International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 10 Issue: 10 | Oct - 2026 SJIF Rating: 8.659 ISSN: 2582-3930

# Image Encryption Method based on Chaotic Maps and Metaheuristic Walrus Optimization Algorithm

**Balwinder Singh[1], Shruti Bansal[2], Kulwinder Singh[3]**
[1,2,3] Bhai Maha Singh College of Enginnering, Sri Muktsar Sahib

**Abstract:** In this paper, we have designed an optimized encryption method based on the chaotic map and metaheuristic algorithm. The chaotic maps (1-D logistic map, cubic map, and tent map) were used for S-box, random key, and shuffling index generation purposes, and a metaheuristic walrus algorithm was used for finding the best input parameter values. Furthermore, a multi-objective function was designed to enhance the multiple security characteristics. The evaluation of the proposed method was done on the standard dataset. Next, we have evaluated the performance of the proposed method using the qualitative and quantitative methods. In the qualitative method, the visual quality of the encrypted image was evaluated, and its validation is done using the chi-square test. On the other hand, in the quantitative analysis, the encrypted image characteristics were assessed using the various parameters, namely, entropy, correlation coefficient (CC), structural similarity index measure (SSIM), and number of pixel change rate (NPCR). The result indicates that the proposed method outperforms the existing approaches and achieves the entropy value of 7.997 near the ideal value of 8, the NPCR value of 99.604%, and the PSRN value of 14.034 dB.

**Keywords:** Chaotic map, Cubic Map, Image Encryption, Logistic Map, Metaheuristic, Multi-Objective Function, Tent Map, Walrus Optimization

## 1. Introduction

In recent years, digital data communication using images has gained much popularity and is being used in several areas like medical, military, and finance. Earlier, conventional methods such as AES, DES, 3DES, and Blowfish were used to encrypt images [1]. These methods process images several times in block form to encrypt them. The encryption is done in several rounds. The basic block size can be 64 or 124 bits, and the round size can be 10, 12, or 14. In images, the correlation among pixels is generally higher because it contains several numbers of pixels. Due to this, encryption of images requires more computation time. Moreover, there is a risk associated with these blocks being attacked by differential attacks. The reason for this is that the same method is used for encrypting every block, and it doesn't depend on others [2]. Therefore, the conventional encryption methods do not provide enough security and take a long computation time. The chaotic map has gained popularity over traditional methods for data encryption because it is highly sensitive to input parameters, meaning that a small variation in the input can significantly alter many pixels in the encrypted image [3-4].

Al-Hyari et al. [5], used two chaotic maps named the logistic map and the Henon map. The logistic map was used for permutation, and the Henon map for generating a key. S. A. Gebereselassie and B. K. Roy [6] studied the suitability of 1D chaotic maps or an integrated approach for encryption tasks. This research considered several maps like sine, logistic, tent, and cubic. The experimental analysis showed that 1D chaotic maps performed better compared to integrated approaches. H. Çelik and N. Doğan [7], developed an encryption approach using an affine transformation on a secret image. After that, the chaotic map was used to produce an S-box for encryption. Hosny et al. [8], used three types of chaotic maps (Hénon, Lorenz, and logistic) for scrambling and diffusing the secret color image. These maps were used to produce matrices for scrambling and diffusion for RGB planes. Wen et al. [9], developed an encryption method at the bit level using permutation, linear transformation, and diffusion. For these processes, the random keys were generated using chaotic maps. Sameh et al. [10], used eight types of chaotic maps for generating keys. The research also used a metaheuristic algorithm to perform hyperparameter tuning. The experimental results demonstrated that the Gauss chaotic map performed better as compared to other maps in terms of computational complexity. On the other hand, the circle map technique performed better for generating random keys. Kumar et al. [11], utilized the metaheuristic JAYA algorithm for adjusting the 3D-CLM algorithm's settings. It focused on generating random keys based on entropy. The image matrix is then shuffled column- and row-wise. A. Srivastava and S. Solanki [12], utilized

the metaheuristic OOBO algorithm for adjusting chaotic maps' parameters for generating random keys. The algorithm is also used to rearrange the image pixels based on the multi-objective fitness function. The fitness function uses the correlation coefficient and entropy.

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

The remaining paper is divided into four sections. Section 2 provides an overview of the chaotic map and metaheuristic walrus optimization algorithm. Section 3 illustrates the proposed image encryption method. Section 4 shows the results and analysis. Finally, the paper is concluded in Section 5.

## 2. Chaotic Maps and Metaheuristic Walrus Optimization Algorithm

### 2.1 Chaotic Maps

In this study, three chaotic maps were used. The chaotic logistic map was used to generate the s-box, the chaotic cubic map was used to generate the random key to perform an exclusive OR with the secret image pixels, and the chaotic tent map was used to generate the index value for shuffling the image matrix. This section provides an overview of these chaotic maps [11-12].

- **Cubic Map:** In the cubic map, the next state is determined using the present state and rho value. It is determined using Eq. (1).

$$X_{n+1} = \rho X_n(1 - X_n^2) \quad (1)$$

In Eq. (1), the $x_n, x_{n+1}$represents the present and next state and its value vary in between 0-1. On the other hand, $\rho$ denotes the control parameter and its value varies in between 2-2.598.

- **Chaotic Logistic Map:** Eq. (2) is used to determine the next state from the present state and control parameter ($\mu$).

$$x_n = \mu x_n(1 - x_n) \quad (2)$$

In Eq. (2), 0< $x$ <1 and $\mu$ = {3.57-3.99}.

- **Chaotic Tent Map:** The CTM is determined using Eq. (3-4) [1].

$$x_{n+1} = f(x_n, \mu) \quad (3)$$

$$f(x_n, \mu) = \begin{cases} f(x_n, \mu) = \mu x_n & if\ (x_i < 0.5) \\ f(x_n, \mu) = \mu(1 - x_n) & Otherwise \end{cases} \quad (4)$$

In Eq. (3-4), $x_i, x_{i+1}$represents the present and next state. On the other hand, $\mu$ denotes the control parameter and in the range of 1.9-2 for image encryption.

In above Equations (1-4), the control parameter values were explored using the walrus optimization algorithm. A detailed description of this algorithm is given below.

### 2.2 Metaheuristic Walrus Optimization Algorithm

It is a population-based algorithm that is inspired by the social and survival behaviours of walruses. Each walrus in the WaOA represents a solution to the problem [13]. So, the walrus position in the search space decides the problem variables' candidate values. The walrus optimization has three phases, as explained below.

**Phase 1: Feeding strategy (exploration):** The walruses eat more than sixty types of species of marine organisms. These include soft corals, sea cucumbers, tube worms, various mollusks, tunicates, and shrimp. But walruses mostly prefer benthic bivalve mollusks and they hunt them by grazing on the ocean floor. The walruses use their sensitive vibrissae and active flipper movements to find mollusks. In the process of searching for food, the strongest walrus (with the longest tusk) guides the other walruses to discover food. Here, the longest tusk in walruses can be represented with the objective function's quality for solutions. As a result, a solution with the best fitness value is considered the strongest walrus. This behaviour of walruses results in different areas of the search space that enhance the WaOA's exploration capabilities while searching globally.

**Phase 2: Migration:** As the air starts to warm in late summer, walruses migrate to rocky beaches or outcrops. This migration process is utilized in WaOA for guiding the walruses to find suitable places.

**Phase 3: Escaping and Fighting against Predators (exploitation):** Walruses are normally attacked by killer whales and polar bears. The walruses' strategies for escaping and combating these predators cause them to shift their position relative to their current location. This behaviour of walruses helps to improve the exploitation power of WaOA in local search around candidate solutions in the problem-solving space.

Using these phases, the metaheuristic walrus optimization algorithm searches the solution space of the parameters of the chaotic map based on the objective function and provides the best value in the output.

### 3. Proposed Image Encryption Method

Figure 1 presents the flowchart of the proposed image encryption method. This method utilizes three 1-D chaotic maps for three purposes: generating random keys, creating s-boxes, and generating image shuffling indices. The image database was collected from USC SIPI Image Database [14]. The working of the proposed method is given below.

Initially, the CLM algorithm's ideal parameter value was determined to produce the S-box. The bijective function was used to generate the s-box. This function helps to achieve a one-to-one mapping between input and output. After that, the secret image was read, and Walrus optimization was initialized. Thereafter, the s-box, secret image, and walrus optimization parameter were given to the OOBO algorithm. In this algorithm, the initial parameter value of the cubic map and tent map was generated. The population was randomly generated for the control parameter of the cubic map. The secret image, cubic map, s-box, and tent map parameters were given to the objective function. In this objective function, an exclusive-OR operation was performed between the secret image and the random key generated using the cubic map. After that, it was passed through the S-box. Finally, the image matrix was shuffled based on the tent map shuffled index value. Finally, the objective function based on entropy, CC, and SSIM was evaluated between the secret image and the encrypted image using Eq. (5).

$$OF = \left[\frac{E}{8} + (1 - |CC|) + (1 - SSIM)\right]/3 \quad (5)$$

This procedure is repeated a certain number of times to search the solution space based on the iteration parameter, and optimal parameter values are determined. Based on these parameter values, the exclusive-OR, substitution based on the s-box, shuffling the image based on the shuffling index value, and exclusive-OR operation were performed to achieve the encryption. In the designed method, the best parameters value of the chaotic map needs to communicate to receiver with encrypted image for decrypt the image on the receiver side.

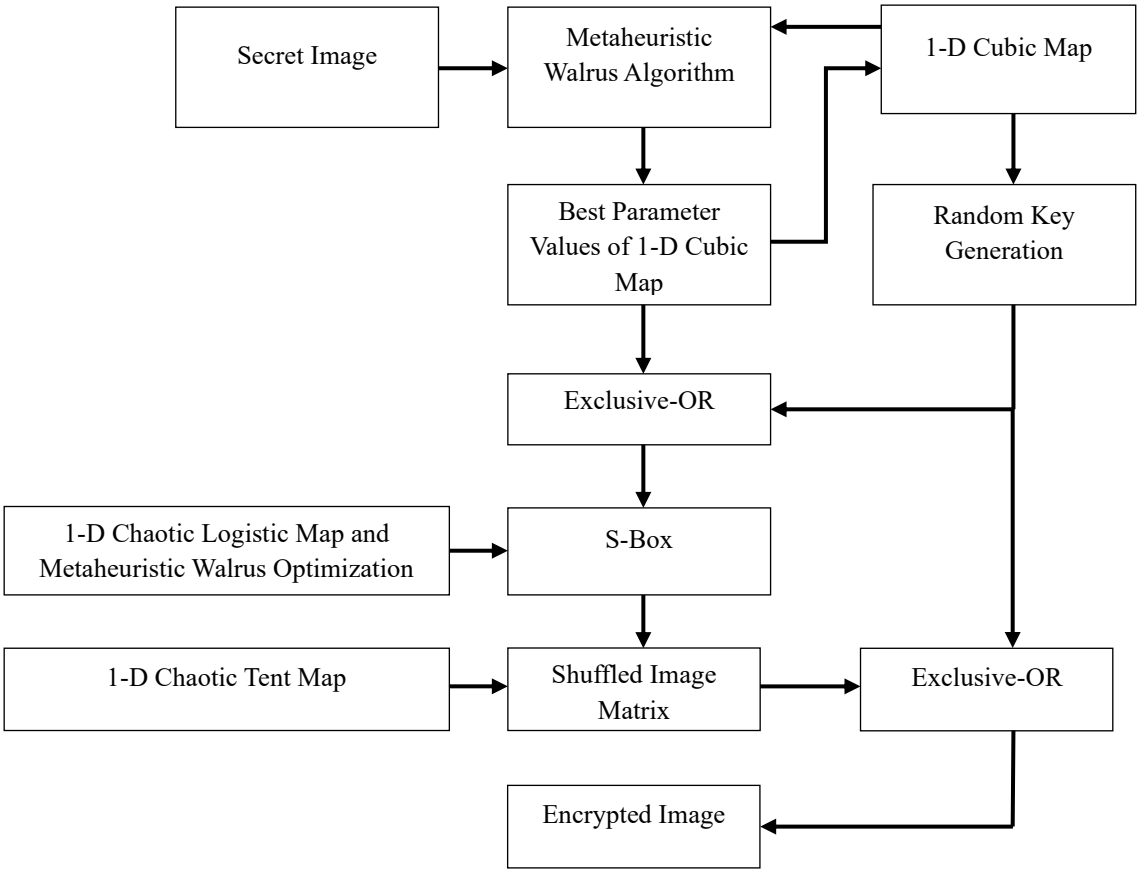



**Figure 1:** Flowchart of the Proposed Image Encryption Method

## 4. Results and Analysis

This section presents the simulation results of the proposed IE method and a comparative analysis of the existing approaches to validate its performance. The system configuration was taken for simulation evaluation purposes: Intel i7 processor, 16GB RAM, 1TB solid-state disk, and 64-bit Windows operating system. The MATLAB 2018 software was used to design and simulate the code.

### 4.1 Evaluation Criteria and Performance Indices

Table 1 presents the parameter configuration of the proposed method. Initially, in this table, the total number of images and their resolution is defined that employed for simulate the proposed method. Next, the lower and upper limits of the chaotic maps is defined. Finally, the parameter value of the metaheuristic walrus algorithm and designed objective function is defined.

**Table 1:** Parameter Configuration of the Proposed Method

| **Parameter** | **Value** |
|---|---|
| Image Resolution | [256 256] |
| Image Format | Grey-Scale |
| Total Images used for Evaluation | 10 |
| Population | 10 |
| Iteration | 50 |
| Cubic Map [x, rho] | [0.1-1]<br>[2.00-2.598] |

| | |
|---|---|
| Tent Map [x, μ] | [0.1-1]<br>[1.9-2] |
| Logistic Map [x, r] | [0.1-1]<br>[3.90-3.99] |
| Objective Function | [Entropy, CC, SSIM] |

**Table 2:** Performance indices parameters for the proposed IE method

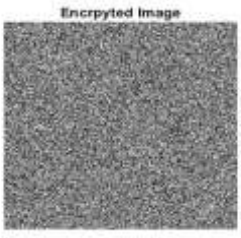
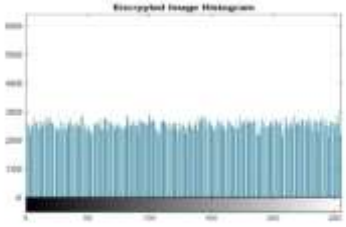
| **Parameter and Description** | **Equation** |
|---|---|
| **Chi-Square:** This analysis is performed to measure the uniformity of the encrypted image histogram to secure the encryption method against statistical attacks performed by attackers. | $\chi^2 = \sum_{i=1}^{255} \frac{(f_i - \varepsilon)^2}{\varepsilon}$ (6)<br>$\varepsilon = \frac{H \times W}{256}$ (7)<br>In above case, $f$ denotes the frequency of the histogram and $\varepsilon$ is the predicted value is determined using Eq. (3). Further, $HW$ denotes the resolution of the image. |
| **Entropy:** This parameter evaluates the randomness of the encrypted image, indicating the unpredictability of pixel intensity. | $H(m) = \sum_{i=0}^{2^N-1} p(e_i) \times \log_2 \frac{1}{p(e_i)}$ (8)<br>where $P(mi)$ represents the probability associated with the pixel intensities. |
| **Number of Pixel Change Rate (NPCR):** The NPCR measures how the pixel values in two encrypted images change when a single pixel in the original image is modified. | $NPCR = \sum_{i-1}^{H} \sum_{j=1}^{W} D(i,j)$ (9)<br>$D(i,j) = \begin{cases} 0 \; if C_1(i,j) = C_2(i,j) \\ 1 \; if \; C_1(i,j) \neq C_2(i,j) \end{cases}$<br>(10)<br>The C1 and C2 denotes the two encrypted image for same secret image with a one-bit modification. |

Table 2 shows the performance indices parameters were determined to evaluate the proposed IE method [15-19].

### 4.2 Simulation Results

In the subjective analysis, the visual quality of the encrypted image and histogram is evaluated, as shown in Table 3. In the ideal scenario, the visual quality of the encryption image should be noisy, and the histogram should be equally distributed. This result reflects that it is difficult for the attacker to recover the secret image by analyzing the characteristics of the encrypted image.

**Table 3:** Subjective Analysis

| **Images** | **Encrypted Image** | **Histogram** |
|---|---|---|
| **1** |  |  |

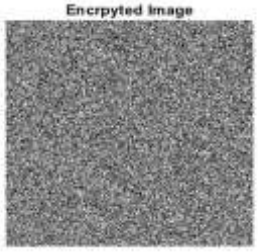
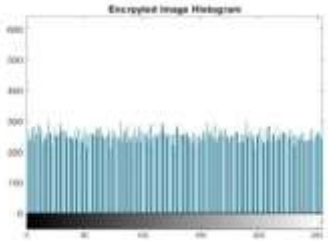
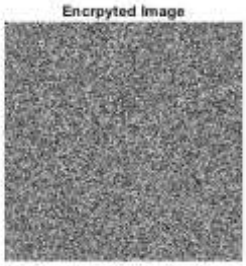
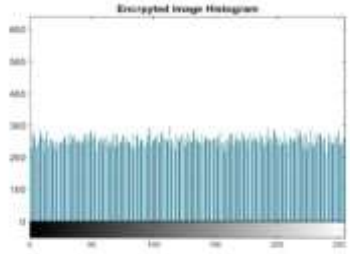
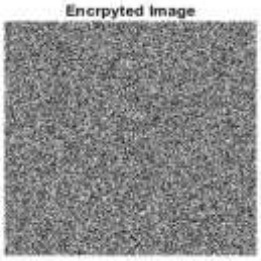
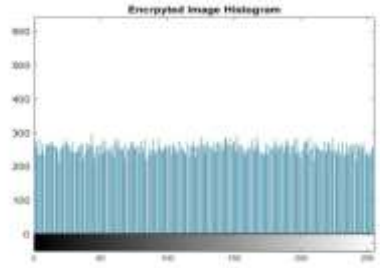
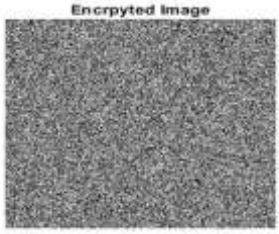
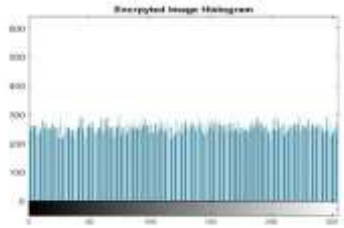
| | | |
|---|---|---|
| **2** |   |  |
| **3** |   |  |
| **4** |   |  |
| **5** |   |  |

Table 4 shows the evaluation of the proposed method based on chi-square, entropy, and NPCR parameter. Table 4 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 224-276, which is less than the reference value (293.83) of the encryption method.

For an 8-bit grayscale image, the ideal entropy is 8, which corresponds to a uniform distribution of pixel intensities. As shown in Table 4, after encryption, the entropy of all images increased to between 7.9968 and 7.9975, with an average of 7.9973, which is very close to the theoretical maximum. In addition, the variation of the output entropy across all images was only 0.0007, indicating that the randomness of the cipher images was independent of the content of the plain image and that the scheme resists entropy-based statistical attacks.

**Table 4:** Evaluation of the Proposed Method based on Chi-Square, Entropy, and NPCR Parameters

| **Images Index** | **Chi-Square Value** | **Entropy** | **NPCR** |
|---|---|---|---|
| 1 | 224 | 7.9974 | 99.6094 |
| 2 | 230 | 7.9974 | 99.5773 |
| 3 | 236 | 7.9973 | 99.6124 |
| 4 | 254 | 7.9970 | 99.6368 |

| | | | |
|---|---|---|---|
| 5 | 276 | 7.9968 | 99.5621 |

Finally, as shown in Table 4, the NPCR values of the test images ranged from 99.5529% to 99.6704%, with an average of 99.6040%, which is very close to the theoretical value. These results show that the proposed method has strong diffusion, as a one-pixel change in the plain image changes almost every pixel in the cipher image, which indicates resistance to differential attacks.

### 4.3 Comparative Analysis

This section shows the comparative analysis of the proposed IE method with the existing approaches. To accomplish this goal, the same dataset images were taken and evaluated based on the entropy, NPCR, and PSNR parameters. Table 5-6 shows the comparative analysis.

**Table 5:** Comparative Analysis based on Entropy Parameter

| **Methods** | **Entropy** |
|---|---|
| Al-Hyari et al. [5] | 7.888 |
| S. A. Gebereselassie and B. K. Roy [6] | 7.968 |
| H. Çelik and N. Doğan [7] | 7.994 |
| Sameh et al. [10] | 7.996 |
| Kumar et al. [11] | 7.996 |
| **Proposed Method** | **7.997** |

Table 5 compares the information entropy of the proposed method with existing schemes. The ideal entropy of an 8-bit encrypted image is 8. The proposed method achieved an entropy of 7.997, the highest among all compared methods. It exceeds the values of Al-Hyari et al. [5] (7.888) and Gebereselassie and Roy [6] (7.968) by 0.109 and 0.029 respectively, and is slightly higher than those of Çelik and Doğan [7] (7.994), Sameh et al. [10] and Kumar et al. [11] (both 7.996). Although the margin over the three best-performing methods is small, the result shows that the proposed scheme produced cipher images with an almost uniform pixel distribution and thus offers strong resistance to entropy-based statistical attacks.

Table 6 presents the NPCR comparison. The theoretical ideal for an 8-bit image is 99.6094%. The proposed method obtained 99.604%, which is only 0.005% below this value. Çelik and Doğan [7] (99.609%) and Al-Hyari et al. [5] (99.608%) are marginally closer to the ideal, and Sameh et al. [10] (99.629%) is slightly above it. In contrast, the NPCR of Kumar et al. [11] (99.272%) and Gebereselassie and Roy [6] (97.067%) deviates considerably from the ideal and falls below the critical values for the NPCR randomness test, which indicates weaker diffusion and a greater vulnerability to differential attacks. The proposed method therefore provides diffusion comparable to the best existing methods and clearly better than the weaker ones.

**Table 6:** Comparative Analysis based on NPCR Parameter

| **Methods** | **NPCR (%)** |
|---|---|
| Al-Hyari et al. [5] | 99.608 |
| S. A. Gebereselassie and B. K. Roy [6] | 97.067 |
| H. Çelik and N. Doğan [7] | 99.609 |
| Sameh et al. [10] | 99.629 |
| Kumar et al. [11] | 99.272 |
| **Proposed Method** | **99.604** |

## 5. Conclusions

In this study, an image encryption method is presented by determining the best parameters of the chaotic map for encryption purposes using the metaheuristic walrus optimization. The chaotic maps were used for generating the substitution box, key, and permutation index. The main novelty of the proposed method is that a multi-objective function was designed by considering the multiple security parameters such as entropy, CC, and SSIM.

The key finding of this study is that the histogram of the encrypted image is equally distributed and its validation is done using the chi-square test. The result indicates that the proposed method has passed the chi-square test for the different images. Furthermore, the security metrics, PSNR, entropy, CC, SSIM, NPCR, and MD, define that the proposed method accomplishes the desired parameter values required in the encryption process. Furthermore, we found that the metaheuristic algorithm effectively determines the optimal parameter values for different secret images, and these parameter values are not fixed.

The comparative analysis with the previous approaches shows that the proposed method achieves a high value of entropy, NPCR, and a lower value of the PSNR due to finding the initial parameter of the chaotic map based on the multi-objective function using the Walrus optimization. From the application perspective, the proposed method is suitable for communicating the secret image in several applications, namely, healthcare, IoT, and defense, for securing the sensitive information of the users.

The limitation of the presented method is that the optimal parameters of the chaotic map must be communicated to the receiver in order to decrypt the encrypted image. Furthermore, the time complexity is dependent on the secret image resolution and parameter values of the metaheuristic Walrus optimization algorithm.

## References

[1] X. Song, S. Feng, W. Yi, and Y. Zheng, “Quantum grey-scale image encryption method based on alternating quantum random walk,” *EPJ Quantum Technology*, vol. 12, no. 1, Jul. 2025, doi: 10.1140/epjqt/s40507-025-00386-7. Available: https://doi.org/10.1140/epjqt/s40507-025-00386-7

[2] H. Kolivand, S. F. Hamood, S. Asadianfam, M. S. M. Rahim, and W. Hurst, “Image encryption framework based on multi-chaotic maps and equal pixel values quantization,” *Multimedia Tools and Applications*, vol. 84, no. 17, pp. 17769–17804, Jul. 2024, doi: 10.1007/s11042-024-19771-y. Available: https://doi.org/10.1007/s11042-024-19771-y

[3] 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

[4] H. Kolivand, S. F. Hamood, S. Asadianfam, and M. S. Rahim, “Image encryption techniques: A comprehensive review,” *Multimedia Tools and Applications*, Jan. 2024, doi: 10.1007/s11042-023-17896-0. Available: https://doi.org/10.1007/s11042-023-17896-0

[5] 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

[6] 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

[7] 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

[8] 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

[9] 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

[10] 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

[11] 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

[12] A. Srivastava and S. Solanki, "Optimized Image Encryption Model based on Hybridization of Chaotic Maps with Metaheuristic OOBO 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

[13] P. Trojovský and M. Dehghani, "A new bio-inspired metaheuristic algorithm for solving optimization problems based on walruses behavior," *Scientific Reports*, vol. 13, no. 1, p. 8775, May 2023, doi: 10.1038/s41598-023-35863-5. Available: https://doi.org/10.1038/s41598-023-35863-5

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

[15] A. Dinu and M. Frunzete, "Image encryption using Chaotic maps: development, application, and analysis," *Mathematics*, vol. 13, no. 16, p. 2588, Aug. 2025, doi: 10.3390/math13162588. Available: https://doi.org/10.3390/math13162588

[16] K. Mahalakshmi and S. Nagarajan, "Comprehensive review and analysis of image encryption techniques," *IEEE Access*, vol. 13, pp. 109783–109813, Jan. 2025, doi: 10.1109/access.2025.3578158. Available: https://doi.org/10.1109/access.2025.3578158

[17] 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

[18] 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

[19] 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