\varepsilon = \frac{H \times W}{256} \quad (3)$$

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.

Table 2 Histogram Distribution Analysis based on Chi-Square Test

Images	Encrypted Image Histogram Distribution	Chi-Square Value
--------	--	------------------

I_1	 <p>The histogram for I_1 shows a uniform distribution of pixel intensities across the 0-255 range. The y-axis represents frequency from 0 to 600, and the x-axis represents intensity from 0 to 255. The bars are teal, and a grayscale color bar is at the bottom.</p>	254
I_2	 <p>The histogram for I_2 shows a uniform distribution of pixel intensities across the 0-255 range. The y-axis represents frequency from 0 to 600, and the x-axis represents intensity from 0 to 255. The bars are teal, and a grayscale color bar is at the bottom.</p>	247
I_3	 <p>The histogram for I_3 shows a uniform distribution of pixel intensities across the 0-255 range. The y-axis represents frequency from 0 to 600, and the x-axis represents intensity from 0 to 255. The bars are teal, and a grayscale color bar is at the bottom.</p>	253
I_4	 <p>The histogram for I_4 shows a uniform distribution of pixel intensities across the 0-255 range. The y-axis represents frequency from 0 to 600, and the x-axis represents intensity from 0 to 255. The bars are teal, and a grayscale color bar is at the bottom.</p>	258
I_5	 <p>The histogram for I_5 shows a uniform distribution of pixel intensities across the 0-255 range. The y-axis represents frequency from 0 to 600, and the x-axis represents intensity from 0 to 255. The bars are teal, and a grayscale color bar is at the bottom.</p>	277

I_6	 <p>The histogram for I_6 shows a uniform distribution of pixel intensities across the range of 0 to 255. The y-axis represents frequency, ranging from 0 to 600. The x-axis represents pixel intensity, ranging from 0 to 255. The bars are teal, and the distribution is relatively flat, indicating good encryption.</p>	236
I_7	 <p>The histogram for I_7 shows a uniform distribution of pixel intensities across the range of 0 to 255. The y-axis represents frequency, ranging from 0 to 600. The x-axis represents pixel intensity, ranging from 0 to 255. The bars are teal, and the distribution is relatively flat, indicating good encryption.</p>	247
I_8	 <p>The histogram for I_8 shows a uniform distribution of pixel intensities across the range of 0 to 255. The y-axis represents frequency, ranging from 0 to 600. The x-axis represents pixel intensity, ranging from 0 to 255. The bars are teal, and the distribution is relatively flat, indicating good encryption.</p>	227
I_9	 <p>The histogram for I_9 shows a uniform distribution of pixel intensities across the range of 0 to 255. The y-axis represents frequency, ranging from 0 to 600. The x-axis represents pixel intensity, ranging from 0 to 255. The bars are teal, and the distribution is relatively flat, indicating good encryption.</p>	262
I_{10}	 <p>The histogram for I_{10} shows a uniform distribution of pixel intensities across the range of 0 to 255. The y-axis represents frequency, ranging from 0 to 600. The x-axis represents pixel intensity, ranging from 0 to 255. The bars are teal, and the distribution is relatively flat, indicating good encryption.</p>	218

- **Entropy Analysis:** The degree of unpredictability or randomness in the data is assessed using the entropy analysis [24]. It is determined by using Equation (4).

$$H(m) = \sum_{i=0}^{2^N-1} p(e_i) \times \log_2 \frac{1}{p(e_i)}$$

(4)

To ensure that the pixel intensities in the encrypted image are distributed equally, a high entropy value is necessary during the encryption process. As a result, it is difficult for the attacker to identify any patterns or determine the distribution of pixels. Table 3 shows the security analysis based on the entropy parameter. The result indicates that the proposed method achieves entropy in the range of 7.9962-7.9975. This value is very near to the ideal value of eight, which is required in the encryption [25].

Table 3 Security Analysis based on Entropy Parameter

Images	Entropy
I_1	7.9971
I_2	7.9972
I_3	7.9971
I_4	7.9970
I_5	7.9969
I_6	7.9972
I_7	7.9971
I_8	7.9973
I_9	7.9970
I_{10}	7.9974

- **CC Analysis:** This analysis is performed to measure the correlation among adjacent pixels of secret and encrypted images. A favorable encryption method provides efficient protection by reducing the correlation between them to near zero value [26]. Eq. (5-8) determines its value, which ranges from -1 to 1, while the ideal value of CC in encryption is zero [27].

$$r_{uv} = \frac{|cov(uv)|}{\sqrt{D(u)} \times \sqrt{D(v)}} \quad (5)$$

$$cov(uv) = \frac{\sum_{j=1}^M (u_j - E(u))((v_j - E(v)))}{M}$$

(6)

$$E(u) = \frac{\sum_{j=1}^M u_j}{M} \quad (7)$$

$$D(u) = \frac{\sum_{j=1}^M (u_j - E(u))^2}{M} \quad (8)$$

Where cov denotes the covariance between the secret and the encrypted image. D(u) and D(v) denote the variance of the secret and encrypted images. Furthermore, M represents the quantity of neighboring pixels. E(u) stands for the expectations of encrypted and secret images. The suggested IE method's CC analysis is shown in Table 4. The findings show that the suggested approach achieves a low correlation coefficient, which is acceptable for encryption and very close to the optimal value.

Table 4 Security Analysis based on CC Parameter

Images	CC
I_1	-0.0014
I_2	0.0018
I_3	0.0025
I_4	0.0068
I_5	-0.0042
I_6	-8.5538e-04
I_7	-0.0030

I_8	-5.1761e-04
I_9	-0.0016
I_{10}	9.0464e-04

- **SSIM Analysis:** This analysis is done to measure the structure similarity among the images by considering the factors (structural information, luminance, and contrast) based on human visual perception [28]. In the encryption method, a low value of SSIM defines the encryption method as effectively obscuring the structural details [29]. It is determined using Eq. (9). The result indicates that the suggested method achieves the SSIM value near to zero (0.0056-0.0115).

$$SSIM(SE) = \frac{(2\mu_S\mu_E + C_1)(2\sigma_{SE} + C_2)}{(\mu_S^2 + \mu_E^2 + C_1)(\sigma_S^2 + \sigma_E^2 + C_2)} \quad (9)$$

In the above equation, $\mu_S\mu_E$ represents the secret and encrypted image's average value. σ_{SE} represents the covariance.

Table 5 Security Analysis based on SSIM Parameter

Images	SSIM
I_1	0.0115
I_2	0.0091
I_3	0.0113
I_4	0.0109
I_5	0.0075
I_6	0.0098
I_7	0.0056
I_8	0.0110
I_9	0.0097
I_{10}	0.0099

- **MSE and PSNR Analysis:** With the secret image, these parameters calculate the overall noise in the encrypted image. To calculate the MSE and PSNR, Eq. (10-11) [30–31] is used.

$$MSE = \frac{1}{WH} \sum_{i=1}^W \sum_{j=1}^H [S_{ij} - E_{ij}]^2 \quad (10)$$

$$PSNR(in\ dB) = 10 \log_{10} \frac{P^2}{MSE} \quad (11)$$

It is necessary for the encryption image to have a low PSNR (ideally 0) between the secret and encrypted images. The security evaluation of the proposed IE approach employing the MSE and PSNR parameters is shown in Table 6. The result indicates that the MSE and PSNR values are in the ranges of 248.2939-8.8598e+03 and 8.6566-24.1811dB, respectively. The low value of the PSNR reflects that the encrypted image contains a high level of noise, and it is difficult for the attacker to retrieve the secret image.

Table 6 Security Analysis based on MSE and PSNR Parameter

Images	MSE	PSNR (in dB)
I_1	3.6117e+03	12.5537
I_2	2.6822e+03	13.8458
I_3	3.5803e+03	12.5917
I_4	3.3477e+03	12.8834
I_5	736.2930	19.4603
I_6	3.7812e+03	12.3545
I_7	248.2939	24.1811

I_8	4.6531e+03	11.4534
I_9	3.8490e+03	12.2773
I_{10}	8.8598e+03	8.6566

- **Maximum Deviation Analysis:** The purpose of this study is to estimate the total difference between the histograms of confidential and secret images [32]. Eq. (12) is used to calculate it. The encryption technique requires a high MD value, indicating that the encrypted image differs significantly from the secret image. The MD analysis is shown in Table 7. The result shows that the MD score varies between 65536 and 65236, respectively. This means that the suggested method can handle the large difference in the encryption image.

$$MD = \frac{H_0 - H_{L-1}}{2} + \sum_{i=1}^{L-2} H_i$$

(12)

In Equation (17), H_i is the difference in the histograms of the images, and L is the image's total intensity level. Its value in the greyscale images ranges from 0 to 255. According to Table 7, the greatest deviation is very close to the optimal value required for the encrypted approach.

Table 7 Security Analysis based on Maximum Deviation Parameter

Images	MD
I_1	42652
I_2	45681
I_3	5.5593e+04
I_4	37498
I_5	58975
I_6	61342
I_7	8.0394e+04
I_8	70353
I_9	55943
I_{10}	67652

- **NPCR Analysis:** To verify that the encryption technique is adaptable to the differential attack, NPCR analysis is performed. In this research, we calculate the number of pixels in the encrypted image whose values change when the secret image changes slightly [34]. To accomplish this analysis, two encrypted images are generated. The first encrypted image is without any change in the secret image whereas the second encrypted image with a minor change in the secret image. It is determined using Eq. (13-14).

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

(13)

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

(14)

Whereas, C_1 and C_2 represent two cipher images that were encrypted from the identical plaintext image with a one-bit modification. Table 8 indicates that the proposed method achieves high NPCR value.

Table 8 Security Analysis based on NPCR Parameter

Images	NPCR (%)
I_1	99.60785
I_2	99.60175

I_3	99.59259
I_4	99.63074
I_5	99.63531
I_6	99.60938
I_7	99.58801
I_8	99.62158
I_9	99.60175
I_{10}	99.58191

- **Execution Time Analysis:** This analysis is done to measure the total time spent for the proposed method to encrypt the secret image [35]. It is measured in seconds. Table 9 shows the execution time analysis for the different images. The results indicate that the proposed IE method takes 20.054789-26.459394 seconds to encrypt the secret images. Further, we have analyzed that the maximum time is spent in the fine-tuning of the parameters of the chaotic maps using the SGO algorithm.

Table 9 Execution Time Analysis for Proposed IE Method

Images	Execution Time (in Seconds)
I_1	21.283892
I_2	26.459394
I_3	24.356926
I_4	20.054789
I_5	24.096446
I_6	21.437874
I_7	21.144685
I_8	24.666482
I_9	22.491049
I_{10}	23.218535

5.3 Comparative Analysis

This section presents the effectiveness of the proposed IE method over the existing methods using the three security parameters. To achieve this objective, the parameters' average value is calculated and contrasted with the suggested approaches. The comparative analysis based on the entropy test findings is shown in Table 10. Compared to the earlier methods, which ranged from 7.968 to 7.996, the proposed approach provides the greatest average entropy value of 7.9971. This reflects that the proposed method has high randomness in the encrypted image.

Table 10 Comparison of Entropy Test Results

Methods	Entropy
Al-Hyari et al. [9]	7.888
S. A. Gebereslassie and B. K. Roy [10]	7.968
H. Çelik and N. Doğan [11]	7.994
Sameh et al. [14]	7.996
Kumar et al. [15]	7.996
Proposed Method	7.9971

The comparison of the results of the NPCR test is shown in Table 11. According to the results, the proposed strategy generates a lower NPCR than the other approaches and is superior than S. A.

Gebereselassie and B. K. Roy [10] and Kumar et al. [15]. This shows that the suggested way makes a big difference in the encrypted pixels but only a small difference in the secret image's pixel value.

Table 11 Comparison of NPCR Test Results

Methods	NPCR (%)
Al-Hyari et al. [9]	99.608
S. A. Gebereselassie and B. K. Roy [10]	97.067
H. Çelik and N. Doğan [11]	99.609
Sameh et al. [14]	99.629
Kumar et al. [15]	99.272
Proposed Method	99.607

Lastly, the comparison analysis based on PSNR test results is shown in Table 12. According to the results, the proposed method outperforms Al-Hyari et al. [9] and Kumar et al. [15] in terms of PSNR while achieving a lower value than the other methods currently in use. This suggests that a high level of noise is achieved in the encrypted image using the suggested approach. As a result, the attacker finds it challenging to reveal the confidential information.

Table 12 Comparison of PSNR Test Results

Methods	PSNR (in dB)
Al-Hyari et al. [9]	19.603
S. A. Gebereselassie and B. K. Roy [10]	9.2357
H. Çelik and N. Doğan [11]	7.9561
Sameh et al. [14]	-
Kumar et al. [15]	14.293
Proposed Method	14.026

5.4 DISCUSSION

The proposed IE technique gets an appropriate value for the security parameter, which is needed in the encryption method to protect the secret images. When compared to earlier approaches, the suggested approach yields low PSNR and near-optimal entropy and NPCR values. Moreover, the primary advantage of the suggested IE technique is that it is hard for attackers to produce the same ideal random key, s-box, and shuffling index value for different images until they have information about optimal parameter values, which is determined using the SGO algorithm. On the other hand, the proposed IE method takes a higher execution time due to searching for the best parameter values for generating random keys, s-boxes, and shuffling indexes using SGO. Additionally, several parameters must be communicated to the receiver in order to decrypt the encrypted image.

6. CONCLUSION AND FUTURE SCOPE

In this paper, we have presented an IE method that achieves the desired security due to utilizing the metaheuristic SGO algorithm to fine-tune the parameters of the chaotic maps to achieve the optimal random key, S-box, and shuffling index matrix. In this research, 1-D CLM is employed for s-box and key generation purposes, whereas CTM for shuffling the index matrix. Further, the proposed method demonstrates for the standard dataset that it achieves the desired security parameter value required in image encryption and works well over the existing methods. Therefore, different applications can utilize the proposed IE method to secure secret images on the open network from attackers. In the future, we can explore high-dimensional chaotic maps to design an image encryption method. Moreover, we can design a multi-objective function that utilizes metaheuristic algorithms to improve various security characteristics.

REFERENCES

- [1] M. Es-Sabry et al., "An efficient 32-bit color image encryption technique using multiple chaotic maps and advanced ciphers," *Egyptian Informatics Journal*, vol. 25, p. 100449, Feb. 2024, doi: 10.1016/j.eij.2024.100449. Available: <https://doi.org/10.1016/j.eij.2024.100449>
- [2] 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. Available: <https://doi.org/10.1007/s11831-018-9298-8>
- [3] H. Kolivand, S. F. Hamood, S. Asadianfam, and M. S. Rahim, "RETRACTED ARTICLE: 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>
- [4] 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. Available: <https://doi.org/10.1155/2021/5012496>
- [5] 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>
- [6] 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>
- [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] R. B. Naik and U. Singh, "A review on applications of chaotic maps in Pseudo-Random Number Generators and Encryption," *Annals of Data Science*, vol. 11, no. 1, pp. 25–50, Jan. 2022, doi: 10.1007/s40745-021-00364-7. Available: <https://doi.org/10.1007/s40745-021-00364-7>
- [9] A. Al-Hyari, M. Abu-Faraj, C. Obimbo, and M. Alazab, "Chaotic Hénon–Logistic Map Integration: A powerful approach for safeguarding digital images," *Journal of Cybersecurity and Privacy*, vol. 5, no. 1, p. 8, Feb. 2025, doi: 10.3390/jcp5010008. Available: <https://doi.org/10.3390/jcp5010008>
- [10] S. A. Gebereselassie and B. K. Roy, "Comparative analysis of image encryption based on 1D maps and their integrated chaotic maps," *Multimedia Tools and Applications*, vol. 83, no. 27, pp. 69511–69533, Jan. 2024, doi: 10.1007/s11042-024-18319-4. Available: <https://doi.org/10.1007/s11042-024-18319-4>
- [11] 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. Available: <https://doi.org/10.1007/s11042-023-16215-x>
- [12] K. M. Hosny, Y. M. Elnabawy, A. M. Elshewey, S. M. Alhammad, D. S. Khafaga, and R. Salama, "New method of colour image encryption using triple chaotic maps," *IET Image Processing*, vol. 18, no. 12, pp. 3262–3276, Jun. 2024, doi: 10.1049/ipr2.13171. Available: <https://doi.org/10.1049/ipr2.13171>
- [13] H. Wen et al., "Security analysis of a color image encryption based on bit-level and chaotic map," *Multimedia Tools and Applications*, vol. 83, no. 2, pp. 4133–4149, May 2023, doi: 10.1007/s11042-023-14921-0. Available: <https://doi.org/10.1007/s11042-023-14921-0>
- [14] 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>
- [15] 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>
- [16] A. Srivastava and S. Solanki, "Optimized Image Encryption Model based on Hybridization of Chaotic Maps with Metaheuristic OBO Algorithm," in *Advances in intelligent systems research/Advances in Intelligent Systems Research*, 2025, pp. 107–116. doi: 10.2991/978-94-6463-700-7_10. Available: https://doi.org/10.2991/978-94-6463-700-7_10
- [17] A. Aggarwal, E. Awasthi, D. Kukreja, J. Kedia, and I. Bala, "Modified moth flame optimization and logistic chaotic map integration for image encryption," *International Journal of Systems Assurance Engineering and Management*, vol. 16, no. 2, pp. 785–804, Dec. 2024, doi: 10.1007/s13198-024-02669-1. Available: <https://doi.org/10.1007/s13198-024-02669-1>
- [18] S. Krishnamoorthi, R. K. Dhanaraj, and S. H. Islam, "CCM-PRNG: Pseudo-random bit generator based on cross-over chaotic map and its application in image encryption," *Multimedia Tools and Applications*, vol. 83, no. 34, pp. 80823–80846, Mar. 2024, doi: 10.1007/s11042-024-18668-0. Available: <https://doi.org/10.1007/s11042-024-18668-0>
- [19] J. J. Jena and S. C. Satapathy, "A new adaptive tuned Social Group Optimization (SGO) algorithm with sigmoid-adaptive inertia weight for solving engineering design problems," *Multimedia Tools and Applications*, vol. 83, no. 1, pp. 3021–3055, Aug. 2021, doi: 10.1007/s11042-021-11266-4. Available: <https://doi.org/10.1007/s11042-021-11266-4>
- [20] A. K. V. K. Reddy and K. V. L. Narayana, "Social group optimization: a-state-of-the-art review," *Multimedia Tools and Applications*, Feb. 2025, doi: 10.1007/s11042-025-20607-6. Available: <https://doi.org/10.1007/s11042-025-20607-6>
- [21] "SIPI Image Database." Available: <https://sipi.usc.edu/database/>

- [22] L. Huang and H. Gao, "Multi-Image encryption algorithm based on novel spatiotemporal chaotic system and fractal geometry," *IEEE Transactions on Circuits and Systems I Regular Papers*, vol. 71, no. 8, pp. 3726–3739, Jun. 2024, doi: 10.1109/tcsi.2024.3407809. Available: <https://doi.org/10.1109/tcsi.2024.3407809>
- [23] 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: 10.3390/e24101344. Available: <https://doi.org/10.3390/e24101344>
- [24] T. Umar, M. Nadeem, and F. Anwer, "Chaos based image encryption scheme to secure sensitive multimedia content in cloud storage," *Expert Systems With Applications*, vol. 257, p. 125050, Aug. 2024, doi: 10.1016/j.eswa.2024.125050. Available: <https://doi.org/10.1016/j.eswa.2024.125050>
- [25] 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. Available: <https://doi.org/10.1007/s11042-022-12595-8>
- [26] A. P. Kari, A. H. Navin, A. M. Bidgoli, and M. Mirnia, "A new image encryption scheme based on hybrid chaotic maps," *Multimedia Tools and Applications*, vol. 80, no. 2, pp. 2753–2772, Sep. 2020, doi: 10.1007/s11042-020-09648-1. Available: <https://doi.org/10.1007/s11042-020-09648-1>
- [27] P. Ding, P. Geng, and W. Hu, "A new controllable multi-wing chaotic system: applications in high-security color image encryption," *The Journal of Supercomputing*, vol. 81, no. 1, Oct. 2024, doi: 10.1007/s11227-024-06635-3. Available: <https://doi.org/10.1007/s11227-024-06635-3>
- [28] B. Harjo and D. Setiadi, "Improved Color Image Encryption using Hybrid Modulus Substitution Cipher and Chaotic Method," *International Journal of Intelligent Engineering and Systems*, vol. 14, no. 2, pp. 157–166, Feb. 2021, doi: 10.22266/ijies2021.0430.14. Available: <https://doi.org/10.22266/ijies2021.0430.14>
- [29] H. Shi, M. Ji'e, C. Li, D. Yan, S. Duan, and L. Wang, "A novel image encryption algorithm based on 2D Self-Coupling Sine Map," *International Journal of Bifurcation and Chaos*, vol. 32, no. 15, Dec. 2022, doi: 10.1142/s0218127422502339. Available: <https://doi.org/10.1142/s0218127422502339>
- [30] A. Ullah et al., "An efficient lightweight image encryption scheme using multichaos," *Security and Communication Networks*, vol. 2022, pp. 1–16, Oct. 2022, doi: 10.1155/2022/5680357. Available: <https://doi.org/10.1155/2022/5680357>
- [31] W. Alexan, K. Hosny, and M. Gabr, "A new fast multiple color image encryption algorithm," *Cluster Computing*, vol. 28, no. 5, Apr. 2025, doi: 10.1007/s10586-024-04919-0. Available: <https://doi.org/10.1007/s10586-024-04919-0>
- [32] J. Arif et al., "A novel chaotic Permutation-Substitution image encryption scheme based on logistic map and random substitution," *IEEE Access*, vol. 10, pp. 12966–12982, Jan. 2022, doi: 10.1109/access.2022.3146792. Available: <https://doi.org/10.1109/access.2022.3146792>
- [33] 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: 10.3390/e24101344. Available: <https://doi.org/10.3390/e24101344>
- [34] P. Kumari and B. Mondal, "Lightweight image encryption algorithm using NLFSR and CBC mode," *The Journal of Supercomputing*, vol. 79, no. 17, pp. 19452–19472, May 2023, doi: 10.1007/s11227-023-05415-9. Available: <https://doi.org/10.1007/s11227-023-05415-9>