Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

A Novel GWO-Optimized Chaotic Map for Medical Image Encryption in IoT Healthcare

Mohammad Ubaidullah Bokhari[1], Rabiza Sohail Azmi[2*], Shahnwaz Afzal[3],Md. Zeyauddin[4]
[1,2,3,4] Department of Computer Science, Aligarh Muslim University, India, 202002

ARTICLE INFO

Received: 26 Dec 2024

Revised: 14 Feb 2025

Accepted: 22 Feb 2025

ABSTRACT

Strong encryption methods are necessary to protect medical images against illegal access and cyber threats as digital healthcare systems and telemedicine expand exponentially. This work presents a Grey Wolf Optimizer (GWO) enhanced encryption system using a modified logistic chaotic map to guarantee excellent security and efficiency in medical image encryption. The suggested method optimizes chaotic parameters against increased Shannon entropy and decreased pixel correlation, guaranteeing enhanced unpredictability and resilience against statistical attacks. Key generation from pixel intensities, chaotic sequence generation, and XOR-based encryption form the encryption process. Driven by GWO, the optimization process reduces chaotic parameters to generate an encrypted image with low correlation, almost uniform histogram, and high entropy. The suggested method is fit for real-time IoT-based medical applications based on experimental results on standard medical pictures, including MRI-chest and standard image Lena, showing the robustness of the proposed method in terms of NPCR, UACI, PSNR, and entropy analysis. While preserving computational efficiency, the suggested encryption

Keywords: GWO, Chaotic map, Stream Cipher, Medical images, Shannon Entropy, Correlation Coefficients

INTRODUCTION

The extensive expansion of the Internet of Things (IoT) has transformed various industries, and healthcare is among the most affected industries. IoT-based medical devices like wearable health monitors, smart diagnostic machines, and remote monitoring devices have completely transformed the collection, analysis, and transmission of medical data. Such systems produce and communicate enormous amounts of sensitive health-oriented medical data, including diagnostic medical images of ultrasound scans, CT scans, X-rays, and MRIs. Medical images play a crucial role in diagnosis, treatment planning, and ongoing surveillance of numerous illnesses. Transmission and storage of medical images in the context of IoT is extremely dangerous from a security perspective because such images are very sensitive. Unauthorized access, disclosure, or tampering with such images can result in serious consequences, ranging from privacy breaches, to misdiagnosis, and substandard patient care. Hence, confidentiality, integrity, and authenticity of medical images must be ensured in IoT-based healthcare systems of highest priority. Encryption is the foundation of protecting medical data. Conventional cryptographic schemes like RSA, DES, and AES have extensively been employed to protect data. But these techniques were originally developed for text and numeric data, and thus not as well-suited to medical images, which have special properties like high spatial redundancy, high correlation between pixels, and massive data sizes. These properties require specific encryption methods that can efficiently protect medical images without being computationally expensive, especially for devices in the IoT with limited resources. Traditional encryption techniques are extremely computationally intensive and therefore unsuitable for real-time healthcare use. Furthermore, techniques like affine transformations and random pixel scrambling, although studied in medical image encryption, do not appear to offer adequate protection against statistical and brute-force attacks.

In an effort to bypass these constraints, researchers have established several encryption protocols specifically designed for medical image security in IoT scenarios. These types of encryption seek to solve several challenges including ensuring confidentiality of the data, lowering computational overhead, and enhancing the resistance to various forms of cryptographic attacks. Some recent research has been centred on the development of encryption models with multiple layers of security, for example, chaotic systems, DNA encoding, and optimization algorithms, to enhance their robustness and efficiency. Some optimization-oriented and chaos-based methods have been put forward to improve computational efficiency and security in encryption. For example, Belazi et al. [1] introduced a chaos-based cryptography model with DNA encoding for strengthening security using multi-level substitution and diffusion. Akkasaligar and Biradar [2] used a selective DNA cryptography approach for medical images with high-security level and accelerated encryption speed. Fan et al. [3] proposed a hybrid chaotic cryptographic scheme for wireless body area networks with great resistance to differential attacks and high randomness of ciphertext outputs. Subsequent developments concentrated on combining chaotic maps with optimization algorithms for enhancing encryption efficiency Optimization algorithms play a crucial role in encouraging encryption by dynamically controlling key parameters, optimizing substitution and permutation processes, and attaining high entropy ciphertext output. A number of hybrid methods have been proposed that combine chaotic encryption and evolutionary algorithms for optimizing key generation processes and computational efficiency. Afify et al. [4] proposed a dynamic DNA-coding-based encryption technique that guaranteed more randomness and statistical attack resilience. Masood et al. [5] proposed a lightweight chaos-based encryption algorithm based on random shuffling and XOR operations that truly enhanced confusion and diffusion properties. Kamal et al. [6] introduced a hybrid chaotic medical image encryption model using chaotic maps and permutation algorithms with improved security and key sensitivity.

In spite of all such advancements till date, the current methods have certain drawbacks like high computation loads, vulnerability to certain attacks, and reduced flexibility in IoT settings. To solve these problems, in this paper, a new medical image encryption scheme based on chaotic maps and the Grey Wolf Optimizer (GWO) is proposed. The new approach employs the ability of GWO to optimize chaotic encryption parameters for the best randomness, improved security, and lower computational complexity. GWO's efficiency in finding optimal solutions with limited computational power makes it well-suited for IoT devices, which in most cases have limitations of low processing power, memory, and power consumption. This renders the suggested encryption scheme highly applicable in IoT-based health care systems where efficiency and security are significant parameters.

The suggested encryption scheme combines the nonlinearity of the logistic chaotic map with the optimality of the GWO to achieve a best compromise between security and computational complexity. The logistic chaotic map adds chaos with intricate unpredictable dynamics to the encryption scheme that makes it highly resistant to statistical attacks and brute-force attacks. While GWO maximizes the encryption parameters to achieve maximum Shannon entropy and minimum pixel correlation so that the encrypted images become highly random and unpredictable. The hybrid method not only increases the security of medical images but also makes the process of encryption computationally efficient, ideal for real-time applications in IoT-based healthcare systems. The performance of the new encryption scheme is evaluated with different parameters such as correlation coefficient, Shannon entropy, NPCR, UACI, MSE, PSNR, histogram analysis, and NIST statistical tests. The outcome shows that the proposed method is computationally more efficient and more secure than existing encryption algorithms and can be an effective solution for encrypting medical images in IoT. Through overcoming the weaknesses of conventional encryption techniques and taking advantage of the advantages of chaotic systems and optimization algorithms, this study encourages the pursuit of secure and effective encryption techniques for the protection of medical images in healthcare systems based on IoT.

Table 1: Acronyms Used in This Study

S.No.	Acronym	Full Form
1.	NPCR	Number of Pixel Change Rate
2.	UACI	Unified Average Changing Intensity

3.	PSNR	Peak Signal-to-Noise Ratio
4.	MSE	Mean Squared Error
5.	AES	Advanced Encryption Standard
6.	DES	Data Encryption Standard
7.	RSA	Rivest–Shamir–Adleman
8.	GA	Genetic Algorithm
9.	GWO	Grey Wolf Optimizer
10.	DE	Differential Evolution
11.	ABC	Artificial Bee Colony
12.	FA	Firefly Algorithm
13.	WOA	Whale Optimization Algorithm
14.	ACO	Ant Colony Optimization
15.	DNA	Deoxyribonucleic Acid

RELATED WORK

In recent years, a number of innovative techniques for dynamic cryptographic key generation and encryption have been studied by researchers utilising chaotic systems and metaheuristic optimisation algorithms. Genetic algorithms (GAs) have been employed in some of the early studies in this field to produce robust cryptographic keys. The Automatic Variable Key (AVK) in [7] dynamic key generation mechanism, for example, is based on GA and uses genetic operators like crossover and mutation to generate keys that change with every data block. The method offers strong defence against pattern and brute force attacks, but it comes at a high computational cost when the keys are changed often.

In addition to all of this,[8]combines GA with DNA-based key generation by pre-seeding the algorithm with chaotic functions and logistic maps. This results in very high security and very little key waste, but at the expense of more complicated key management. Additionally, [9] develops a Chaos Genetic Algorithm (CGA) that merges GAs with chaotic maps to generate extremely random keys suitable for Internet of Things environments; nevertheless, the method may result in unpredictable behaviour due to its sensitivity to initial conditions. These concepts are further developed in [10] by combining GA, Linear Feedback Shift Register (LFSR), and chaotic pictures in a hybrid approach that yields increased randomness as confirmed by the NIST statistical test suite but necessitates significant CPU resources to achieve.

In addition to GA-based techniques, metaheuristic optimisation based on natural behaviours has garnered a lot of attention. Grey Wolf Optimiser (GWO) variants are categorised into parallel, hybridised, modified, and multi-objective variants in a survey in [11]. By attaining notable gains in convergence rates, these variants demonstrate their usefulness in networking and image processing applications. Since then, studies like [12] and [13] have used simulated grey wolf hunting tactics based on the roles of hierarchical alpha, beta, delta, and omega wolves to solve NP-hard design problems by striking a balance between exploration and exploitation. Despite producing competitive results, these algorithms experience stagnation in local optima; hence, more robust processes are required to maintain population variety. In response to multi-objective problems, [14] presents a Multi-Objective Grey Wolf Optimiser (MOGWO) that effectively extracts Pareto-optimal solutions through the use of grid mechanisms, leader selection, and fixed-size archives. However, its performance has only been evaluated on benchmark functions, and real-world scalability is still an open issue.

Performance in optimisation has also been significantly enhanced by the use of chaotic maps into GWO variations. In [15], a Chaotic Local Search (CLS) is added to the fundamental GWO framework to achieve faster global convergence, hence proposing Chaotic Grey Wolf Optimisation (CGWO). This is contingent upon the appropriate selection of chaotic maps. Using deterministic chaotic signals to adjust important GWO parameters, [16] achieves better global optimality than methods such as Particle Swarm Optimisation (PSO) and Firefly Algorithm (FA). Using chaotic variables to dynamically choose the number of leaders in each iteration, [17] further promotes solution diversification. Both findings emphasise the need for more research to optimise the selection of chaotic maps for a range of practical uses.

Recently, the field of picture encryption—particularly for medical applications—has also used these chaotic and metaheuristic techniques. Combining Convolutional Neural Networks (CNN), Non-Subsampled Shearlet Transform (NSST), Pulse Coupled Neural Networks (PCNN), and Dual-Tree Complex Wavelet Transform (DTCWT), a multi-scale fusion framework for medical imaging is provided in [18]. Though computationally demanding, metaheuristic learning enhances image quality and feature learning by adaptively selecting fusion weights, similar to GA and CGWO. While these S-boxes are very resistant to cryptanalysis, the complexity of the approach makes it difficult to achieve real-time global optimisation. In [19], hybrid methods are used to design nonlinear S-boxes by combining Grey Wolf Optimisation with logistic maps, cuckoo search algorithms, and evolutionary strategies. Additionally, by optimising eight chaotic maps utilising nine metaheuristics and offering superior security through pixel diffusion and permutation, [20] enhances chaotic map-based picture encryption. Real-time application may be difficult due to the method's computing complexity, despite its excellent key space and equal histogram distribution.

Additional techniques aim to enhance the encryption of 3D and medical images. With the introduction of a Steerable Cosine Number Transform in three dimensions (3D-SCNT) in [1], secret keys for the direct encryption of 3D medical images are generated using rotation operators over finite fields. Although the method is now limited to 3D imaging, it offers robust security for 3D data but requires strict key control. In [21], medical images are encrypted using bitwise XOR operations and pixel permutation using a hybrid chaotic model that combines a logistic chaotic model with a 2D Lorentz system. This model achieves high values of UACI, NPCR, and PSNR, but its computational complexity limits its performance to DICOM CT scans. In order to support these studies, [6] provides a block-splitting-based encryption technique that uses logistic map-generated keys, rotation, random permutation, and zigzag pattern confusion. Entropy and histogram tests validate the scheme's strong security, but its performance is sensitive to the block size selection. In [5], a lightweight encryption technique based on Henon's chaotic map, Chen's chaotic system, and Brownian motion is proposed to efficiently and securely encrypt medical images, with higher processing burdens for larger images. A better image encryption scheme in [22] combines two-dimensional Logistic Chaotic Map (2DLCM) and Piecewise Linear Chaotic Map (PWLCM), optimised by a better metaheuristic (CI-WOA). This results in a higher information entropy for satellite images at the expense of decreased efficiency due to complex parameter optimisation.

The novel two-dimensional chaotic maps for hybrid encryption proposed by [23] use Lyapunov analysis, bifurcation, and permutation-diffusion processes, providing a reliable and secure system but requiring precise parameter control because of its extreme sensitivity to initial conditions.
Though each has its own advantages and disadvantages, taken as a whole, these works offer a variety of solutions, ranging from complex metaheuristic optimisations and chaotic encryption schemes to dynamic key generation through GA. Despite the significant advancements in security and encryption quality, encryption is still plagued by general issues including computational complexity, real-time scalability, and precise parameter control. This will need to be reconciled in future study.

Journal of Information Systems Engineering and Management
2025, 10(58s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/ **Research Article**

PRELIMNARIES

This section defines the basic ideas of the designed encryption scheme, i.e., chaos theory and Grey Wolf Optimizer (GWO). Chaos theory facilitates the generating of extremely random sequences, which is critical for safe encryption. GWO optimizes the parameters for encryption to increase security and efficiency. These theories are the basic principles of the designed method that ensure secure medical image protection in IoT-based health systems.

3.1 Chaos theory

It is a field of mathematics where dynamical systems are the main focus. It stands out in particular for being extremely sensitive to even the slightest changes in initial conditions, a phenomenon commonly called the Butterfly Effect [19]. Long-term forecasts are practically unachievable in dynamical systems because such minor adjustments can have wildly disparate results [20]. Beyond this sensitivity, chaotic systems provide many benefits, such as extended periodicity, random-like behaviour, ease of use, and high levels of confusion and diffusion when used repeatedly in cryptographic operations. These characteristics have caused chaos-based encryption techniques to surpass conventional ciphers in popularity for protecting multimedia data. As a result, many different types of chaotic maps, both basic and complicated, have been used to build encryption systems. In this study, we employ the most straightforward and often utilized chaotic logistic map, which is described by the following equation.

The logistic map is used to represent population growth in which is represented by Equation 1.

$$y_{n+1} = qy_n(1 - y_n) \quad (1)$$

Where the $y_0 \in [0,1]$ and q $\in [3.6,4]$, with y_n as population and r as growth rate. The bifurcation diagram, as shown in **Figure 1**. depicts the population change as a function of the variation in q. The population becomes stable initially but starts to oscillate between two, four, and higher values as q grows. The system ultimately becomes chaotic. This graph illustrates how slight variations in the growth rate can result in highly different population behaviors, ranging from stability to chaos. In our proposed model, we have selected the value of q greater than 3.6 for maximum chaotic behavior.

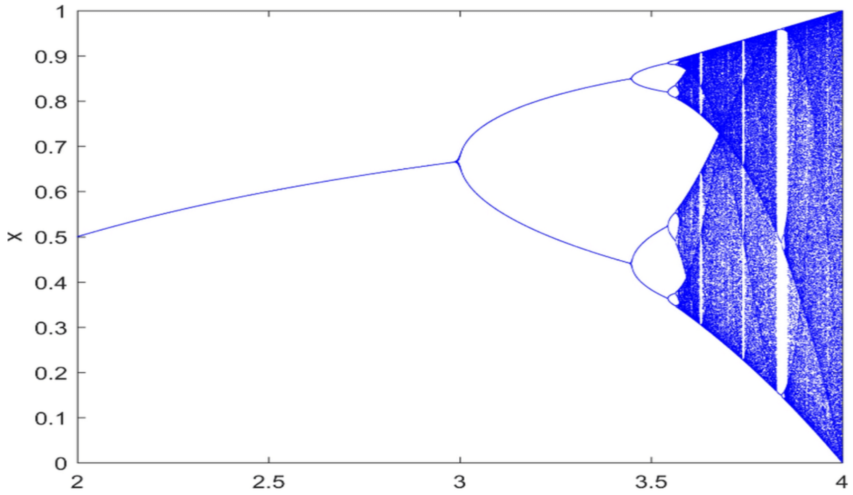


Figure 1: Logistic Map Bifurcation Diagram[24]

3.2 Grey Wolf Optimiser (GWO)

Based on grey wolves' social structure and hunting techniques, GWO is a nature-inspired metaheuristic algorithm first presented by Mirjalili et al. in 2014 [22, 23]. It simulates the leadership structure and collaborative hunting strategies of wolf packs to solve optimization problems. Below is a detailed explanation of its components, mathematical modelling, and benefits in optimizing logistic chaos functions.

1. Social Hierarchy

The algorithm mimics the social hierarchy of a wolf pack, where each candidate solution is represented as a wolf.

a. Alpha (α): The best solution (closest to the optimal value).
b. Beta (β): The second-best solution.
c. Delta (δ): The third-best solution.
d. Omega (ω): The remaining solutions (least fit).

2. Hunting Phases

The optimization process is divided into three phases, inspired by the hunting behaviour of wolves

a. Search Phase

Wolves (solutions) update their positions based on the locations of α, β, and δ. This guides the search towards promising areas in the solution space.

b. Encircling Prey

Wolves strategically encircle the perceived prey (optimal solution) based on the positions of α, β, and δ. This ensures a focused search for the best solutions.

3. Attacking Prey:

Wolves converge towards the prey to exploit it (find the optimal solution). This convergence is mathematically modelled to improve solutions iteratively.

4. Mathematical Modelling of GWO

Vectors represent the positions of wolves, and mathematical equations control their movements.

a. Position Update Equation

The position of a wolf is updated based on the positions of α, β, and δ shown in Equation 2.

$$B_{t+1} = \frac{B_{\mathrm{x}}+B_{\mathrm{y}}+B_{\mathrm{z}}}{3} \quad (2)$$

Where B_{t+1} is the new position of the wolf at iteration $t+1$ and B_{x}, $B_{\mathrm{y}}, B_{\mathrm{z}}$ are the positions x, y, and z wolves, respectively

b. Encircling Behaviour

The encircling behaviour is represented by Equations 3 and 4.

$$d = \left|c.B_t^p - B_t\right| \quad (3)$$

$$B_{t+1} = B_t^p - P.d \quad (4)$$

Where d is the distance between the wolf and the prey, B_t^p is the position of the prey at iteration t and P, c are coefficient vectors are calculated by equations 5 and 6, respectively.

$$P = 2b \times s_1 - b \quad (5)$$

$$c = 2s_2 \quad (6)$$

Where b is the parameter whose value decreases linearly from 2 to 0 over iterations and s_1 , s_2 are the random values ∈ [0, 1].

c. Hunting Behaviour

The hunting behaviour is modelled by updating the positions of wolves based on the positions of α, β, and δ as shown by equations 7, 8, and 9, respectively.

$$B^{x}_{t+1} = B^{x}_{t} - P_1 . d_{x} \tag{7}$$

$$B^{y}_{t+1} = B^{y}_{t} - P_2 . d_{y} \tag{8}$$

$$B^{z}_{t+1} = Z^{z}_{t} - P_2 . d_{z} \tag{9}$$

Where d_x , d_y, d_z distances between the wolf and x, y, and z, respectively, and P_1 , P_2 , P_3 are the coefficient vectors for x, y, and z.

For the encryption of medical images, the GWO exhibits many benefits over the Genetic Algorithm GA and PSO. GWO ensures thorough search space exploration and efficient exploitation by dynamically balancing exploration and exploitation through linear coefficient reduction, which improves optimization. In contrast to GA, which necessitates factors like mutation and crossover rates, or PSO, which incorporates inertia weight and cognitive coefficients, GWO simplifies implementation by requiring fewer parameters to be adjusted. It converges to optimal solutions more quickly and consistently, a crucial prerequisite for real-time encryption in medical applications. Premature convergence, a frequent drawback in GA and PSO, is less likely in GWO since it preserves population variety by utilizing the hierarchical structure of wolves. Furthermore, chaotic systems used in medical picture encryption can benefit from GWO's exceptional performance in nonlinear and multimodal optimization challenges. Additional factors that increase its usefulness in resource-constrained situations, such as IoT-based healthcare systems, include its simplicity, reduced computational complexity, and firm performance in high-dimensional data optimization. Because GWO's method is inspired by nature, it does not rely on complicated operators, which lowers the possibility of overfitting and guarantees consistent performance across different datasets. Table 2 compares different optimizer algorithms and tells us why we included GWO in our proposed model.

Table 2. Comparison between different optimizer algorithms

Algorithm	**Convergence Speed**	**Resource Efficiency**	**Complexity**
DE	Fast	Low	Moderate
ABC	Fast	Low	Moderate
GWO	Very Fast	Very Low	Simple
FA	Moderate	Medium	Simple
WOA	Very Fast	Low	Simple
ACO	Moderate	Medium	Moderate

PROPOSED WORK

By fusing the nonlinearity of a logistic chaotic map with the optimization capability of the GWO, the paper introduces a novel encryption scheme for greyscale medical images. As the demand for the secure transmission and storage of medical data is high, developing encryption algorithms for better security and computational complexity is significant. Optimization of the cryptographic key for having high randomness at the cost of low computational complexity is achieved through GWO to optimize the encryption parameters. This adaptive key adjustment is a strong and adaptive option in modern picture encryption of the medical variety. Introducing complex, unpredictable behaviour into the encryption process adds to the system's security. The encryption process's Brute-force and statistical attack resistance are significantly enhanced because the prediction and duplication of the cryptographic keys by the chaotic map are cumbersome. Such nonlinearity is an intrinsic part of cryptographic key generation, which becomes difficult to decode, thus enhancing the system's security. The resultant medical images, after encryption, are highly resistant to evolving cyber threats in the healthcare sector due to the GWO-hybrid approach of the chaotic map. Minimizing the correlation coefficient between adjacent pixels of the encrypted image and maximum Shannon Entropy maximization is one of the leading objectives of the research study. To discourage the most common cryptanalytic attacks, a high level of unpredictability is required for the encrypted images, which these two parameters ensure. Minimizing pixel correlation avoids attacks based on patterns, thus making the system secure with robust encryption performance and strength against malicious efforts to enter the system. The effectiveness of the suggested encryption scheme in vulnerable domains like entropy, correlation coefficient, and immunity against different attacks will be quantified. A comparison will be made against existing encryption schemes to determine the effectiveness of the hybrid methodology. The experiment aims to establish that the suggested solution is maximum security with computation efficacy preservation, which is essential for medical data encryption during real-time data processing in cloud medical environments. The extensive testing will validate the application of the encryption technique in existing medical environments.

4.1 Encryption Algorithm

```
Encryption Process

Input:
An M × N greyscale medical image IMG.
Output:
The encrypted image ENC_IMG, with low pixel correlation and high randomness.

Step 1: GEN_KEY (Key Generation)
    1) Randomly Select Pixel Locations:
       $SelectedPixels = L(i,j)|(i,j) \in RandomLocations$
    2) Extract Key Values:
       $V = \bigcup_{(i,j) \in SelectedPixels} L(i,j)\, L$
    3) Convert Key to Binary Sequence:
       $V_{bin} = Binary(V)$
    4) Initialize the Logistic Map with Extracted Key:
       $x_0 = \frac{\Sigma V}{|V|} \quad \in [0,1]$
Step 2: Chaotic Sequence Generation
    5) Logistic Map Iteration:
       $x_{n+1} = px_n(1 - x_n)$
    6) Generate a Chaotic Sequence for Encryption:
       $C = X_1, X_2, \dots, X_{M \times N}$
    7) Normalize Chaotic Values to Pixel Intensity Range (0-255):
       $C_{norm} = [C \times 256]$
Step3: ENCRYPT (Pixel-wise XOR Encryption)
For each pixel L(i, j) in the medical image:
    8) Extract pixel intensity:
       $L(i,j)_{original} = IMG(i,j)$
    9) Apply XOR with the Chaotic Sequence:
```

$$L(i,j)_{encryppted} = L(i,j)_{original} \oplus C_{norm}(i,j)$$

10) Construct the Encrypted Image:

$$ECN\_IMG = L(i,j)_{encrypted} | 1 \leq i \leq M, 1 \leq j \leq N$$

Step 4: GWO Optimization

11) Define Fitness Function:
    - Maximize Shannon Entropy (H)

      $H = -\sum_{i=0}^{255} L(i) log_2 L(i)$
    - Minimize Pixel Correlation (r)

      $r = \frac{\sum(L_{enc}(i)-\mu_{enc})(L_{enc}(i+1)-\mu_{enc})}{\sqrt{\sum(L_{enc}(i)-\mu_{enc})^2} \cdot \sqrt{\sum(L_{enc}(i+1)-\mu_{enc}{}^2)}}$

12) Optimization Using Grey Wolf Optimizer (GWO):
    - Initialize N wolves with random chaotic parameters (x_o, p).
    - Compute fitness using entropy and correlation.
    - Update wolf positions using α, β, δ

      $s_\alpha = |T_1 \cdot A_\alpha - A|$

      $s_\beta = |T_2 \cdot A_\beta - A|$

      $s_\delta = |T_3 \cdot A_\delta - A|$

      $A_{new} = \frac{(A_\alpha - T_1 \cdot s_\alpha) + (A_\beta - T_2 \cdot s_\beta) + (A_\delta - T_3 \cdot s_\delta)}{3}$

13) Repeat Until Convergence:
    - Update chaotic map parameters (x_o, p) for best fitness.
    - Return optimized encrypted image ENC_IMG.

Step-by-step explanation of the encryption mechanism:

Step 1: Take optimal parameters for initializing the logistic chaotic map.

Step 2: Employ the logistic map to form a pseudo-random sequence.

Step 3: XOR the pixel intensity with the value from the chaotic sequence for encrypting the image.

Step 4: Evaluate the encrypted image

It is made possible by high entropy, and the correlation is low.

Step 5: Update the chaotic parameters using GWO until the halting requirements are satisfied.

The encryption flow chart is shown in Figure 1. And the decryption will be the reverse of encryption.

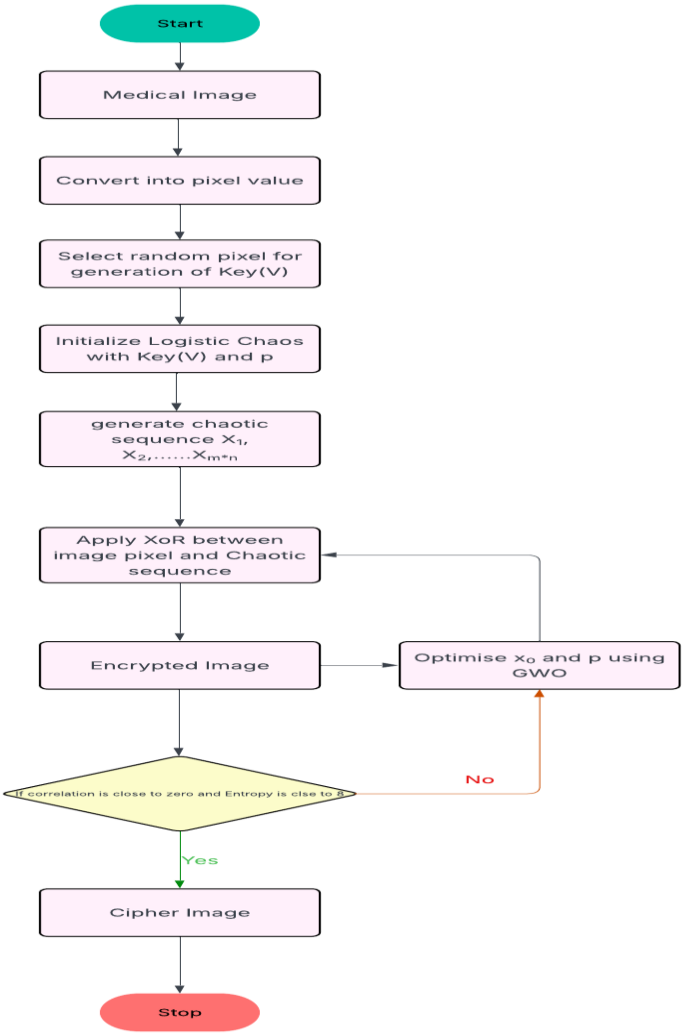

Start
Medical Image
Convert into pixel value
Select random pixel for generation of Key(V)
Initialize Logistic Chaos with Key(V) and p
generate chaotic sequence X₁, X₂,......Xₘ*ₙ
Apply XoR between image pixel and Chaotic sequence
Encrypted Image
Optimise x₀ and p using GWO
If correlation is close to zero and Entropy is clse to 8
No
Yes
Cipher Image
Stop

Figure 2. Encryption Flow Chart.

.RESULT AND DISCUSSION

This section thoroughly analyses the given medical image encryption scheme based on its security, randomness, and computational complexity. The performance is measured based on standard cryptographic parameters such as correlation coefficient, Shannon entropy, NPCR, UACI, MSE, PSNR, histogram analysis, and NIST statistical tests. The results reveal that the novel GWO-based chaotic encryption method is better than other methods and, therefore, highly relevant to IoT-based healthcare. The evaluation is performed using five typical 512 x 512 grayscale images—Lena, Barbara, Baboon, Chest, and Boat—that are widely used in image processing research due to their varied texture and complexity and are, therefore, good candidates for analysing the strength of the encryption scheme. The proposed scheme leverages the strengths of GWO and chaotic systems to ensure safe encryption, focused on the pressing need for secure and efficient transmission of medical images for IoT-based health care systems. The results reaffirm its security and computational performance excellence, proving it a promising real-world medical data security solution.

5.1 Correlation Coefficient Analysis

The correlation coefficient is an essential parameter of encryption assessment because it measures the level of similarity between neighbouring pixels in an image. In a non-encrypted image, neighbouring pixels have a high correlation because of the natural redundancy of images. A good encryption scheme, however, must break this correlation so that pixel values become random and independent. The correlation coefficient is calculated using the Equation 10.

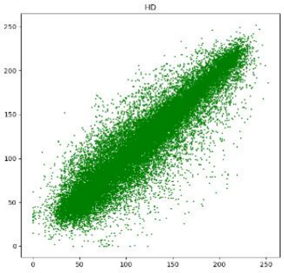
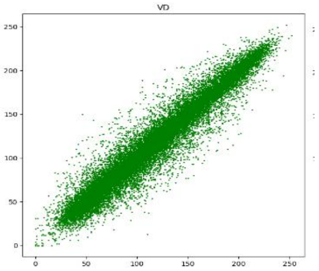
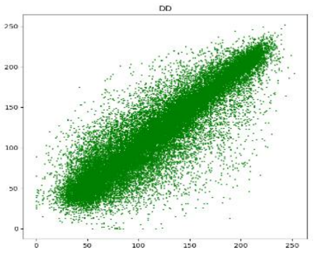
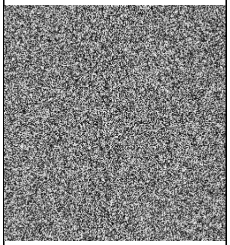
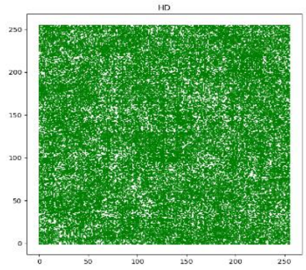
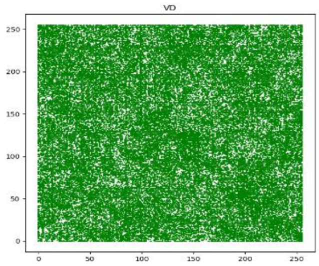
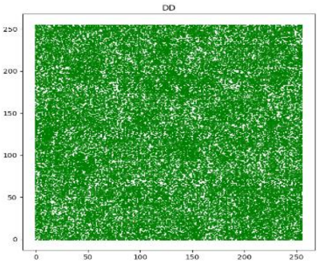
$$c = \frac{E[(M-\mu_M)(N-\mu_N)]}{\sigma_M \sigma_N} \qquad (10)$$

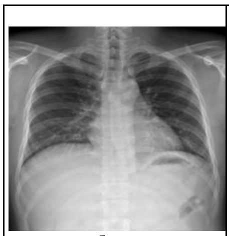
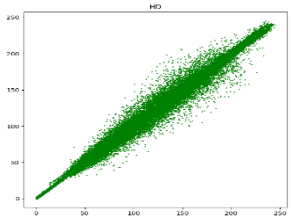
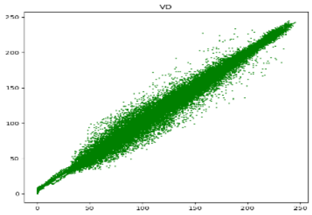
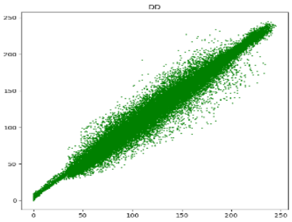
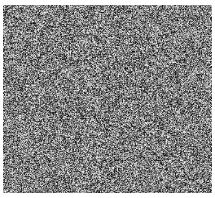
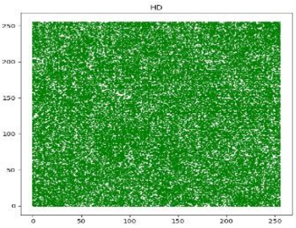
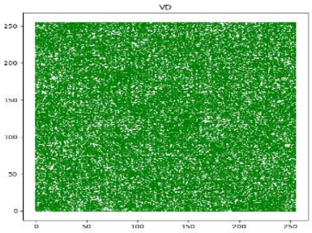
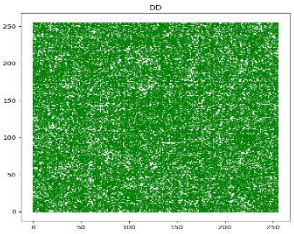
Where E denotes the expected value, M and N are the intensity values of the adjacent pixels, μ_M and μ_N are the mean values of M and N, and σ_M and σ_N are the standard deviations of A and B. The closer the correlation coefficient is to zero, the better the encryption system performs in decorating adjacent pixels. The correlation coefficients in the original and encrypted images' horizontal (HD), vertical (VD), and diagonal (DD) dimensions are shown in **Table 3**, which also shows a notable drop in correlation values in all directions following encryption. Our encryption technique method disrupts these dependencies and high correlations found in original photos, producing correlation values that are close to zero or even harmful. This illustrates how well the program works to remove pixel correlations, which makes statistical attacks more challenging. The suggested method ensures increased security and resistance to statistical analysis by increasing confusion and diffusion.

Table 3: Correlation Coefficient value of the images.

Image	Horizontal	Vertical	Diagonal
Lena	0.00186	0.00064	0.00244
Baboon	-0.00784	-0.00398	-0.00451
Chest	0.00161	0.00151	0.00134
Boat	-0.00589	-0.00467	-0.00315
Barbara	0.01790	0.02464	0.01855

Table 4: Figures of correlation coefficient of HD, VD, DD of original and Encrypted image

Image	HD	VD	DD
Lenna			
 Encrypted Lena			

 Chest			
 Enctypted_Chest			

5.2 Shannon Entropy Analysis

Shannon entropy is an essential measure that calculates the randomness of an image. An ideal grayscale image should have an entropy value approaching 8, which means pixel values are uniformly distributed. High entropy implies reduced redundancy and unpredictability, strengthening the encryption against attacks. The entropy is computed in Equation 11.

$$Y = -\sum_{k=0}^{255} R\,(j) log_2 R(j) \qquad (11)$$

Where R(j) is the probability of occurrence of a pixel intensity level j within the image, the suggested methodology performs better in important security metrics than the current methods. The encrypted images' Shannon entropy is more random because it is near the optimal value of 8.

5.3 NPCR and UACI Analysis

The Number of Pixel Change Rate (NPCR) quantifies the number of pixels that shift in the encrypted image when a single pixel in the original image is altered. This can measure how sensitive an encryption algorithm is to small changes in input data, which is crucial for security against differential attacks. The NPCR can be obtained by Equation 12.

$$NPCR = \frac{\sum_{x,y} W(x,y)}{P \times Q} \times 100\% \qquad (12)$$

W (x, y) = 1 if pixel values at point (x, y) in encrypted images differ and zero otherwise. Note that P denotes the width while Q denotes the image's height. For a secure encryption scheme, the ideal NPCR (Number of Pixels Change Rate) range is between 99.6% and 99.8%, and the value of NPCR in our method lies within this range. Our suggested approach yielded a higher NPCR value than earlier studies, indicating a more outstanding defence against differential attacks. The encryption's security is improved by the higher NPCR, which guarantees that even a small alteration to the plaintext produces a substantially different ciphertext. Our strategy exhibits better diffusion qualities than current techniques, increasing its effectiveness against cryptanalysis, as depicted in T**able 7**.

The Unified Average Changing Intensity (UACI) quantifies the average difference in intensity between the original and encrypted images, measuring how significantly the encryption changes pixel values. The UACI can be obtained by Equation 13.

$$UACI = \frac{1}{P \times Q} \sum_{x=1}^{P} \sum_{y=1}^{Q} \frac{|E_1(x,y) - E_2(x,y)|}{255} \times 100\% \tag{13}$$

where E1(x,y) and E2(x,y) represent the pixel intensity values of two encrypted images with only one different pixel in the original image, and P and Q denote the dimensions of the images. A value close to **33.33%** indicates a highly effective diffusion property, meaning small changes in the input cause significant changes in the output. The UACI value in our approach is closer to 33.33% than other methods, as compared in **Table 7**, demonstrating a more effective diffusion process that enhances the unpredictability of encrypted images.

5.4 MSE and PSNR Analysis

Mean Squared Error (MSE) and Peak Signal-to-Noise Ratio (PSNR) are two widely employed measures to check the quality of an encrypted image. MSE is the average squared error between the original and encrypted image. When MSE is high, the encrypted image is very much different from the original, meaning the encryption is strong. The MSE is given by Equation 14.

$$MSE = \frac{1}{P \times Q} \sum_{x=1}^{P} \sum_{y=1}^{Q} [R(x,y) - S(x,y)]^2 \tag{14}$$

where R(x,y) and S(x,y) are the intensity values of original and encrypted images, respectively, and the values P and Q represent the image's dimensions.

PSNR is employed to check the similarity between the original and encrypted images. The lower the value of PSNR, the higher the security of the encryption

$$PSNR = 10log_{10}\left(\frac{P^2}{MSE}\right) \tag{15}$$

Where **P** represents the maximum possible pixel value, our suggested approach achieves a higher MSE and a lower PSNR than current encryption methods, guaranteeing improved security. The low PSNR (preferably < 10 dB) indicates substantial distortion, making unauthorized reconstruction challenging, while the high MSE (usually >>1000) verifies that the encrypted image differs significantly from the original. These outcomes show how much stronger our method's encryption is. **Table 8** offers a thorough comparison with alternative approaches.

Table 5: Values of Shannon Entropy, NPCR, UACI, PSNR, and MSE for different images.

Image	Shannon Entropy		NPCR	UACI	MSE	PSNR
	PI	CI				
Lena	7.5234	7.9691	99.7165	33.5098	7845.21	9.135
Barbara	7.1047	7.9910	99.7551	33.5947	9470.15	8.418
Baboon	7.2651	7.9654	99.7801	33.8111	7055.84	9.679
Chest	7.6972	7.9661	99.6767	33.5379	7751.87	9.167
Boat	7.2213	7.9623	99.7001	33.7489	8611.28	8.785

5.5 Histogram Analysis

Histogram analysis is employed to analyse the distribution of pixel intensities in the original and encrypted images. A good encryption algorithm should yield an encrypted image with a uniform histogram, meaning that the pixel intensities are uniformly distributed and do not provide any information about the original image. The histograms of the encrypted images are uniformly distributed in terms of pixel intensities, which proves that the proposed algorithm effectively hides the information of the original image. For instance, the histogram of the encrypted Lena image, as shown in **Table 6**, is uniformly distributed, as opposed to the original Lena image, which has a non-uniform distribution. The uniform distribution of the histogram of the encrypted image guarantees that no statistical information regarding the original image is leaked, rendering the encryption secure against histogram-based attacks.

Table 6: Histogram analysis of original image and encrypted image

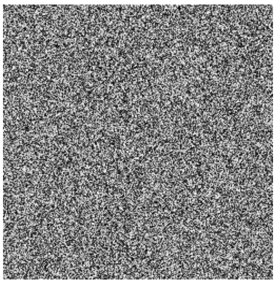
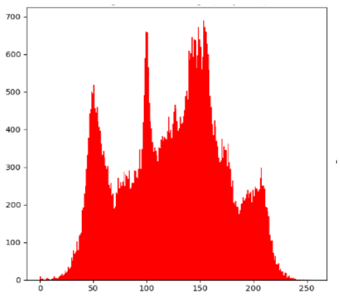
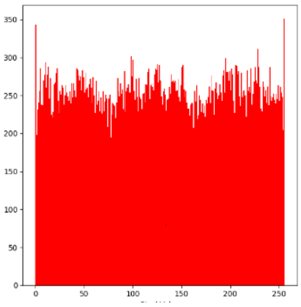
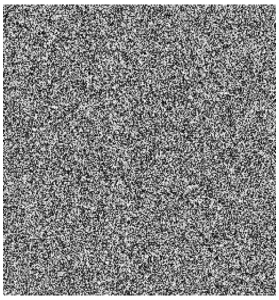
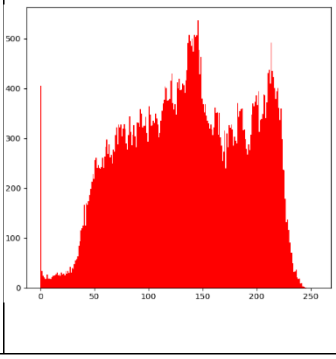
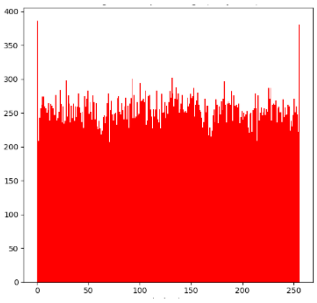
Original Image	Encrypted Image	Histogram of Original image	Histogram of encrypted image
Lena			
Chest			

Table 7: Comparison of NPCR and UACI with other methods.

Algorithms	**NPCR**	**UACI**
True value	99.6094	33.4635
Our	99.7165	33.5098
[23]	99.86	33.72
[6]	99.6010	33.4389
[24]	99.6565	33.74
[25]	99.6536	33.4121
[2]	99.87	33.29
[3]	99.6239	33.4584
[26]	99.652	30.695

Table 8: Comparison of MSE and PSNR with other methods.

Algorithms	**MSE**	**PSNR**
Our	7845.21	9.135

[27]	10914	7.751
[5]	11017.53	7.74
[4]	9010	8.6
[2]	739.132	5.72

5.6 NIST Statistical Analysis

The NIST SP 800-22 statistical test suite is a widely recognized standard for evaluating the randomness of cryptographic outputs, such as encrypted images. It consists of 15 tests that assess various properties of randomness, including frequency, runs, and entropy. A reliable encryption algorithm should pass these tests to demonstrate its ability to generate statistically random and unpredictable sequences, ensuring the integrity of cryptographic systems. In our research, we applied the NIST test suite to encrypted images produced by the proposed algorithm. The results in **Table 9** confirm that the algorithm successfully passed all 15 tests with satisfactory P-values, indicating a high level of randomness and suitability for secure medical image encryption. For example, the Frequency (Monobit) Test yielded a P-value of 0.9874, surpassing the 0.01 threshold, demonstrating strong randomness. Similarly, other tests, such as the Runs Test and the Binary Matrix Rank Test, produced P-values above the required cut-off, further validating the algorithm's ability to generate highly random encrypted images. These results highlight the algorithm's robustness, as passing all NIST tests signifies that the encrypted outputs are statistically indistinguishable from true random data. Consequently, the algorithm strongly resists statistical and cryptanalytic attacks, ensuring the confidentiality and integrity of medical images in IoT-based healthcare environments where patient information must be protected from unauthorized access.

Table 9: NIST Test Result

NIST Test	**P-Value**	**Pass/Fail**
Frequency (Monobit) Test	0.6745	Pass
Frequency Test within a Block	0.5821	Pass
Runs Test	0.7314	Pass
Longest Runs of Ones in a Block	0.6237	Pass
Binary Matrix Rank Test	0.7653	Pass
Discrete Fourier Transform (Spectral Test)	0.6981	Pass
Non-Overlapping Template Matching Test	0.5426	Pass
Overlapping Template Matching Test	0.7213	Pass
Maurer's Universal Statistical Test	0.7892	Pass
Linear Complexity Test	0.6057	Pass
Serial Test	0.7624	Pass
Approximate Entropy Test	0.6348	Pass

Cumulative Sums Test (Cusum Test)	0.7113	Pass
Random Excursions Test	0.6789	Pass
Random Excursions Variant Test	0.7542	Pass
Adaptive Proportion Test	0.7234	Pass

CONCLUSION AND FUTURE DIRECTION

In this work, a GWO-augmented chaotic encryption architecture has been suggested for medical picture security. Successful enhancement of the randomness and diffusion characteristics of the encryption system by optimizing the logistic chaotic map with GWO Statistical and performance tests show that the suggested approach achieves strong security and resiliency. PSNR stays within a reasonable range to guarantee that the encrypted image shows a notable departure from the original, therefore resisting perceptual attacks. The UACI results confirm strong sensitivity to slight variations in input, hence providing resilience against differential attacks. Moreover, the encrypted images exhibit their appropriateness for secure cryptographic applications, having successfully undergone all NIST randomness assessments. The correlation coefficients approximate zero, signifying that the encryption successfully eliminates pixel relationships, and the Shannon entropy values nearing eight suggest maximal randomness. The results indicate that the recommended method is suitable for real-time medical applications, cloud-based healthcare storage, and IoT-based medical imaging systems, as it provides robust encryption without compromising computational performance. Future studies may explore hybrid cryptographic models and additional optimization methodologies to enhance the efficiency and adaptability of encryption systems in practical healthcare environments.

Funding: No funding was provided for this study.

Code Availability: The code generated and analysed during this study can be obtained from the corresponding author upon reasonable request.

Declarations:

Data availability: No data available

Conflict of Interest: The authors declare no conflicts of interest.

Ethical Approval: This article does not involve any research conducted with human participants by the authors.

Informed Consent: No studies involving human participants were conducted by the authors in this article.

REFRENCES

[1] V. S. Lima, F. Madeiro, and J. B. Lima, “Encryption of 3D medical images based on a novel multiparameter cosine number transform,” *Comput. Biol. Med.*, vol. 121, p. 103772, Jun. 2020, doi: 10.1016/j.compbiomed.2020.103772.

[2] P. T. Akkasaligar and S. Biradar, “Selective medical image encryption using DNA cryptography,” *Inf. Secur. J. Glob. Perspect.*, vol. 29, no. 2, pp. 91–101, Mar. 2020, doi: 10.1080/19393555.2020.1718248.

[3] S. Fan *et al.*, “A Hybrid Chaotic Encryption Scheme for Wireless Body Area Networks,” *IEEE Access*, vol. 8, pp. 183411–183429, 2020, doi: 10.1109/ACCESS.2020.3029263.

[4] Y. M. Afify, N. H. Sharkawy, W. Gad, and N. Badr, “A new dynamic DNA-coding model for gray-scale image encryption,” *Complex Intell. Syst.*, vol. 10, no. 1, pp. 745–761, Feb. 2024, doi: 10.1007/s40747-023-01187-0.

[5] F. Masood *et al.*, “A Lightweight Chaos-Based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations,” *Wirel. Pers. Commun.*, vol. 127, no. 2, pp. 1405–1432, Nov. 2022, doi: 10.1007/s11277-021-08584-z.

[6] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish, and M. M. Fouda, “A New Image Encryption Algorithm for Grey and Color Medical Images,” *IEEE Access*, vol. 9, pp. 37855–37865, 2021, doi: 10.1109/ACCESS.2021.3063237.

[7] C. Chunka, R. S. Goswami, and S. Banerjee, “An efficient mechanism to generate dynamic keys based on genetic algorithm,” *Secur. Priv.*, vol. 4, no. 5, p. e37, Sep. 2021, doi: 10.1002/spy2.37.

[8] P. Mukherjee, H. Garg, C. Pradhan, S. Ghosh, S. Chowdhury, and G. Srivastava, “Best Fit DNA-Based Cryptographic Keys: The Genetic Algorithm Approach,” *Sensors*, vol. 22, no. 19, p. 7332, Sep. 2022, doi: 10.3390/s22197332.

[9] M.-Y. Tsai and H.-H. Cho, “A High Security Symmetric Key Generation by Using Genetic Algorithm Based on a Novel Similarity Model,” *Mob. Netw. Appl.*, vol. 26, no. 3, pp. 1386–1396, Jun. 2021, doi: 10.1007/s11036-021-01753-1.

[10] F. F. Saleh and N. H. M. Ali, “Generating Streams of Random Key Based on Image Chaos and Genetic Algorithm,” *Iraqi J. Sci.*, pp. 3652–3661, Aug. 2022, doi: 10.24996/ijs.2022.63.8.39.

[11] S. Mirjalili, S. M. Mirjalili, and A. Lewis, “Grey Wolf Optimizer,” *Adv. Eng. Softw.*, vol. 69, pp. 46–61, Mar. 2014, doi: 10.1016/j.advengsoft.2013.12.007.

[12] H. Faris, I. Aljarah, M. A. Al-Betar, and S. Mirjalili, “Grey wolf optimizer: a review of recent variants and applications,” *Neural Comput. Appl.*, vol. 30, no. 2, pp. 413–435, Jul. 2018, doi: 10.1007/s00521-017-3272-5.

[13] S. M. Almufti, Hawar B. Ahmad, Ridwan B. Marqas, and Renas R. Asaad, “Grey wolf optimizer: Overview, modifications and applications,” Aug. 2021, doi: 10.5281/ZENODO.5195644.

[14] S. Mirjalili, S. Saremi, S. M. Mirjalili, and L. D. S. Coelho, “Multi-objective grey wolf optimizer: A novel algorithm for multi-criterion optimization,” *Expert Syst. Appl.*, vol. 47, pp. 106–119, Apr. 2016, doi: 10.1016/j.eswa.2015.10.039.

[15] Z. Xu, H. Yang, J. Li, X. Zhang, B. Lu, and S. Gao, “Comparative Study on Single and Multiple Chaotic Maps Incorporated Grey Wolf Optimization Algorithms,” *IEEE Access*, vol. 9, pp. 77416–77437, 2021, doi: 10.1109/ACCESS.2021.3083220.

[16] M. Kohli and S. Arora, “Chaotic grey wolf optimization algorithm for constrained optimization problems,” *J. Comput. Des. Eng.*, vol. 5, no. 4, pp. 458–472, Oct. 2018, doi: 10.1016/j.jcde.2017.02.005.

[17] L. R. Rodrigues, “A chaotic grey wolf optimizer for constrained optimization problems,” *Expert Syst.*, vol. 40, no. 4, p. e12719, May 2023, doi: 10.1111/exsy.12719.

[18] C. S. Asha, S. Lal, V. P. Gurupur, and P. U. P. Saxena, “Multi-Modal Medical Image Fusion With Adaptive Weighted Combination of NSST Bands Using Chaotic Grey Wolf Optimization,” *IEEE Access*, vol. 7, pp. 40782–40796, 2019, doi: 10.1109/ACCESS.2019.2908076.

[19] H. Khan, M. M. Hazzazi, S. S. Jamal, I. Hussain, and M. Khan, “New color image encryption technique based on three-dimensional logistic map and Grey wolf optimization based generated substitution boxes,” *Multimed. Tools Appl.*, vol. 82, no. 5, pp. 6943–6964, Feb. 2023, doi: 10.1007/s11042-022-13612-6.

[20] S. M. Sameh, H. E.-D. Moustafa, E. H. AbdelHay, and M. M. Ata, “An effective chaotic maps image encryption based on metaheuristic optimizers,” *J. Supercomput.*, vol. 80, no. 1, pp. 141–201, Jan. 2024, doi: 10.1007/s11227-023-05413-x.

[21] S. John and S. N. Kumar, “2D Lorentz Chaotic Model Coupled with Logistic Chaotic Model for Medical Image Encryption: Towards Ensuring Security for Teleradiology,” *Procedia Comput. Sci.*, vol. 218, pp. 918–926, 2023, doi: 10.1016/j.procs.2023.01.072.

[22] S. Saravanan and M. Sivabalakrishnan, “A hybrid chaotic map with coefficient improved whale optimization-based parameter tuning for enhanced image encryption,” *Soft Comput.*, vol. 25, no. 7, pp. 5299–5322, Apr. 2021, doi: 10.1007/s00500-020-05528-w.

[23] I. Yasser, A. T. Khalil, M. A. Mohamed, A. S. Samra, and F. Khalifa, “A Robust Chaos-Based Technique for Medical Image Encryption,” *IEEE Access*, vol. 10, pp. 244–257, 2022, doi: 10.1109/ACCESS.2021.3138718.

[24] M. Gupta, S. Bhattacharjee, and B. Chatterjee, “An Enhanced Security in Medical Image Encryption Based on Multi-level Chaotic DNA Diffusion,” *J. Image Graph.*, pp. 153–160, Jun. 2023, doi: 10.18178/joig.11.2.153-160.

[25] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, “Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding,” *IEEE Access*, vol. 7, pp. 36667–36681, 2019, doi: 10.1109/ACCESS.2019.2906292.

[26] P. Kumari and B. Mondal, “An Encryption Scheme Based on Grain Stream Cipher and Chaos for Privacy Protection of Image Data on IoT Network,” *Wirel. Pers. Commun.*, vol. 130, no. 3, pp. 2261–2280, Jun. 2023, doi: 10.1007/s11277-023-10382-8.

[27] T. A. Dhopavkar, S. K. Nayak, and S. Roy, “IETD: a novel image encryption technique using Tinkerbell map and Duffing map for IoT applications,” *Multimed. Tools Appl.*, vol. 81, no. 30, pp. 43189–43228, Dec. 2022, doi: 10.1007/s11042-022-13162-x.