Image encryption using Wolf Optimizer and DNA encoding.

Alpana[1], Maitreyee Dutta[2]

[1]ME Student,NITTTR Chandigarh
[2] Head of Department (CSE), NITTTR Chandigarh

ABSTRACT

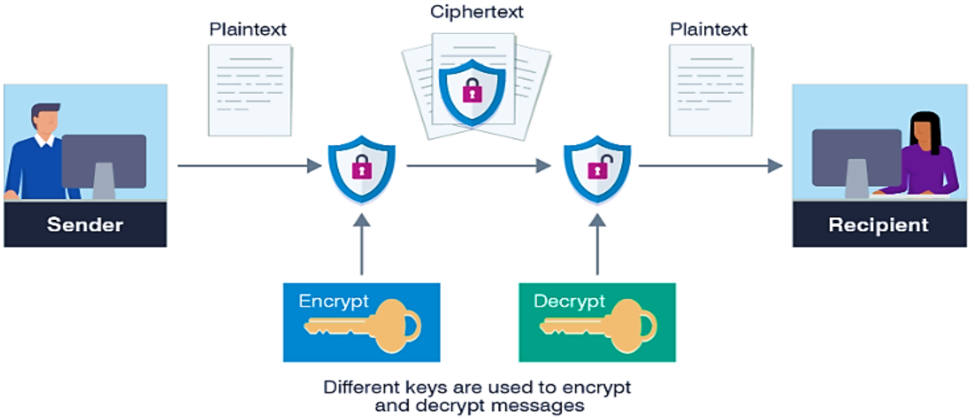
The utilization of chaotic mixing expands the security of the proposed strategy and in the host image, it offers an extra feature of undetectable encryption of the image proprietor logo. The results based on coding of an image are determined from real size of an image and with an encoded file, are equivalent to the outcomes acquired through considerably more refined and computationally compound techniques. Furthermore, the calculation based on the algorithm has been applied to the image multiplexing scenario so as to get upgraded level of security alongside compression. At this point, a single layer of encryption includes the mechanism of bit plane mixing. Compressed and Encrypted image is applied to concealing algorithms. The proposed method uses DNA encoding via optimizing the scrambled blocks and pixels. In proposed approach scrambling process, scrambling mix the pixels values randomly and increase the security but it's not improved the image quality parameters for that optimize the scrambling process by optimizer. The final encrypted image is obtained by repeating the preceding steps once more with GWO optimised block and pixel wise secret keys. Both security assessments and computer simulations support the proposed scheme's feasibility. Because of its low entropy and high PSNR, it is well suited for real-time and stable image applications. **Keywords: encryption, images, scrambling, GWO, DNA sequencing**

1. Introduction

Security is an essential necessity for all the applications to ensure information while transmitted and stored over open network systems. Along these lines, this prerequisite is important to build clients 'trust in correspondence systems to finish their transactions safely. Digitally advanced images involve an enormous piece of our day by day communications [6]. The massive changes in innovations have brought about a plenty propelled PCs and PEDs (Portable Electronic Devices) to be an instrument of interpersonal. Computerized phones, cameras, and PCs have made the way toward processing, catching, and further sharing pictures between interpersonal via unrestricted and instant communication incredibly sensitive in nature. The capacity and the utilization of the images are stored and afterward utilized all through different applications, for example, Facebook, WhatsApp, and Twitter. The way that numerous zones, for example, the military and the clinical field convey sensitive advanced digital pictures must be made safe and protected against assaults insufficient ways. The data-based encryption of sensitive information is vital; the algorithms based on encryption are intended to secure informational data and guarantee confidentiality and the main approved recipient can get access to the decryption form of data [3]. Encryption represents a procedure that converts data by unapproved clients utilizing cryptographic calculations to save information. It is utilized to keep sensitive information with the goal that it may be hard for unapproved clients to see it. The procedure of encryption is utilized to save sender messages through the air or vacuum. Good algorithms must be tested to meet the necessities of the security which ensure the components of encryption [3, 6]. The image-based encryption procedures are not the same as information encryption systems. There are a few security issues related with digital image transmission and processing, so it is important to keep up the confidentiality and integrity of the image [13]. Figure 1.1 represents a general process of image encryption utilizing any algorithm of image encryption and the resultant encrypted or encoded image.

1.1 Cryptographic Systems

Encryption is utilized to change over information to secret codes while being transmitted over the public system network. It permits the clients to encrypt sensitive/delicate data to be put away securely or transmitted over the safe systems with the goal that it can't be perused by anybody other than the proposed beneficiary (recipient) and the encryption of data is required. Along these lines, encryption is utilized to make data endless if unapproved people seize the process of transmission. The undeniable type of data is known as the first informational data; however, the immeasurable variant is known as a ciphertext [10, 16].



2. **Figure 1.1:** Image Encryption [21]

The way toward changing over the primary content into a coded structure is known as the encryption process, while the way toward restoring the encrypted or encoded content is known as the process of decryption. Generally, most of the cryptographic algorithms utilize a secret key. The encrypted data-based security relies totally upon two things: the secret key and the strength of cipher algorithm. The key is utilized in both the decryption and encryption and should be stayed secretly quiet, needing both the sender and recipient to coordinate on a similar key before any information is sent. The key is free of the plaintext. Thusly, the equivalent scrambled text encodes to various ciphertext with various keys, so the two procedures are inconceivable without utilizing the right key [4, 7]. There is both weak and solid encryption. The quality based on strength of encryption relies upon the time and the devices that necessarily require plain text returning. Solid encryption usually makes the ciphertext hard to comprehend without an uncommon tool or device to unscramble or decrypt it. The sender and the recipient must keep up the privacy key between the two gatherings or parties so nobody can unscramble the content deprived of knowing the secret key [12,15].While the process of cryptography represents the craft of composing or solving codes, cryptanalysis represents the study of investigating and breaking ensured communication, and thusly, it is the way toward recovering the key or plaintext by utilizing the data and the ciphertext of algorithm. For the most part, there are two sorts of algorithms: symmetric algorithm using a single/individual key for both the processes of encryption and decryption, asymmetric algorithm using one key for encryption process and the other for the process of decryption [1, 9][19]. Consequently, the quality of the algorithm utilized for encryption is fundamental. Since the unapproved element or entity can take the encrypted text and attempt to break the process of encryption by attempting to choose the mystery key dependent on the encoded content. Encryption is utilized to guarantee the way of communication through a) data-based integrity and non-alteration during the process of transmission; b) non-refusal is accomplished through advanced marks/digital signatures; c) verification through authentication d) security is the way toward guaranteeing conveyance of the proposed object. This work comprises of two related encryption classifications: symmetric key encryption and open (public) key encryption [10]. The process of asymmetric encryption represents an open key utilized for both the encryption and decryption. The open key is distributed and known to every party. The private key is hard to comprehend to anybody aside from the recipient. It is a couple of keys, the first one for encryption and the other for decryption. This guarantees the security of the message during the process of transmission. There are two sorts of algorithms: Asymmetric that utilizes one encryption and the decryption key, and the additional one is symmetric that utilizes the cryptographic key for the process of decryption [16].

2. RELATED WORK

Mousomi Roy et al. (2019) talked about some uses of cryptographic strategies which are utilized to shield biomedical pictures from undesirable access and alterations. This work can be exceptionally useful in future-based research in biomedical image protection just as multimedia data-based security [1]. **Majed O. Al-Dwairi et al. (2019)** proposed an effective and exceptionally secure method for color-based image encryption and decryption. The proposed system was actualized and tried, and the trial results indicated the accompanying ends: (1) The proposed strategy is extremely productive by expanding the throughput and diminishing times. (2) The proposed procedure is 100% exact by accomplishing infinite PSNR and zero MSE between the first image and the one which is decrypted [2]. **S Geetha et al. (2018)** proposed an investigation of encryption which is measured as one of the procedures that guarantee the security of images utilized in different areas like safe medical imaging services, military intelligence, e-banking, internet and intranet communication, image communication based on social networking like WhatsApp, Facebook, Twitter and so on. Every one of these images travel in an open and free system either during; consequently, their security ends up being a critical need in the grounds of individual privacy and protection. This article surveys and condenses different systems of image encryption in order to advance improvement of image encryption strategies that encourage expanded adaptability and security [3]. **Wisam Elmasry (2018)** It is intended to link multiple systems in order to create another technique for shading or color-based image steganography in order to increase effectiveness, achieve a larger payload cap, and provide security and integrity checks with cryptography all at the same time. The proposed work strengthens a wide variety of payload configurations. The proposed technique begins by framing the codeword with its CRC-32 checksum and secret information; it is then compressed using Gzip shortly before being encrypted using AES; finally, it is applied to encrypted header data for additional processing and then installed into the cover picture. The process of installing the encoded information and header data makes use of a Fisher-Yates Shuffle algorithm to determine the next pixel area. To conceal a single byte, the distinct LSBs of all the shading channels of the selected pixel are usually used. To evaluate the proposed strategy, similar execution tests are performed against a variety of spatial image steganographic schemes, using a subset of the most widely used image quality measurements / metrics. [5].**Muhammad Faheem Mushtaq et al. (2017)** examined the security implications and procedures associated with the design and use of the most widely used symmetric encryption algorithms, including the Triple Data Encryption Standard (3DES), the Data Encryption Standard (DES), the Advanced Encryption Standard (AES), the Hybrid Cubes Encryption Algorithm (HiSea), and Blowfish. Additionally, this paper evaluated and compared these encryption-based algorithms in terms of encryption and decryption time, key size, avalanche effect, throughput, entropy, and correlation. Thus, among the existing cryptographic algorithms, the analysts choose an acceptable encryption algorithm based on a variety of parameters that are most compatible with the client's requirements. [6]. **Rim Zahmoul et al. (2017)** made new chaotic maps dependent on Beta function capacity. The utilization of these maps is to create chaotic sequences. These sequences were utilized in the encryption procedure. The proposed procedure is isolated into three phases: Diffusion, Substitution, and Permutation. The generation of various pseudo arbitrary successions was completed to rearrange the position of image pixels and to confound the connection between the original and the encrypted image, fundamentally expanding the protection from assaults. The gained aftereffects of the various sorts of investigation show that the proposed technique has high security and sensitivity contrasted with past plans [7].

PROPOSED WORK

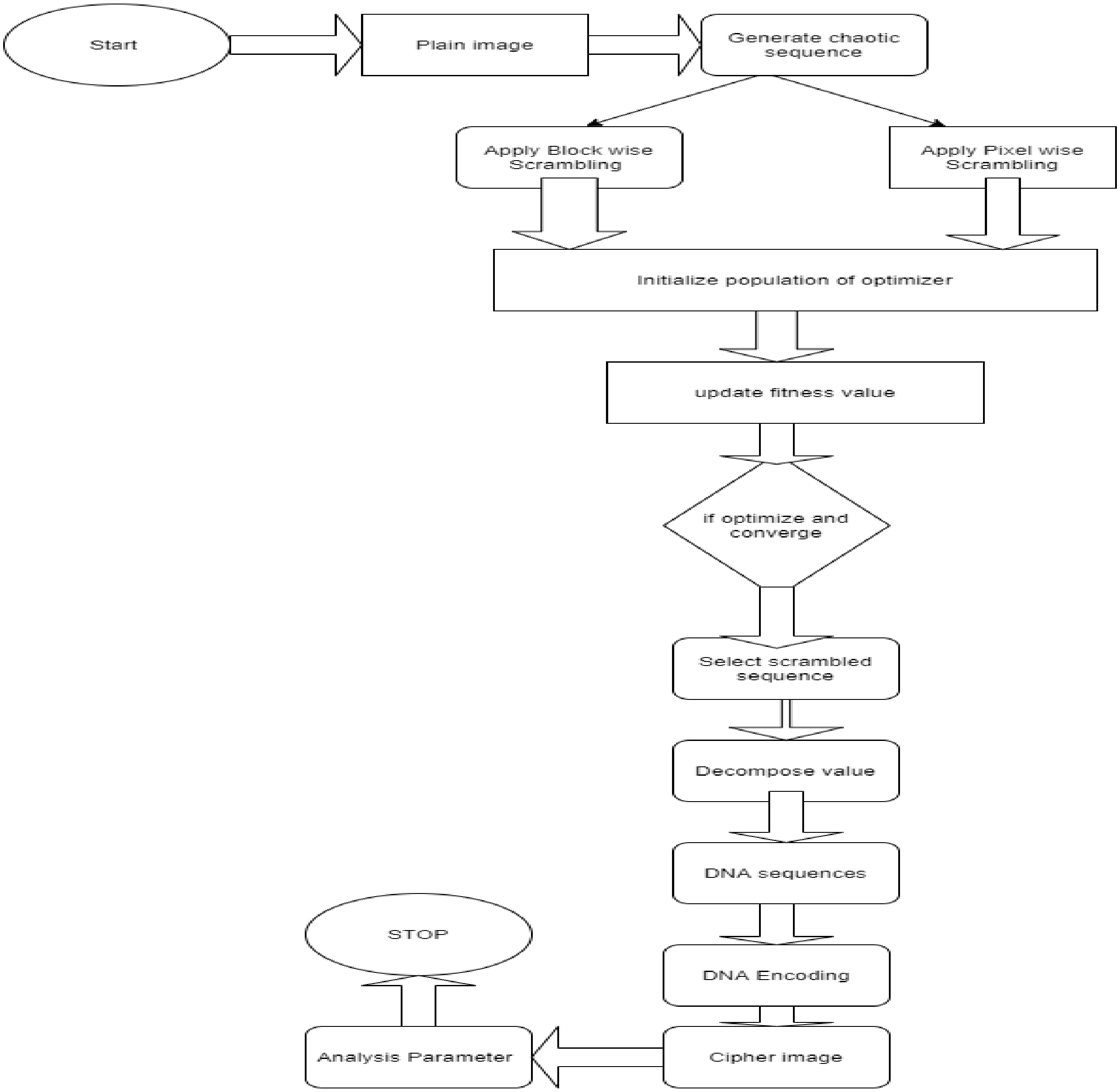

Start
Plain image
Generate chaotic sequence
Apply Block wise Scrambling
Apply Pixel wise Scrambling
Initialize population of optimizer
update fitness value
if optimize and converge
Select scrambled sequence
Decompose value
DNA sequences
DNA Encoding
Cipher image
Analysis Parameter
STOP

Fig3.1: Proposed flow chart

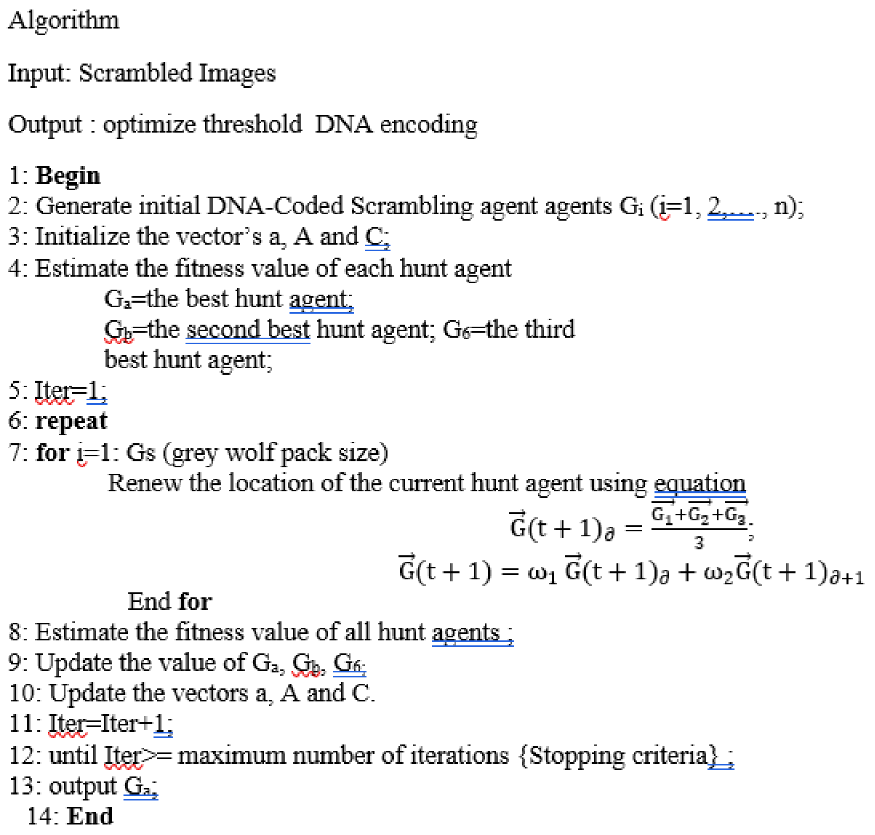
For achieving the objectives in this research proposed approach is used as steps given below:

Step1: In step1 select data set of images. Images should be plane images and after pre-process, generate chaotic sequences. But do not select any chaotic sequence because chaotic sequence behaviour is non-linear, so effective non-linear sequence is selected in this research proposed work.

Step2: First scramble the chaotic sequence in the form of two metadata, first is block base, show its global sequencing and secondly local sequencing by pixel wise scrambling. Combine these scrambling sequences and select effective sequence by intelligent optimization.

Step3: In the second step as described earlier optimize the threshold parameters by fitness function, if fitness function optimizes and converges then send the threshold parameters to scrambling sequence and select decomposed values of the participated sequences and send them to the DNA encoding.

Step4: According to DNA encoding make cipher image and after decryption analysis communicate with the PSNR, MSE and other parameters.



Algorithm

Input: Scrambled Images

Output : optimize threshold DNA encoding

```
1: Begin
2: Generate initial DNA-Coded Scrambling agent agents $G_i$ (i=1, 2,…., n);
3: Initialize the vector's a, A and C;
4: Estimate the fitness value of each hunt agent
        $G_a$=the best hunt agent;
        $G_b$=the second best hunt agent; $G_6$=the third
        best hunt agent;
5: Iter=1;
6: repeat
7: for i=1: Gs (grey wolf pack size)
        Renew the location of the current hunt agent using equation
            $\vec{G}(t+1)_\partial = \frac{\overrightarrow{G_1}+\overrightarrow{G_2}+\overrightarrow{G_3}}{3}$;
            $\vec{G}(t+1) = \omega_1 \vec{G}(t+1)_\partial + \omega_2 \vec{G}(t+1)_{\partial+1}$
    End for
8: Estimate the fitness value of all hunt agents ;
9: Update the value of $G_a$, $G_b$, $G_6$;
10: Update the vectors a, A and C.
11: Iter=Iter+1;
12: until Iter>= maximum number of iterations {Stopping criteria} ;
13: output $G_a$;
14: End
```

RESULT AND ANALYSIS

4.1 Experiment setup and parameters

4.1.1 Performance Parameters

(a) PSNR and MSE

PSNR, a term for the ratio between the highest potential value (gain) of a images and the power of distorting noise that influences the accuracy of its representation, is often referred to as peak signal-to-noise ratio (PSNR). PSNR is commonly expressed in terms of the logarithmic decibel scale due to the fact that certain images have a very broad dynamic range.

MSE = (1/(m*n))*sum(sum((f-g).^2)) .....(1)

PSNR = 20*log(max(max(f)))/((MSE)^0.5)......(2)

- When f is applied to our original image, it represents the matrix data of our original image.
- the matrix data of our degraded image in question is represented by g
- I represents the index of the row of pixels and m represents the numbers of rows of pixels in the images.
- The "n" at the top represents the number of columns of pixels in the image, and the "j" after it is the number of the column that has been highlighted.
- "known to be fine" picture, which means we have a maximum signal value in MAXf.

(b) Global And Local Entropy

Global entropy is a statistical measure of randomness, which is defined as

$$H(X) = -\sum_{k} p(x_k) \log_2 (p(x_k)) \quad \text{[bits]},$$

where p(xk) denotes the probability of the symbol xk appearing. The ideal entropy value is obtained when all pixels appear with the same probability, implying that the pixel distribution is uniform. Entropy at its optimal or ideal value equals log2 (28) = 8 bits.

$$\overline{H_{n,n_p}}(\mathbf{B}) = \frac{1}{n}\sum_{j=1}^{n} H(\mathbf{B}_j) .$$

In contrast to the intrinsically quantitative global Shannon entropy, which can struggle to quantify an image's true randomness, the local Shannon entropy is used to qualitatively quantify an image's randomness.

4.1.2 Experiments and analysis

Table 4.1 Comparison of PSNR on proposed and exiting approaches.

IMAGES	DNA-Encoding	DNA-ENCODING-Scrambling	DNA-ENCODING-SCRAMBLING-GWO
CAR-TESLA	25.64	26.12	28.34
CR-CHEST	26.78	25.98	27.56
CT-CARDIAC	28.67	27.67	29
Girl-image	23.45	26.78	29.23
CT-Head	22.12	28.9	30.12
MR-Shoulder	25.12	26.45	31.12

In table 4.1 and figure 4.1 show the analysis of PSNR values of proposed Optimization base scrambling and existing approaches. In images use take normal image like Tesla Image and other are biomedical images. PSNR show the improvement in images or signals. In figure 4.1 show significance improvement in proposed approach.

Analysis:

Table 4.1 and figure 4.1 show significance improvement in all images. By Experiment proposed approach improve because of following reasons.

- In proposed approach apply block wise and pixel wise scrambling so it provides local and semi global information of pixel variations. According to variation define the population of GWO. Optimization process given efficient scrambled images.

- Scrambled images optimize and DNA sequencing Encrypted. So, its decrypted form variation of optimize value which work as secret key and get efficient images.
- Above reason reduce The MSE and increase the PSNR.
- In results show PSNR improve 5-8% average to existing approaches.

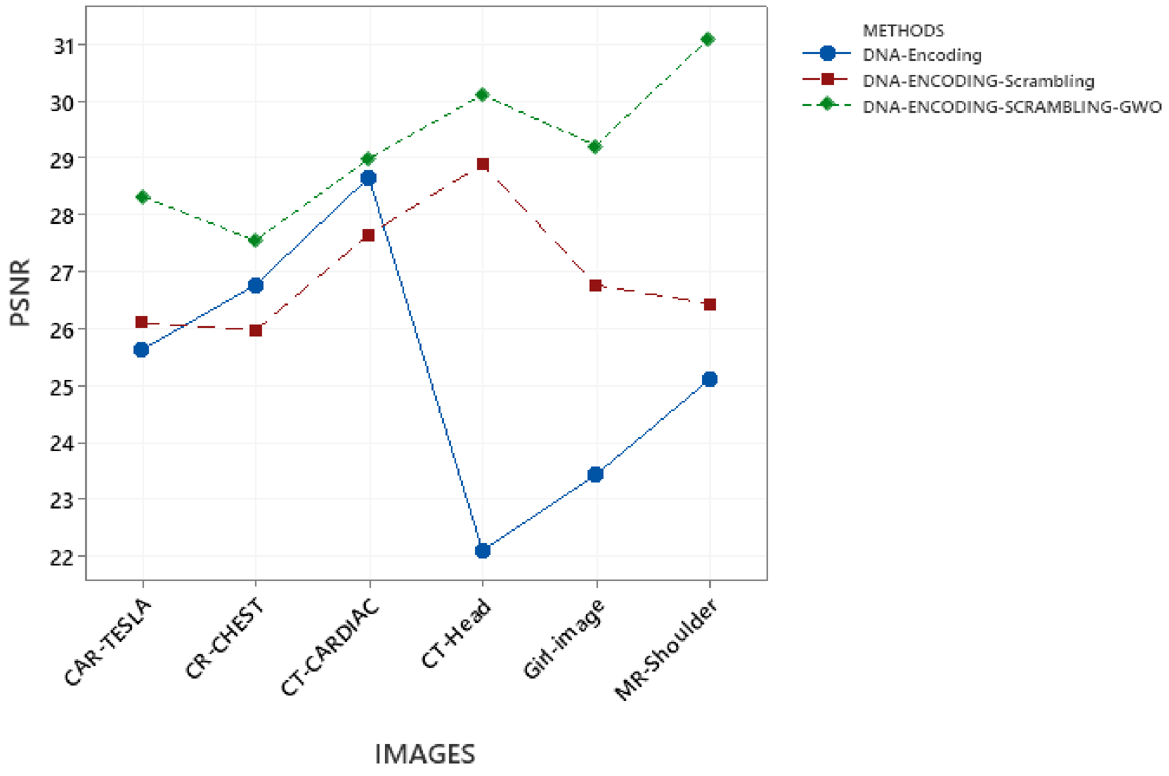


figure 4.1 Comparison of PSNR on proposed and exiting approaches.

Table 4.2 Comparison of MSE on proposed and exiting approaches.

IMAGES	DNA-Encoding	DNA-ENCODING-Scrambling	DNA-ENCODING-SCRAMBLING-GWO
CAR-TESLA	200.7889	170.5636	164.3524
CR-CHEST	189.8884	168.7401	179.2921
CT-CARDIAC	210.25	191.407225	205.492225
Girl-image	213.598225	179.2921	137.475625
CT-Head	226.8036	208.8025	122.3236
MR-Shoulder	242.1136	174.900625	157.7536

In table 4.2 and figure 4.2 show the analysis of MSE values of proposed Optimization base scrambling and existing approaches. In images use take normal image like Tesla Image and other are biomedical images. MSE show the changes of original and decrypted images . In figure 4.1 show significance improvement in proposed approach.

Analysis:

Table 4.2 and figure 4.2 show significance improvement in all images. By Experiment proposed approach improve because of following reasons.

- In above analysis is the same reason of reduction of MSE.
- Apart od\f that MSE reduction is depend on optimization approach because threshold use for encryption and decryption.
- Its reduce or improve 7-10% from existing approach.

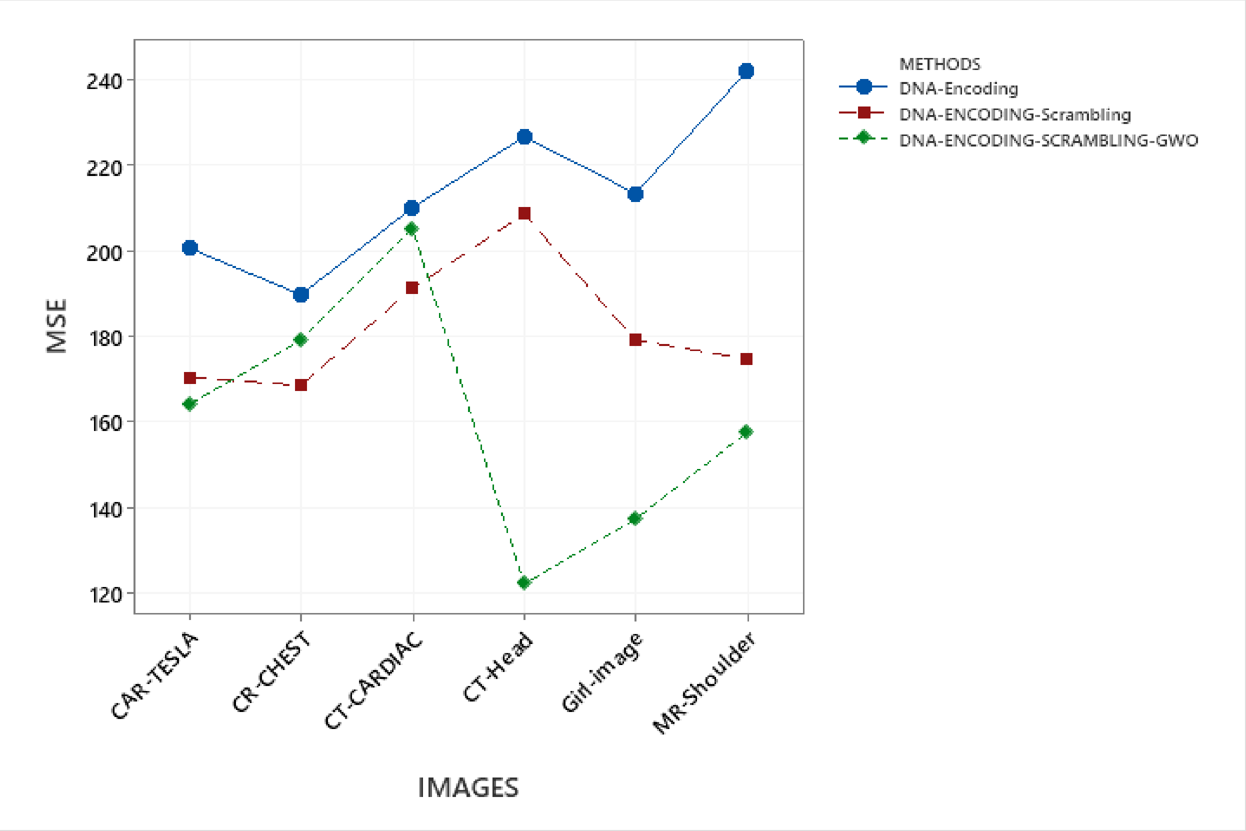


Figure 4.2 Comparison of MSE on proposed and exiting approaches.

Table 4.3 Comparison of Global Entropy on proposed and exiting approaches.

IMAGES	DNA-Encoding	DNA-ENCODING-Scrambling	DNA-ENCODING-SCRAMBLING-GWO
CAR-TESLA	8.9	8.5	7.8
CR-CHEST	7.9	7.5	7.7
CT-CARDIAC	9.2	9	8.2
Girl-image	9.6	9.2	8
CT-Head	8.2	8	7.6
MR-Shoulder	8.23	7.8	7.45

In table 4.3 and figure 4.3 show the analysis of Global entropy values of proposed Optimization base scrambling and existing approaches. In images use take normal image like Tesla Image and other are biomedical images. Global entropy shows the block entropy and its mean value near to 8 is idle. In figure 4.3 proposed approach near idle value, it varies 7.45 to 8.2.

Analysis:

Table 4.3 and figure 4.3 show near the idle global entropy. By Experiment proposed approach improve because of following reasons.

- Global entropy Show block wise randomness. By GWO optimization its variation change to some limits and it reached near to its idle value which show in experiment values.
- Global entropy improves 2-4% average of all images.

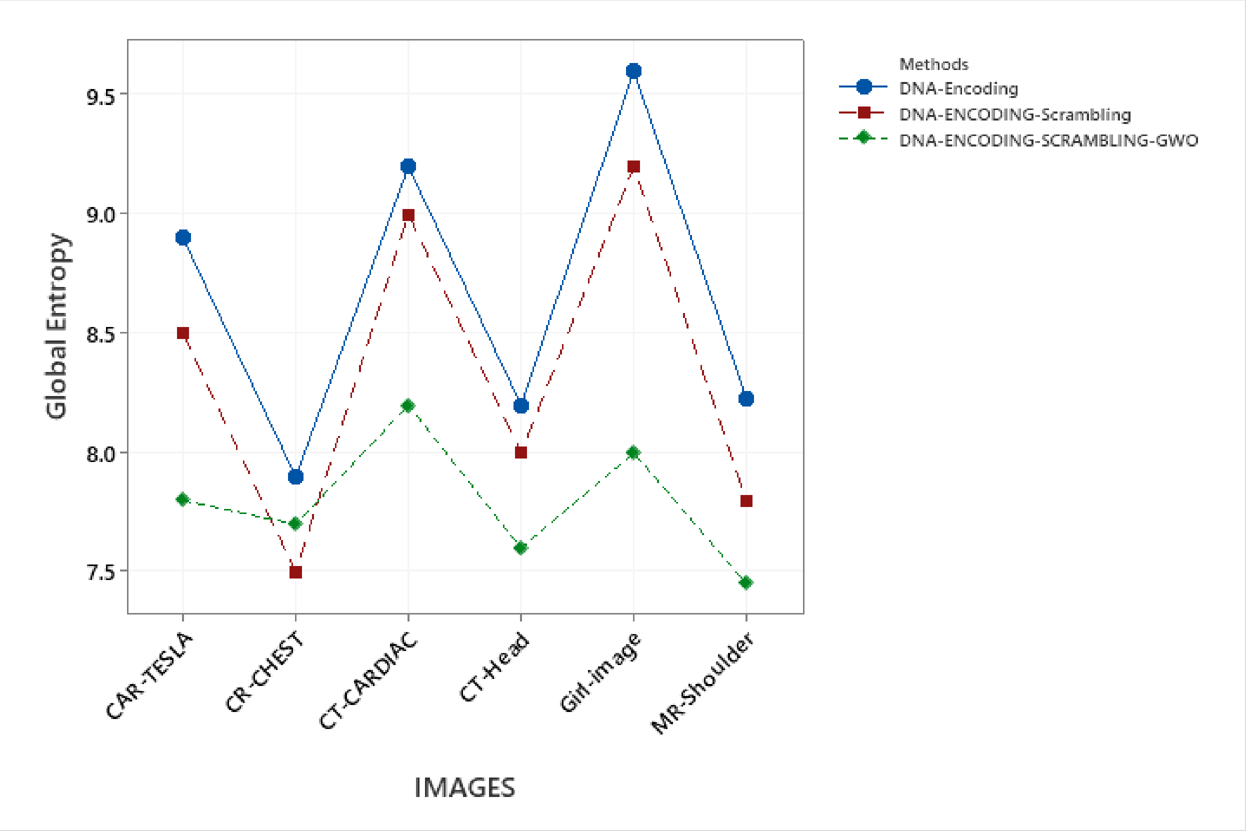


figure 4.3 Comparison of Global Entropy on proposed and exiting approaches.

Table 4.4 Comparison of Local Entropy on proposed and exiting approaches.

IMAGES	DNA-Encoding	DNA-ENCODING-Scrambling	DNA-ENCODING-SCRAMBLING-GWO
CAR-TESLA	8.7	8.15	8
CR-CHEST	7.7	7.6	7
CT-CARDIAC	9.1	8.6	8
Girl-image	9.4	8.6	7.9
CT-Head	8.1	7.8	7.4
MR-Shoulder	8.015	7.625	7.12

In table 4.4 and figure 4.4 show the analysis of Local entropy values of proposed Optimization base scrambling and existing approaches. In images use take normal image like Tesla Image and other are biomedical images. Local entropy shows the block overlapping entropy and its mean value near to 8 is idle. In figure 4.4 proposed approach near idle value, it varies 7.12 to .

Analysis:

Table 4.4 and figure 4.4 show near the idle local entropy. By Experiment proposed approach improve because of following reasons.

- Global entropy Show block wise randomness. By GWO optimization its variation changes to some limits and it reached near to its idle value which show in experiment values. For this reason reduce block overlapping reduce
- Global entropy improves 3-4% average of all images.

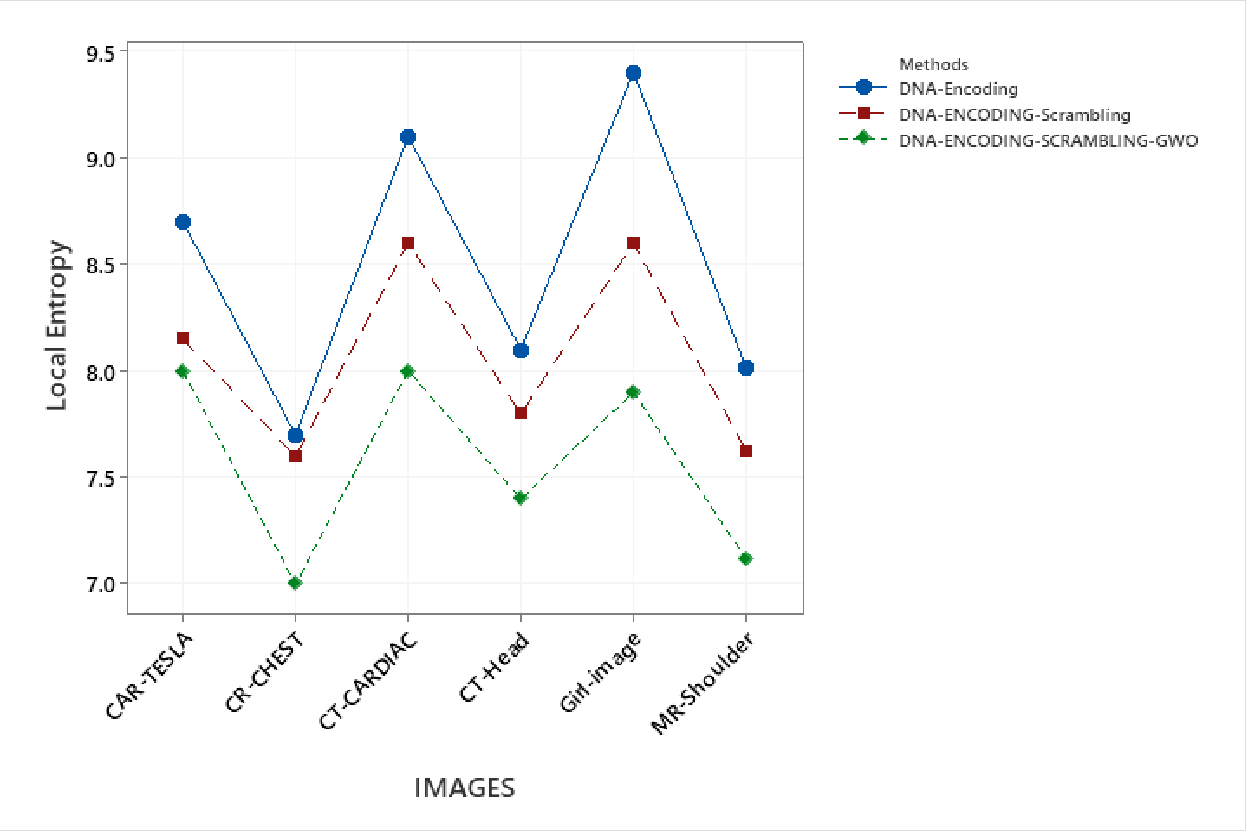


figure 4.4 Comparison of Local Entropy on proposed and exiting approaches.

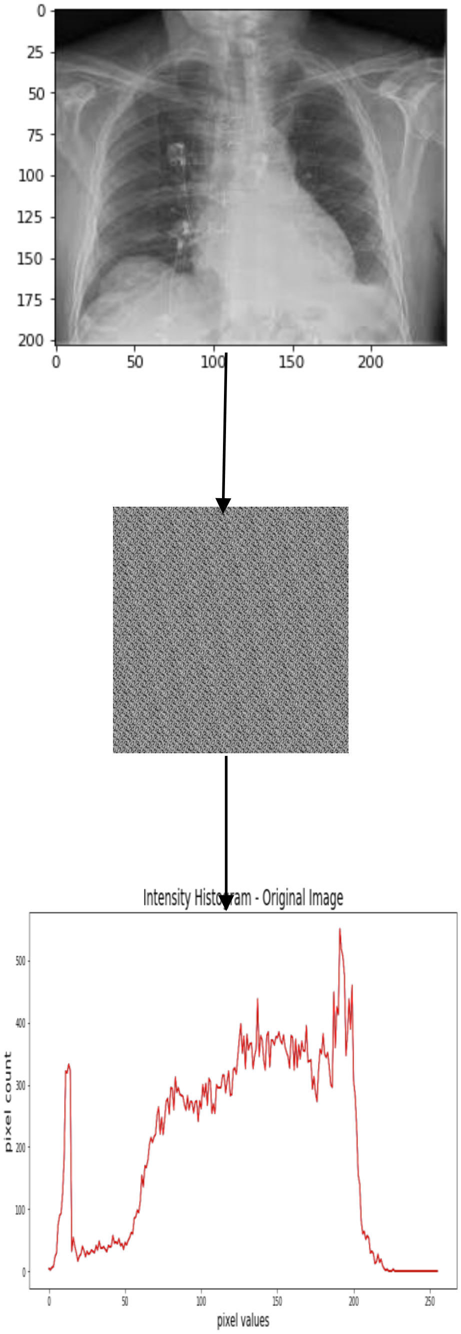


figure 4.5 Proposed approach Encryption and Entropy .

In figure 4.5 show the scrambling base GWO optimize encryption and show entropy.

CONCLUSION

The proposed research work is focusing on reliable methods of DNA-based image encryption against various security attacks. Two map-based image encryption methods, namely chaotic neural network-based image encryption and robust image encryption using chaotic logistic, have been used. The proposed approach updates the pixels both image and block-wise and scrambles pixels by optimizing grey wolf optimization. The advantage of improving random pixel combinations of blocks and pixel increase the mix of scrambling encoding. Scrambling encoding sequence develops the DNA sequences, and DNA sequences improve PSNR and MSE image. Apart of these also analysis entropy parameters. All performance improves because of following reasons.

- In proposed approach apply block wise and pixel wise scrambling so it provides local and semi global information of pixel variations. According to variation define the population of GWO. Optimization process given efficient scrambled images.
- Scrambled images optimize and DNA sequencing Encrypted. So, its decrypted form variation of optimize value which work as secret key and get efficient images.
- entropy Show block wise randomness. By GWO optimization its variation changes to some limits and it reached near to its idle value which show in experiment values. For this reason reduce block overlapping reduce

REFERENCES

[1] Roy, M., Mali, K., Chatterjee, S., Chakraborty, S., Debnath, R., & Sen, S. (2019, February). A study on the applications of the biomedical image encryption methods for secured computer aided diagnostics. In *2019 Amity International Conference on Artificial Intelligence (AICAI)* (pp. 881-886). IEEE.

[2] Al-Dwairi, M. O., Hendi, A., & AlQadi, Z. (2019). An efficient and highly secure technique to encrypt-decrypt color images. *Engineering, Technology & Applied Science Research*, *9*(3), 4165-4168.

[3] Geetha, S., Punithavathi, P., Infanteena, A. M., & Sindhu, S. S. S. (2018). A literature review on image encryption techniques. *International Journal of Information Security and Privacy (IJISP)*, *12*(3), 42-83.

[4] Barakat, M., Eder, C., & Hanke, T. (2018). An Introduction to Cryptography. *Timo Hanke at RWTH Aachen University*, 1-145.

[5] Elmasry, W. (2018). New LSB-based colour image steganography method to enhance the efficiency in payload capacity, security and integrity check. *Sādhanā*, *43*(5), 68.

[6] Mushtaq, M. F., Jamel, S., Disina, A. H., Pindar, Z. A., Shakir, N. S. A., & Deris, M. M. (2017). A survey on the cryptographic encryption algorithms. *International Journal of Advanced Computer Science and Applications*, *8*(11), 333-344.

[7] Zahmoul, R., Ejbali, R., & Zaied, M. (2017). Image encryption based on new Beta chaotic maps. *Optics and Lasers in Engineering*, *96*, 39-49.

[8] Poh, G. S., Chin, J. J., Yau, W. C., Choo, K. K. R., & Mohamad, M. S. (2017). Searchable symmetric encryption: designs and challenges. *ACM Computing Surveys (CSUR)*, *50*(3), 1-37.

[9] Mohammad, O. F., Rahim, M. S. M., Zeebaree, S. R. M., & Ahmed, F. Y. (2017). A survey and analysis of the image encryption methods. *International Journal of Applied Engineering Research*, *12*(23), 13265-13280.

[10] Kumari, S. (2017). A research paper on cryptography encryption and compression techniques. *International Journal of Engineeringa and Computer Science*, *6*(4).

[11] Yassein, M. B., Aljawarneh, S., Qawasmeh, E., Mardini, W., & Khamayseh, Y. (2017, August). Comprehensive study of symmetric key and asymmetric key encryption algorithms. In *2017 international conference on engineering and technology (ICET)* (pp. 1-7). IEEE.

[12] Cao, W., Zhou, Y., Chen, C. P., & Xia, L. (2017). Medical image encryption using edge maps. *Signal Processing*, *132*, 96-109.

[13] Younes, M. B. (2016). Literature survey on different techniques of image encryption. *J Sci Eng Res*, *7*(1), 93-98.

[14] Jain, M., & Lenka, S. K. (2016). A review of digital image steganography using LSB and LSB array. *International Journal of Applied Engineering Research*, *11*(3), 1820-1824.

[15] Joshi, M. R., & Karkade, R. A. (2015). Network security with cryptography. *International Journal of Computer Science and Mobile Computing*, *4*(1), 201-204.