

Improved Chaotic Logistic Map Algorithm based on Bio-Inspired Algorithm for Image Encryption

Ajay Kumar, Electronics & Communication Engineering Dept., Thapar Institute of Engineering & Technology

Patiala, India. ajay.kumar@thapar.edu

Abhijit Karmakar, Integrated Systems Dept. CSIR-Central Electronics Engineering Research Institute Pilani, India. abhijit.karmakar@gmail.com

Alpana Agarwal, Electronics & Communication Engineering Dept., Thapar Institute of Engineering & Technology

Patiala, India. alpana@thapar.edu

Abstract: In this paper, a bio-inspired black widow optimization algorithm has been employed to determine the optimal parameter values of the chaotic logistic map algorithm for image encryption. The Black widow optimization algorithm is based on the mating behaviour of black widow spiders and it provides early convergence over the other algorithms due to an exclusive stage known as cannibalism. This stage removes the inappropriate solutions in each iteration. The proposed method employs the traditional confusion and diffusion architecture. Initially, in the proposed method, optimal parameter values of the chaotic logistic map algorithm are determined using the Black Widow optimization algorithm and a random key is generated. After that, an Exclusive-OR operation is performed between the secret image and a random key to achieve confusion. Next, to achieve diffusion, the image matrix is randomly circular shifted horizontally and vertically. The simulation evaluation is performed on standard dataset images. Further, subjective and objective analyses are performed for the proposed method to evaluate its performance over the existing methods. At last, comparative analysis was done with the existing methods and it was found that the proposed method provides better entropy and number of pixel change rates than the existing methods.

Keywords: Bio-Inspired, Black Widow Optimization, Chaotic Map, Confusion-Diffusion, Cryptography, Image Encryption, Security.

Tob Regul Sci. TM 2022;8(1): 1915-1928

DOI: doi.org/10.18001/TRS.8.1.146

1. Introduction

Due to advancement in the technology and improvement of the people's living demand, the text-oriented communication is gradually moved towards images [1]. Images are prone to attack on the internet. Therefore, cryptography is used to secure the images on the internet [2]. In the literature, a number of image encryption methods are proposed to secure the images. However,

images contain some inherent features such as large amount of data, high redundancy and strong correlation between adjacent pixels [3]. Thus, traditional cryptography methods such as data encryption standard (DES) and advanced encryption standard (AES) are not efficient for image encryption [4].

Chaotic function is most preferred over traditional cryptography methods for image encryption because it provides numerous advantages such as extreme sensitive to initial conditions, provides non-linearity and unpredictability [5]. Fridrich was the first to combine chaotic systems theory with cryptography theory and apply it to an image cryptosystem in 1998. This effectively ensured that the method could work as intended. Since then, image cryptosystems based on chaotic systems have grown into an important topic of cryptography, with a number of promising findings emerging from the field. For image encryption, several chaotic maps such as logistic maps, tent maps, henon maps and cubic maps are employed [6]. As it is known, initial parameter values play an important role in chaotic map and inappropriate selection of parameter value, negatively impact the security parameter. Therefore, in the literature, bio-inspired optimization algorithms are successfully applied for determining the optimal parameter values of chaotic function. In the literature, genetic algorithm [7], grasshopper optimization [8], gravitational search algorithm [9], teaching learning-based optimization [9], and dynamic harmony search [10] algorithms are successfully applied for calculating the optimal parameter values of chaotic map algorithm. Out of these, genetic algorithm is the most preferred algorithm [7,11-13]. However, genetic algorithm faces numerous challenges such as low convergence rate and local optima problem. Therefore, other optimization algorithms are explored that provides faster convergence rate and global solutions. It is seen that black widow optimization algorithm is the most superior algorithm because black widow spiders can mate in parallel and generate number of offspring's [14]. Thus, it can explore more possible solutions. Besides that, it contains one stage known as cannibalism. This stage eliminates the inappropriate solutions in each iteration. Thus, new solutions are generated with best populations in the sub-sequent iterations. Black widow optimization algorithm is successfully applied for number of applications in the literature such as image segmentation [15], feature selection [16], suspended sentiment load prediction [17], object detection [18], and in multilevel thresholding [19].

The main contribution of this paper is to calculate the optimal parameter values of chaotic logistic map algorithm using the bio-inspired black widow optimization algorithm for image encryption. To achieve this goal, we have designed an objective fitness function using entropy parameter. Based on this fitness function, a complete random key is generated. Image encryption method based on traditional confusion and diffusion architecture. Further, to achieve image encryption, in the confusion stage, XOR operation is performed between secret data and random key. After that, in the diffusion stage, horizontal and vertical circular shift is performed to achieve final encryption. The simulation evaluation shows that the convergence rate is fast because black widow optimization algorithm quickly searches the optimal parameter values. Further, encrypted image

is completely noisy and the proposed method achieves higher values of entropy, Mean square error, number of pixel change rate and low value of correlation coefficient, PSNR.

The remaining paper is organized into 6 sections. Section 2 illustrates the related work. Section 3 describes the chaotic logistic map and the black widow optimization algorithm. Section 4 explains the proposed image encryption method. Section 5 shows the results and analysis. Finally, conclusion and future scope is drawn in Section 6.

2. Related Work

Chaotic map is successfully applied for image encryption due to its numerous advantages such as extreme sensitivity to initial conditions, non-linearity, unpredictability, and ergodicity [20]. Multiple chaotic maps such as logistic map, tent map, henon map, and cubic map are used for image encryption [6]. Out of these, chaotic logistic map is the most preferred in the literature. In the initial phase, manually parameter values are selected. Therefore, easy to cryptanalyzed.

Bio-inspired algorithms were effectively employed to find the parameters in recent times. The optimum or nearly optimal solution may be found through bio-inspired optimization methods [21]. In the first phase, an initial population is formed, the size of which is determined by the specifics of the situation at hand. Most solutions in the population are in the hundreds so that one can try them all. Such answers are often attained by chance. After that, the fitness function for each population is determined. The fitness function is utilized to resolve the optimal answer and so its selection is of the utmost importance. Based on the characteristics of the issue, the fitness function may be minimized or maximized. Finally, the genetic algorithm uses biologically-inspired processes like crossover and mutation to produce new solutions from the original population. The efficiency of the new solutions is then compared to the best solution; if the new solutions are more appropriate, the optimal solution is altered. The generating procedure is continued until a good solution is identified.

In 2012, Abdullah et al. [7], generated n number of encrypted images using original image and chaotic function. After that, encrypted images used a population for genetic algorithm to determine the best encrypted image that provides high entropy and low correlation coefficient. In 2016, Khadijeh Mirzaei Talarposthi and Mehrzad Khaki Jamei [10], designed a two-stage step to maximize entropy and minimize correlation coefficient using dynamic harmony search algorithm. In 2018, Noshadian et al. [9], optimized chaos-based image encryption scheme using teaching learning-based optimization (TLBO) and gravitational search algorithm (GA). The TLBO provides superior results over gravitational search algorithm. In 2019, Shelza Suri and Ritu Vijay [11], deployed the genetic algorithm for chaotic function. Further, single and multi-objective functions are designed. The hybrid combination of entropy and correlation coefficient as an objective function provides superior results over other combination of objective functions. In 2020, Bhaskar Mondal and Tarni Mandal [12], hybrid the linear feedback shift register, chaotic tent and logistic map algorithm for key generation. Thereafter, process the original image in fixed block size. Further, perform XOR and genetic operations to get encrypted image in the output. In

2020, Niu et al. [13], uses the keccak, henon map, DNA encoding, and genetic operations to achieve image encryption. In 2022, Khalaf et al. [8], determine the optimal parameter values of r and x_n using grasshopper optimization algorithm and uses entropy as an objective function.

3. Introduction to Chaotic Logistic Map and Bio-Inspired Black Widow Optimization Algorithm

In this section, chaotic logistic map and black widow optimization will be described briefly.

3.1 Chaotic Logistic Map Algorithm

Unlike noise signals, which can only be approximated, chaotic functions may be accurately replicated as long as we know the fundamental values and the corresponding drawing function. The following are a few of the many benefits of these signals [8].

- Sensitivity to Primary Conditions: By this benefit, we imply that a very small adjustment to the initial sum may have far-reaching effects on the succeeding metrics. It just takes a little shift in the total signal strength to produce a radically different output.
- Apparently Accidental Feature: To replicate accidental numbers, we only need to know the main quantities along with the drawn function, in contrast to the production of accidental natural numbers, where the range of numbers cannot be duplicated.
- Deterministic Work: The chaotic functions are perfectly accurate because of their accidental manifestation. With the sketched function and the fundamental quantities, one can generate and replicate seemingly random sets of numbers.

In the literature, chaotic logistic map is the most preferred algorithm in the chaotic function and is determined using Eq. (1).

$$x_{n+1} = rx_n(1 - x_n) \quad (1)$$

In Eq. (1), $r \in (0,4)$ is a logistic parameter and $x_n \in (0,1)$ system variable, respectively. On the other hand, n is the iteration number. Figure 1 shows the bifurcation diagram of the chaotic logistic map algorithm. Figure shows that chaotic logistic map has chaotic behaviour when $r \in (3.57,4)$.

3.2 Black Widow Optimization Algorithm

Black widow optimization algorithm is an evolutionary algorithm and it is based on mating behaviour of black widow spiders. The flowchart of it is shown in Figure 1 [14].

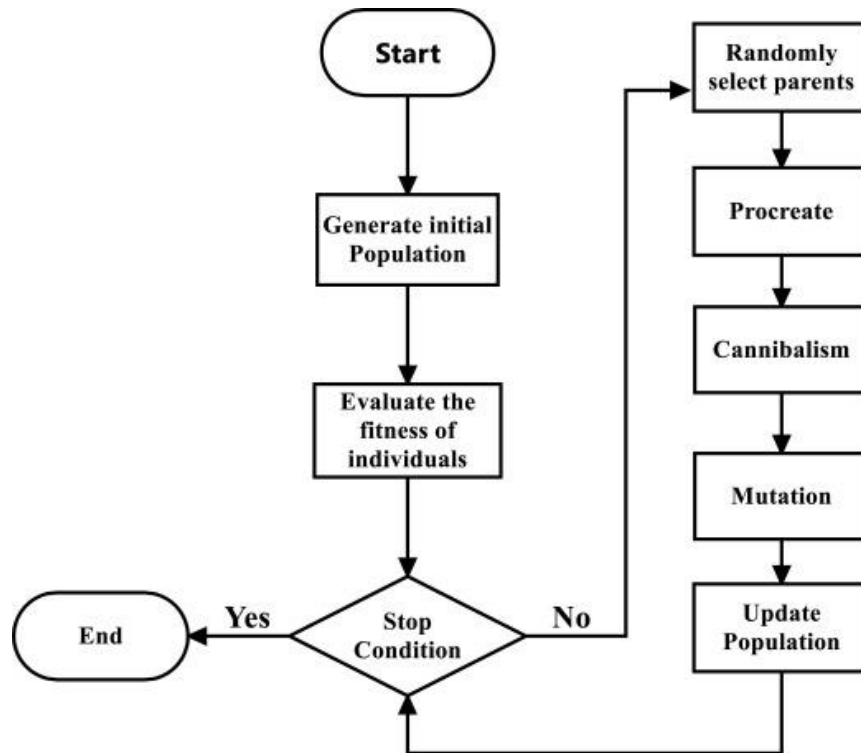


Figure 1 Flowchart of the Black Widow Optimization Algorithm [14]

- Initialization of Population: In order to find a workable solution to an optimization process, the numbers of the relevant variables need to take a certain shape. In the terminology of PSO and GA, this structure is described as a chromosome and in the terminology of PSO, it is referred to as a particle location; however, in the black widow optimization method (BWO), it is referred to as a widow. Each possible answer is compared to a Black Widow spider in the Black Widow Optimization Algorithm (BWO). Black widow spiders represent the issue variables and their values. For the purpose of this work, the structure may be thought of as an array for the purpose of solving benchmark functions.

The answer to an optimization issue with Nvar dimensions is represented as a widow, an array of size $1 \times Nvar$. The following is the syntax for defining this array:

$$widow = [x_1, x_2, \dots, x_{Nvar}] \quad (2)$$

The fitness of widow is obtained by evaluation of fitness function f at a widow of $(x_1, x_2, \dots, x_{Nvar})$. So $Fitness = (widow) = f(x_1, x_2, \dots, x_{Nvar})$

First, a spider population, denoted by Npop, is formed to populate a potential widow matrix, of size Nvar. The next phase is for a randomly chosen set of parent couples to carry out the mating process and at this point the female black widow will consume the male.

- Procreate: As the couples are autonomous from one another, they begin to mate in order to generate a new generation simultaneously. This replicates how mating occurs in nature, where each pair does it in its own web, independently of the others. In the actual world, each successful mating result in the production of around one thousand eggs, but in the end, some of the spider infants survive to become stronger adults. Thus, in this reproducing technique, one need to first generate

a widow array containing random values (named alpha), and then we use alpha in the following formula (equation 3), where x_1 and x_2 are the parents, and y_1 and y_2 are the offspring.

$$\begin{cases} y_1 = \alpha \times x_1 + (1-\alpha) \times x_2 \\ y_2 = \alpha \times x_2 + (1-\alpha) \times x_1 \end{cases} \quad (3)$$

While conducting this procedure $Nvar/2$ times, one should take care to avoid duplicating any of the randomly chosen numbers. Cannibalism score is then used to choose some of the fit people to add to the newly formed population. Afterwards, the offspring and the mother are placed to an array and ordered by their overall fitness value. These procedures are applicable to both sets.

- **Cannibalism:** Specifically, there are three distinct forms of cannibalism in action. The first kind of cannibalism is known as sexual cannibalism and it occurs when a female black widow consumes her husband while they are mating or shortly thereafter. The fitness scores were used to distinguish between male and female users of this method.

Cannibalism may also occur amongst members of the same species, such as when powerful spiderlings consume their weaker siblings. The number of survivors is calculated in this algorithm based on a cannibalism rating (CR) that we have established. It is not uncommon to see the third kind of cannibalism, in which the young spiders consume their mother. The fitness value is used to rank baby spiders on a scale of how healthy they are.

- **Mutation:** First, a sample of the population equal to $Mutepop$ is chosen at random. Each one of the optimal solutions, shuffles the array by exchanging any two adjacent members at random. $Mutepop$ is determined by the mutation rate.

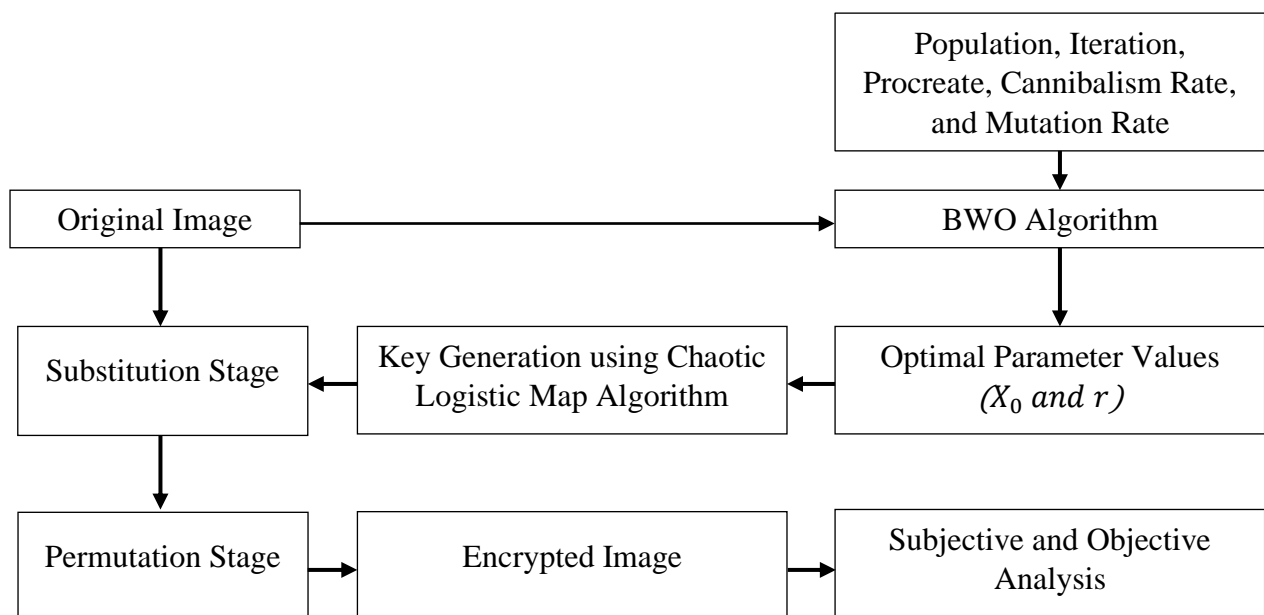


Figure 2 Proposed Image Encryption Method

4. Proposed Image Encryption Method

Figure 2 illustrates the working of the proposed method used for image encryption. The proposed method employs traditional confusion and diffusion architecture which is achieved using substitution and permutation stage. In substitution stage, exclusive-OR operation is performed between original image pixel and random key. A random key is generated using the chaotic logistic map algorithm. The optimal parameter values of chaotic logistic map are determined using the black widow optimization (BWO) algorithm. The BWO algorithm gives the optimal parameter values based on the objective function. We have designed an objective function based on entropy parameter. Further, in the permutation stage, circular shifting is performed horizontally and vertically based on two random numbers, K_1, K_2 to get encrypted image. K_1 performs the circular shift row-wise to achieve horizontal permutation, whereas K_2 performs the circular shift column-wise to achieve vertical permutation. The value of $K_1 K_2$ is determined by how many odd pixels are available in the row and column-wise. Next, subjective and objective analysis of encrypted image is performed to validate its performance over the existing method. In the last, encrypted image along with optimal parameter values of rx_n is communicated to the receiver to decrypt the image.

4.1 Determination of Optimal Parameter Values using BWO Algorithm

In this section, we have explained the way BWO algorithm determines the optimal parameter values of chaotic logistic map function.

1. In the first step, total number of populations, objective function, iterations, procreate rate, cannibalism rate, and mutation rate are defined.
2. In the second step, initial population of r and x_n is generated in the range of $[3.57 - 4]$ and $[0-1]$. Therefore, the dimension of each population is 2. The first value represents r and second value x_n .
2. In the third step, fitness evaluation of each population is done based on the objective function and best population is determined as best solution value of r and x_n .
3. In the fourth step, randomly populations are selected to generate new offspring's using procreate step.
4. In the fifth step, generated offspring are added in the initial population. Next, initial population is sorted based on the objective function.
5. In the sixth step, inappropriate population which provides inferior solutions are removed from the population using the cannibalism step.
6. In the seventh step, mutation step is performed randomly to update the population.
7. The whole process of generation is performed until optimal parameter values are found.

5. Results and Discussion

In this section, the simulation results and analysis are performed and compared with the existing methods to validate the performance of the proposed method. The benchmark grey scale images are taken under consideration for encryption purposes. The size of the images is 512×512 . The

benchmark images are published available on the USC SIPI image database [22]. MATLAB software is used for simulation and the system configurations are 2.70GHz-Intel(R) core (TM) i7-7500U CPU, 8GB RAM, and a 64-bit operating system. Table 1 shows the input parameter values of BWO algorithm to determine optimal parameter values of chaotic logistic map algorithm. Further, subjective and objective analysis of the proposed method is done and compared with the existing methods.


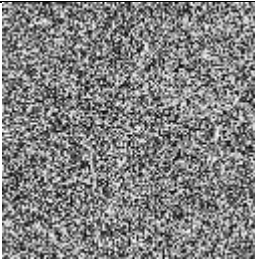

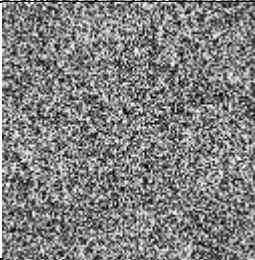

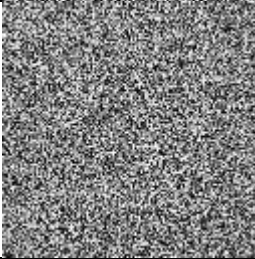
Table 1 Parameter Values of BWO Algorithm

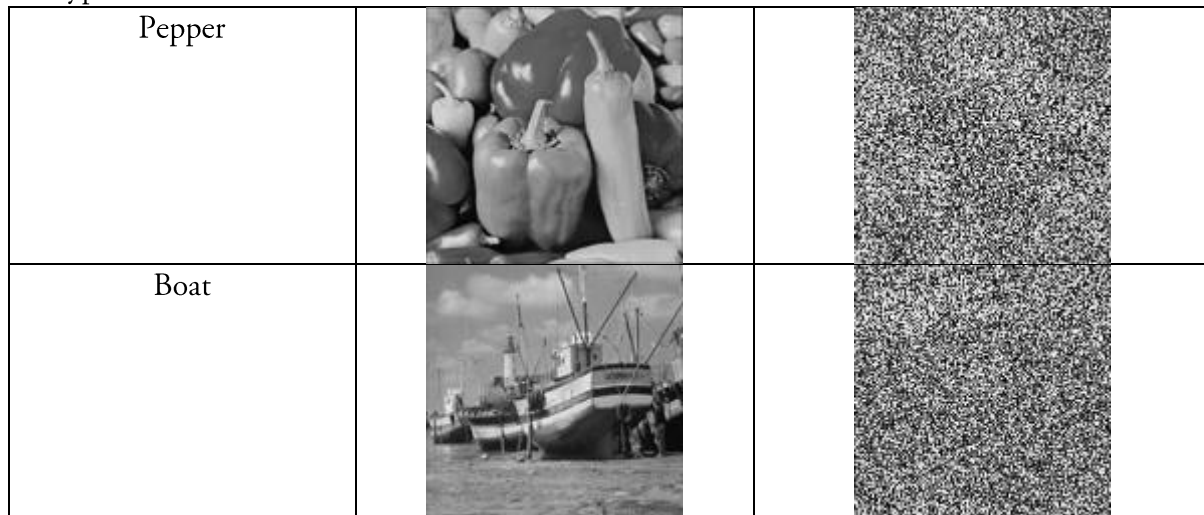
Parameter	Values
Population	50
Iterations	100
Procreate Rate	0.50
Cannibalism Rate	0.50
Mutation Rate	0.1
Lower and Upper Bound Values of x_n and r	(0,1) and (3.57,4)

5.1 Subjective Analysis

Table 2 shows the subjective analysis of the proposed method. Based on the visual quality, original and encrypted images are compared in this analysis. The result shows that the encrypted image is completely noisy. Thus, it is difficult for the attacker to determine original image from it.

Table 2 Subjective Analysis

Images	Original Image	Encrypted Image
Lena		
Baboon		
Barbara		



5.2 Objective Analysis

In this section, objective analysis of the proposed method is done to evaluate its performance and parameters are determined for it is explained below [23-26].

- **Convergence Rate:** Convergence rate defines how quickly bio-inspired algorithm searches the optimal solution. It is plotted between iteration v/s fitness function. Figure 3 shows the convergence rate of the BWO algorithm to determine the optimal parameter values of chaotic logistic map algorithm for Different Images. The result depicts that the BWO algorithm quickly searches the optimal solution due to parallel mating process and cannibalism stage.

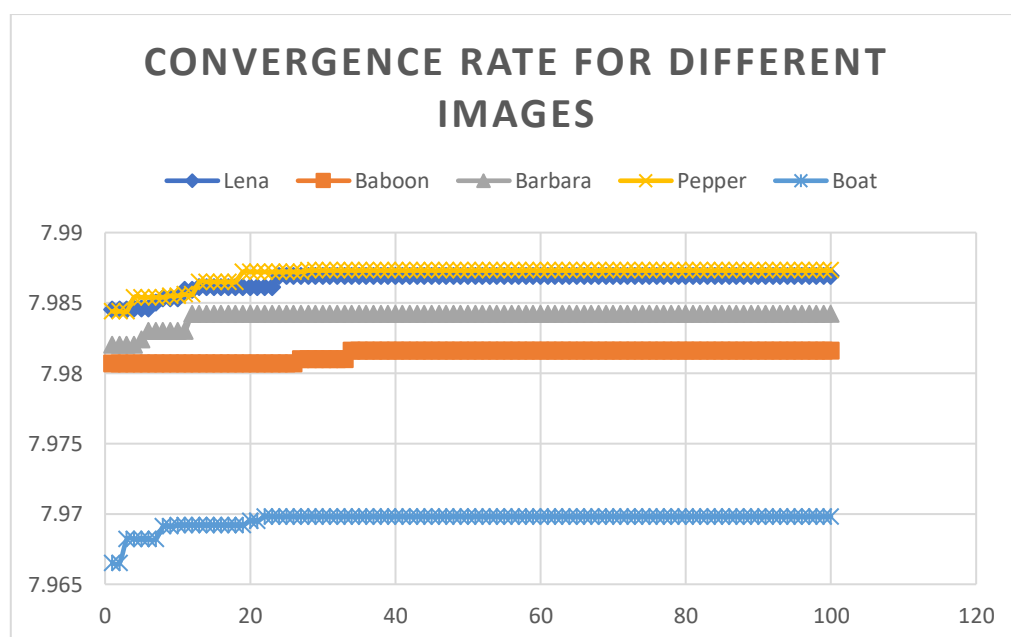


Figure 3 Convergence Rate for Different Images

- **Entropy:** This parameter measures the degree of uniformity and the uncertainty distribution in an encrypted process. It is determined using Eq. (4).

$$H(m) = \sum_{i=0}^{2^M-1} p(m_i) \times \log_2 \left(\frac{1}{p(m_i)} \right) \quad (4)$$

In Eq. (4), $p(m_i)$ denotes the probability of the pixel. The ideal value of entropy in the encryption process is 8. As a result, entropy closer to 8 indicates greater randomness in the image. Table 3 shows the entropy value of different images. The result shows that the proposed method achieves entropy near to 8. Thus, proposed method provides randomness in the image.

Table 3 Values of Entropy for Different Images

Images	Lena	Baboon	Barbara	Pepper	Boat
Original Entropy	7.4113	7.1293	7.3634	7.5517	7.1192
Encrypted Entropy	7.9869	7.9816	7.9842	7.9873	7.9698

- **Correlation Coefficient:** This parameter measures the amount of correlation between original and encrypted image. It is determined using Eq. (5).

$$r = \frac{\sum_{i=1}^M \sum_{j=1}^N (OI_{ij} - \overline{OI})(EI_{ij} - \overline{EI})}{\sqrt{((\sum_{i=1}^M \sum_{j=1}^N (OI_{ij} - \overline{OI})^2)(\sum_{i=1}^M \sum_{j=1}^N (EI_{ij} - \overline{EI})^2))}} \quad (5)$$

In Eq. (5), OI, EI denotes the original and encrypted image and $\overline{OI}, \overline{EI}$ denotes the mean values of it. In the encryption process, a lower value of correlation coefficient is required. This reflects a minimum correlation between original and encrypted image. Table 4 shows the correlation coefficient for different images. The result shows that the proposed method achieves correlation coefficient near to 0 value. This reflects that minimum correlation between original and encrypted image.

Table 4 Values of Correlation Coefficient for Different Images

Images	Lena	Baboon	Barbara	Pepper	Boat
CC	-0.0152	-0.0132	-0.0173	-0.0045	0.0455

- **Mean Square Error (MSE):** MSE determines the mean square error between original and encrypted image using Eq. (6).

$$MSE = \frac{\sum_{i=1}^M \sum_{j=1}^N (OI_{ij} - EI_{ij})^2}{M \times N} \quad (6)$$

In Eq. (6), OI, EI denotes the original and encrypted image and MN denotes the row and column of the images. A higher value of MSE required in image encryption methods. Table 5 shows MSE value of different images. The result shows that the proposed method achieves high value of MSE.

Table 5 Values of MSE for Different Images

Images	Lena	Baboon	Barbara	Pepper	Boat
MSE	3299.1	3098.2	2309	3102	3493.5

- Peak Signal to Noise Ratio (PSNR): It is determined using Eq. (7). A lower value of PSNR is required in the encryption process.

$$PSNR = 10 \log_{10} \frac{P^2}{MSE} \quad (7)$$

In Eq. (7), P denotes the peak value of the image. In the grey-scale images, its value is 255. Table 6 shows the PSNR values of different images. The result shows that the proposed method achieves low value of PSNR.

Table 6 Values of PSNR for Different Images

Images	Lena	Baboon	Barbara	Pepper	Boat
PSNR (in dB)	12.9469	13.2198	14.4966	13.2145	12.6982

- Number of Pixel Change Rate (NPCR): This parameter determines the rate of change of pixel values in two encrypted images with change of one pixel value in the original image. It is determined using Eq. (8).

$$NPCR = \frac{\sum_{i=1}^M \sum_{j=1}^N D(i,j)}{M \times N} \times 100 \quad (8)$$

In Eq. (8), $D(i,j)$ denotes the difference between two encrypted images. A higher value represents the strong encryption. Table 7 shows the NPCR value of different images. The result shows that the proposed method achieves high NPCR near to 100.

Table 7 Values of NPCR for Different Images

Images	Lena	Baboon	Barbara	Pepper	Boat
NPCR	99.4751	99.5361	99.6094	99.9920	99.5300

5.3 Comparative Analysis

Table 8 show the comparative analysis is performed with the existing methods based on entropy and number of pixel change rate. The result shows that the proposed method achieves superior results over Shelza Suri and Ritu Vijay [11] and approximate near values to Khadijeh Mirzaei Talarposthi and Mehrzad Khaki Jamei [10].

Table 8 Comparative Analysis based on Entropy Parameter

Images	Khadijeh Mirzaei Talarposthi and Mehrzad Khaki Jamei [10]	Shelza Suri and Ritu Vijay [11]	Proposed Method
Lena	7.9815	7.82200	7.9869
Baboon	7.9839	-	7.9816
Pepper	7.9857	-	7.9873
Boat	7.9784	-	7.9698
Cameraman	7.9893	7.79944	7.9779
Coin	-	7.80898	7.9765
Rice	-	7.82904	7.9461

Table 9 Comparative Analysis based on NPCR Parameter

	Khadijeh Mirzaei Talarposthi and Mehrzad Khaki Jamei [10]	Shelza Suri and Ritu Vijay [11]	Proposed Method
Lena	99.5918	99.2188	99.4751
Baboon	99.6027	-	99.5361
Pepper	99.6409	-	99.9920
Boat	99.6265	-	99.5300
Cameraman	99.6171	99.5117	99.9920
Coin	-	99.5117	99.4202
Rice	-	99.5117	99.3041

6. Conclusion and Future Scope

In this paper, a bio-inspired algorithm is successfully applied to determine the optimal parameter values of the chaotic logistic map algorithm that enhances its security. To achieve this goal, the black widow optimization algorithm is taken under consideration due to its faster convergence rate than the existing methods. The simulation evaluation is performed on standard dataset images. Furthermore, subjective analysis shows that the encrypted images are completely noisy, whereas objective analysis shows that the proposed method achieves high values of entropy, MSE, NPCR, and low values of correlation coefficient and PSNR. In the last, comparative analysis shows that the proposed method is superior results over Shelza Suri and Ritu Vijay [11] and approximate near values to Khadijeh Mirzaei Talarposthi and Mehrzad Khaki Jamei [10]. In the future, we will explore other chaotic map algorithms to enhance their security using bio-inspired optimization algorithms.

Acknowledgement

The authors are grateful to MeitY for the financial support through the ‘Visvesvaraya Fellowship’ and SMDP chips to system design’ project. The authors also want to express their sincere gratitude towards the Director, Thapar Institute of Engineering and Technology, Patiala for his persistent support and encouragement.

References

- [1] Kaur, Mandeep, Surender Singh, and Manjit Kaur. "Computational image encryption techniques: a comprehensive review." *Mathematical Problems in Engineering* 2021 (2021).
- [2] Arul Murugan, Chinnandi, and P. KarthigaiKumar. "Survey on image encryption schemes, bio cryptography and efficient encryption algorithms." *Mobile Networks and Applications* (2018): 1-6.

- [3] Zhang, Xiaoqiang, Xuesong Wang, and Yuhu Cheng. "Image encryption based on a genetic algorithm and a chaotic system." *IEICE Transactions on Communications* 98, no. 5 (2015): 824-833.
- [4] Samhita, Poluri, Prateek Prasad, K. Abhimanyu Kumar Patro, and Bibhudendra Acharya. "A secure chaos-based image encryption and decryption using crossover and mutation operator." *Int J Control Theory Appl* 9, no. 34 (2016): 17-28.
- [5] Kaur, Manjit, and Dilbag Singh. "Multiobjective evolutionary optimization techniques based hyperchaotic map and their applications in image encryption." *Multidimensional Systems and Signal Processing* 32, no. 1 (2021): 281-301.
- [6] Kanwal, Shamsa, Saba Inam, Mohamed Tahar Ben Othman, Ayesha Waqar, Muhammad Ibrahim, Fariha Nawaz, Zainab Nawaz, and Habib Hamam. "An Effective Color Image Encryption Based on Henon Map, Tent Chaotic Map, and Orthogonal Matrices." *Sensors* 22, no. 12 (2022): 4359.
- [7] Abdullah, Abdul Hanan, Rasul Enayatifar, and Malrey Lee. "A hybrid genetic algorithm and chaotic function model for image encryption." *AEU-International Journal of Electronics and Communications* 66, no. 10 (2012): 806-816.
- [8] Khalaf, K. S., M. A. Sharif, and M. S. Wahhab. "Digital Communication Based on Image Security using Grasshopper Optimization and Chaotic Map." *International Journal of Engineering* 35, no. 10 (2022): 1981-1988.
- [9] Noshadian, Saeed, Ata Ebrahimzade, and Seyed Javad Kazemitabar. "Optimizing chaos based image encryption." *Multimedia Tools and Applications* 77, no. 19 (2018): 25569-25590.
- [10] Talarposhti, Khadijeh Mirzaei, and Mehrzad Khaki Jamei. "A secure image encryption method based on dynamic harmony search (DHS) combined with chaotic map." *Optics and Lasers in Engineering* 81 (2016): 21-34.
- [11] Suri, Shelza, and Ritu Vijay. "A Bi-objective genetic algorithm optimization of chaos-DNA based hybrid approach." *Journal of Intelligent Systems* 28, no. 2 (2019): 333-346.
- [12] Mondal, Bhaskar, and Tarni Mandal. "A secure image encryption scheme based on genetic operations and a new hybrid pseudo random number generator." *Multimedia Tools and Applications* 79, no. 25 (2020): 17497-17520.
- [13] Niu, Ying, Zheng Zhou, and Xuncaizhang. "An image encryption approach based on chaotic maps and genetic operations." *Multimedia Tools and Applications* 79, no. 35 (2020): 25613-25633.
- [14] Hayyolalam, Vahideh, and Ali Asghar Pourhaji Kazem. "Black widow optimization algorithm: a novel meta-heuristic approach for solving engineering optimization problems." *Engineering Applications of Artificial Intelligence* 87 (2020): 103249.
- [15] Houssein, Essam H., Bahaa El-din Helmy, Diego Oliva, Ahmed A. Elngar, and Hassan Shaban. "A novel black widow optimization algorithm for multilevel thresholding image segmentation." *Expert Systems with Applications* 167 (2021): 114159.
- [16] Hu, Gang, Bo Du, Xiaofeng Wang, and Guo Wei. "An enhanced black widow optimization algorithm for feature selection." *Knowledge-Based Systems* 235 (2022): 107638.

- [17] Panahi, Fatemeh, Mohammad Ehteram, and Mohammad Emami. "Suspended sediment load prediction based on soft computing models and Black Widow Optimization Algorithm using an enhanced gamma test." *Environmental Science and Pollution Research* 28, no. 35 (2021): 48253-48273.
- [18] Mukilan, P., and Wogderess Semunigus. "Human object detection: An enhanced black widow optimization algorithm with deep convolution neural network." *Neural Computing and Applications* 33, no. 22 (2021): 15831-15842.
- [19] Al-Rahlawee, Anfal Thaer Hussein, and Javad Rahebi. "Multilevel thresholding of images with improved Otsu thresholding by black widow optimization algorithm." *Multimedia Tools and Applications* 80, no. 18 (2021): 28217-28243.
- [20] Zolfaghari, Behrouz, and Takeshi Koshiba. "Chaotic Image Encryption: State-of-the-Art, Ecosystem, and Future Roadmap." *Applied System Innovation* 5, no. 3 (2022): 57.
- [21] Kaur, Mandeep, Surender Singh, Manjit Kaur, Arjun Singh, and Dilbag Singh. "A systematic review of metaheuristic-based image encryption techniques." *Archives of Computational Methods in Engineering* (2021): 1-15.
- [22] "SIPI Image Database." n.d. Sipi.usc.edu. <https://sipi.usc.edu/database/>.
- [23] Zhen, Ping, Geng Zhao, Lequan Min, and Xin Jin. "Chaos-based image encryption scheme combining DNA coding and entropy." *Multimedia Tools and Applications* 75, no. 11 (2016): 6303-6319.
- [24] Abraham, Lini, and Neenu Daniel. "Secure image encryption algorithms: A review." *International journal of scientific & technology research* 2, no. 4 (2013): 186-189.
- [25] Avasare, Minal Govind, and Vishakha Vivek Kelkar. "Image encryption using chaos theory." In *2015 International Conference on Communication, Information & Computing Technology (ICCICT)*, pp. 1-6. IEEE, 2015.
- [26] Poursad, Yaghoub, Ramin Ranjbarzadeh, and Abbas Mardani. "A new algorithm for digital image encryption based on chaos theory." *Entropy* 23, no. 3 (2021): 341.