Original Article

War Optimization Method for Image Encryption Algorithm Based on A Chaotic Bit-Plane Decomposition

S. Kaliswaran[1], M. Y. Mohamed Parvees[2]
[1]Research Scholar, Annamalai University, Chidambaram
[2]Research Supervisor, Annamalai University, Chidambaram
Email: kaliswaran1976@gmail.com
DOI: 10.47750/pnr.2022.13.S06.343

Abstract

In this paper, develop image encryption algorithm based on a chaotic bit-plane decomposition and optimization algorithm of a War Optimization Algorithm (WOA). Initially, utilization of SHA-256 hash algorithm for computing the plaintext images hash parameter as initial parameter of the fractional Lorenz hyperchaotic system after the process. Use the chaotic sequence for permuting plaintext image in a bit plane to achieve the scrambled images. After that, block the scrambles image into four sub images of similar size and count the hash parameter of every row of every block through the SHA-256 hash algorithm as the initial parameter of the Sine-Tent Logistic chaotic system. Utilize the achieved chaotic sequence to substitute the images. After that, the four sub-block images to get the last encrypted image and the population can be achieved. At last, utilization information entropy of ciphertext images as the fitness function of WOA. Choose the ciphertext image with the optimal information entropy of ciphertext images as the fitness function of the WOA. Select the ciphertext image with the best information entropy from the population as the optimal encrypted image, and then, return the position value of the best war source meanwhile. The proposed method is implemented in MATLAB and performance is analyzed with performance metrices. The proposed method is compared with the conventional techniques.

Keywords: image encryption, war optimization algorithm, ciphertext image, SHA-256 hash algorithm and chaotic bit plane decomposition.

1. INTRODUCTION

Of late, image encryption has been an attractive area of research. It is widely regarded as an effective strategy for secure exchange [1]. Each image encryption computation aims to produce high quality of a noisy image to be sensible. Also, image encryption has a great part to ensure classified transmission and image range over the Internet. Advanced correspondence has become more extensive with the rapid advancement of internet innovation. Individuals can send a computerized image over the Internet anytime [2], anywhere. This has brought about the advancement of computerized image encryption [3]. The variety of techniques that address computerized image encryption in exams is related to the ever-expanding need for security. Image encryption in light of chaos technique is an original encryption strategy for images, where a random disordered group is used to scramble the image as a successful way to take care of the immobility problems of deep secure and fast image encryption
[4]. Throughout recent years, various adaptations of the mash process have been introduced. Four methods have been adopted for image encryption, using different standards separately and achieving similar goals.

The four standards cover partition and secret division, continuous state, chaotic dynamical structures, and present-day cryptography [5], each with extraordinary highlights. Chaotic-based Compressive Specific Image Coding. To begin with, the plain text image is first divided into some blocks by the proposed process [6]. The link is still up in the air. The module with the most significant coupling coefficients is pixel-wise eXclusive OR-2ed (XORed), which consists of random numbers from a slanted tent guide according to a predetermined edge value. Finally, the entire image is sequenced by two arbitrary continuums made of Two-Dimensional Ellipse Reflecting Chaotic System (TD-ERCS) chaotic guides. Be that as it may, applying cryptographic techniques to image information conflicts with textual information. Image information is not easily and quickly obtained by traditional text encryption calculations, for example, RSA and DES, due to factors such as complexity [7], high increments, and image focus, especially high connectivity between continuous applications.

Another problem with these computations is length, and their main feature is that, due to the amount of scrambled information, the use of constrained-length keys makes the strategy insecure against ciphertext attacks [8]. With the advancement of enterprise innovation, the age of news gathering is approaching, and data and information security is becoming increasingly important. Due to its natural, clear and sensible characteristics, image data has become a key transporter in human social connections and data movements [9]. Security of photos is really important. Image encryption is a specific innovation used to address image security concerns. Conventional encryption techniques, such as DES and AES, cannot meet the current needs of image encryption due to the enormous number of attributes, areas of strength for information, and high apparent repetition. Accordingly, sets of encryption computations such as the compressed sensing theory, the chaos theory [10], and the DNA coding theory have been proposed.

The main contribution of the research is providing as follows,

- In this paper, develop image encryption algorithm based on a chaotic bit-plane decomposition and optimization algorithm of a WOA. Initially, utilization of SHA-256 hash algorithm for computing the plaintext images hash parameter as initial parameter of the fractional Lorenz hyperchaotic system after the process.

- Use the chaotic sequence for permuting plaintext image in a bit plane to achieve the scrambled images. After that, block the scrambles image into four sub images of similar size and count the hash parameter of every row of every block through the SHA-256 hash algorithm as the initial parameter of the Sine-Tent Logistic chaotic system.

- Utilize the achieved chaotic sequence to substitute the images. After that, the four sub-block images to get the last encrypted image and the population can be achieved. At last, utilization information entropy of ciphertext images as the fitness function of WOA.

- Choose the ciphertext image with the optimal information entropy of ciphertext images as the fitness function of the WOA. Select the ciphertext image with the best information entropy from the population as the optimal encrypted image, and then, return the position value of the best war source meanwhile.

The remaining portion of the paper is pre-arranged as follows; section 2 provides the literature review of the image encryption techniques. Section 3 provides the background study of the image encryption technique. Section 4 given the detail explanation of the proposed methodology. The outcome evaluation of the system is given in the section 5.

2. Literature Review

In literature, few works are reviewed related with image encryption for enhance the security specially for images.

Yaghoub Pourasad et al., [11] introduced a chaotic technique based digital image encryptions to combat image. This process uses irregular chaos successions for encrypting images and is a deep and fast technique for image encryption. Limited accuracy is one of the disadvantages of this procedure. This paper examines the wavelet transform value of chaos sequence and find gaps. Later, an original method for digital image encryption was proposed and worked out in past calculations.

Arslan shafique et al., [12] introduced a noise resistant image encryption scheme. Here, a cubiclogistic map, discrete wavelet transform (DWT) and bit-plane extraction technique are used to encrypt medical images at bit level instead of pixel level. The proposed work is divided into three sections; In the first and last part, the image is scrambled in spatial space. A central section of the proposed computation is dedicated to DWT integrated recurrence space encryption. Since the recurrence space encoding section is a sandwich between two spatial area encoding sections, it was considered a "sandwich encryption". The proposed computation is lossless in that it can decode specific pixel inversions of an image.

Fawad Masood et al., [13] have presented a lightweight cryptosystem in view of Henan chaotic guide, Brownian motion and Chen's chaotic structure. The performance of the proposed framework is demonstrated by histogram investigation, adjacent pixels connectivity test, variance test, homogeneity test, power test, NIST test, mean square error, data entropy, pixel number generation rate, normalized force, changing rate and timing precision from above. Experimental results show that the proposed cryptosystem is a lightweight algorithm that can achieve a better level of security for individual image-based patient data encryption.

Ali momeni asl et al., [14] introduced a scale-invariant different image encryption technique in three-layer space. From the beginning, the two-layer colour image is transformed into a three-layer space, and in this situation, the red, green, and blue type ranges are isolated into a set of dark level square sub-images. Then, 3D transformation and 3D transform operation are performed on sub-images to have distortion and diffusion properties. In the shift operations, the pixel overlays of the sub images are shifted with the correct keys with the help of XOR and round shift operators. In the position function, the location of the pixels was transformed using a scaled three-layer Bedlam mapping. To have a size-invariant three-layer condition, the subimages were divided into at least one window of equal size, and then 3D isolated perturbation guidance tasks were performed in each window with independent keys.

S. Saravanan et al., [15] have developed an improved HCM for improving novel image encryption. The proposed image encryption model includes 4 stages, for example, image pre-processing, key generation, image encryption using efficient HCM, and image unscrambling. In pre-processing, the RGB image is converted to a grayscale image, and the key was generated by SHA-256 cryptographic hash calculation. Also, image encryption was done by HCM combined with 2DLCM and PWLCM.

3. Background study of the model

This background sturdy of the projected structure is given in this portion. Based on the sensitivity, uncertainty, ergodicity, randomness to initial parameters and conditions, chaotic structures can be efficiently utilized in privacy communication architectures. This paper utilizes the sine tent logistic chaotic structure and fractional order super Lorenz chaotic systems. The WOA is utilized to optimize the encrypted image to achieve an encrypted image with a best encryption operation. The background study model of the system is presented in this section.

The sine tents logistic chaotic system

Integer order chaotic system contains hyperchaotic systems and one-dimensional chaotic systems. One dimensional chaotic system normally consists the tent chaotic map. Many of the one-dimensional chaotic structure contains one variable in addition some variables designing them vulnerable to resulting and attackers in data leakage [16]. In this paper, utilize the sine tent logistic chaotic system. The mathematical formulation of the system is presented as follows,

$$z_{N+1} = \begin{cases} \sin\left[\pi\left((1-2*|z_N-0.5|)+\left(\mu*z_N*(1-z_N)\right)\right)\right] & z_N > 1 \\ \sin\left[\pi\left((1-2*|z_N-0.5|)+\left(\mu*z_N*(1-z_N)\right)\right)\right] & z_N < 0 \end{cases} \quad (1)$$

In the sine tent logistic chaotic system, the Lyapunov index of the chaotic system is higher than 0 at different parameter in the value $\mu\epsilon(0,8)$. The chaotic sequence created contain best pseudorandom behaviours.

The fractional hyper Lorenz chaotic system

The fractional order chaotic dynamic structure contains a complicated in addition rich dynamic characteristics than the integer order architecture with the additional advantages of empowering unpredictability and randomness behaviour. Additionally, a fractional order chaotic system is offer high essential variables for the encryption system, which empowers the key space in addition empowering the security behaviours of the structure. The chaotic sequence complexity may be efficiently empowered in addition the encryption is high sage which thanks to the fractional chaotic systems unique memory characteristics. Different academics contains fractional order chaotic systems to encrypt photos in recent years. The mathematical design of fractional hyper-Lorenz chaotic system is presented as follows,

$$\begin{cases} \frac{d^{Q1}X}{dt^{Q1}} = \sigma(Y - X) + \omega \\ \frac{d^{Q2}X}{dt^{Q2}} = RX - Y - XZ \\ \frac{d^{Q4}X}{dt^{Q4}} = d\omega - XZ \end{cases} \quad (2)$$

Here, Z, Y, X, ω can be defined as the state variables of the architecture. Here, $Q1, Q2, Q3, Q4 = 0.995$, $d = 1.3, r = 28, \beta = \frac{8}{3} and\ \sigma = 10$ which is in a chaotic state.

4. Proposed System Model

This paper initially utilizes the fractional Lorenz hyperchaotic architecture to scramble every bit plane of the plaintext image after that its recombined by 8-bit planes into a scrambled image after scrambling. The scrambled image can be split into blocks after that every piece can be substitutes through the consideration of sine tent logistic chaotic system to create an initial population consisting different encrypted images. Here, WOA is utilized to optimize the entropy parameter of the encrypted image which achieved by considering the fitness function. Different ways are considered to achieve the optimal ciphertext image with the efficient data entropy, the position parameter of the optimal war source returns to manage subsequent decryption process.

The complete architecture of the proposed method is presented in the figure 1.

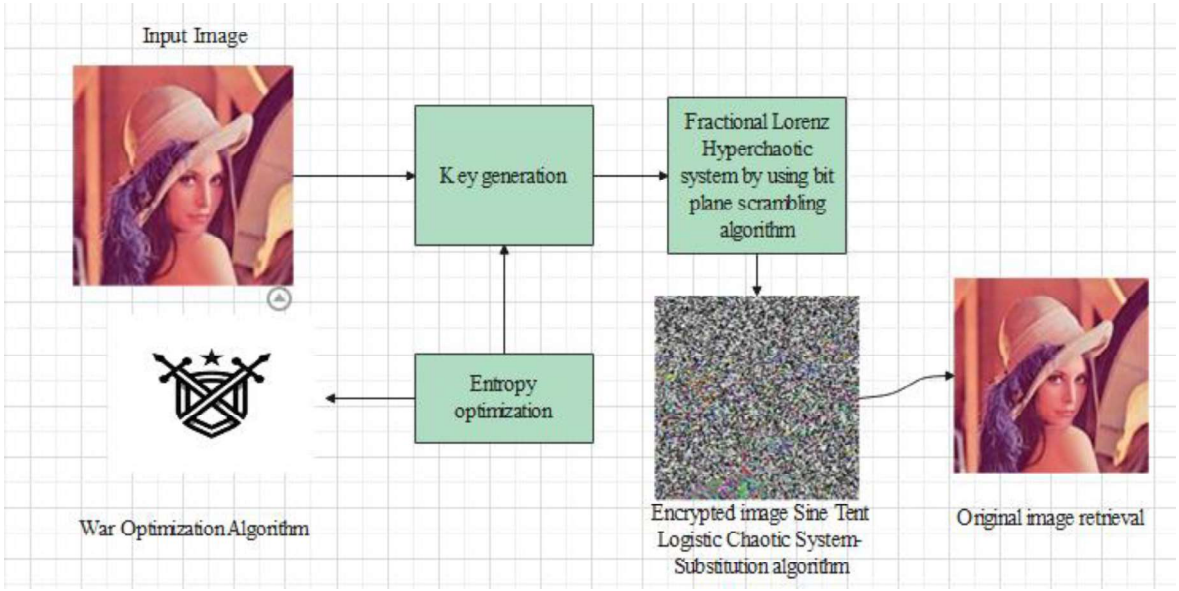


Figure 1: Block diagram of the projected technique

This encryption process can be presented as follows,

4.1. Key generation

In the key generation, two main parts are considered. The initial part can be the key required in bit plane scrambling. Compute the hash parameter of the plaintext image related to the SHA-256 technique. The outcome of the SHA-256 hash technique can

be a 256bit has parameter. Each 4bit binary variable can be changed into hexadecimal count, at last achieved a string of 64 hexadecimal numbers:

$$Key_1 = \{K_1, K_2, \dots, K_{64}\} \qquad (3)$$

After a starting parameter substitution iteration, the fractional hyper Lorenz chaotic system is created four groups of various chaotic sequences W,X,Y and Z. In this research, it requires to scramble 8-bit planes, eight groups of chaotic sequences can be required. It is required to create 8 starting parameters that can be divided into two clusters and substitutes into the fractional hyperchaotic architecture to create 8 chaotic sequences. Hence, it is required to split the key1 into eight blocks based on the below equation,

$$Key_{1I} = K_{8I-7}, K_{8I-6}, \dots, K_{8I}, \qquad I = \{1,2, \dots,8\} \qquad (4)$$

Based on 〖Key〗_1I, can be an 8bit hexadecimal variation which should be quantized to generate a decimal count among 0 and 1, which utilize as the initial parameter of the fractional hyper-Lorenz chaotic system in addition substitute it into the chaotic system to iteratively achieve the chaotic sequence through the below formulation,

$$u_I = \frac{hex\ 2\ dec\ (Key_{1I})}{hex\ 2\ dec\ (FF \dots F)}, \qquad I = \{1,2, \dots,8\} \qquad (5)$$

Here, $(FF \dots F)$ can be defined as the maximum parameter in eight-bit hexadecimal number, $hex\ 2\ dec$ can be a function in MATLAN which convert hexadecimal numbers to decimal numbers. Additionally, $u_I, I = \{1,2, \dots,8\}$ to $x_0, y_0, z_0, w_0, x_1, y_1, z_1, w_1$. Based on this clusters of chaotic systems for iterative operation, eight, clusters of chaotic sequences to scramble the it planes of the normal plaintext image can be achieved. The secondary part can be the key required in the substitution procedure after bit plane scrambling. Achieve a scrambled image after the bit plane permutation function completes [17]. The scrambled image can be split into four sub block images of similar size adopt the SHA-256 algorithm to compute the hash parameter of complete pixel parameters of every block in addition every line to compute the key based on below equation,

$$Key_{2I,J} = \frac{hex\ 2\ dec(hash(x_{i,1}, x_{i,2}, \dots, x_{i,m/2})}{hex\ 2\ dec(FF \dots F)}, I = 1,2,3,4, J = \left\{1,2, \dots \frac{N}{2}\right\} \qquad (6)$$

Here, $x_{i,1}, x_{i,2}, \dots, x_{i,m/2}$ can be defined as complete pixel parameter of the last row of the block image and hash calls the SHA-256 hash algorithm considered in this paper to achieve a 64bit hexadecimal number string. Utilize the hex 2 dec operation to get decimal number by changing hexadecimal number in addition quantize it to 0-1 as the general parameter of the sine tent logistic chaotic system.

4.2. Fractional Lorenz Hyperchaotic system by using bit plane scrambling algorithm

Various non-negative integer N is defined as the string of n bit binary sequences. In the images, the range of pixel parameters is among [0,255]. Hence, every pixel parameter is defined with the series of 8-bit binary sequences. This image can be decomposed into 8-bit plane images. The final bit plane is composed of the ith bit of the binary of every pixel parameter. The bit plane decomposition of the initial image achieved eight-bit plane images. Bit-plane scrambling not only depends on the global scrambling of image pixel location additionally it varies the pixel parameter. It is smooth out the histogram of scrambled photos, decreasing the risk of information leaking.

4.3. Sine Tent Logistic Chaotic System-Substitution algorithm

In this process, the pixel value is changed from the original image data to create the various image. This portion utilizes the sine tent logistic system to analysis substitution processing on the scrambled image in addition concurrent the operation N/2 times to create the initial population required for the subsequent WOA technique. The specific substitution phases can be presented as follows,

 The scrambled image achieved in the preceding phase is split into four blocks in addition the size of every block is defined as M/2*N/2.

 Based on the above section, compute the hash parameter of every block and every row after block in addition consider it as the chaotic initial parameter of sine tent logistic after quantization.

 In order to achieve three various chaotic sequences, pair of three various parameters of the chaotic systems into the sine tent logistic chaotic system. Pre-iterate the chaotic map 1000 times to reduce the adverse consequences happened by transient reactions in addition manage to iterate M/2*N/2 times. This process is formulated as follows,

$$\begin{cases} U_1 = Round\left(STL\left(u_0, \mu_1, \frac{M}{2} \times \frac{N}{2}\right) * 255\right) \\ U_2 = Round\left(STL\left(u_0, \mu_1, \frac{M}{2} \times \frac{N}{2}\right) * 255\right) \\ U_3 = Round\left(STL\left(u_0, \mu_1, \frac{M}{2} \times \frac{N}{2}\right) * 255\right) \end{cases} \quad (7)$$

In the consideration of below equation, the pixel parameters of every block can be substitutes with the consideration of three chaotic sequences, in addition the substitutes image of every block can be achieved,

$$Encrypta(I) = (U_1 \oplus \left(U_2 \oplus \left(U_3 \oplus a(I)\right)\right), \ I = 1,2,3,4 \quad (8)$$

Here, a(I) is defined as scrambled image of every block. At last, the four substituted images are recombined related to the below equation, in addition the final encrypted image is achieved,

$$Img = \begin{bmatrix} Encrypta\ 1 & Encrypta\ 2 \\ Encrypta\ 3 & Encrypta\ 4 \end{bmatrix} \quad (9)$$

To create the initial population for WOA, the above steps are repeated. It empowers the hash parameter of every variable in every block and line is utilized as the initial parameter of chaos in addition the initial population call array consists of N/2 various encrypted images can be achieved.

4.4. War Optimization Algorithm

In each cycle, each player has an equal chance of becoming a ruler or a power contingent on their fighting strength (well-being value). Together the ruler then the commander go as vanguards on the battlefield. A Lord and Commander grow in the field of conflict to lead other players. Chances are the lord or officer will face stiff opposition from a rival warrior (adjacent optima) who has enough cohesion to trick the vanguard. To evade this, combatants are guided by the situation of the ruler or alternate commander, and additionally by their integrated development strategies [18].

Fitness Evaluation

In the projected organization, the WOA is used to improve the aging of the battery lifetime. To empower the battery lifetime, the fitness function is formulated which is presented as follows,

$$FF = H \qquad (10)$$

Based on the order of fitness function from small to large, to sort every encrypted images in the cell array to achieve celling, every individual can be regarded as a war and search optimization can be performed through changing the position of the war technique.

Attack Strategy

We have shown binary collision techniques. In the main case, each combatant updates its location by considering the positions of the ruler and the administrator. The Lord is looking for a precious situation to send a terrible attack on the opposition. Accordingly, the officer with the best offensive power or health is seen as the ruler [19].

$$X_I(t+1) = X_i(t) + 2 \times \rho \times (c - k) + RAND \times (w_i \times k - X_i(t)) \qquad (11)$$

Here, k can be defined as the king position, c can be defined as the previous position of the commander, $X_I(t+1)$ can be a new position, w_i can be defined as the weight.

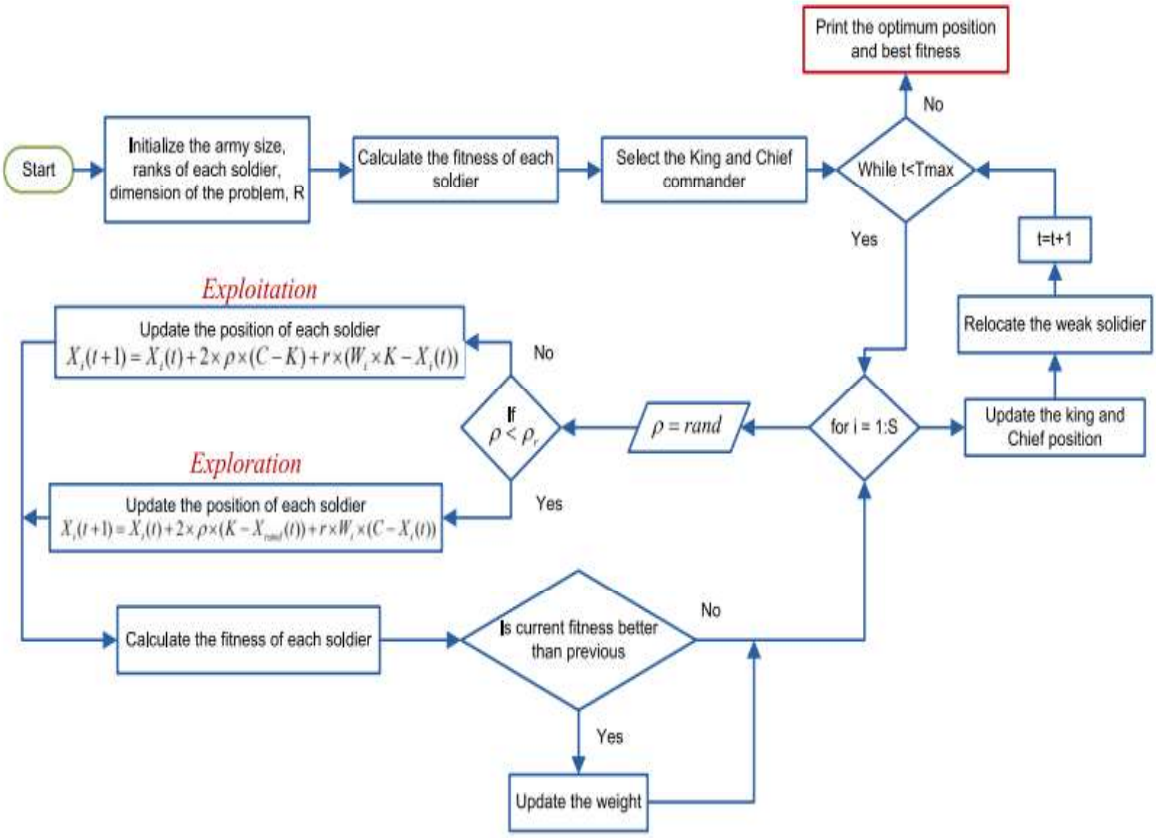


Figure 2: Flowchart of the proposed methodology

Rank and weight Updation

Each search specialist's status update depends on the communication of the commander, commandant, and position of each troop. The position of apiece combatant is contingent on his prosperity past in the conflict arena, which is represented under the conditions, which will affect the weighting factor w_i accordingly. Each fighter's position reproduces how near the trooper (search specialist) remains to the objective (health rate).

$$X_I(t+1) = X_I(t+1) \times \left(f_n \geq f_p\right) + X_I(t) \times \left(f_n < f_p\right) \qquad (12)$$

The fitness of the new position f_n is compared with less than the last location f_p, the soldier considered as a previous location. If the soldier upgrades the location efficiently, the rank R_i of the soldier is promoted,

$$R_I(t+1) = (R_I + 1) \times \left(f_n \geq f_p\right) + R_I \times \left(f_n < f_p\right) \qquad (13)$$

Related to the rank, the new weight can be computed as follows,

$$w_i = w_i \times \left(1 - \frac{R_I}{Maximum\ iteration}\right)^a \qquad (14)$$

Defense method

Subsequent tech-level upgrades depend on the levels of the Lord, Warlord, and Irregular Troops. Although the rest of the parts are refreshing in terms of positioning and weight.

$$X_I(t+1) = X_i(t) + 2 \times \rho \times (c - Xrand(t)) + RAND \times (w_i \times c - X_i(t)) \qquad (15)$$

This combat mode explores more hunting space as opposed to the previous mode as it involves an arbitrary combatant's location. For great improvements Wi, the troops make great strides and improve their conditions. For minor advancements, Wi Warriors makes minor advancements when they refresh the status.

Spare/transfer of weak sold

For each priority, classify the most brutally weak fighter's fitness,

$$X_w(t+1) = LB + RAND \times (UB - LB) \qquad (16)$$

Subsequent steps move the weaker warrior closer to the middle of a full armed force on a conflict field. This method further recovers the assembly performance of the computation.

Exploration And Exploitation

Inquiry (for Global Optima) and Dual Contract (for assembly) are the two basic steps for any metaheuristic progress calculations. A decent compromise between these two characteristics would make the calculation heartier. The production attack process addresses the double handling defense technique addresses the investigation. The common advantages of the WOA are presented as follows,

- The proposed calculation makes a great compromise between exploitation and exploration.
- Each provision (officer) has an interesting weight in light of his position.

 In the refresh step, each fighter's weight is refreshed assuming the fighter is working effectively on his health. In this way, weight regeneration is completely dependent on a molecular position relative to lords and lordship.

 Loads change non-linearly. The loads vary in large increments during the initial stress and in smaller increments during the last cycles. This prompts rapid compounding for the global best value.

 The stage regeneration cycle involves two phases. It further enhances the investigative capacity for global best arrangement.

 The proposed computation is straightforward and requires less computational weight.

Based on this algorithm, the image entropy is computed. Compute the information entropy of every encrypted image, here the encrypted image with the optimal fitness function is efficient encrypted image achieved and output its related position data to facilitate subsequent decryption.

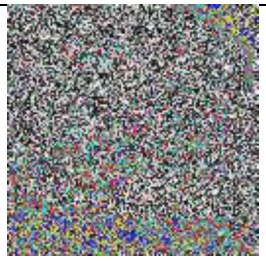
5. Performance Evaluation

In this section, planned method exhibits are recognized through execution and selection hearing. The proposed technique is implemented on an Intel Center i5-2450M computer chip 2.50GHz PC and 6GB RAM to recognize the introduction of the planned encryption procedure. This strategy is carried out in MATLAB Programming R2016b. To validate the description of the proposed strategy, image information sites are collected from [20], in which 512*512 feature tagged as Lena, boat, hairstyle woman, Barbara, hill station, low fragment ratio images. The proposed strategy can be investigated using performance metrics such as PSNR, error rate, CC, encryption time, and decryption time. The projected technological implementation boundaries are given in Table 1.

Table 1: Proposed method variables

S. No	Method	Description	Value
1	Proposed method	Number of populations	50
2		Number of iterations	100
3		Lower bound	-10
4		Upper bound	10
5		Number of search agent	50

Table 2: Analysis of the proposed method

S. No	Input image	Encrypted image	Output image
1			

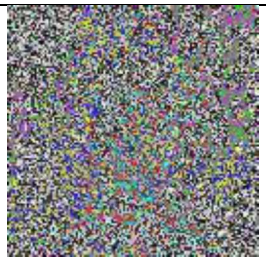
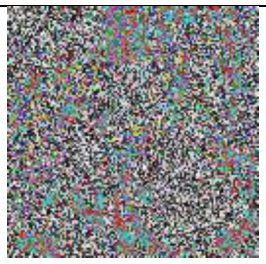
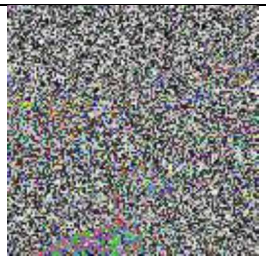
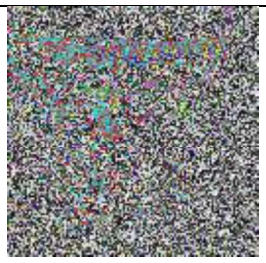
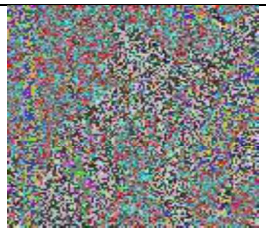
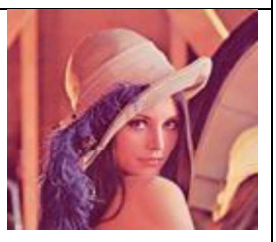
2			
3			
4			
5			
6			

Table 2: Analysis of the proposed method

S. No	Input image	PSNR	Error	CC	Encryption Time	Decryption Time
1	Image 1	48.4125	0.9854	1	0.00421	0.001754
2	Image 2	48.2897	0.9578	1	0.00128	0.001254
3	Image 3	48.2531	1	1	0.001341	0.00151
4	Image 4	48.2255	0.9754	1	0.001245	0.001635
5	Image 5	48.2085	1	1	0.001354	0.001454
6	Image 6	48.1987	0.9784	1	0.001054	0.001254

The proposed method is validated by six images which are presented in table 2. The input image, encrypted image, and output images are illustrated. With the assistance of the projected technique, the images are encrypted. The encryption process is proceeding with the encryption algorithm. Encryption algorithm is utilized to secure the image data. The projected method is mainly designed to secure the image as well as empower the user authentication process. The projected technique is assessed by performance measures which are given in table 2. The projected technique is achieved secure image data. The projected technique is authenticated with the assistance of performance measures like PSNR, CC, Error, encryption time, and decryption time which mathematically formulated as follows,

PSNR

The PSNR is utilized to authenticate the projected methodology. To compute the noise ratio among the cipher in addition, plain images which formulated as follows,

$$PSNR\ (P,C) = 10log_{10}\left(\frac{MAX^P}{MSE}\right) \qquad (30)$$

Where, 〖MAX〗 ^P is the plain image maximum pixel value P, C can be described as cipher image and P can be described as plain image.

CC

The correlation coefficient is computed based on the below equation,

$$R = \frac{(N\sum X^I Y^I - \sum X^I \sum Y^I)}{\sqrt{NX_I^2 - (\sum X^I)^2}\sqrt{NY_I^2 - (\sum Y^I)^2}} \qquad (31)$$

Where R can be described as the interval [-1,1].

MSE

The error can be calculated related on the below equation,

$$MSE = \frac{1}{N*M}\sum_{X=1}^{N}\sum_{Y=1}^{M}\left[I_{image}(A,B) - I_{d-image}(A,B)\right]^2 \qquad (32)$$

Where, $I_{d-image}(A,B)$ is described as decrypted images and $I_{image}(A,B)$.

Encryption time and Decryption time

The encryption time and decryption time are computed as the processing time of the proposed encryption as well as the decryption process.

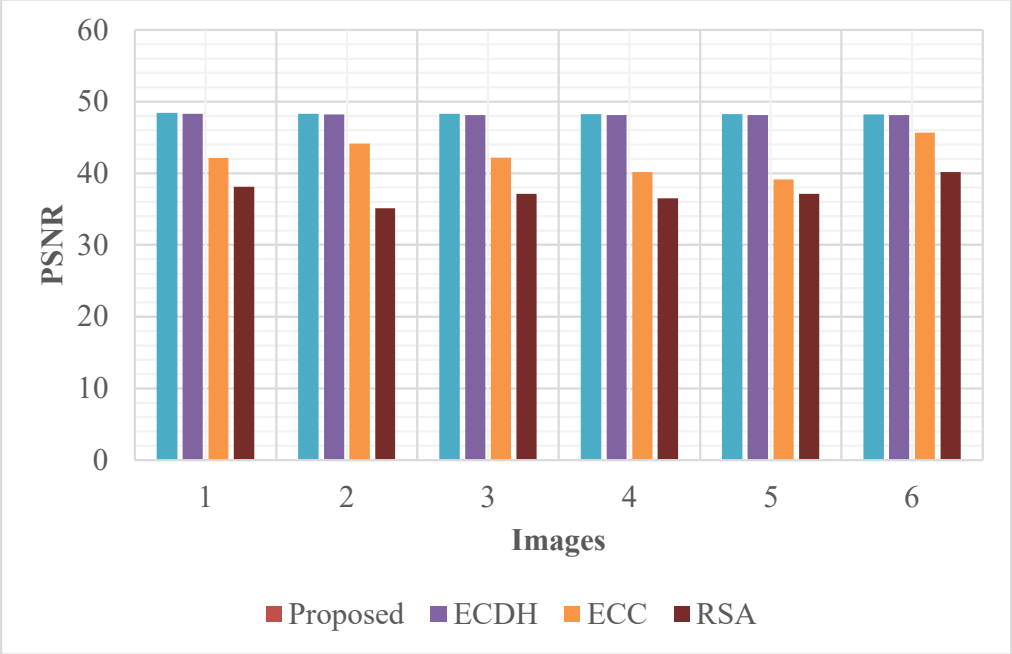


Figure 3: Analysis of PSNR

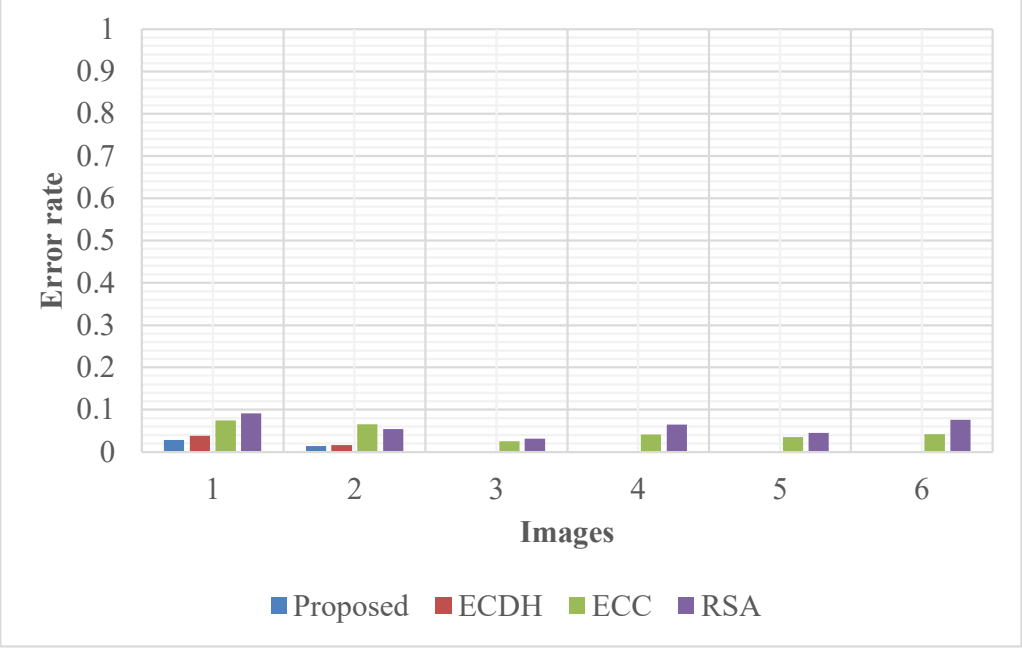


Figure 4: Analysis of MSE

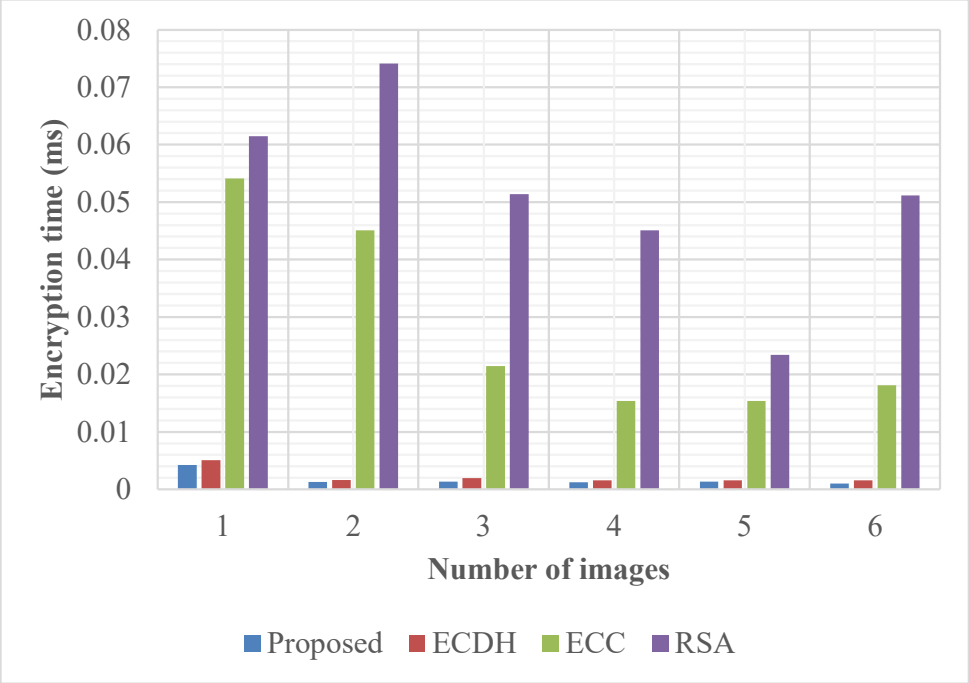


Figure 5: Analysis of encryption time

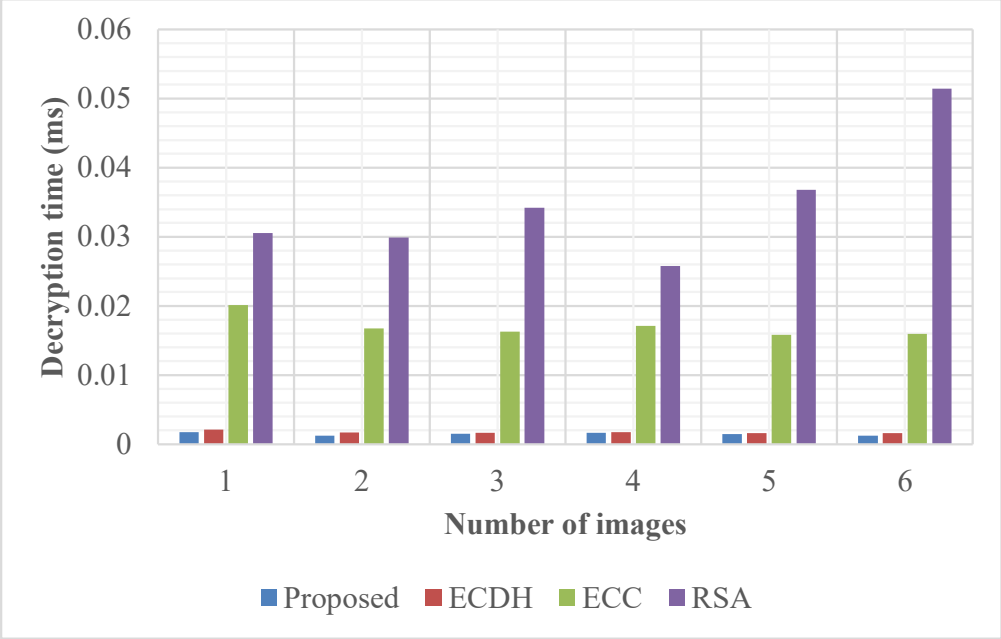


Figure 6: Analysis of decryption time

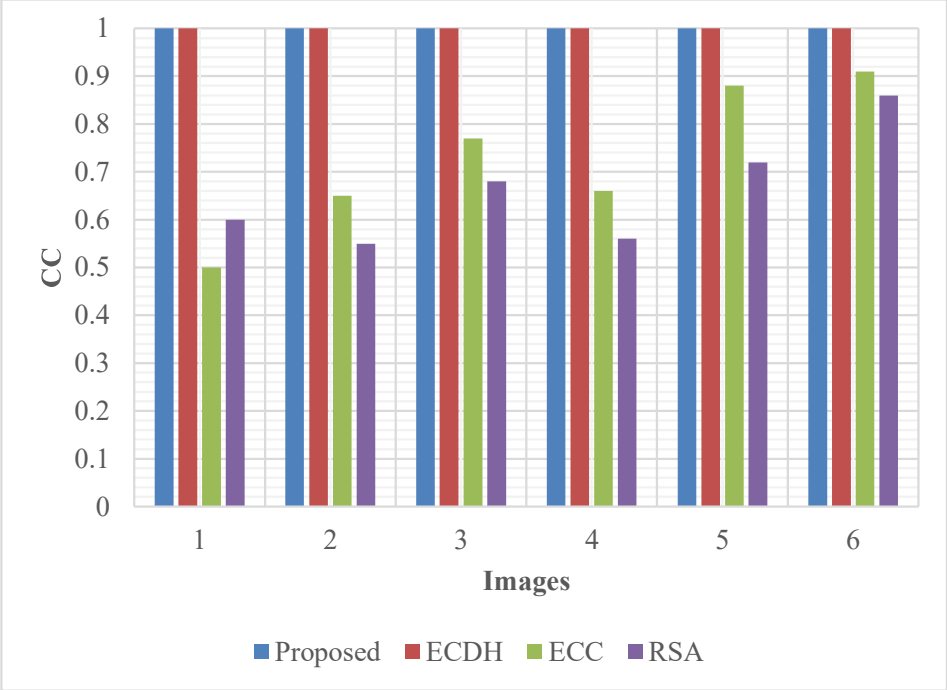


Figure 7: Analysis of CC

The presentation of the projected methodology can be authenticated through performance metrics. Additionally, the proposed method is contrasted with the previously designed methods like ECDH, ECC and RSA. The PSNR of the projected methodology can be illustrated in figure 3. The proposed method is achieved the 48.4125 PSNR rate for image 1. The ECDH is achieved the 48.3008 PSNR rate for image 1. Similarly, the ECC is achieved the PSNR is 42.12 for image 1. The RSA is achieved the PSNR is 38.12 for an image 1. From the analysis, we can conclude, the proposed method is achieved a higher PSNR rate contrasted with the conventional techniques like ECDH, ECC in addition RSA. The MSE of the proposed methodology is presented in figure 4. The projected technique is attained the 0.2854 error rate for image 1. The ECDH is attained the 0.0383 error rate for image 1. Similarly, the ECC has achieved an error rate is 0.0745 for image 1. The RSA has achieved an error rate is 0.0912 for image 1. From the analysis, we can conclude, the proposed method is contrasted with the previously designed methods like ECDH, ECC and RSA. The encryption time of the projected methodology can be illustrated in figure 5. The projected method is achieved the 0.00421 encryption time for image 1 The ECDH is achieved the 0.005097 encryption time for image 1. Similarly, the ECC is achieved the encryption time is 0.05412 for image 1. The RSA is achieved the encryption time is 0.0615 for an image. From the analysis, we can conclude, the proposed method is achieved a lower encryption time compared with the existing methods such as ECDH, ECC and RSA. The encryption time of the proposed methodology is illustrated in figure 6. The proposed method is achieved the 0.001754 decryption time for image 1. The ECDH is achieved the 0.00201 decryption time for image 1. Similarly, the ECC is achieved the decryption time is 0.0201 for image 1. The RSA is achieved the decryption time is 0.0305 for an image. From the analysis, we can conclude, the projected technique is contrasted with the previously designed methods like ECDH, ECC and RSA. The CC value of the projected methodology is illustrated in figure 7. The proposed technique is achieved the 1 decryption time for image 1. The ECDH is achieved the 1 decryption time for image 1. Similarly, the ECC is achieved the CC is 0.5 for image 1. The RSA is achieved the CC is 0.6 for an image. From the analysis, we can conclude, the proposed method is achieved a higher CC compared with the previously designed methods like ECDH, ECC and RSA.

6. Conclusion

In this paper, develop image encryption algorithm based on a chaotic bit-plane decomposition and optimization algorithm of a WOA. Initially, utilization of SHA-256 hash algorithm for computing the plaintext images hash parameter as initial parameter of the fractional Lorenz hyperchaotic system after the process. Use the chaotic sequence for permuting plaintext image in a bit plane to achieve the scrambled images. After that, block the scrambles image into four sub images of similar size and count the

hash parameter of every row of every block through the SHA-256 hash algorithm as the initial parameter of the Sine-Tent Logistic chaotic system. Utilize the achieved chaotic sequence to substitute the images. After that, the four sub-block images to get the last encrypted image and the population has been achieved. At last, utilization information entropy of ciphertext images as the fitness function of WOA. Choose the ciphertext image with the optimal information entropy of ciphertext images as the fitness function of the WOA. Select the ciphertext image with the best information entropy from the population as the optimal encrypted image, and then, return the position value of the best war source meanwhile.

REFERENCES

1. Ye, Guodong, Min Liu, and Mingfa Wu. "Double image encryption algorithm based on compressive sensing and elliptic curve." Alexandria Engineering Journal 61, no. 9 (2022): 6785-6795.
2. Kamal, Sara T., Khalid M. Hosny, Taha M. Elgindy, Mohamed M. Darwish, and Mostafa M. Fouda. "A new image encryption algorithm for grey and color medical images." IEEE Access 9 (2021): 37855-37865.
3. Shafique, Arslan, Jameel Ahmed, Mujeeb Ur Rehman, and Mohammad Mazyad Hazzazi. "Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain." IEEE Access 9 (2021): 59108-59130.
4. Zhang, Xiaoqiang, and Yangming Hu. "Multiple-image encryption algorithm based on the 3D scrambling model and dynamic DNA coding." Optics & Laser Technology 141 (2021): 107073.
5. Hosny, Khalid M., Sara T. Kamal, Mohamed M. Darwish, and George A. Papakostas. "New image encryption algorithm using hyperchaotic system and fibonacci q-matrix." Electronics 10, no. 9 (2021): 1066.
6. Shahna, K. U., and Anuj Mohamed. "Novel hyper chaotic color image encryption based on pixel and bit level scrambling with diffusion." Signal Processing: Image Communication 99 (2021): 116495.
7. Al-Roithy, Budoor Obid, and Adnan Gutub. "Remodeling randomness prioritization to boost-up security of RGB image encryption." Multimedia Tools and Applications 80, no. 18 (2021): 28521-28581.
8. Asl, Ali Momeni, Ali Broumandnia, and Seyed Javad Mirabedini. "Scale invariant digital color image encryption using a 3D modular chaotic map." IEEE Access 9 (2021): 102433-102449.
9. Wang, Xingyuan, Cheng Liu, and Donghua Jiang. "A novel triple-image encryption and hiding algorithm based on chaos, compressive sensing and 3D DCT." Information Sciences 574 (2021): 505-527.
10. Parida, Priyansi, Chittaranjan Pradhan, Xiao-Zhi Gao, Diptendu Sinha Roy, and Rabindra Kumar Barik. "Image encryption and authentication with elliptic curve cryptography and multidimensional chaotic maps." IEEE Access 9 (2021): 76191-76204.
11. Pourasad, Yaghoub, Ramin Ranjbarzadeh, and Abbas Mardani. "A new algorithm for digital image encryption based on chaos theory." Entropy 23, no. 3 (2021): 341.
12. Shafique, Arslan, Jameel Ahmed, Mujeeb Ur Rehman, and Mohammad Mazyad Hazzazi. "Noise-resistant image encryption scheme for medical images in the chaos and wavelet domain." IEEE Access 9 (2021): 59108-59130.
13. Masood, Fawad, Maha Driss, Wadii Boulila, Jawad Ahmad, Sadaqat Ur Rehman, Sana Ullah Jan, Abdullah Qayyum, and William J. Buchanan. "A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations." Wireless Personal Communications (2021): 1-28.
14. Asl, Ali Momeni, Ali Broumandnia, and Seyed Javad Mirabedini. "Scale invariant digital color image encryption using a 3D modular chaotic map." IEEE Access 9 (2021): 102433-102449.
15. Saravanan, S., and M. Sivabalakrishnan. "A hybrid chaotic map with coefficient improved whale optimization-based parameter tuning for enhanced image encryption." Soft Computing 25, no. 7 (2021): 5299-5322.
16. Wang, Xingyuan, and Nana Guan. "2D sine-logistic-tent-coupling map for image encryption." Journal of Ambient Intelligence and Humanized Computing (2022): 1-21.
17. Zhou, Yanqi, Erfu Wang, Xiaomeng Song, and Mengna Shi. "Image Encryption Algorithm Based on Artificial Bee Colony Algorithm and Chaotic System." Security and Communication Networks 2022 (2022).
18. Ayyarao, Tummala SLV, N. S. S. RamaKrishna, Rajvikram Madurai Elavarasan, Nishanth Polumahanthi, M. Rambabu, Gaurav Saini, Baseem Khan, and Bilal Alatas. "War strategy optimization algorithm: a new effective metaheuristic algorithm for global optimization." IEEE Access 10 (2022): 25073-25105.
19. Kaveh, Ali, and Taha Bakhshpoori. "Tug of War Optimization Algorithm." In Metaheuristics: Outlines, MATLAB Codes and Examples, pp. 123-135. Springer, Cham, 2019.
20. http://imageprocessingplace.com/root_files_V3/image_databases.html