Using Whale Optimization Algorithm and Chaotic Map to Encrypt Images

[1]Narjis Mezaal Shati, [2]Dina Riadh Alshibani and [3]Musaab Riyadh
[1,2,3]Department of Computer Science, College of Sciences, Mustansiriyah University, Baghdad, Iraq.
[1]dr.narjis.m.sh@uomustansiriyah.edu.iq, [2]dinashibani@uomustansiriyah.edu.iq, [3] m.shaibani@uomustansiriyah.edu.iq

Correspondence should be addressed to Narjis Mezaal Shati : dr.narjis.m.sh@uomustansiriyah.edu.iq

Article Info
Journal of Machine and Computing (https://anapub.co.ke/journals/jmc/jmc.html)
Doi : https://doi.org/10.53759/7669/jmc202505102
Received 18 October 2024; Revised from 02 March 2025; Accepted 30 March 2025.
Available online 05 April 2025.

Abstract – Developing innovative methods to protect data transmitted over the Internet and stop unauthorized access to it is one of the most important challenges researchers encounter. A new approach to image data encryption has been introduced in this research, which is based on the chaotic map and Whale Optimization Algorithm (WOA). The encryption algorithm, which is entitled IEBCWOA, consists mainly of two phases: The first phase deals with shuffling the pixel positions by employing two keys for column and row permutation, respectively, generated by the Zaslavskii map, while the second phase deals with choosing the optimal substitution key by employing WOA and Zaslavskii Map. Several experiments have been carried out, and the results are compared to those of other researchers. The test findings indicated a satisfactory safety rate when compared to other existing techniques.

Keywords – Zaslavskii Map, Correlation, Whale Optimization Algorithm.

I. INTRODUCTION

With the recent revolutions of smart devices and the massive expansion of communications technologies in the last two decades, security has become a pressing requirement in data storage and communications. Image security specifically requires an extra application layer solution to shield transmitted data from undesired leaks or alteration while in transit. To maintain anonymity between authorized users, picture encryption algorithms seek to transform a typical image into an unidentifiable format [1,2]. The images contain high inter-pixel coherence features along with significant redundancy. Along with bulk data capacity, which makes traditional encryption standards inapplicable for image encryption as it is time-consuming with low encryption quality [3].

Numerous image encryption techniques, including ones based on DNA encryption, have recently been introduced in the literature [4,5,6], in addition to chaotic maps and cellular automata techniques [7]. Most of these methods have computational complexity and high costs.

At this time, optimization algorithms appeared to be the ideal solution in image encryption algorithms. PSO represents one of the standard optimization methods along with ACO and GA which are utilized for image encryption ([8][9] [10]).

This work proposes the use of WOA and 2D chaotic map-based image encryption. In the approach, the Zaslavskii Map is used to generate column and row permutation keys, respectively. Then it is used to generate several initial substitution keys. Additionally, to find the ideal substitution key, the created initial substitution keys are then added to the WOA technique. The optimization aims to minimize the correlation of the image's neighboring pixels.

This paper's remainder is arranged as follows: The basic ideas used in this paper have been presented in section 2. Although the performance measures are explained in section 3, the key generation and the proposed explanation in section 4, The experimental results are discussed in section 5. Comparisons with different algorithms are provided in section 6, and the final section concludes.

II. THEORETICAL BACKGROUND

This section provides an overview of the fundamental concepts related to the proposed approach, including the Zaslavskii Map and the WOA, which play a crucial role in improving optimization efficiency in the proposed image encryption.

Chaotic Map

Chaotic maps have great features such as non-periodicity, sensitivity to key values and parameters, mixing property, random behavior, etc., which make them a good candidate for cryptographic operations, especially image encryption [11,12]. In this research, 2D Zaslavskii maps are examined among the different maps.

Zaslavskii Map
It is a 2d chaotic map, defined as [13]:

$$xz_i = (xz_{i-1} + \delta(1 + \alpha yz_{i-1}) + \gamma\delta \cos(2\pi xz_{i-1}))mod\ 1 \quad (1)$$

$$yz_i = e^{-\tau}\ (yz_{i-1} + \gamma\cos(2\pi xz_{i-1}) \quad (2)$$

Where xzi and yzi are the new generated chaotic values while xzi-1 and yzi-1 are current chaotic values, and (γ,δ,α) are control parameters and e is exponentiation. This map evolve chaotically when δ=12.6695, α =9.1 and γ=3.0.

Whale Optimization Algorithm
The way whales hunt in the wild served as the model for WOA. the behavers of Whales can be categorized into three distinct behaviors: surrounded hunting, spiral encirclement, and random search. Equations 3-6 provide the definition of the mathematical model of encircled behavior [14].

$$W_s^d\ (t+1) = W_s^d\ (t) - \gamma\delta \quad (3)$$

$$\delta = |\omega W_b^d\ (t) - W_s^d\ (t)| \quad (4)$$

Where the updated location of the s individual in t is represented by W_s^d (t+1) , W_s^d (t) indicate S's current position , Iteration count is represented by t , wherein d stands for the dimension of the solution. γ and ω are defined as in Eq. 5 and 6 [15].

$$\gamma = (2c_1 - 1)\alpha \quad (5)$$

$$\omega = 2c_2 \quad (6)$$

Where c1 and c2 are random generated numbers in range of [0,1]. α in range [0,2] linearly decreases. The definition of the spiral encircled behavior mathematical model is found in Equations 7-8.

$$W_s^d\ (t+1) = W_s^d\ (t) + \beta_b e^{bl}\, cos(2\pi l) \quad (7)$$

$$\beta_b = |W_b^d\ (t) - W_s^d\ (t) \quad (8)$$

Where W_b^d best position in t, a random number in the interval [-1,1] is identified as l . Finally, the mathematical model of random search as defined in Eq.9 and 10 [16].

$$W_s^d\ (t+1) = W_s^d\ (t) - \gamma\delta \quad (9)$$

$$\delta = |\omega W_{ran}^d\ (t) - W_s^d\ (t)| \quad (10)$$

Where W_{ran}^d is a randomly selected solution. γ is a control parameter used to switch between random search behavior and spiral behavior.

III. PERFORMANCE METRIC

This section provides a general idea about the performance metrics which is used in the proposed approach, including the information entropy, the correlation, along the differential attacks.

Information Entropy
Randomization levels in gray pixel value distribution serve as a measurement basis. The mathematical model of information entropy is defined as in Eq. 11 [17].

$$H(m) = \sum_{i=1}^{M} p(m_i) log \frac{1}{p(m_i)} \quad (11)$$

Where The symbol m's occurrence probability is denoted by p(mi), and M is the total amount of bits that each symbol contains. In theory, the optimal value of entropy is 8.

Correlation

The similarity or dissimilarity between adjacent image pixels is measured by a correlation coefficient. The correlation coefficient exists between -1 and 1 which shows negative correlation at -1 and positive correlation at +1 while 0 stands for absence of correlation. Correlation mathematical model expressed as defined in Eq. 12 [18,19].

$$r_{x,y} = \frac{cov(n,m)}{\sqrt{D(n)}\sqrt{D(m)}} \tag{12}$$

$$cov(x,y) = \frac{1}{N}\sum_{i=1}^{N}(n_i - E(n))(m_i - E(m)) \tag{13}$$

$$D(n) = \frac{1}{N}\sum_{i=1}^{N}(n_i - E(n))^2 \tag{14}$$

$$E(x) = \frac{1}{N}\sum_{i=1}^{N}(n_i) \tag{15}$$

Differential Attack

To examine how altering a single bit or pixel in the plain image affects the cipher image, UACI and NPCR are used. The mathematical representation of UACI and NPCR are defined in Eq. 16 and 17 [20,21,22].

$$UACI(c1,C2) = \frac{\sum_{i=1}^{M}\sum_{i=1}^{N}|c1(i,j)-c2(i,j)|/255}{M\times N}\times 100 \tag{16}$$

$$NPCR(c1,C2) = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}D(i,j)}{M\times N}\times 100 \tag{17}$$

Where

$$D(i,j)\begin{cases}0 \quad if\ C1(i,j) = c2(i,j)\\ 1\ if\ C1(i,j) \neq C2(i,j)\end{cases} \tag{18}$$

IV. THE PROPOSED SYSTEM

There are primarily two steps in the proposed IEBCWOA algorithm. Dealing with the pixel positions shuffling is the first step. While the second stage has been used to change the characteristics of the pixels. The general layout of the proposed IEBCWOA algorithm is displayed in **Fig 1**.

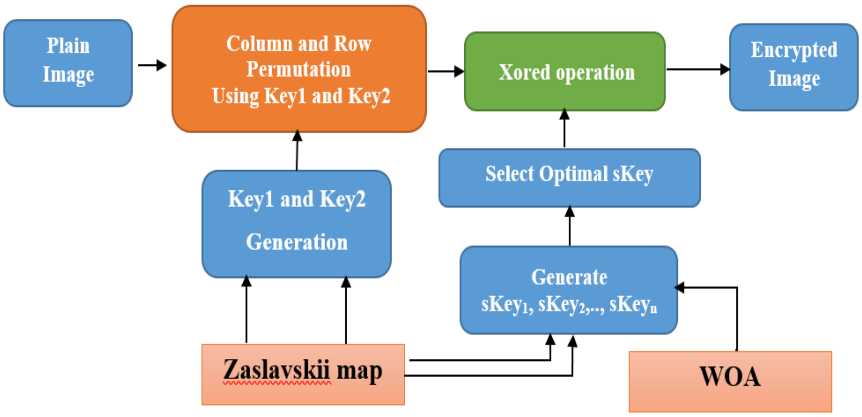

Fig 1. The Suggested IEBCWOA Algorithm General Structure.

The following succinctly describes the baseline of the suggested image encryption system:

- a M×M grayscale image (gimg) has been read.
- The very first phase consists of:
    - Generate chaotic shuffling keys (key1 and key2).
    - Shuffle the image column with key1.
    - Shuffle the image rows with key2.
- Second phase includes:
    - Generate initial substitution keys (sKey1, sKey2,.., sKeyn) by using chaotic map.
    - Select the optimal sKey by WOA.

- Pass the optimized sKey and the first phase's output image through an XOR operation.

The encryption mentioned above is similar to the decryption process, however it is done in reverse.

Encryption Key Generation

In most encryption systems, the encryption key is an important feature. The encryption system will be easily cracked if the key is improperly chosen or the key space is too tiny, regardless of how carefully thought out and designed the encryption method is. The complexity of key generation is therefore a crucial objective in the design of a cryptosystem.

Shuffling Keys Generation

The chaotic generated values as described by the equations are first crossed to build a chaotic matrix mat of size (M+M), where M is the number of image columns and rows, respectively. Next, copy the mat's first M elements into (Per_C) and its second M elements into (Per_R). Then Apply LPV rules to Per_C and Per_C to obtain key1 and key2. **Fig 2** shows the shuffling keys generation.

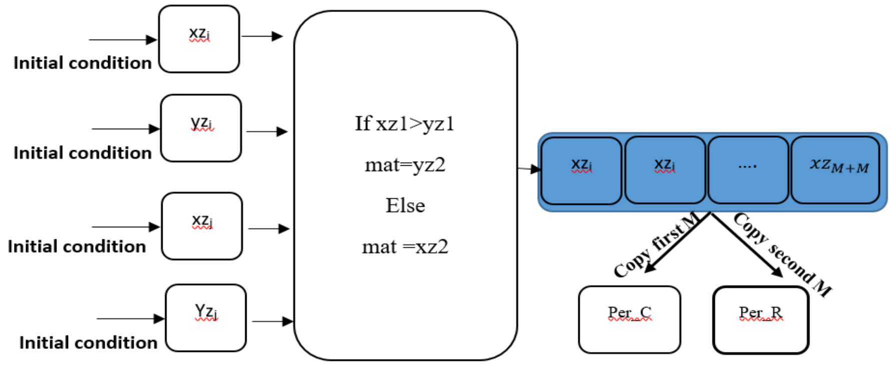

Fig 2. The Shuffling Keys Generation.

Substitution Keys Generation

The Zaslavskii map has been used to formulate the initial substitution keys by generating real values random numbers, which are converted into an integer number and xored with the shuffled image.

The first step is to generate initial substitution keys. The Zaslavskii map is iterated for M×M times, where M represents the dimension of the shuffled image; the ith key is represented as a one-dimensional continuous vector, namely *ckey*. Then LPV rule is employed to convert the continuous values of *the ckey* vector into the discrete vector, namely *dkey*, which is further converted into a 2-dimensional matrix of size M × M, namely skey, which further XORed with the shuffled image. Finally, the correlation value is computed and stored for the ith key. This process is repeated for N times where N is the number of the initial keys. The second step is to choose the optimal substitution key by using WOA. Algorithm 1 show the details of selecting the optimal substitution key.

The Encryption Algorithm

After selecting the optimal substitution key, the final encryption process is performed by xored the optimal encryption key and the permutated image.

```
Algorithm 1
Input: initializing the substitution keys to isKeys.
Output: the optimal substitution key osKeys
L←number of isKeys.
Initialized a one-dimensional matrix cor of size L.
    For each sKey in isKeys do
        Calculate the correlation c by xored the shuffled image and sKey.
        cor[sKey]←c.
    End for
Sort cor matrix in ascending order.
bKey←sKey with lowest correlation.
Bc←cor[0].
    While( i < maximum number of iterations ) do
        For each sKey in isKeys do
            Convert skey into one dimensional vector oKey of size M × M
            isKeys[sKey]←oKey.
        End for
        For each oKey in isKeys do
            Update WOA parameter
            If (p<0.5)
                If (|A|<1)
                    Update the currnet sKey as defined in Eq.
                else
                    Select a random key rKey
                    Update sKey with rKey as defined in Eq.
                End if
            else
                pdate the currnet sKey as defined in Eq.
            End if
        End for
        Convert each key into an integer values using LPV rule.
        Formulate each key into a 2matrix and Xored with the shuffled image
        Calculate the correlation for all the updated keys.
        Update bKey and Bc
    End while
Return bKey.
End of algorithm
```

V. RESULTS AND DISCUSSION

In this section, a detailed investigation of the proposed IEBCWOA algorithm performance has been introduced. Security analysis, including some crucial ones like histogram analysis, key sensitivity analysis, statistical sensitivity, etc., has been described in order to demonstrate the suggested IEBCWOA's effectiveness against the most frequent assaults. Six 128× 128 grayscale pictures are chosen.

The proposed approach has been tested on a laptop running Matlab software on a 64-bit operating system running Windows 11 and equipped with a 13th Gen Intel(R) Core (TM) i7-13700H 2.40 GHz CPU and 16 GB of RAM. The suggested algorithm for IEBCWOA **Fig 3** shows the results of the performance of the suggested IEBCWOA.

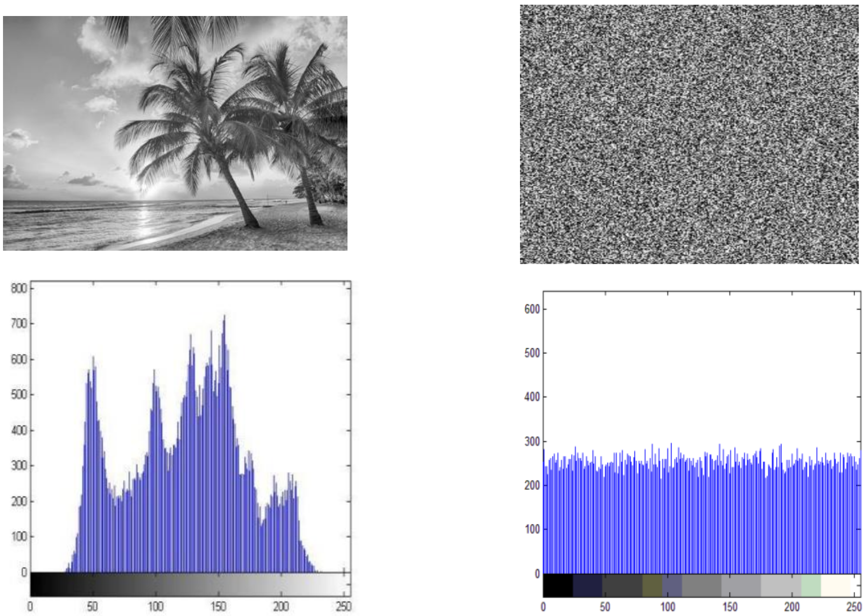

Fig 3. The Suggested IEBCWOA Outcome and Histogram Examination.

Histogram Analysis

Fig 3 depicts the result of this examination. The figure indicates that the encrypted image has a widespread range over the different gray values which is very close to being uniform indicating that the proposed IEBCWOA provides a strong barrier against numerical attack.

Correlation

The correlation values for plain images and their encrypted counterparts are displayed in **Tables 1 and 2**, respectively. **Table 1** and **Table 2** show that the plain image correlation values are near to 1, while the encrypted correlation values are close to 0, implying that the proposed algorithm has the capability to remove the correlation between neighboring pixels.

Table 1. Correlation Values for Plain Images

No.	Horizontal	Vertical	Diagonal
Image 1	0.9823	0.9863	0.9731
Image 2	0.8179	0.8132	0.7314
Image 3	0.9174	0.9623	0.8726
Image 4	0.9760	0.9350	0.8527
Image 5	0.9458	0.9315	0.8861
Image 6	0.9359	0.9194	0.8742

Table 2. Correlation Values for Encrypted Images

No.	Horizontal	Vertical	Diagonal
Image 1	-0.0007	0.0024	-0.0137
Image 2	-0.0020	0.0057	-0.0067
Image 3	0.0027	-0.0061	-0.0086
Image 4	0.0052	-0.0017	0.0153
Image 5	-0.0035	0.0026	0.0048
Image 6	0.0095	-0.0069	0.0074

Table 3. Entropy Values for Plain and Encrypted Images

No.	Plain image	Encrypted image
Image 1	7.2710	7.9981
Image 2	7.4797	7.9976
Image 3	7.4644	7.9986
Image 4	7.4696	7.9978
Image 5	6.5751	7.9962
Image 6	6.9798	7.9979

The entropy values of the plain image and the equivalent encrypted image are shown in **Table 3**. The table indicates that the encrypted image's entropy is closer to 8. This indicates the potential of the proposed IEBCWOA algorithm to resist statistical attack by introducing high randomness to the encrypted image, which makes inferring any information very insignificant.

Table 4. UACI and NPCR Metrics Values

No.	UACI Metric	NPCR Metric
Image 1	33.50	0.9952
Image 2	33.62	0.9981
Image 3	33.82	0.9994
Image 4	33.74	0.9968
Image 5	33.67	0.99384
Image 6	33.58	0.99720

The UACI and NPCR values for the suggested IEBCWOA algorithm are displayed in **Table 4.** Looking at the table, it can be seen that the UACI is closer to 33.50, which shows the ability of the proposed IEBCWOA algorithm to cope with differential attacks. Furthermore, the NPCR values are very close to 100%, this illustrates the great sensitivity of the proposed IEBCWOA algorithm to slight modifications of plain pictures and its high ability to counter plaintext attacks.

VI. COMPARISON WITH EXISTING WORK

Several approaches indicated in [8] and [9] have been compared with the findings of the introduced method in this section. While entropy, NPCR, and UACI are listed in **Table 6**, the correlation analysis is presented in **Table 5**. According to the results mentioned, the introduced approach performs better than the [8] and [9].

Table 5. Correlation Values

Method	Horizontal	Vertical	Diagonal
Original image	0.8687	0.9810	0.8221
[8]	−0.0021	−0.0032	0.0037
[9]	0.0036	0.0023	0.0039
IEBCWOA	-0.0032	-0.0046	-0.0015

Table 6. Comparison Values

Method	UACI	NPCR	Entropy
[8]	31.40	0.8641	7.8760
[9]	32.51	0.8970	7.7865
IEBCWOA	33.92	0.9996	7.9995

VII. CONCLUSION

This subject has been extensively studied and addressed in earlier research on chaotic maps. However, this study offers a reliable and effective technique for encrypted images that uses an optimization algorithm and chaotic map. Greyscale images measuring 128 by 128 pixels have been used to test the suggested approach. According to the experimental findings, the highest values are obtained for UACI, NPCR, entropy, and correlation. Based on the testing findings, it can be said that the proposed algorithm has a respectable level of security because it can effectively withstand a range of statistical attacks.

Acknowledgement

The author thanks the Department of Computer Science, College of Science, Mustansiriyah University, Baghdad-Iraq for supporting this work.

CRediT Author Statement

The authors confirm contribution to the paper as follows:

Conceptualization: Narjis Mezaal Shati, Dina Riadh Alshibani and Musaab Riyadh; **Methodology:** Narjis Mezaal Shati and Dina Riadh Alshibani; **Software:** Musaab Riyadh; **Data Curation:** Narjis Mezaal Shati; **Writing- Original Draft Preparation:** Narjis Mezaal Shati, Dina Riadh Alshibani and Musaab Riyadh; **Visualization:** Musaab Riyadh; **Investigation:** Narjis Mezaal Shati and Dina Riadh Alshibani; **Supervision:** Narjis Mezaal Shati and Musaab Riyadh;**Validation:** Narjis Mezaal Shati and Dina Riadh Alshibani; **Writing- Reviewing and Editing:** Narjis Mezaal Shati, Dina Riadh Alshibani and Musaab Riyadh; All authors reviewed the results and approved the final version of the manuscript.

Data Availability

No data was used to support this study.

Conflicts of Interests

The author(s) declare(s) that they have no conflicts of interest.

Funding

No funding agency is associated with this research.

Competing Interests

There are no competing interests

References

[1]. Ahmad, M., Alam, M. Z., Umayya, Z., Khan, S., & Ahmad, F. An image encryption approach using particle swarm optimization and chaotic map. International Journal of Information Technology, (2018), 10, 247-255. https://doi.org/10.1007/s41870-018-0099-y

[2]. Kocak, O., Erkan, U., Toktas, A., & Gao, S. PSO-based image encryption scheme using modular integrated logistic exponential map. Expert Systems with Applications, (2024), 237, 121452. https://doi.org/10.1016/j.eswa.2023.121452

[3]. Huang, W., Jiang, D., An, Y., Liu, L., & Wang X. A novel double-image encryption algorithm based on Rossler hyperchaotic system and compressive sensing. IEEE Access, (2021), 9, 41704-41716. Doi:10.1109/ACCESS.2021.3065453

[4]. Alshibani, D. R., Shati, N.M., & Ahmed, N.T. DNA Genetic Recombination based Image Encryption using Chaotic Maps. Indian Journal of Public Health Research & Development , (2019), 10, no. 6. Doi: 10.5958/0976-5506.2019.01432.3

[5]. Alshibani, D. R., & Qassir S. A. Image enciphering based on DNA Exclusive-OR operation union with chaotic maps. In 2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA), (2016), pp. 1-6. doi: 10.1109/AIC-MITCSA.2016.7759944

[6]. Allawi, S. T., & Alshibani, D. R. Color image encryption using LFSR, DNA, and 3D chaotic maps. International journal of electrical and computer engineering systems 13, (2022), 10, 885-893. https://doi.org/10.32985/ijeces.13.10.4

[7]. Li, L., Luo Y., Qiu, S., Ouyang, X., Cao, L., & Tang, S. Image encryption using chaotic map and cellular automata. Multimedia Tools and Applications 81, (2022), 28, 40755-40773. https://doi.org/10.1007/s11042-022-12621-9

[8]. Karthikeyini, S., Sagayaraj, R., Rajkumar, N., & Pillai, P.K. Security in Medical Image Management Using Ant Colony Optimization. Information Technology and Control 52, (2023), 2, 276-287. https://doi.org/10.5755/j01.itc.52.2.32532

[9]. Baagyere, E. Y., Agbedemnab, P. A.-N., Qin, Z., Daabo, M. I., & Qin, Z. A multi-layered data encryption and decryption scheme based on genetic algorithm and residual numbers. IEEE Access , (2020), 8, 100438-100447. doi: 10.1109/ACCESS.2020.2997838

[10]. Wang, J., Song, X., & Abd El-Latif, A. A. Single-objective particle swarm optimization-based chaotic image encryption scheme. Electronics 11, (2022), 16, 2628. https://doi.org/10.3390/electronics11162628

[11]. Ghazanfaripour, H., & Broumandnia, A. Designing a digital image encryption scheme using chaotic maps with prime modular. Optics & Laser Technology, (2020), 131, 106339. https://doi.org/10.1016/j.optlastec.2020.106339

[12]. Wang, S., Peng, Q., & Du, B. Chaotic color image encryption based on 4D chaotic maps and DNA sequence. Optics & Laser Technology , (2022), 148, 107753. https://doi.org/10.1016/j.optlastec.2021.107753

[13]. Ramakant Parida, R. N., Kumar Singh, B., & Pradhan, C. A Novel Approach for Image Encryption Using Zaslavskii Map and Arnold's Cat Map. In Data Engineering and Intelligent Computing: Proceedings of ICICC 2020, (2021), 1407,269-282. Springer Singapore. https://doi.org/10.1007/978-981-16-0171-2_26

[14]. Qu, S., Liu, H., Xu, Y., Wang, L., Liu, Y., Zhang, L., Song, J., & Li, Z. Application of spiral enhanced whale optimization algorithm in solving optimization problems. Scientific Reports 14, (2024), 1, 24534. https://doi.org/10.1038/s41598-024-74881-9

[15]. Liu, L. S. & Zhang, R. S. Multistrategy Improved Whale Optimization Algorithm and Its Application. Comput. Intel. Neurosci, 2022, Article ID 3418269. https://doi.org/10.1155/2022/3418269

[16]. Chen, X. Research on New Adaptive Whale Algorithm. IEEE Access, (2020), 8, 90165–90201. doi: 10.1109/ACCESS.2020.2993580

[17]. Alexan, W., ElBeltagy, M., & Aboshousha, A. Rgb image encryption through cellular automata, s-box and the lorenz system. Symmetry, (2022), 14, 3, 443. https://doi.org/10.3390/sym14030443

[18]. Allawi, S.T. & Alagrash, Y.H., A New Image Encryption Method Combining the DNA Coding and 4D Chaotic Maps. International Journal of Intelligent Engineering & Systems, (2025), 18,1,860-873. DOI:10.22266/ijies2025.0229.61

[19]. Mehdi, S. A., & Ali, Z. L. Image encryption algorithm based on a novel six-dimensional hyper-chaotic system. Al-Mustansiriyah journal of science, (2020), 31, 1, 54-63. https://doi.org/10.23851/mjs.v31i1.739

[20]. Maryoosh, A. A., Dhaif, Z. S., & Mustafa, R. A. Image confusion and diffusion based on multi-chaotic system and mix-column. Bulletin of Electrical Engineering and Informatics 10, (2021), 4, 2100-2109. https://doi.org/10.11591/eei.v10i4.2942

[21]. Thabit, Z. H., Mehdi, S. A., & Nema, B. M. Enhancing Color Image Security: Encryption with Dynamic Chaotic Three-Dimensional System and Robust Security Analysis. Al-Mustansiriyah Journal of Science , (2023), 34, 4, 87-95. https://doi.org/10.23851/mjs.v34i4.1411

[22]. Caffey JC, Moe R, Freund MA, Hutton J, inventors; Carbomedics Inc., assignee. Heart valve stent with alignment posts. United States patent US 6,635,085. 2003 Oct 21.