

Original Article

A Novel Optimal Key Selection Approach for Medical Image Encryption

Afreen Fatima Mohammed^{1,2}, Syed Shabbeer Ahmad³

¹Department of Computer Science & Engineering, Faculty of Engineering, Osmania University, Telangana, India.

²Department of CSE (Data Science), CVR College of Engineering, Telangana, India.

³Department of Computer Science & Engineering, Muffakham Jah College of Engineering & Technology, Telangana, India.

¹Corresponding Author : afreen0422@gmail.com

Received: 10 April 2024

Revised: 15 July 2024

Accepted: 30 July 2024

Published: 28 August 2024

Abstract - The medical industry has been facing challenges in protecting the medical records of patients. To sustain privacy, it is important to secure medical images during their transmission. Therefore, a security mechanism must be implemented while transmitting medical images over the network. In order to handle security concerns, health organizations must implement efficient security strategies such as encryption techniques that would employ a better key generation and selection practice. In this study, chaotic maps are employed for the generation of keys. A novel approach is proposed to perform the optimal key selection process, which is vital in influencing the performance of an encryption algorithm. Thereby, in this paper, a novel Chaotic Bio-inspired Boosted Remora Optimization Algorithm is proposed for achieving a secure image transmission system based on an optimal key selection approach.

Keywords - Chaotic maps, Lightweight elliptic curve cryptography, Optimization algorithm, Secret share construction approach.

1. Introduction

The healthcare field has security concerns related to patient privacy and confidentiality, legal and regulatory compliance, preventing unauthorized access and data breaches, maintaining data integrity, ensuring availability and reliability, protecting against cyber security threats, and building patient trust and confidence. Medical images often contain sensitive information about patient's health conditions, diagnoses, and treatments. Unauthorized access or disclosure of these images can lead to patient privacy and confidentiality breaches, violating ethical standards and legal regulations. Medical images stored in digital format are vulnerable to unauthorized access, hacking, and data breaches. Medical image integrity can be maintained by preventing tampering, alteration, or unauthorized modifications. Any unauthorized changes to medical images could lead to incorrect diagnoses, inappropriate treatments, and compromised patient care. The security and confidentiality of medical images are prominent for building and maintaining patient trust and confidence in the healthcare system. To address these security concerns, healthcare organizations must implement comprehensive security strategies and best practices for securing medical image data. This includes implementing encryption, access controls, authentication mechanisms, data backup and recovery processes, regular security assessments and audits, staff training and awareness programs, and adherence to regulatory

requirements and industry data security and privacy standards. Chaos theory has been exhaustively used for medical image encryption and generating random sequences of keys through chaotic maps. Chaotic maps are significant to initial condition sensitivity, simplicity, and randomness. Numerous chaotic maps are considered in the literature for generating the random sequences.

The problem has been identified: chaotic maps produce sequences that appear random, but their raw output may not be suitable for encryption without additional processing or selection. Chaotic maps exhibit complex and random behavior, but their outputs may still exhibit patterns or correlations that the attackers could manipulate. Therefore, the desired level of security for encryption cannot be provided by simply using the raw output of chaotic maps. The paper emphasises selecting keys from the generated sequences using an optimization algorithm and ensuring their security and unpredictability. The selected keys are then utilized to generate keys for Encryption.

This paper applies chaotic maps corresponding to Logistic maps and Fuzzy Triangular tent maps to generate two sets of chaotic, random sequences of keys. The key generation approach introduced in the paper is a modification to the work done in [21], in which it was stated that chaotic sequences from the Logistic map and Fuzzy Triangular Tent map were



XORed. Since two sets of random sequences of keys are required, a logistic map and a fuzzy triangular tent map are applied separately. In this paper, a novel optimal key selection process is proposed. Boosted Remora Optimization Algorithm is devised for optimal key selection from the random sequences derived through a Logistic map and Fuzzy triangular Tent map.

The secret keys from selected optimal keys are generated by applying the Elliptic Curve Diffie Hellman (ECDH) Key Exchange algorithm [27]. The summarization of the major contribution in the paper is stated below:

- Apply Logistic and Fuzzy Triangular Tent map to generate two sets of random sequences of keys.
- Propose a Boosted Remora Optimization algorithm to select optimal private and public keys.
- Apply the Elliptic Curve Diffie Hellman (ECDH) Key Exchange algorithm to generate a secret and public key for the sender using the optimal selected private key.
- Devise a Secret Share Construction Approach to construct shares from an image.
- Apply the Lightweight Elliptic Curve Cryptography Algorithm on each share using the keys shared through ECDH.
- The proposed approach is assessed for performance analysis regarding security and quality metrics against existing algorithms.

2. Related Work

Chaos Theory has a prominent role in the cryptography field. The chaotic maps possess confusion and diffusion properties. The encryption scheme based on hybrid chaotic maps performs permutations in two dimensions of an image [11]. Some image encryption techniques employ a few rounds of scrambling and diffusion operations that would shuffle random neighboring pixels in an image [12]. Patient data confidentiality, such as medical images, is provided through a lightweight encryption approach [16]. Today's healthcare sector is augmented by numerous IoT medical devices necessary to track patients' health conditions [24].

Medical images generated by X-ray, MRI, and CT scanner devices must be monitored constantly. The images need to be secured before they are transmitted to the recipient. The recipient can be a local server or a cloud server. Numerous security mechanisms have been employed in literature, such as detecting image forgery [23]. An image must be properly encrypted before it is transmitted. A lightweight encryption algorithm employing permutation techniques would provide a secure mechanism for encrypting medical images [3]. A comparative study was done between chaos and ECC-based encryption, and a good execution time was obtained from the application of chaos [4]. To ensure the effectiveness of encryption for medical images, it is essential to adhere to best practices for key generation, such as using cryptographic algorithms with sufficient key lengths,

leveraging secure random number generators, and implementing key management practices to safeguard the confidentiality of keys themselves. Regular audits and assessments should also be conducted to evaluate the strength and adequacy of encryption keys used in healthcare systems. The generation of encryption keys is crucial to medical image security. Shamir proposed a secure medical image sharing paradigm through a secret share construction approach, which involves breaking the image into its constituent pixels or blocks [1]. In Shamir's Secret Sharing scheme, Lagrange interpolation is used to reconstruct the polynomial and, hence, reconstruct the original image. Depending on the specific requirements, additional techniques such as encryption of shares, watermarking, or steganography may be employed to enhance security or provide additional functionalities.

The tampering of shares can be avoided by encrypting each share with the Advanced Encryption Standard (AES) algorithm, thereby reducing fraudulent shares. This offers a better security solution [13]. Encryption through Elliptic curve cryptography has provided another security service layer. The histograms of original and encrypted key frame images have vast variations [14-17]. Applying an optimization algorithm for key selection enhances the security of medical images through lightweight cryptography algorithms [18-20]. In this paper, the Secret Sharing Construction approach is applied based on the work done in [22].

3. Proposed Work

Chaotic maps play a major role in the generation of keys. This paper applies logistic and fuzzy triangular tent maps to generate different sets of random sequences of keys. Since selecting an optimal key is a vital process in encryption, this paper proposes a novel key selection approach using a bio-inspired Boosted Remora Optimization Algorithm. Medical image security can be enhanced using a strategy in which, instead of encrypting the whole medical image at once, the image can be divided into a set of shares by employing a secret share construction approach and then encrypting each share separately. The secret share construction approach divides the image into twelve shares. Lightweight Elliptic Curve Cryptography is adapted to encrypt each share.

The Boosted Remora Optimization Algorithm (BROA) is proposed to optimize the key selection process. Before optimizing the key, the key generation process is accomplished through the Logistic and Fuzzy Triangular Red Panda Optimization (LFT-RPO) Algorithm to construct a random sequence number employed as secure keys for encryption [21]. Lastly, the decryption and share reconstruction processes are executed on the receiver side to construct the original images. As a result, medical image security is strengthened by integrating BROA into the cryptography process, making it more resilient to attacks via unauthorized users.

Secret Share Construction Approach

The main concept of the Secret Share Construction Approach (SSCA) is to transform the input image into several shares in an unreadable format. Once shares are constructed, each share is encrypted separately. The decrypted shares are recombined to reconstruct an original image during decryption. The performance of SSCA can be assessed based on four factors: reconstruction accuracy, security, computational complexity, and storage needs. For each band of an image, four shares are constructed using the SSCA approach. Thus, the medical image is transformed into twelve sets of shares, as shown in Figure 1. An overall pixel value of the image Pix is calculated by computing the sum of the pixel intensities for each band of an image (r_n, g_n, b_n) . It is specified by the Equation (1):

$$Pix = \sum r + g + b \quad (1)$$

RGB shares are computed as shown in Equation (2), (3) and (4).

$$r_s = \int_1^{lf} \frac{lim}{l \rightarrow 1tonbc} \quad (2)$$

$$g_s = \int_1^{lf} \frac{lim}{l \rightarrow 1tonbc} \quad (3)$$

$$b_s = \int_1^{lf} \frac{lim}{l \rightarrow 1tonbc} \quad (4)$$

While b and c designate the matrix positions r_s, g_s and b_s signify the RGB share, and $r_{bc} g_{bc}$ and b_{bc} represents image pixel component. Two elementary matrices corresponding to the share formation are characterized by b_{m1} and b_{m2} . Initially xr_1 and xr_2 are computed prior to sharing as follows:

$$xr_1 = 128 - b_{m1} \quad (5)$$

$$xr_2 = b_{m2}$$

The red band shares are further computed by applying an XOR operation between the key matrix and the basic matrix.

$$rs1 = xr_1 \oplus k_m \quad (6)$$

$$rs2 = xr_2 \oplus xr_1 \quad (7)$$

$$rs3 = xr_2 \oplus rs1 \quad (8)$$

$$rs4 = rs1 \oplus r \quad (9)$$

Similarly, the shares of blue and green bands are constructed. To reconstruct an original medical image, shares are XORed for each band as given below:

$$r = rs1 \oplus rs2 \oplus rs3 \oplus rs4 \oplus k_m \quad (10)$$

$$g = gs1 \oplus gs2 \oplus gs3 \oplus gs4 \oplus gs4 \oplus k_m \quad (11)$$

$$b = bs1 \oplus bs2 \oplus bs3 \oplus bs4 \oplus bs4 \oplus k_m \quad (12)$$

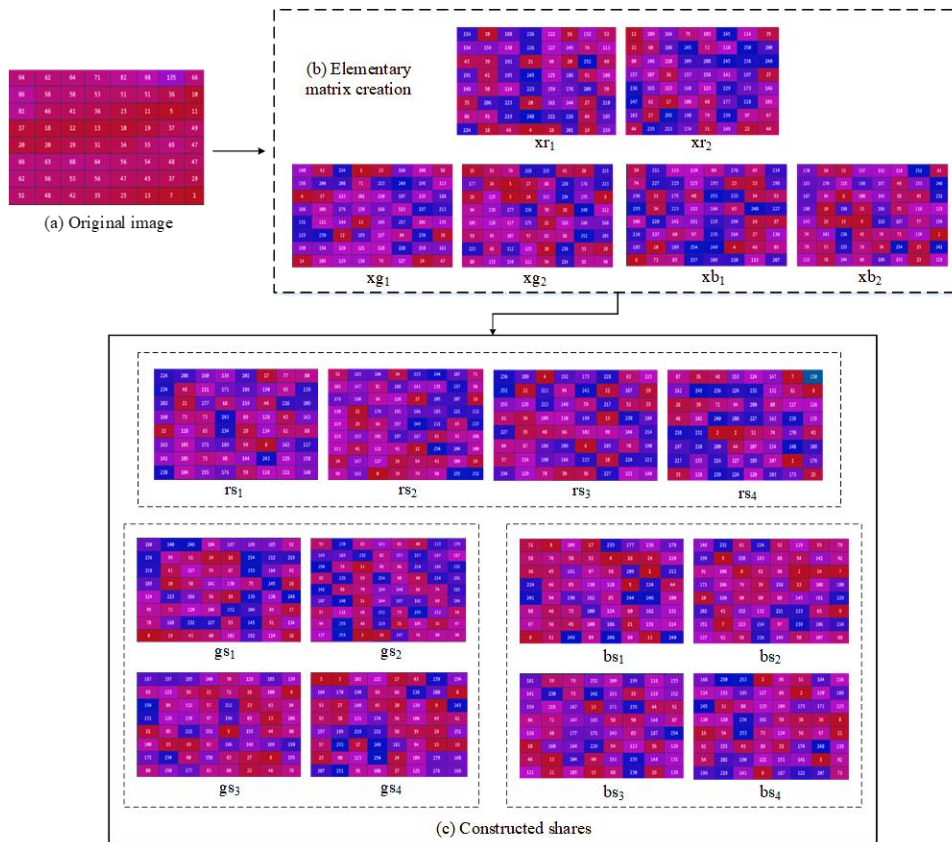


Fig. 1 SSCA approach for share construction [22]

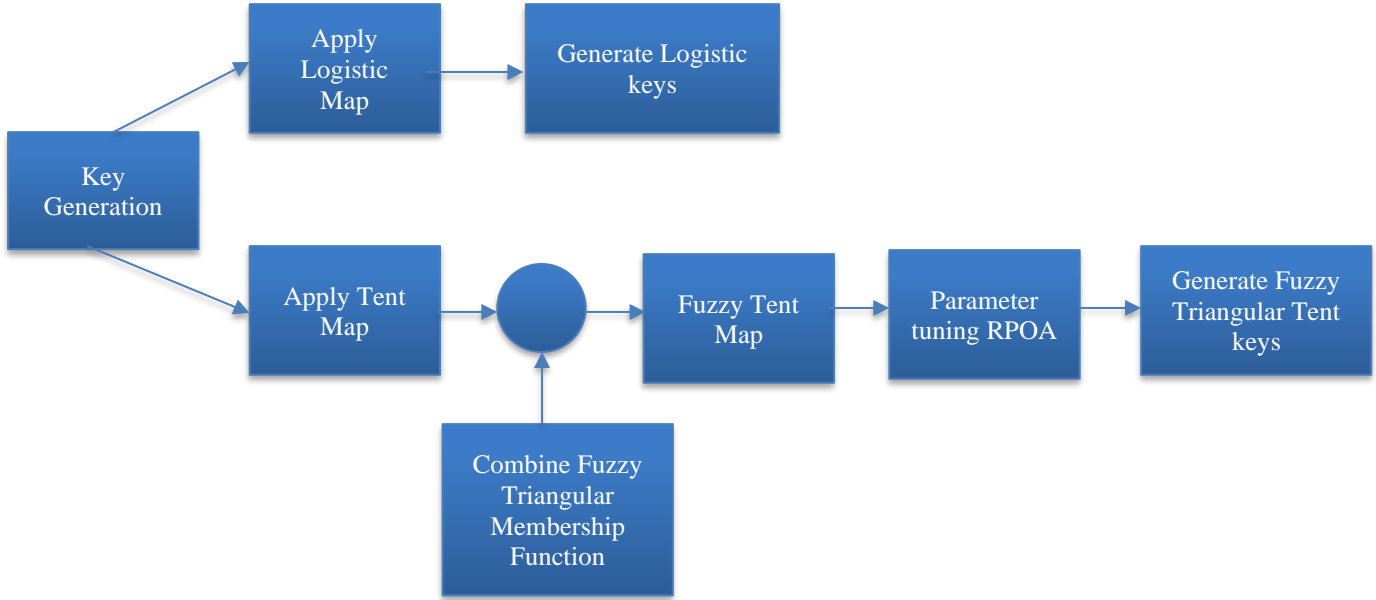


Fig. 2 Key generation process

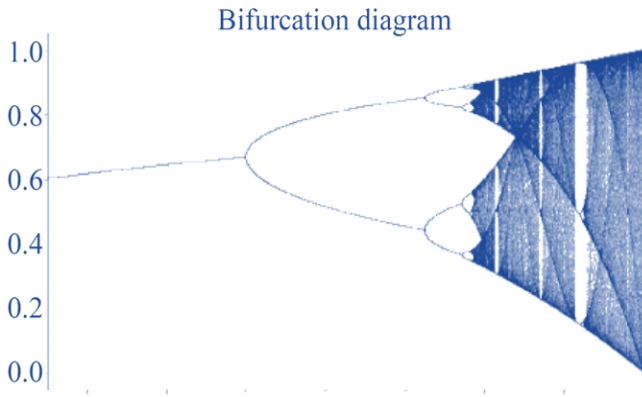


Fig. 3 Bifurcation diagram $r \in [2.5, 4]$

3.1. Key Generation Using Fuzzy Membership Based Chaotic Maps and Red Panda Optimization

A unique key generation approach, Fuzzy membership based chaotic maps and Red Panda Optimization (FM-CM-RPO) that use chaotic maps and bio-inspired meta-heuristic Optimization, is employed to secure medical image transmission [21]. The main objective of the FM-CM-RPO process is to generate a set of random sequences of keys by employing a Logistic map and a Fuzzy Triangular Tent map. The parameters of a chaotic map are significant to the mapping behavior, so to obtain the optimal parameter value, Red Panda Optimization Algorithm (RPOA) is applied [2]. The key generation process is provided in Figure 2.

3.1.1. Logistic Map

A logistic map is a one-dimensional chaotic map [15]. The numerical expression of the logistic map is provided below as follows:

$$y_{(j)}(\log i) = v_1 \times y_{(j-1)} \times (1 - y_{(j-1)}) \quad (13)$$

Where v_1 implies the control parameter and its value is $[0, 4]$. The logistic map is extremely sensitive to initial conditions $y_{(j)}$, which range from 0 to 1. The bifurcation diagram depicting the chaotic behavior of the logistic map is represented in Figure 3, which depicts chaotic behavior when $r \in [2.5, 4]$.

3.1.2. Tent Map

A tent map is another nonlinear, dynamic, chaotic map. It is employed to create random number sequences that can be applied as encryption keys for image encryption. The numerical expression of the tent map is resembled below as follows:

$$a_{(j)} = \begin{cases} v_2 \times a_{(j-1)}, & \text{if } 0 \leq a_{(j-1)} < \frac{1}{2} \\ v_2 \times (1 - a_{(j-1)}), & \text{if } \frac{1}{2} \leq a_{(j-1)} \leq 1 \end{cases} \quad (14)$$

Where $v_2 \in (0.5, 2)$ implies the parameter and its initial value range is $[0, 1]$.

3.1.3. Fuzzy Number

Fuzzy numbers are mathematical concepts employed to express imprecision and uncertainty in data. A membership function that provides a membership degree to every component of the universe of discourse is used to represent fuzzy numbers. The membership degree ranges between 0 and 1. 0 signifies no membership and 1 represents full membership. Fuzzy numbers have been applied to clustering, segmentation, encryption, and image classification in the context of image processing. Three parameters are utilized to control inputs in the triangular fuzzy membership function, particularly the minimum, maximum, and middle values, which are positioned at the triangle peak. Whereas b and d are placed at the bottom of the triangle, thereby $b \leq c \leq d$.

The expression of the triangular membership function is provided as follows:

$$f(y, b, c, d) = \text{Maxi} \left(\text{Mini} \left(\frac{y-b}{c-b}, \frac{d-y}{d-c} \right), 0 \right) \quad (15)$$

The fuzzy tent map combines the tent map and triangle membership values created using the triangular membership function. This generates an intricate and random sequence number that can be employed as encryption keys in the encryption process.

3.1.4. Fuzzy Triangular Tent Map

As tent maps can provide complicated and unpredictable behavior, fuzzy mathematics ideas are commonly used to develop highly chaotic systems for image encryption. Therefore, the proposed method integrates the fuzzy mathematics concept into a tent map. The complex behavior exhibited by the map is used to encrypt the image securely. By employing the properties of both concepts, the proposed method intends to offer a greater level of security. Now, the implementation of a fuzzy triangular function to tent map is given as follows:

$$y_{(j+1)} = \begin{cases} v_2 \times f_{zz} \times a_{(k-1)}, & \text{if } 0 \leq a_{(j-1)} < \frac{1}{2} \\ v_2 \times f_{zz} \times (1 - a_{(j-1)}), & \text{if } \frac{1}{2} \leq a_{(j-1)} \leq 1 \end{cases} \quad (16)$$

Where f_{zz} implies the fuzzy triangular.

3.1.5. Fuzzy Membership Based Chaotic Maps and Red Panda Optimization

The sequence of random numbers constructed by hybrid map and fuzzy concept is utilized as a secret key for encryption. The logistic map is reflected to be used as a key during the process of encryption for enhancing confidentiality and security of image data. The concept of fuzzy mathematic is employed to generate values that influence initial keys in every iteration and create new cipher images. In FM-CM-RPOA, the keys generated using logistic map and fuzzy tent map in the initial phase is constituted with XOR operation to obtain the final key. Now, the expression of final key generation is given as follows:

$$E_{Key} = y_{(j)} (\log i) \oplus y_{(j+1)} \quad (17)$$

Moreover, in the key generation algorithm, the parameters v_1 and v_2 play a significant role in defining the map behavior and these values are adjusted using RPOA to attain enhanced outcomes. RPOA is a new bio-inspired meta-heuristic algorithm that mimics the characteristics of red pandas in the wild. The primary design concept of RPOA is enthused by two natural characteristics of red panda such as foraging policy and climbing trees to rest. Here, the exploration stage is modeled depending on the foraging policy of red pandas, whereas the exploitation stage is modeled depending on the movement of red pandas as they

climb trees. RPOA cannot require a parameter adjustment procedure since there exists no control parameter in its mathematical modeling and it is considered as its primary advantage. Thus, the proposed method has employed RPOA to adjust the parameters v_1 and v_2 of chaotic map. Now, the parameter updating modeled using the exploration of RPOA is provided in the following expression:

$$Y_j = y_{j,k} + s.(sfs_{j,k} - J.y_{j,k}) \quad (18)$$

Where, Y_j implies the new location of j^{th} red panda, s specifies the random number in interval $[0,1]$, $sfs_{j,k}$ resembles the chosen food source for j^{th} red panda in k^{th} dimension, J implies the random number chosen from the set $\{1,2\}$. After key generation, the optimal keys are selected using BROA.

3.2. Boosted Remora Optimization Algorithm

Boosted Remora Optimization Algorithm (BROA) is a bio-inspired metaheuristic optimization algorithm. It works on the foraging strategy of remoras. Remoras are small fishes which attach themselves to large marine animals for transportation [9]. BROA aims to optimize complex problems by mimicking nature's cooperative behavior and movement patterns.

The Boosted Remora Optimization Algorithm (BROA) is employed in the proposed method for optimal key selection. Levy flight and Brownian mutation are incorporated into the ROA algorithm to expand its searchability. Levy flight enables remoras to explore search space. Furthermore, the hybrid algorithm's exploitation ability is strengthened, and individuals are supported in escaping the local optimal solution by applying Brownian mutation. In the proposed method, remoras are considered key.

Initialize the population with random sequences generated from a logistic map. Each random number signifies a remora. The current location of the remora is represented as $U_l = (U_{l1}, U_{l2}, U_{l3}, \dots, U_{lg})$ where l designates the current remora and g specifies the dimensions in the remora search area. The fitness function is computed for each candidate solution as $h(U_l) = h(U_{l1}, U_{l2}, U_{l3}, \dots, U_{lg})$. The optimal solution $U_{DV} = (U_1^*, U_2^*, U_3^*, \dots, U_g^*)$, is derived based on the best fitness function value computation. The location of remoras is then updated in the exploration phase based on the best fitness values generated. The location update is represented as follows:

$$U_l^{w+1} = U_{DV}^w - \left(\text{Rand}(0,1) * \left(\frac{U_{DV}^w + U_{Rand}^w}{2} \right) - U_{Rand}^w \right) \quad (19)$$

Where w represents the current iteration and U_{Rand} specifies the random position. When the remoras

change the host, the location of the remoras is updated as follows:

$$U_{cvv}^{w+1} = U_i^w + (U_i^w - U_{pre}^w) * Randn \tag{20}$$

Where U_{pre}^w indicates the location of the preceding generation and U_{cvv}^{w+1} implies the tentative step, $Randn$ represents a random number. Host change represents a small global movement. The feeding strategy of remoras is repeated in each iteration. In each iteration, the fitness values are computed and the current solution $h(U_i^w)$ fitness value is compared with the fitness value of the attempted previous solution $h(U_{cvv})$. If it is larger than the attempted solution, the remora selects another feeding strategy for local optimization.

$$h(U_i^w) > h(U_{cvv}) \tag{21}$$

An exploitation stage is represented using Equation (21). On the other hand, if the fitness value of the current solution is lesser than the attempted solution, then Remora would perform a host switch [9]. In the exploitation stage, the location of the next remora is updated mathematically as follows:

$$U_{l+1}^w = G * e^\delta * \cos(2\pi\delta) + U_l^w \tag{22}$$

$$\delta = rand.(a - 1) + 1 \tag{23}$$

$$a = -(1 + \frac{w}{W}) \tag{24}$$

$$G = | U_{DV}^w - U_l^w | \tag{25}$$

Where, G indicates the difference between the best position and current position and δ indicates the random number in the range $[-1,1]$ and ‘ a ’ linearly decreases from -1 to -2.

3.2.1. Improvement with Levy Flight and Brownian Motion

Levy flight is a type of random walk that explores the solution space. It generates a step size based on the Levy distribution [29]. With frequent short-distance steps, it accomplishes occasional long-distance walking.

The following is the mathematical expression for Levy flight:

$$Levy = 0.01 \times \frac{s_1 \times \alpha}{|s_2|^\eta} \tag{26}$$

$$\alpha = \left(\frac{\Gamma(1+\eta) \times \sin(\frac{\pi\eta}{2})}{\Gamma(\frac{1+\eta}{2}) \times \eta \times 2^{\frac{(\eta-1)}{2}}} \right)^{\frac{1}{\eta}} \tag{27}$$

Where, η implies the constant equal to 1.5, s_1 and s_2 specify the random value between $[0,1]$. Brownian motion is another type of random walk. It models small random movements, which are used in the exploitation phase of BROA. It is represented as:

$$F_{Brownian}(y, \lambda, \rho) = \frac{1}{\sqrt{2\pi\rho^2}} \exp\left(-\frac{(y-\lambda)^2}{2\rho^2}\right) = \frac{1}{\sqrt{2}} \exp\left(-\frac{y^2}{2}\right) \tag{28}$$

Where, y implies the point following the motion, $\lambda = 0$ and $\rho^2 = 1$. Improved expressions by applying Levy flight and Brownian motion are given as:

$$U_{cvv} = \alpha U_i^w + F_{Brownian}(y, \lambda, \rho) * (U_i^w - U_{pre}^w) * Randn \tag{29}$$

$$U_{l+1}^w = G * F_{Brownian}(y, \lambda, \rho) * e^\delta * \cos(2\pi\delta) + U_l^w \tag{30}$$

3.3. Encryption of Shares Using Lightweight Elliptic Curve Cryptography

Lightweight Elliptic Curve Cryptography (LWECC) is a variant of the traditional Elliptic Curve Cryptography algorithm. LWECC is optimized for resource-constrained devices. It employs elliptic curve-based encryption algorithms but focuses on minimizing computational and memory requirements. LWECC involves generating a public-private key pair [4]. The selected optimal Logistic Keys are treated as public keys, and optimal Fuzzy Triangular Tent keys are considered private. Both the keys are considered as initially selected keys. The Elliptic Curve Diffie Hellman (ECDH) Key Exchange algorithm is applied to generate a secret and public key for the sender using optimal selected private keys. Each share is then encrypted through Lightweight Elliptic Curve Cryptography [21]. Only authorized parties possessing the private key can decrypt the encrypted medical share. Decryption involves applying the decryption algorithm provided by the LWECC scheme to the encrypted data using the private key [4]. After decryption, the original share is reconstructed by reversing the encryption process and merging the RGB bands to reconstruct the original image. Figure 6 depicts an encryption process for each share using the optimal key selected through the BROA approach.

3.3.1. Elliptic Curve Diffie Hellman Key Exchange

Elliptic Curve Diffie Hellman Key Exchange is applied to generate a secret and public key for the sender using optimal selected private keys. Let the sender indicate an IoT enabled medical device that initiates medical image transfer to the recipient. The recipient can be a local server or a cloud server. In the algorithm below, User A represents the sender, and User B represents the recipient.

3.3.2. ECDH Key Exchange Algorithm

Step 1: User A Key Generation

User A selects an optimal private key n_A , derived from logistic map, selected through BROA algorithm. It then calculates a public key P_A as:

$$P_A = n_A * G \tag{31}$$

Where G is the generator point on the curve.

Step 2: User B Key Generation

User B selects Private Key n_B , calculate Public Key P_B :

$$P_B = n_B * G \quad (32)$$

Step 3: Calculation of Secret key by User B

$$K = n_B * P_A \quad (33)$$

Step 4: Calculation of Secret key by User A

$$K = n_A * P_B \quad (34)$$

Step 5: Exchange of keys by both Users A and B: K

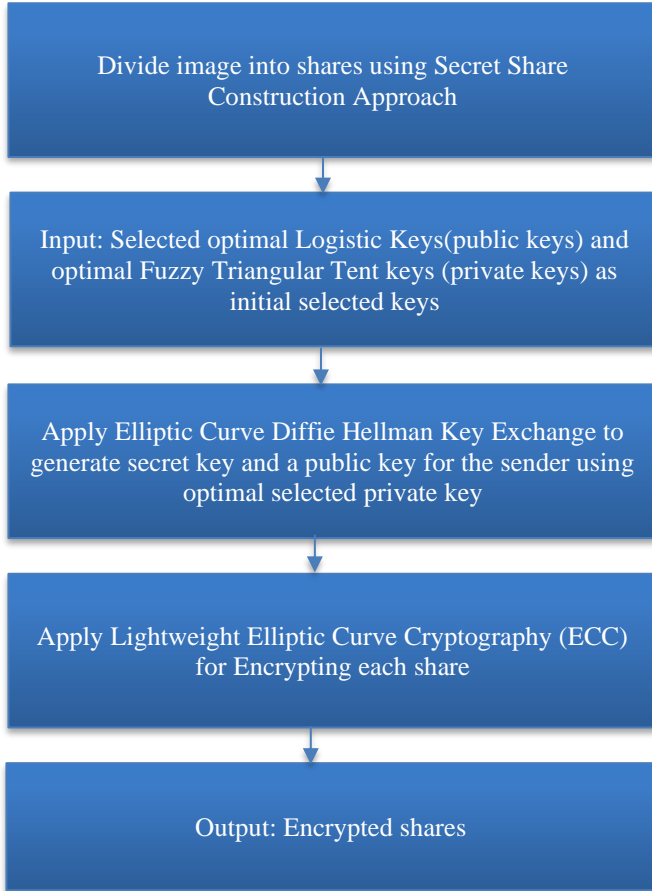


Fig. 4 Encryption process

3.3.3. LWECC Encryption

In this paper, the SECP256R1 Elliptic curve is applied. The curve is represented by an equation $y^2 = x^3 + ax + b$. The curve operates in the prime field of size p , where

$$P = 2^{256} - 2^{224} + 2^{192} + 2^{96} - 1 \quad (35)$$

This means arithmetic operations in the elliptic curve are performed using modulo P . The curve has a specific generator point, G . It is treated as a base point for cryptography operations. The generator point G has coordinates (x_G, y_G) such that $y_G^2 = x_G^3 + ax_G + b$, satisfying the curve equation. Initially, an image is converted into bytes and then encoded as a point on the curve.

Encryption by User A

User A is the sender, who encrypts each share using its own public key P_A generated from Equation (31). The chunk of each share is encrypted as shown in Equation (36):

$$\begin{aligned} Encrypted_chunk &= Encrypt(public_key\ of\ User\ A, chunk) \\ Encrypted_chunk &= Encrypt(P_A, chunk) \end{aligned} \quad (36)$$

The Cipher chunk of each share is generated as:

$$C_M = (KG, P_M + K P_B) = (C1 + C2) \quad (37)$$

Let $C1 = KG$

$C2 = P_M + K P_B$, where P_B is the public key of the receiver,

M is an encoded point on Elliptic curve

Therefore $C_M = (C1 + C2)$

Decryption by User B

Let K is the secret generated by User B, given as:

$$K = n_B * P_A \quad (38)$$

The decrypted chunk is shown using Equation (39):

$$Decrypted_chunk = Decrypt(Private\ key\ of\ user\ B, encrypted_chunk) \quad (39)$$

$$P_M = C2 - Private\ key * C1 \quad (40)$$

$$= P_M + K P_B - (n_B * KG) \quad (41)$$

Since $P_B = n_B * G$

$$= P_M + K P_B - (K P_B) = P_M \quad (42)$$

The Encryption process on shares using LWECC is represented in Figure 4 and is summarized by the below steps:

- Step 1: A medical image to be transmitted is divided into twelve shares using the Secret Share Construction Approach.
- Step 2: Apply the Elliptic Curve Diffie Hellman (ECDH) key exchange algorithm to generate secret and public keys for the sender using optimal selected private keys.
- Step 3: Each share is encrypted by using Lightweight Elliptic Curve Cryptography
- Step 4: Decryption and share reconstruction processes are executed on the receiver side to construct the original images.

4. Experimental Results and Discussion

The proposed work is demonstrated to assess its performance by evaluating different metrics in terms of quality analysis and security analysis. Also, the attained performances are compared with other existing methods to show the efficacy of the developed approach. This paper takes medical images from the MRI brain tumor dataset [25] and COVID-19 X-ray datasets [26].

The experiment is conducted on the Python platform. The evaluated results of quality and security metrics are shown in Table 1 in comparison with existing algorithms ROA[9], EOSA[7], SOA[10], GOA[8], and AOA[6]. Tables 2 and 3 depict the Quality and Security Analysis done for a set of Brain MRI images in Figure 5. Table 4 gives the correlation coefficients images of the original and encrypted share 1 images of Figure 5. The evaluated metrics are stated in the previous study of this work.

4.1. Quality Analysis

Quality analysis is evaluated using statistical, error metric, and data loss analysis.

4.1.1 Statistical Analysis

Statistical Analysis is measured by evaluating the correlation, histograms, entropy and Structural Similarity Index (SSI) of original and encrypted images. The weakness of an encryption process is uncovered by statistical analysis. The histograms of the original images and encrypted images of Figure 5 are shown in Figures 7 and 8.

4.1.2 Error Metric Analysis

Error metric analysis is measured using MSE and PSNR to assess the quality of an image.

4.1.3 Data Loss Analysis

Data loss analysis of an image involves evaluating how

well the image maintains its quality when subjected to data loss. Bit per Error Rate (BER) is also used to measure the data loss. It is evaluated at 0.000001, indicating that the proposed approach resists data loss attacks.

4.2. Security Analysis

Security Analysis deals with Differential Attack Analysis, Noise Analysis, Computational Analysis, and Key Analysis.

4.2.1. Differential Attack Analysis

NPCR (Number of Pixel Change Rate) and UACI (Unified Average Change Intensity) are called differential analyses. These are used to evaluate the encrypted images with keys to find the average pixel changes.

They evaluate the quality and security of an image encryption algorithm. Histograms of five images taken from the MRI brain tumour dataset of Figure 5 are shown in Figure 7. Since each share is encrypted independently, the histograms of encrypted images of share 1 are shown in Figure 8.

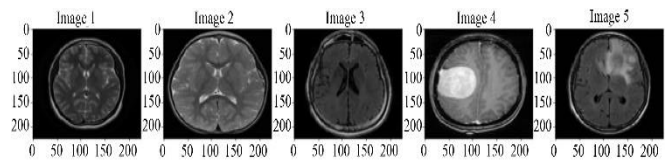


Fig. 5 MRI images of the brain

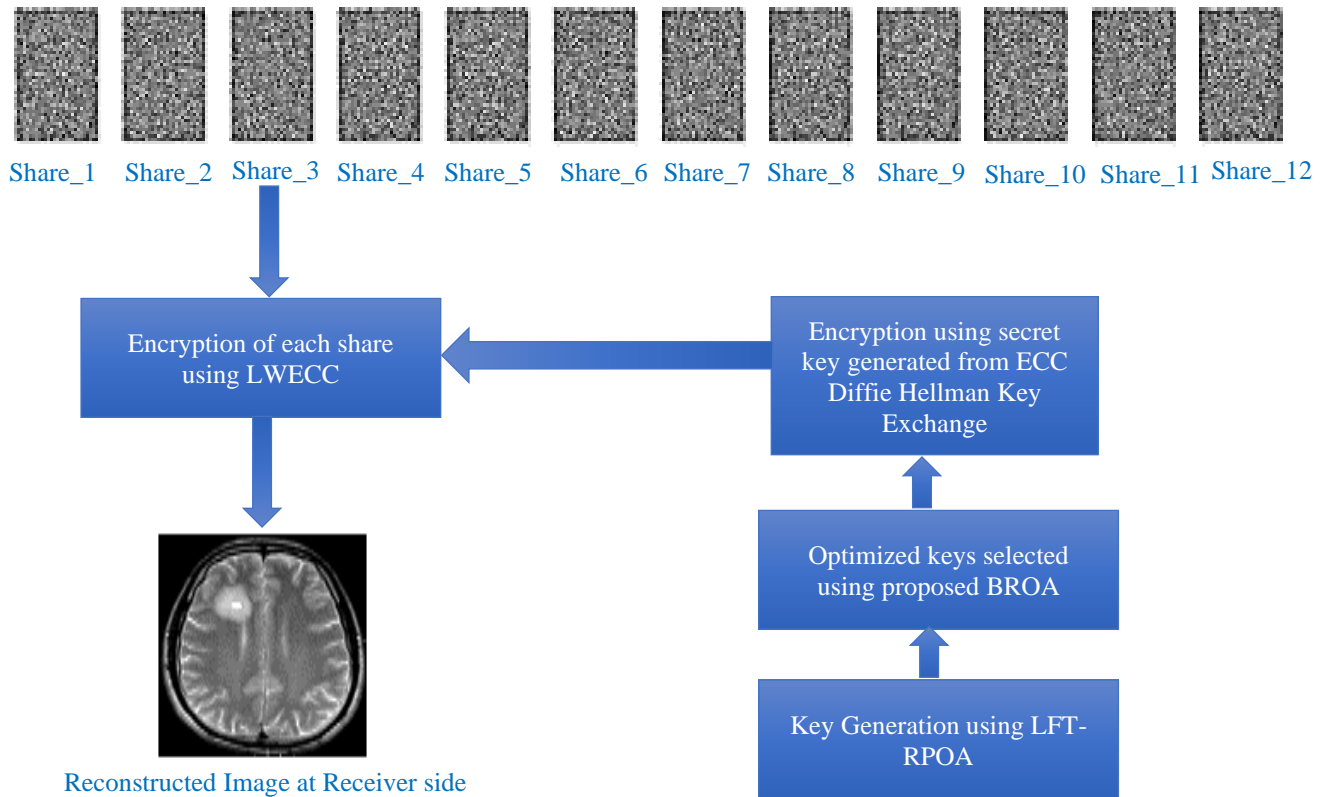


Fig. 6 Encryption of shares using LW ECC

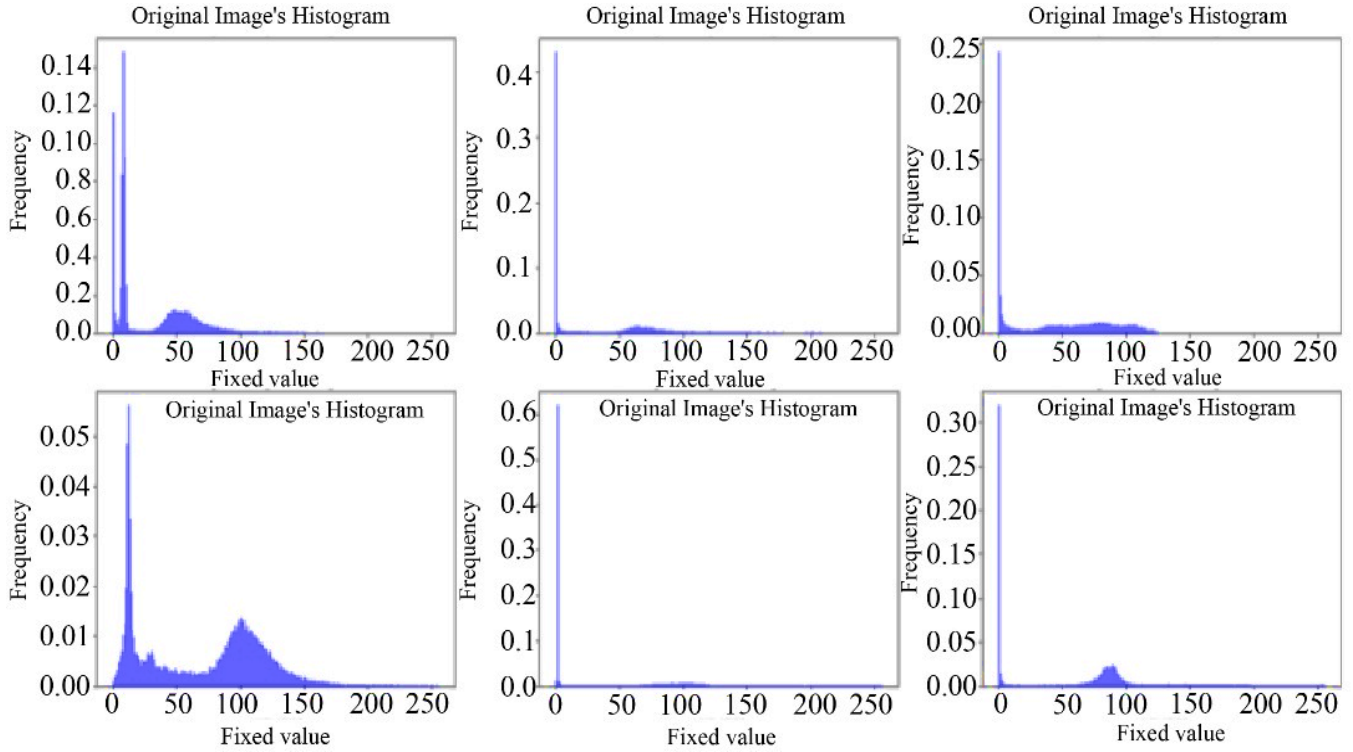


Fig. 7 Histograms of original images

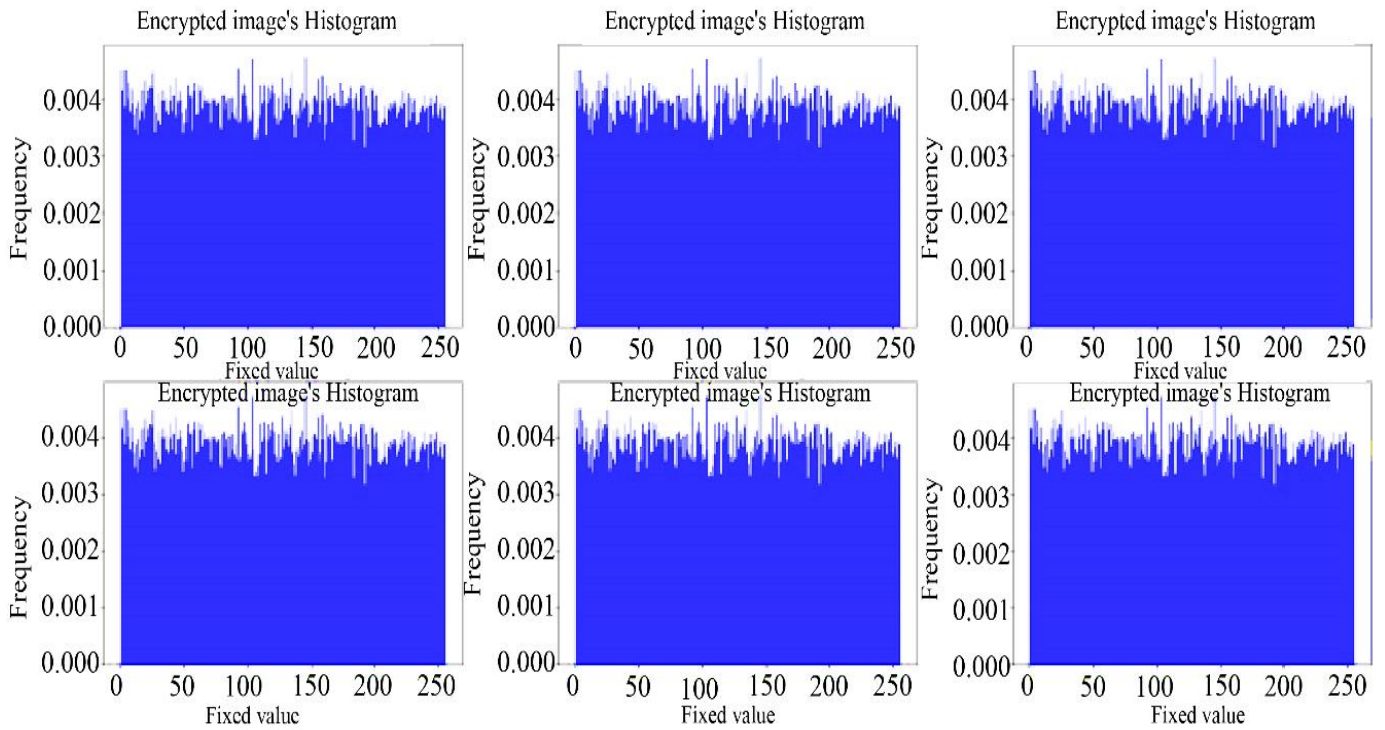


Fig. 8 Histograms of encrypted share 1

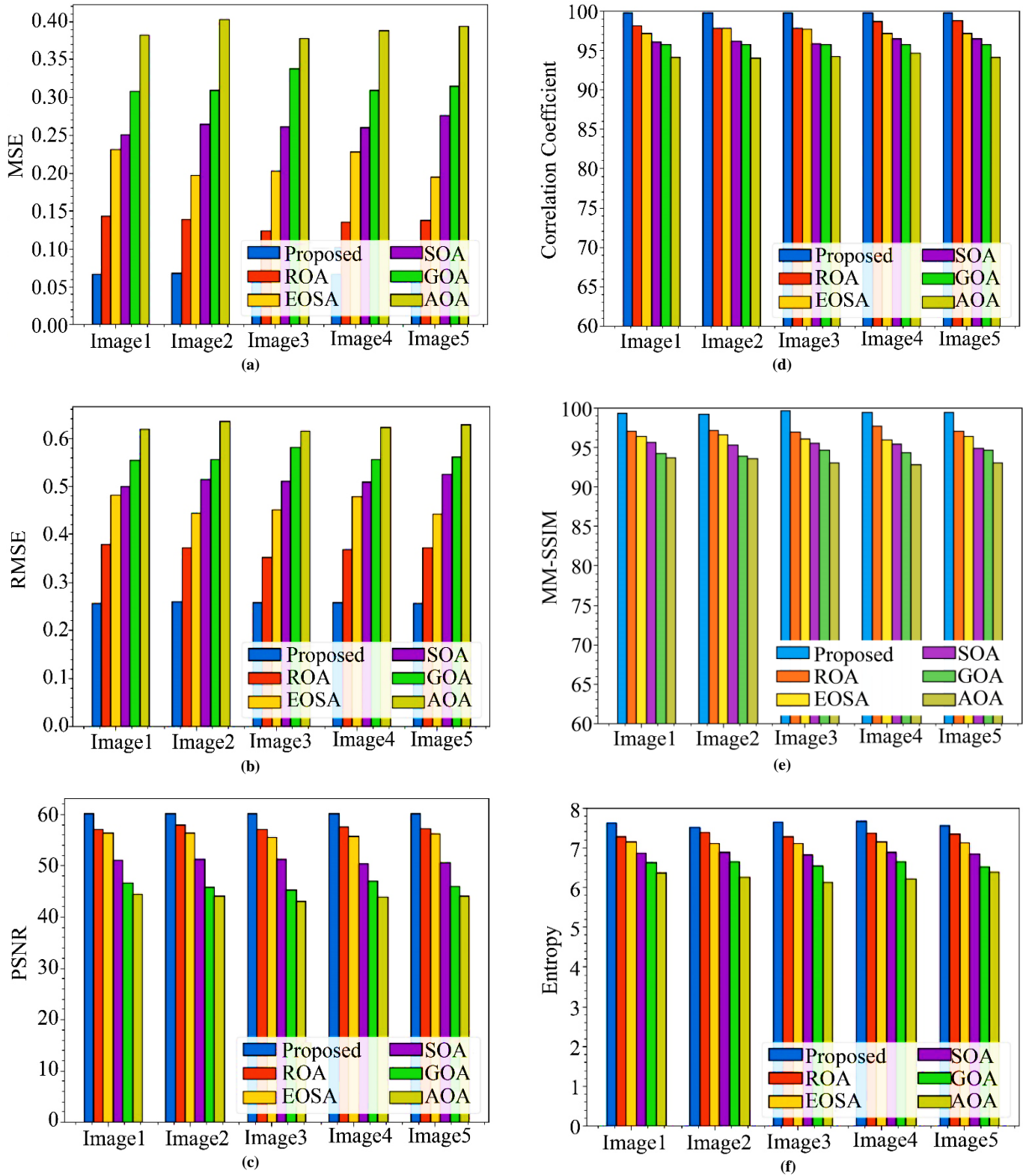


Fig. 9 (a-f) Comparison of metrics of the proposed approach with ROA[9], EOAS[7], SOA[10], GOA[8], AOA[6]

Table 1. Comparison of the proposed approach with existing algorithms

Algorithm/ Metrics	Proposed	ROA [9]	EOSA [7]	SOA [10]	GOA [8]	AOA [6]
MSE	0.07	0.126	0.193	0.252	0.3235	0.368
RMSE	0.26	0.355	0.440	0.502	0.568	0.607
PSNR (dB)	60.11	57.13	55.77	51.81	46.318	43.09
CC	0.98	0.978	0.976	0.976	0.957	0.941
MM-SSIM	0.993	0.974	0.961	0.948	0.942	0.934
Encryption time(secs)	10.749	18.14	19.60	0.247	21.604	22.11
Decryption time(secs)	4.634	8.428	9.126	10.24	11.358	12.64
Response time(secs)	36.17	34.32	35.51	36.65	37.646	38.16
UACI	33.28	32.66	31.345	31.66	30.122	30.18
NPCR	99.57	98.75	97.818	96.76	95.787	94.80
Entropy	7.9	7.33	7.121	6.805	6.503	6.288
SSI	0.997	0.984	0.975	0.963	0.954	0.942
Key Sensitivity	0.960	0.9	0.86	0.84	0.78	0.75

Table 2. Quality analysis

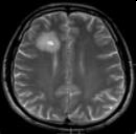

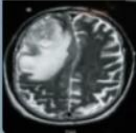

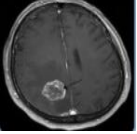
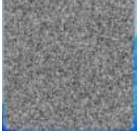

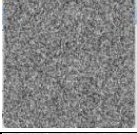


Original Image	Encrypted Share 1 Image	Quality Analysis				
		PSNR (dB)	MSE	SSI	Entropy	MS-SSIM
		60.11	0.07	0.99	7.77	0.99
		60.11	0.07	0.99	7.90	0.994
		60.42	0.07	1.00	7.89	1.0
		60.30	0.07	1.00	7.83	1.0
		60.48	0.06	1.00	7.65	1.0

Figure 9 (a-f) shows the comparison of metrics MSE, RMSE, PSNR, Correlation coefficients, MS-SSIM, and Entropy evaluated using the proposed scheme with existing algorithms ROA [9], EOSA [7], SOA [10], GOA [8], AOA [6]. Figure 10(a) refers to the original image taken from the MRI data set, and Figure 10(b) represents the encrypted image of share 1 of Figure 10(a).

4.2.2. Noise Analysis

Noise analysis of an image involves evaluating how well it maintains its integrity when subjected to salt and pepper

noise. Figure 10(c) depicts an attacked image, whereas the original image in Figure 10(a) is subjected to salt and pepper noise. The attacked image resulted in an NPCR value of 74.9097 and a UACI value of 2.172, which is considerably less when compared to the unattacked image. An unattacked image resulted in an NPCR value of 99.57 and a UACI value of 33.28.

4.2.3. Computational Analysis

Computation analysis is performed in terms of encryption time, decryption time, response time and delay time, as depicted in Table 3.

4.2.4. Key Analysis

The key analysis is measured in terms of key space and key sensitivity analysis. As the key size is 128 bits, the key space is evaluated as $\sim 2^{128}$, and the key sensitivity is 0.9600 bits/key. Key analysis is shown in Table 3.

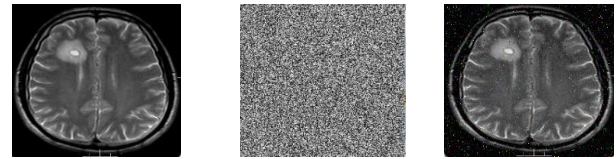


Fig. 10 (a) Original image

(b) Encrypted share1

(c) Attacked image

Table 3. Security analysis

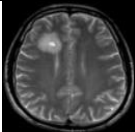
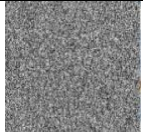
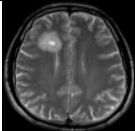
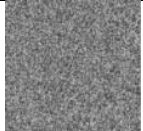
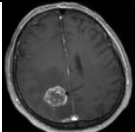


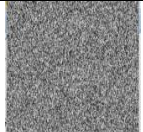

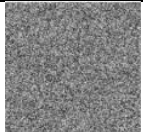
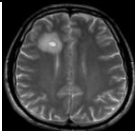
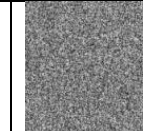
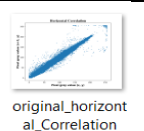
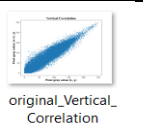
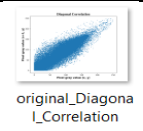
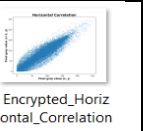
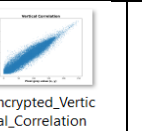
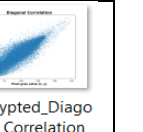
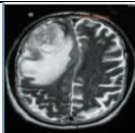
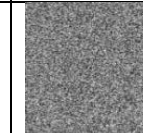
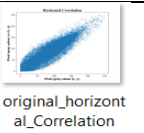
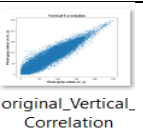
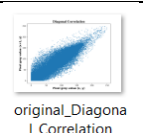
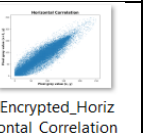
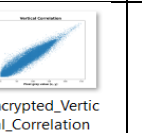
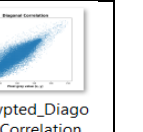
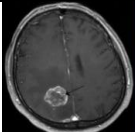
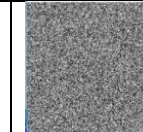
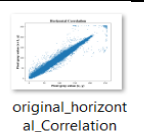
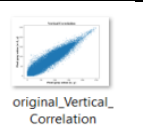
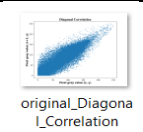
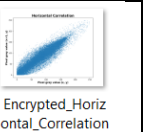
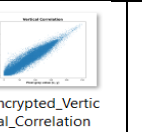
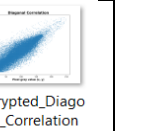
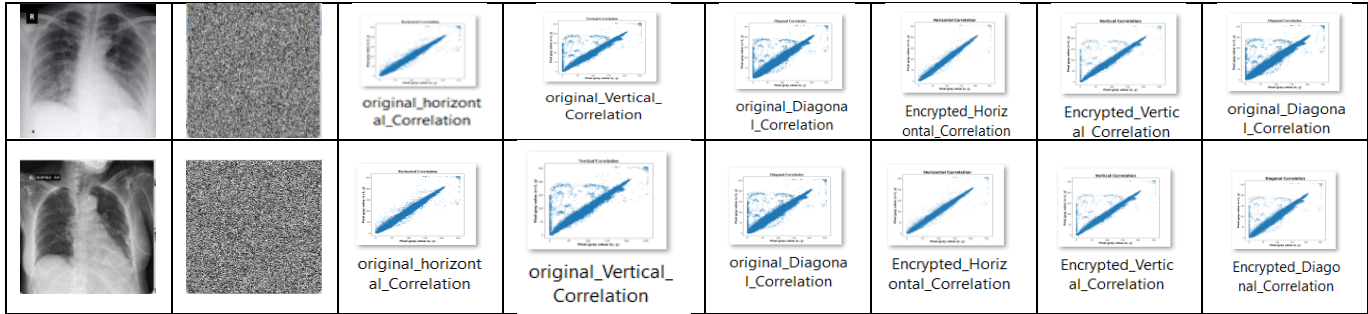
Original Image	Encrypted Share 1 Image	Security Analysis							
		Differential Attack Analysis		Computational Analysis				Key Analysis	
		NPCR	UACI	Encryption Time (secs)	Decryption Time (secs)	Response Time (secs)	Delay Time (secs)	Key Space	Key Sensitivity (bits/key)
		99.585	33.36	10.61	4.558	31.537	0.52	$\sim 2^{128}$	0.9600
		99.627	33.11	19.69	7.2467	47.648	0.61	$\sim 2^{128}$	0.9600
		99.531	33.669	32.10	13.993	67.760	0.23	$\sim 2^{128}$	0.9700
		99.607	33.592	31.77	14.0968	79.566	0.60	$\sim 2^{128}$	0.9700
		99.625	33.620	35.16	14.911	180.96	0.25	$\sim 2^{128}$	0.9700

Table 4. Correlation coefficient

Original Image	Encrypted Share 1 Image	Correlation Coefficient Original Image			Correlation Coefficient Encrypted Share 1 Image		
		Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
		 original_horizontal_Correlation	 original_Vertical_Correlation	 original_Diagonal_Correlation	 Encrypted_Horizontal_Correlation	 Encrypted_Vertical_Correlation	 Encrypted_Diagonal_Correlation
		 original_horizontal_Correlation	 original_Vertical_Correlation	 original_Diagonal_Correlation	 Encrypted_Horizontal_Correlation	 Encrypted_Vertical_Correlation	 Encrypted_Diagonal_Correlation
		 original_horizontal_Correlation	 original_Vertical_Correlation	 original_Diagonal_Correlation	 Encrypted_Horizontal_Correlation	 Encrypted_Vertical_Correlation	 Encrypted_Diagonal_Correlation



5. Comparison with Existing Work

The results shown in Section 4 outline the proposed approach's performance analysis. While in a few publications, for example, the authors in [22] have used a similar SSCA approach for creating shares, the work in [22] is based on an optimal key generation process. In contrast, the proposed work in this paper is based on the optimal key selection process from the keys generated from chaotic maps. The comparison with the work in [28] is unfair as there is an unaccountable difference between our proposed work in terms of the area of work and the identified problem. The authors in [28] have used a machine-learning approach for prediction, which is unrelated to the work done in this paper.

6. Conclusion

This paper proposes a novel key selection approach based on the bioinspired Boosted Remora Optimization algorithm.

References

- [1] Ali Adel Kalso, and Mohammad Ghebleh, "An Efficient Lossless Secret Sharing Scheme for Medical Images," *Journal of Visual Communication and Image Representation*, vol. 56, pp. 245-255, 2018. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [2] Hadi Givi, Mohammad Dehghani, and Štěpán Hubálovský, "Red Panda Optimization Algorithm: An Effective Bio-inspired Metaheuristic Algorithm for Solving Engineering Optimization Problems," *IEEE Access*, vol. 11, pp. 57203-57227, 2023. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [3] Mohammad Kamrul Hasan et al., "Lightweight Encryption Technique to Enhance Medical Image Security on Internet of Medical Things Applications," *IEEE Access*, vol. 9, pp. 47731-47742, 2021. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [4] Mustapha Benssalah, Yasser Rhaskali, and Mohamed Salah Azzaz, "Medical Images Encryption Based on Elliptic Curve Cryptography and Chaos Theory," *2018 International Conference on Smart Communications in Network Technologies (SaCoNeT)*, El Oued, Algeria, pp. 222-226, 2018. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [5] Fawad Masood et al., "A Lightweight Chaos-Based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations," *Wireless Personal Communications*, vol. 127, pp. 1405-1432, 2021. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [6] Laith Abualigah et al., "Aquila Optimizer: A Novel Meta-Heuristic Optimization Algorithm," *Computers & Industrial Engineering*, vol. 157, 2021. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [7] Olaide Nathaniel Oyelade et al., "Ebola Optimization Search Algorithm: A New Nature-Inspired Metaheuristic Optimization Algorithm," *IEEE Access*, vol. 10, pp. 16150-16177, 2022. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [8] Jeffrey O. Agushaka, Absalom E. Ezugwu, and Laith Abualigah, "Gazelle Optimization Algorithm: A Novel Nature-Inspired Metaheuristic Optimizer," *Neural Computing and Applications*, vol. 35, pp. 4099-4131, 2022. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [9] Heming Jia, Xiaoxu Peng, and Chunbo Lang, "Remora Optimization Algorithm," *Expert Systems with Applications*, vol. 185, 2021. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [10] Ibrahim Al-Shourbaji et al., "An Efficient Parallel Reptile Search Algorithm and Snake Optimizer Approach for Feature Selection," *Mathematics*, vol. 10, no. 13, pp. 1-20, 2022. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]

The selected keys are then used to derive keys for encryption and decryption. The performance of the proposed Boosted Remora Optimization algorithm is compared with the existing optimization algorithm.

The security and quality metrics parameters are evaluated and the results have shown that the critical space is evaluated to $\sim 2^{128}$ and BER as 0.000001. NPCR is evaluated approximately to 99.6 and UACI as 33, and entropy has reached 7.9. The outcomes depicted that the proposed approach is secure. As for future work, other lightweight encryption algorithms can be explored to enhance security.

Acknowledgment

We acknowledge the support of CVR College of Engineering for providing the infrastructure to carry out the research work.

- [11] V. Sangavi, and P. Thangavel, "An Exotic Multi-Dimensional Conceptualization for Medical Image Encryption Exerting Rossler System and Sine Map," *Journal of Information Security and Applications*, vol. 55, 2020. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [12] Jalaluddin Khan et., "Medical Image Encryption Into Smart Healthcare IOT System," *2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing*, Chengdu, China, pp. 378-382, 2019. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [13] K. Shankar, and P. Eswaran, "Sharing a Secret Image with Encapsulated Shares in Visual Cryptography," *Procedia Computer Science*, vol. 70, pp. 462-468, 2015. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [14] Srinivasan Nagaraj, G.S.V. Prasada Raju, and K. Koteswara Rao, "Image Encryption Using Elliptic Curve Cryptography and Matrix," *Procedia Computer Science*, vol. 48, pp. 276-281, 2015. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [15] Hui Lu et al., "A Chaotic Non-Dominated Sorting Genetic Algorithm for the Multi-Objective Automatic Test Task Scheduling Problem," *Applied Soft Computing*, vol. 13, no. 5, pp. 2790-2802, 2013. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [16] Ahmed A. Abd EL-Latif et al., "Controlled Alternate Quantum Walks Based Privacy Preserving Healthcare Images in Internet of Things," *Optics & Laser Technology*, vol. 124, 2020. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [17] Jalaluddin Khan et al., "SMSH: Secure Surveillance Mechanism on Smart Healthcare IoT System with Probabilistic Image Encryption," *IEEE Access*, vol. 8, pp.15747-15767, 2020. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [18] M. Geetha, and K. Akila, "Survey: Cryptography Optimization Algorithms," *International Journal of Emerging Technology and Innovative Engineering*, vol. 5, no. 1, pp. 1-6, 2019. [[Google Scholar](#)] [[Publisher Link](#)]
- [19] Mohamed Elhoseny et al., "Hybrid Optimization with Cryptography Encryption for Medical Image Security in Internet of Things," *Neural Computing and Applications*, vol. 32, pp. 10979-10993, 2020. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [20] Archana S. Nadhan, and I. Jeena Jacob, "Enhancing Healthcare Security in the Digital Era: Safeguarding Medical Images with Lightweight Cryptographic Techniques in IoT Healthcare Applications," *Biomedical Signal Processing and Control*, vol. 88, 2024. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [21] Sonali Rout, and Ramesh Kumar Mohapatra, "Secure Video Steganographic Model Using Framelet Transform and Elliptic Curve Cryptography," *Multimedia Tools and Applications*, vol. 83, pp. 25191–25212, 2024. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [22] B.T. Geetha et al., "Pigeon Inspired Optimization with Encryption Based Secure Medical Image Management System," *Computational Intelligence and Neuroscience*, vol. 2022, no. 1, pp. 1-13, 2022. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [23] Ravikumar Ch et al., "A Comparative Analysis for Deep Learning-Based Approaches for Image Forgery Detection," *International Journal of Systematic Innovation*, vol. 8, no. 1, pp. 1-10, 2024. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [24] G. Suryanarayana et al., *IOT for Healthcare*, Modern Approaches in IoT and Machine Learning for Cyber Security, Springer, Cham, pp. 201-218, 2023. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [25] Navoneel Chakrabarty, Brain MRI Images for Brain Tumor Detection, Kaggle, 2019. [Online] Available: <https://www.kaggle.com/datasets/navoneel/brain-mri-images-for-brain-tumor-detection?select=yes>
- [26] Joseph Paul Cohen, Covid-Chestxray-Dataset, Github, 2020. [Online]. Available: <https://github.com/ieee8023/covid-chestxray-dataset/tree/master/images>
- [27] Guangyue Kou et al., "Latin-Square-Based Key Negotiation Protocol for a Group of UAVs," *Electronics*, vol. 12, no. 14, pp. 1-19, 2023. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [28] Sachin Dattatraya Shingade, and Rohini Prashant Mudhalwadkar, "Hybrid Extreme Learning Machine Based Bidirectional Long Short-Term Memory for Crop Prediction," *Concurrency and Computation: Practice and Experience*, vol. 35, no. 2, 2023. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]
- [29] David W. Sims et al., "Lévy Flight and Brownian Search Patterns of a Free-Ranging Predator Reflect Different Prey Field Characteristics," *Journal of Animal Ecology*, vol. 81, no. 2, pp. 432-442, 2012. [[Crossref](#)] [[Google Scholar](#)] [[Publisher Link](#)]