INTERNATIONAL RESEARCH JOURNAL OF ENGINEERING & APPLIED SCIENCES
ISSN: 2322-0821(O)
ISSN: 2394-9910(P)
VOLUME 13 ISSUE 4
Oct 2025 - Dec 2025
www.irjeas.org

Research Article

Integration of Chaotic Map with Metaheuristic Walrus Algorithm for Enhanced Security of Image Encryption Method

[1]Monika Gupta, Shashi Bala[2], Tarandeep kaur[3]*

[1-3]Computer Science and Engineering Department, Thapar Polytechnic College, Patiala, India.
monika4779@rediffmail.com
s_atwal121@yahoo.com
tpc.taran@gmail.com

**Corresponding Author*: monika@rediffmail.com

DOI–10.55083/irjeas.2025.v13i04012

Abstract: Image encryption (IE) methods have been used to secure the sensitive secret images and overcome the data breach attacks. In these methods, the chaotic map algorithms gained popularity over other security algorithms. However, these algorithms are highly sensitive to input parameters that impact the security of the encryption method. Therefore, in this paper, we have strengthened the security of the IE method by integrating the chaotic map with the metaheuristic walrus algorithm to hyper-tune the input parameters according to the chi-square objective function. In the presented methodology, the open-source database images were collected for evaluation purposes. Thereafter, it was passed through three stages of encryption to produce the final encrypted image. The first and last stages utilize the shuffling method to rearrange the secret image, while the second stage employs an exclusive-OR operation with a random key. The shuffling method index value and random key were generated using the 3-D chaotic map. According to the results, the proposed strategy achieves a high entropy value and reduced CC, SSIM, and PSNR values while passing the chi-square test.

Keywords: Chaotic Map, Confusion, Diffusion, Encryption, Metaheuristic, Random key, Security.

1. INTRODUCTION

Digital data protection has become an important issue due to the continuous increase in data breaches and cyberattacks in today's digital environment. Basically, any way of sending or receiving data, especially images, needs to be protected to make sure that the data is kept private, accurate, and authentic [1]. In general, images may be secured via encryption, watermarking, and steganography, as shown in Figure 1 [2]. One of the most often

used methods for guaranteeing this security is cryptography, which comprises making data unreadable to anybody who does not possess the necessary keys to decode it. Text data may be effectively encrypted using conventional techniques like the AES and DES. However, because of features like high redundancy and significant pixel correlation, they are limited when applied to images [3]. To encrypt images, the main mechanisms are dispersion and confusion. To accomplish the confusion process, a secret key changes the locations and values of the plain image pixels at random. This procedure makes it harder for an attacker to decipher the encryption key, even if they know parts of the original/encrypted image. Furthermore, the diffusion feature is shown by the fact that changing just one pixel's place can cause big changes in the cipher image [4].

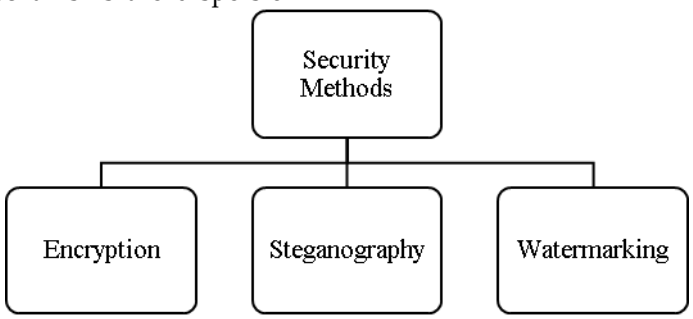


Figure 1 Different Security Methods

Over the last ten years, chaos theory has been more popular in IE techniques because of its high performance, ergodicity, unpredictability, and sensitivity to new situations [5]. However, the performance of the chaos-based encryption method is highly dependent on its initial and control parameters. Therefore, utilizing the optimal parameter value enhances the security [6]. In the previous studies, grid search, random search, and metaheuristic optimization algorithms have been utilized for optimal parameter selection. In this paper, we have focused on the metaheuristic optimization algorithm due to its superior performance over others and its ability to search for the best parameter values based on the desired objective function [7]. Entropy (E), correlation coefficient (CC), Number of pixels change rate (NPCR), and Structure Similarity Index Measure (SSIM) are the popular objective functions used in the literature.

In this paper, we have improved the picture encryption technique's security by integrating the 3-D chaotic map and metaheuristic walrus optimization algorithm. In the proposed method, we have generated the multiple random keys for encrypting the secret image by employing the 3-D chaotic logistic map. Additionally, we identified the optimal parameters of the 3-D chaotic logistic map (CLM) using the walrus optimization algorithm, with the chi-square test serving as the objective function. The evaluation on the standard dataset indicates that the histogram distribution of the encrypted image is uniformly distributed, regardless of the input histogram distribution. Furthermore, the proposed method accomplishes the lower value of SSIM, CC, and PSNR and the higher value of the NPCR parameter as required in the encryption method.

This manuscript is further subdivided into five sections. Section 2 defines the previously proposed IE methods in the related work. Section 3 gives an in-depth overview of the 3-D chaotic map and metaheuristic walrus optimization. In Section 4, the suggested IE method is explained in more depth. Section 5 shows the result and discussion to validate the performance of the presented IE method over existing methods. Section 6 finally draws the conclusion and outlines the future scope.

2. RELATED WORK

Sameh et al. [8] evaluated the performance of several chaotic maps by optimizing the parameters using the different metaheuristic

algorithms. The result indicates that the Gauss chaotic map is computationally inexpensive, and the circle map generates the most completely random keys over the others. In [9], evaluated the different 1-D chaotic maps and hybrid approaches based on them. In their work, they have considered the sine, cubic, tent, and logistic map. Furthermore, they have designed three hybrid approaches, namely, sine-cubic, tent-logistic, and sine-logistic. Their finding suggests that the sine-based encryption method accomplishes the best performance over others in terms of CC (0.0017), PSNR (9.204 dB), MSE (7809.1), and NPCR (95.3903). Hosny et al. [10], considering the three 2D chaotic maps (2D logistic map, Henon, and Baker) for generating the multiple keys for IE Method. In their work, initially, the image was split into RGB planes. Following that, the RGB plane images went through a randomization process, and finally, a diffusion process was performed using the XORing operation with random keys. Kumar et al. [11] generated random keys for the color secret image using the 3-D logistic map algorithm, hyper-tuned its parameters with the JAYA algorithm, and achieved entropy close to the ideal value required for the encryption method. A. Srivastava and S. Solanki [12] considered the two 1-D chaotic maps (logistic and tent maps) to design an encryption method. In their work, logistic map-based random key generation was done, whereas the tent map was used to shuffle the secret image. Furthermore, they have optimized the parameter values using the OOBO algorithm based on the E and CC-based objective function. They achieved the entropy value of 7.99704.

In the previous studies, the authors used the chaotic map for key generation and shuffled the secret image by hyper-tuning the parameters using the metaheuristic algorithm. Furthermore, they have taken the entropy parameter as the objective function to evaluate the randomness of the encrypted image. However, the entropy parameter checks the overall randomness and uncertainty in the image pixels, not the uniform distribution of the histogram pixels. Therefore, we have presented an enhanced IE method in this paper by considering the 3-D chaotic logistic map and optimizing the parameters of it using the chi-square test and the objective function in the metaheuristic walrus optimization (WO) algorithm.

3. CHAOTIC MAP AND METAHEURISTIC WALRUS OPTIMIZATION

This section presents an overview of the 3-D chaotic map, and the WO algorithm is employed to design the proposed encryption method.

3.1 Chaotic Map

In this paper, we have used the 3-D chaotic map to generate the shuffling index and random key for encrypting the secret image. The basic equation for it is defined below [11].

$$a_{n+1} = \alpha a_n(1 - a_n) + \beta b_n^2 a_n + \gamma c_n^3 \quad (1)$$

$$b_{n+1} = \alpha b_n(1 - b_n) + \beta c_n^2 b_n + \gamma a_n^3 \quad (2)$$

$$c_{n+1} = \alpha c_n(1 - c_n) + \beta a_n^2 c_n + \gamma b_n^3 \quad (3)$$

In Eq. (1-3), the range of the variable is 0< a, b, c <1, α={3.68-3.99}, β= {0-0.022}, γ= {0-0.015}.

3.2 WO Algorithm

The WO algorithm is a new type of metaheuristic algorithm that was created by looking at how walruses behave in nature. The primary sources of inspiration of this algorithm are the processes of eating, moving, escaping, and combating predators used by walrus. The exploration, migration, and exploitation are the three main stages [13].

Phase 1: Exploration Stage: In this optimization technique, walruses eat several marine organisms, including soft corals, shrimp, tunicates, sea cucumbers, tube worms, and a variety of mollusks. However, the walrus like benthic bivalve mollusks, especially clams. It finds these animals by grazing on the sea bottom and using its strong limbs and sensitive vibrissae to find food. Throughout this process, the strongest and largest tusks walruses lead the group in their hunt for food. The objective function values of the offered solutions are equivalent to walrus tusk length. Thus, the strongest walrus is the solution with the highest objective function value. This way of searching by walruses leads to different parts of the search space being scanned, which makes the WaOA better at exploring the global search.

Phase 2: Migration: Walruses move to rocky coastlines or outcrops because of the late-summer air warming, which is one of their normal habits. To guide the walruses in the search space to the right places, the WaOA uses this migratory process.

Phase 3: Exploitation Stage: The walrus is perpetually at risk of attack from killer whales and polar bears. The walruses' positions around their current location alter because of their escape and defense tactics against these predators. Walrus behavior simulation boosts WaOA exploitation power in the local problem-solving space surrounding candidate solutions.

4. PROPOSED IE METHOD

The main novelty of the presented IE method is the generation of random keys and shuffling indexes through the 3-D chaotic map, which utilizes the best parameters identified by the metaheuristic walrus algorithm. Furthermore, we have considered the chi-square test an objective function to evaluate the uniformity of the encrypted histogram. The block diagram of the IE method is presented in Figure 2.

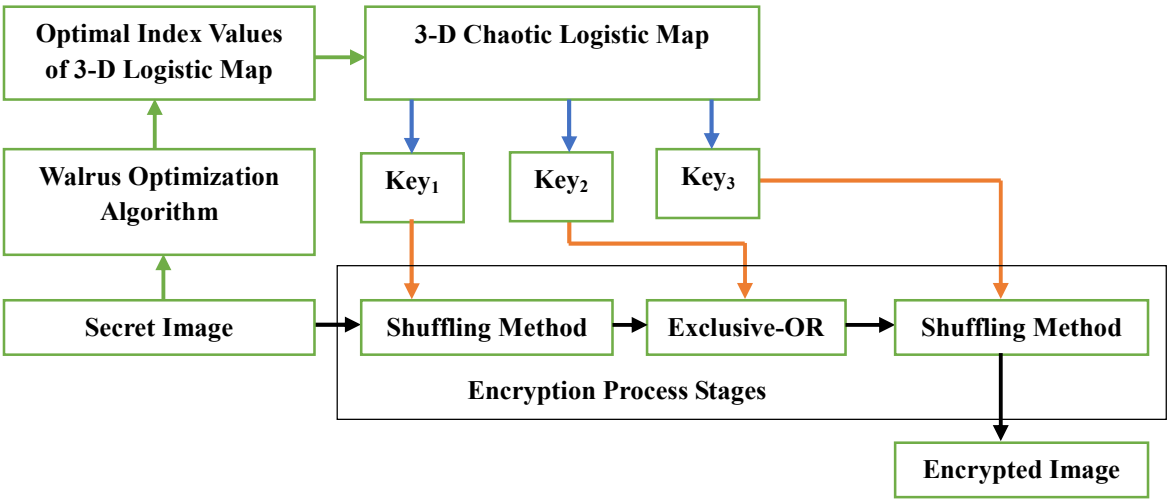


Figure 2 Block Diagram of the IE Method

Initially, a grayscale secret image was read and passed through three stages of encryption to encrypt it. The first and third stages were based on the shuffling method to shuffle the image matrix, whereas the second stage was employed to perform the exclusive-OR operation with the random key. The shuffling method index value and random key were generated by the 3-D logistic map algorithm, utilizing the best input parameter values determined through the WO algorithm, which was based on the chi-square objective function. In the WOA, initial parameters were defined, and a random population was generated in the boundaries of the chaotic map parameter values. Using this generated population, the encryption was performed, and the objective function was evaluated according to the chi-square value, allowing for the identification of which population yielded the lowest value compared to others. This operation was performed for a predefined

iterations to update the population and to determine the lowest value. The population that produced the lowest value was then used in the 3-D logistic map algorithm to perform the shuffling and random key operation.

5. RESULTS AND DISCUSSION

The demonstration was done on MATLAB 2018a software. We have taken open-source database images from the USC-SIPI Image Database [14]. This database contains images in the grayscale and color formats. Furthermore, these images are available in standard resolutions, such as 256x256, 512x512, and 1024x1024.

5.1 Evaluation Criteria and Performance Indices

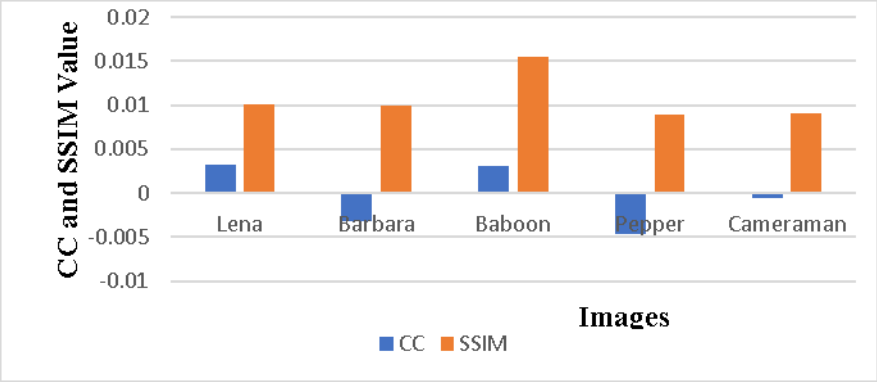
In this article, we have taken grayscale images of a resolution size of 256x256. We have chosen five images (*lena, Barbara, baboon, pepper, cameraman*) for simulation purposes. Furthermore, in the proposed approach, metaheuristic walrus optimization algorithm was initialized to find the best parameter values of the 3-D logistic map. We have taken $Walrus_{pop}$ size value of 10, iterations value 30, and chi-square function as the objective function. The objective function was minimized while exploring the best parameter value. The size of the random keys were generated using the 3-D CLM was same as the resolution of the secret image. Next, this section presents the performance indices are determined for evaluate the encrypted image with respect to the secret image using chi-square, entropy, CC, PSNR, and SSIM [11,15].

5.2 Simulation Results

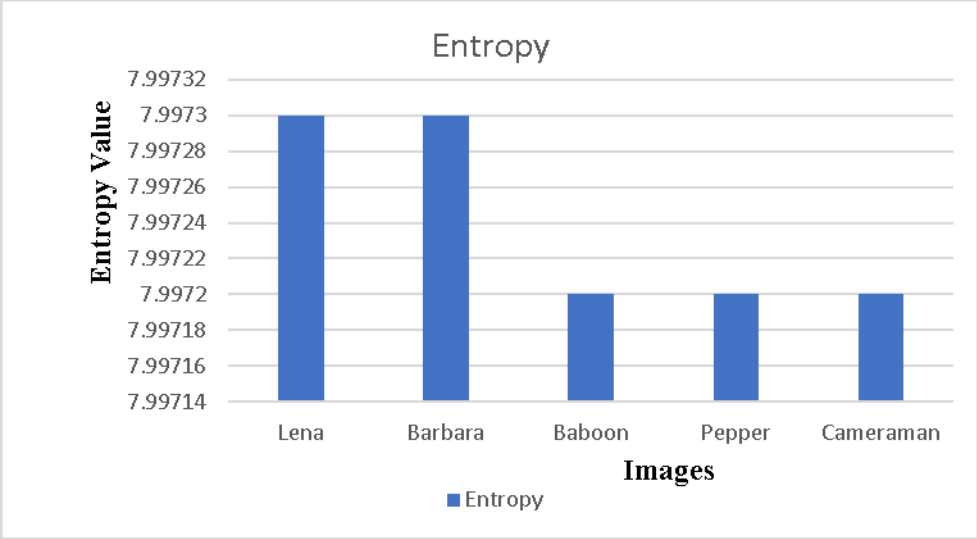
Table 1 shows the performance analysis of the proposed method. The result indicates that the proposed method accomplishes the desired chi-square value required in the encryption process (lesser than 292.2478), which represents the uniform histogram distribution of the encrypted image. Furthermore, the average entropy value is higher than 7.9971 (approx. 8 i.e. ideal value), the CC and SSIM values are near to zero, and the PSNR is less than 14dB for different images, as shown in Figure 3.

Table 1 Performance Evaluation of the Proposed IE Method

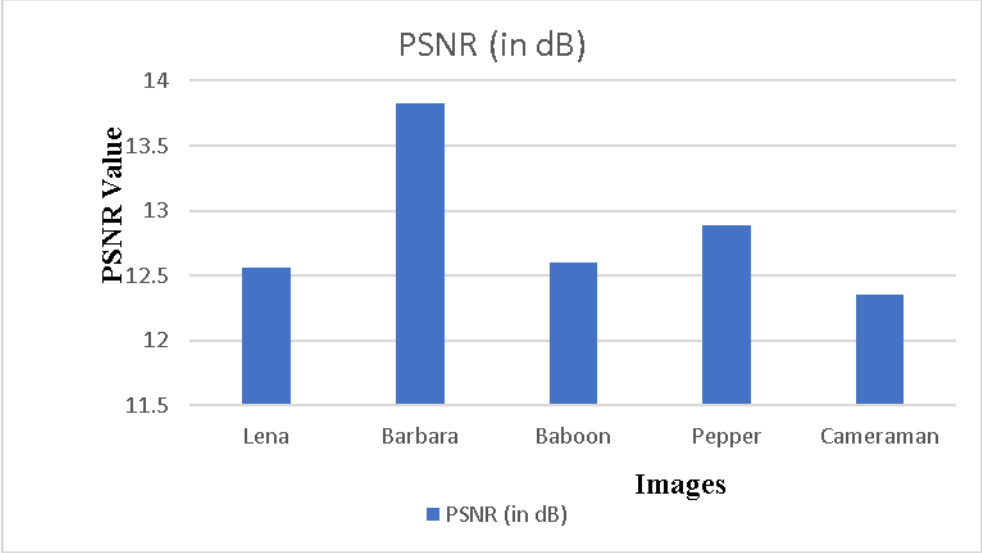
Images	Chi-Square Value	Entropy	CC	SSIM	PSNR (in dB)
Lena	232	7.9973	0.0032	0.0101	12.5632
Barbara	234	7.9973	-0.0032	0.0099	13.8236
Baboon	248	7.9972	0.0031	0.0155	12.5981
Pepper	244	7.9972	-0.0047	0.0089	12.8853
Cameraman	240	7.9972	-5.9842e-04	0.0090	12.3578



(a) CC and SSIM for the Different Images



(b) Entropy for the Different Images



(c) PSNR for the Different Images

Figure 3 Evaluation using Various Parameters for the Proposed Method

Table 2 presents a comparison between the proposed approach and past approaches for the same database images based on the entropy parameter. The entropy value of the proposed approach is higher than the previous one due to fine-tuning the parameter of the 3-D logistic map based on the metaheuristic walrus algorithm, as shown in Figure 4.

Table 2 Comparative Analysis with Previous Approaches

Images	Sameh et al. [8]	Kumar et al. [11]	A. Srivastava and S. Solanki [12]	Proposed Method
Cameraman	7.9956	7.9970	7.99648	7.9972
Elaine	7.9951	7.9966	7.99688	7.9974
Lena	7.9978	7.9971	7.99702	7.9973
Pepper	7.9961	7.9969	7.99704	7.9972

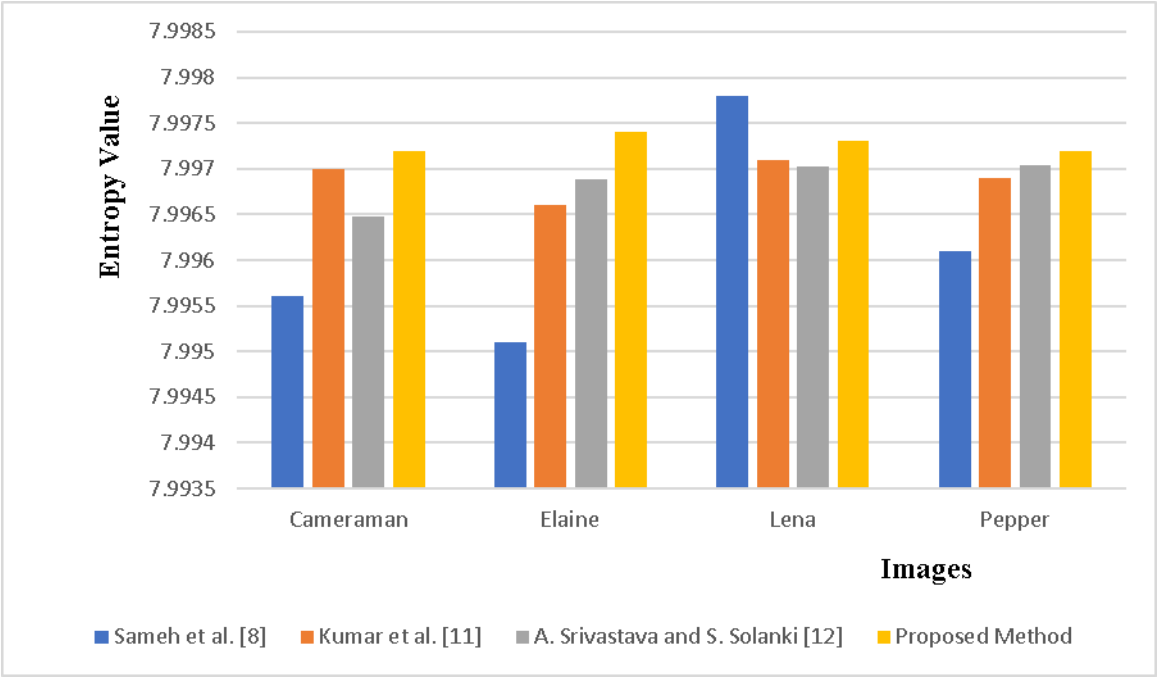


Figure 4 Comparative Analysis

5.3 Discussion

The main key finding for the proposed method is that fine-tuning the chaotic map's parameters enhances the security parameter value. However, the computational complexity of the proposed method is dependent on the parameter values of the walrus algorithm and the objective function.

6. CONCLUSION AND FUTURE SCOPE OF THE WORK

In this paper, we have introduced an IE method that secures the secret image on the internet against various attacks. In this approach, we have shuffled the image pixels and encrypted them with a random key by performing the exclusive-OR operation. Furthermore, the shuffling index and random key are generated using the 3-D chaotic map, and fine-tuning of parameters is done using the walrus optimization algorithm. The result indicates that the proposed method accomplishes the desired security parameters and outperforms the existing methods. In the future, we will design the substitution box using the chaotic map and explore the other security parameters to design a multi-objective function to enhance the proposed method.

REFERENCES

[1] N. E. Ghouate *et al.*, "A high-entropy image encryption scheme using optimized chaotic maps with Josephus permutation strategy," *Scientific Reports*, vol. 15, no. 1, Aug. 2025, doi: 10.1038/s41598-025-14784-5. Available: https://doi.org/10.1038/s41598-025-14784-5

[2] S. Minocha, S. R. Sharma, B. Singh, and A. H. Gandomi, "Adaptive image encryption approach using an enhanced swarm intelligence algorithm," *Scientific Reports*, vol. 15, no. 1, Mar. 2025, doi: 10.1038/s41598-025-86569-9. Available: https://doi.org/10.1038/s41598-025-86569-9

[3] S. Benaissi, N. Chikouche, and R. Hamza, "A novel image encryption algorithm based on hybrid chaotic maps using a key image," *Optik*, vol. 272, p. 170316, Nov. 2022, doi: 10.1016/j.ijleo.2022.170316. Available: https://doi.org/10.1016/j.ijleo.2022.170316

[4] E. Winarno, K. Nugroho, P. W. Adi, and D. R. I. M. Setiadi, "Combined interleaved pattern to improve Confusion-Diffusion Image

encryption based on hyperchaotic system," *IEEE Access*, vol. 11, pp. 69005–69021, Jan. 2023, doi: 10.1109/access.2023.3285481. Available: https://doi.org/10.1109/access.2023.3285481

[5] 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

[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] 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

[9] 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

[10] K. M. Hosny, Y. M. Elnabawy, R. A. Salama, and A. M. Elshewey, "Multiple image encryption algorithm using channel randomization and multiple chaotic maps," *Scientific Reports*, vol. 14, no. 1, Dec. 2024, doi: 10.1038/s41598-024-79282-6. Available: https://doi.org/10.1038/s41598-024-79282-6

[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, 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] P. N. Andono and D. R. I. M. Setiadi, "Improved Pixel and Bit Confusion-Diffusion based on mixed chaos and hash operation for image encryption," *IEEE Access*, vol. 10, pp. 115143–115156, Jan. 2022, doi: 10.1109/access.2022.3218886. Available: https://doi.org/10.1109/access.2022.3218886

Conflict of Interest Statement: *The authors declare that there is no conflict of interest regarding the publication of this paper.*

Generative AI Statement: *The author confirms that no Generative AI tools were used in the preparation or writing of this article.*

Publishers Note: *All statements made in this article are the sole responsibility of the author(s) and do not necessarily reflect the views of their affiliated institutions, the publisher, editors, or reviewers. Any products mentioned or claims made by manufacturers are not guaranteed or endorsed by the publisher.*

Cite this Article

Monika Gupta, Shashi Bala, Tarandeep kaur. Integration of Chaotic Map with Metaheuristic Walrus Algorithm for Enhanced Security of Image Encryption Method. International Research Journal of Engineering & Applied Sciences (IRJEAS). 13(4), pp. 125-133, 2025. https://doi.org/10.55083/irjeas.2025.v13i04012