IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Traitement du Signal
Vol. 41, No. 4, August, 2024, pp. 1807-1821
Journal homepage: http://iieta.org/journals/ts

Partial Encryption Scheme of Medical Images Based on DWT, Secret Image Sharing and Hyperchaotic System

Ali Hasan Alwan[1*], Ashwaq T. Hashim[2], Suhad A. Ali[3]

[1] Department of Computer Science, Faculty of Computer Science and Mathematics, University of Kufa, Kufa 54001, Iraq
[2] Department of Control and Systems Engineering, University of Technology-Iraq, Baghdad 10011, Iraq
[3] Department of Computer Science, Science College for Women, University of Babylon, Babylon 51001, Iraq

Corresponding Author Email: alih.alashour@student.uokufa.edu.iq

https://doi.org/10.18280/ts.410413

Received: 20 September 2023
Revised: 18 March 2024
Accepted: 12 June 2024
Available online: 31 August 2024

Keywords:
medical image, image encryption, IWT, partial encryption, secret image sharing, hyperchaotic system

ABSTRACT

There has been a significant increase in the demand for secure image storage in healthcare organizations in recent years. Encryption is used to address the challenge of encrypting sizeable digital image files, as full encryption can be computationally expensive and take a long time to process. In this paper, partial and selective encryption is proposed for medical images. First, deep learning based on U-Net is used to localize a tumor region called (ROI) a region of interest. A diffusion phase of the proposed system handles pixel values and positions based on linear and hyperchaotic systems. It includes converting an image's pixel values and repositioning pixels in a predetermined order. In the confusion phase, one level of Integer Discrete Wavelet Transform (IWT) is applied to divide the scrambled region into four sub-bands. Then, a Feistel network based on polynomial-based secret image sharing (SIS) encrypts the lowest frequency band only while the three bands LH, HL, and HH are diffused using a mapping technique based on the Morton scan to swap coefficients positions and then confused based on the hyperchaotic system. The culmination of these techniques results in generating a test image cipher characterized by robust confusion and diffusion properties. Importantly, this methodology has yielded remarkable results, reducing the encryption time by up to 96%. This efficiency is achieved without compromising the security or quality of the encrypted medical images. as high entropy is attained post-encryption. Furthermore, by employing the Integer Discrete Wavelet Transform (IWT), the integrity and fidelity of the encrypted images remain uncompromised. Additionally, to bolster the level of confusion in the encryption process, a substantial key space of 2^{1628} has been employed, further enhancing the resilience of the encryption method.

1. INTRODUCTION

The proper handling of medical images is of utmost importance due to the sensitive patient and diagnostic information they contain. These images are shared among hospitals, doctors, and patients over public networks, making it essential to have strong security measures for their storage and transmission to protect patients' privacy. However, traditional cryptographic techniques are insufficient for encrypting images due to the unique characteristics of digital image data, such as high redundancy, pixel correlation, and large size. This has increased demand for advanced and specialized image encryption algorithms, as conventional methods are no longer reliable. As a result, many low-complexity encryption techniques explicitly tailored for medical images have been developed to meet this challenge [1].

In contrast to conventional full-image encryption approaches, the proposed method focuses on encrypting only specific portions of the secret image. This selective encryption is grounded because only certain parts of the secret image are sensitive or require confidentiality. Determining the target portion can be manual or automatic [2]. Recent years have witnessed significant interest in chaotic systems, maps, attractors, and sequences within the research community [3, 4]. Applications of chaotic encryption techniques have been widely used for security purposes in various domains, including smart grids and communication systems [5, 6].

Additionally, these techniques are extensively utilized to safeguard different types of content, such as images [7, 8]. Chaotic image encryption algorithms offer the advantage of being easily implementable in software and hardware, contributing to their popularity among scholars. These algorithms typically rely on scrambling and diffusion techniques to obscure the statistical properties of plain images, thereby enhancing the statistical quality of the resulting ciphertext [9]. Transform domain encryption, such as the use of (DCT) discrete cosine transform [10], (FRFT) fractional Fourier transform [11], or (DWT) discrete wavelet transform [12], offers increased security compared to spatial encryption. However, the complexity of such algorithms presents a challenge for potential attackers aiming to decode the data illegally. The presented paper introduces a novel symmetric encryption algorithm that leverages the benefits of transform

domain encryption. The proposed work has made significant contributions, which are outlined below:

·A practical image encryption model designed for medical images.

·An efficient diffusion model is adopted based on a linear system and chaotic map.

·Implementation of polynomial-based secret image sharing for encryption of the lowest frequency band.

·Utilization of partial Encryption to address the computational overhead and processing time challenges posed by sizeable digital image sizes.

·Repositioning of pixels within the Region of Interest (ROI) through linear and hyperchaotic systems.

·Creation of a partial encryption system that amalgamates the strengths of the hyperchaotic map, secret image sharing, integer discrete wavelet transforms, and hash function. This system is highly dependent on the initial values and can be easily implemented.

The proposed encryption can cipher all medical images, such as X-rays, CT scans, and MRIs. It can safeguard patients' private and sensitive information within medical images from unauthorized access and maintain confidentiality. A partial or selective encryption scheme is utilized to enhance the speed of encryption medical image algorithms.

An increasing number of medical equipment, such as insulin pumps and pacemakers, is connected to the Internet and other networks. Encrypting the data transmitted between these devices and other systems is essential to protect patient information from unauthorized access. This security measure can help safeguard sensitive medical information and prevent data breaches.

The paper's structure can be outlined as follows: Section 2 will discuss related works, while Section 3 will explain Preliminaries. Section 4 will elaborate on the proposed method, and Section 5 will present the experimental results and analysis. Lastly, Section 6 will outline the conclusions.

2. RELATED WORK

Various industries, including healthcare, have significantly transformed the modern digitalization landscape. As a vital aspect of this evolution, telemedicine has revolutionized the exchange of medical information, mainly by sharing medical images. However, the convenience of such information exchange comes with the challenge of ensuring robust confidentiality and security. This is especially critical in the healthcare sector, where electronic health records contain sensitive personal information. Unauthorized access to medical images can lead to fraudulent activities, identity theft, and other privacy breaches. Consequently, there is a pressing need for advanced encryption methods to safeguard these valuable assets.

Overcoming Security Challenges In response to these security concerns, researchers have delved into medical image encryption, seeking innovative solutions to ensure the integrity and confidentiality of patient data. Several works in this domain have explored diverse techniques, each aiming to address specific security and efficiency challenges.

The proliferation of medical information exchange, particularly through medical images, necessitates robust confidentiality measures in telemedicine [13]. This study, conducted in 2021, introduces a novel cryptosystem tailored for telemedicine applications. It employs a hybrid approach to encrypt diverse medical images, enhancing security and key space. By individually scrambling two plain images using chaotic maps, they are then fused using Cramer's rule-based mathematical expression, bolstering the cryptosystem's resilience. Image encryption involves permutation and diffusion via Logistic-May and Henon maps and Logistic-Sine scrambling. Security analysis and experimental simulations confirm the algorithm's efficacy in maintaining robust encryption.

In 2021, a recent study [14] introduced a new medical image encryption algorithm that uses DNA cryptography and is highly robust. The approach involves image masking before encryption, enhancing the original image's randomness without requiring a key. The process includes confusion and diffusion on the masked image, rendering the resulting cipher-image devoid of perceptual or statistical information. The proposed algorithm employs the confusion step in the generalized Arnold's Cat Map and introduces a unique diffusion operating on pixel and DNA-plane levels. The DNA encoding, decoding, and XOR rules are selected based on the values generated by the Chaotic 2D-Logistic Sine Coupling Map. This approach enhances resistance against brute force and statistical attacks. The cipher image remains impervious to intrusion without the correct key while maintaining efficient decryption with the valid key. Extensive testing showcases its effectiveness on medical and natural images, exhibiting low inter-pixel correlation and high entropy. The algorithm also demonstrates robustness against various attacks, ensuring a secure image cryptosystem.

A lightweight cryptosystem has been introduced in the study [15], which integrates the Henon chaotic map, Chen's chaotic system and Brownian motion to provide robust encryption for medical images. The proposed approach has been thoroughly analyzed, covering a range of factors, including histogram analysis, pixel correlation, contrast, mean square error, energy, homogeneity, NIST compliance, entropy, pixel change rate, average intensity change, signal-to-noise ratio, and time complexity. Based on experimental results, this method is highly effective in securing confidential patient image data, making it a reliable solution for medical image encryption.

In 2020, this work [16] addressed the secure transmission of medical images, preserving sensitive regions through an innovative algorithm. Key areas are identified, and data hiding with texture analysis is employed, safeguarded by an Arnold transformation. A QR code replaces the original key regions, ensuring authorized access. The method ensures secure storage and recovery of patient data while controlling image quality. Experimental validation confirms its effectiveness.

In 2020, Yan et al. [17] introduced an Adaptive Partial Image Secret Sharing (APISS) scheme using salience detection, image inpainting, and linear congruence. Unlike classic Image Secret Sharing (ISS), APISS encrypts only the sensitive part of a secret image. The scheme automatically detects the salient part and encrypts it into meaningful shares using linear congruence and image inpainting. Decryption involves progressively adding shares until full lossless decryption is achieved. The method offers efficiency benefits and is validated through experiments.

In 2020, George et al. [18] proposed a selective image encryption approach to enhance efficiency. Unlike traditional methods, which encrypt the entire image, this technique encrypts specific portions to reduce computational complexity and encryption/decryption time. It employs a Discrete Cosine

Transform (DCT)--b-based compression algorithm in YCbCr and RGB colour spaces. Results indicate improved image quality and compression ratios using YCbCr over RGB. 1-D DCT reduces transform time significantly compared to 2-D DCT. Adaptive scalar quantization preserves visual quality. DC coefficients are differentially encoded, and AC coefficients are compressed using Run Length Encoding (RLE). Encryption is applied selectively to these bulks, substantially reducing decryption time. The proposed approach efficiently balances compression and encryption, enhancing overall performance.

In 2022, Noori Ghanim and Raheem Khoja [19] applied a one-level Discrete Wavelet Transform to coloured images, dividing them into four subbands. A Gabor filter and K-means clustering enables texture segmentation on the lowest frequency band, serving as a novel scrambling method. Scrambled segments are then encrypted using alternating AES and RC4 Algorithms, involving XOR operations with the key of the other algorithm. Rigorous security and performance analyses reveal the method's resistance to various attacks and its potential for real-time image transmission and encryption.

In 2022, Yousif et al. [20] introduced enhanced criteria for medical image encryption. It eliminates pixel correlation by scrambling and diffusing via polynomial-based secret sharing. Integer wavelet transform encrypts image frequencies with AES, ensuring robust security. The LL part becomes the diffusion image, secured using inverse Haar wavelet transform. Reversing and shuffling frequencies restore the original image. The extensive statistical evaluation confirms the algorithm's resistance against attacks, surpassing other image cryptography methods in security.

In 2022, Salman et al. [21] introduced a secure and efficient algorithm that encrypts predetermined regions to minimize encryption, decryption complexity, and time. Image processing divides images into (ROI) and (RONI); polynomial-based secret image sharing and chaotic mapping techniques are used to encrypt the Region of Interest (ROI) component. This approach ensures effective diffusion and confusion, enhancing concealment. A firm reliance on key improvement is seen in secure decryption. The encryption solution's breadth thwarts brute-force attacks, addressing protection issues during network transmission of medical images.

In 2022, Kiran and Parameshachari [22] presented a low-complexity Block Cipher-based Region of Interest (ROI) medical image encryption with multiple maps. ROI extraction using Laplacian edge detection identifies essential regions. Arnold's cat map circularly permutes ROI, and then the duffling system encrypts it while preserving unimportant parts. The proposed algorithm exhibits robust security against attacks, outperforming recent chaotic encryption methods. Experiments validate its efficacy in safeguarding medical image confidentiality.

In 2023, Natsheh et al. [23] addressed the need for efficient yet robust DICOM image security. A novel selective encryption approach is introduced, automatically identifying regions using pixel thresholding segmentation and then encrypting them based on importance. Single and multi-frame DICOM images benefit from adaptive two-region Encryption, with the Region of Background (ROB) using light encryption and the Region of Interest (ROI) using advanced encryption. Approach I for multi-frame DICOM images achieves substantial time savings and compression, while Approach II for single-frame images enhances efficiency through multi-region selective encryption. Comprehensive cryptanalysis metrics confirm the methods' robustness against diverse attacks. The approach I use shows superior performance based on estimated processing time.

In 2023, Al-Barzinji and Abd Abrahim Mosslah [24] introduced a novel partial image encryption approach focusing on DCT coefficient frequencies. Encrypting all data in specific applications can be impractical due to decryption processing demands. Partial encoding offers a solution, meeting application needs without overwhelming processing. The proposed method preserves public bit value and aligns with the JPEG format. It achieves enforceability, spatial selectivity, self-sufficiency, and coordination compliance, addressing real-time application requirements. The approach's effectiveness is compared to other technologies like quadtree AES.

In 2021, Harshitha et al. [25] proposed a method for encrypting images to protect medical image data. This is achieved using a chaotic logistic map and a linear feedback shift register (LFSR) to generate pseudo-random sequences. The generated sequences are combined using an XOR operation to create an encryption key. This key, along with security transformations, encrypts medical images, benefiting from the chaotic maps' random behaviour and sensitivity to initial conditions for added security. The proposed approach effectively secures diverse medical image formats and resists brute force and man-in-the-middle attacks.

In 2021, El-Shafai et al. [26] addressed the need for medical image encryption in telemedicine and healthcare by presenting an efficient cryptosystem that leverages DNA rules and chaos maps. The proposed approach utilizes a logistic chaos map, a piecewise linear chaotic map (PWLCM), and DNA encoding. The process involves generating a secret key image using PWLCM, encoding images using DNA rules and chaos maps, and iterating through columns for optimal ciphering. Experimental results demonstrate the cryptosystem's robust security, acceptable processing time, and resilience against various attack types.

These endeavours collectively demonstrate the ongoing commitment of researchers to enhancing the security landscape of medical image encryption, catering to the unique demands of telemedicine and healthcare systems.

In conclusion, the increasing reliance on digital technologies in healthcare and telemedicine mandates robust security measures to safeguard sensitive medical images and patient data. The diverse approaches presented in the related works exemplify the innovative strategies employed to address these challenges. From hybrid encryption schemes to DNA-based cryptography and selective encryption methods, each approach contributes to the evolving landscape of medical image security. As telemedicine continues to grow, these advancements promise to ensure patient privacy, data integrity, and secure image communication within the healthcare ecosystem.

As shown in Table 1, the previous work had some gaps in time consumption, lack of efficient similarity measurement, absence of partial methods, and the need for more efficient encryption techniques to provide better entropy levels. In this proposed work, a new and novel approach to providing security for medical images is presented by exploiting and employing the idea of secret image sharing based on polynomials, hyperchaotic maps, and DWT transform for selective and partial image encryption. The proposed algorithm aims to reduce space and bandwidth usage by

localizing the vital area (ROI) and focusing on the essential ROI information concentrated in the low parts of frequent DWT. This valuable information is used as coefficients of the secret image-sharing polynomials. The frequency domain is advantageous for encryption as it simplifies finding the crucial areas that need to be encrypted. Connecting between spatial domain pixel values and frequency domain values is challenging, which makes the image safe from numerous assaults, including known plaintext attacks and Ciphertext-only attacks. The DWT reconstruction processes make it impossible to discern between sections that are encrypted and those that are not. To overcome the security issue for high frequencies of DWT (I.H, HL, and HH), the diffusion step is used to hide the correct locations of the transformed image coefficients of these bands.

In the proposed method, the SHA-512 hash values were employed as the system's initial parameters generator for plaintext sensitivity, and a hyperchaotic was used as a subkeys generator for the polynomials as coefficients. High-dimensional hyperchaotic systems are better suited for image encryption due to their intricate structure and reliability in generating suitable. In addition, the algorithm uses the Morton scan traversal technique to strengthen the system.

The suggested encryption was more secure as a result of all these actions than many others that have been documented in the literature. Furthermore, as far as we know, none of the image ciphers found in literature have been created utilizing these acts. Many excellent features of the suggested scheme are evident, such as its high randomness, low processing cost, huge key space, flexible parameter space, significant sensitivity to plaintext and keys, and quick execution speed. Consequently, the suggested plan protects private digital photos against cryptographic assaults.

Table 1. Summary table of related works

Ref.	Methods	Limitations	Achievements	All/Partial Encryption
[15]	Using Henon Chaotic Map (HCM) Brownian Motion (BM) Chen Chaotic system (CCS)	time-consuming using two different chaotic maps do not use key	the good Correlation coefficient of the encrypted image is closer to the ideal entropy cipher image	All
[19]	Discrete Wavelet Transform K-means AES and RC4	The entropy of the encrypted image is not closer to the ideal time-consuming	against ciphertext-only attacks. Using real-time application	All
[20]	Discrete Wavelet Transform AES	using for 2D images	against ciphertext-only attacks. known plaintext attacks lower security and the file size	All
[21]	Quadratic chaotic map Polynomial-based SIS	time-consuming for larger images using for 2D images	reduce the encryption/decryption time, and enhance image processing methods.	Partial
[23]	Selection mechanisms compression AES	time-consuming not using similarity measurement do not use segmentation methods	combination of lossless compression and segmentation	All
[24]	Lightweight DCT multiple encryptions Pluralism	need more than 2 points' to encrypt the image	trade-off time and power usage reduce the encrypted and decrypted time	All
[27]	Selective Encryption Sharing & Embedding	time-consuming	Distinguish sensitive and non-sensitive information of plain images before making encryption	All / Partial

3. METHODOLOGY

3.1 Secret image sharing

Thien and Lin's contribution in 2002 [28] brought forth a novel concept by integrating the secret-sharing scheme proposed by Shamir [29]. In their approach, they harnessed the potential of the secret image to generate a set of n shared images, where restoring the original secret image necessitates k or more shared images. Impressively, k-1 shares remain insufficient to unveil any details regarding the secret image. A key innovation of their method lies in utilizing subsequent pixel values as the coefficients in the polynomial equation, deviating from conventional random numbers. This innovative approach led to a reduction in the size of shared images by a factor of 1/k. e importance of robust security considerations in the design of image-sharing methods.

Thien and Lin's image secret-sharing scheme involves sharing a secret image (S) among participants. The group comprises n participants, each assigned a unique identifier (id_1, id_2, … , in) in a finite field. The allocator selects n distinct non-zero elements as identifiers and makes them public. The secret image has w pixels, and the allocator takes the grayscale value of the first k pixels in S as the value of a_0, a_1, … , a_{k-1}. These values are used to form a polynomial. The threshold for the scheme is ∅, and the correspondence between each participant

and their identifier is also public and can be expressed using the following equation:

$$f(x) = \left(a_0 + a_1 x + a_2 x^2 + \cdots + a_{(\emptyset-1)} x^{(\emptyset-1)}\right) mod p \quad (1)$$

The allocator generates n secrets to distribute among n participants, with each secret corresponding to the identifier of the first pixel (S^i_1) in each shadow image.

$$S^i = \mathrm{f}(\mathrm{id}_1), i = 1, \ldots, n \quad (2)$$

The allocator performs the previously described operation on the kth+1 to 2kth pixel in S using the values of a_0, a_1, …, a_{k-1} to generate S^i_2, i=1, … , n. The secret sharing process is repeated for all pixels in S, resulting in $S^i_{w/k}$, i=1, … , n.

Thien and Lin's scheme for recovering secret images involves using k shadow images (S_1, S_2, …, S_n) and their corresponding IDs (id_1, id_2, …, id_n) to recover the secret image. This is done by extracting the 1st pixel of each shadow image (S_1, S_2, …, S_n) and applying the formula of Lagrange's interpolation.

$$f(x) = \sum_{i=1}^{\emptyset} f(x_i) \prod_{h \neq i}^{1<h<\emptyset} \frac{(x - x_h)}{(x_i - x_h)} \quad (3)$$

have

$$f(x) = \sum_{i=1}^{\emptyset} S^i 1 \prod_{h \neq i}^{1<h<\emptyset} \frac{(x - id_h)}{(id_i - id_h)} \quad (4)$$

To obtain the grayscale value first to the K^{th} pixel of a secret image as a secret message (a_0, a_1, …, a_{k-1}), one can use $f(x)$ coefficients. For Lagrange's interpolation, the 2nd pixel of each shadow image (S^1_2, S^2_2, …, S^k_2) can be obtained.

$$f(x) = \sum_{i=1}^{\emptyset} S^i 2 \prod_{h \neq i}^{1<h<\emptyset} \frac{(x - id_h)}{(id_i - id_h)} \quad (5)$$

The secret image, S, can use the coefficients of the polynomial function $f(x)$. need to extract a_0, a_1, … , a_{k-1} as the kth+1st to 2kth pixels from $f(x)$. This process is repeated until we have recovered all the pixels in S, resulting in the complete secret image. The reference [30] explains this process in detail.

For a better understanding, refer to Figure 1, which illustrates the image secret-sharing construction process for (2, 4) with k=2 and n=4. This method enables the creation of a first-order polynomial function.

$$Sx(i,j) = (110 + 112x)\ (mod\ 251, 3) \quad (6)$$

The first two-pixel values in the Lena image are 110 and 112 [31].

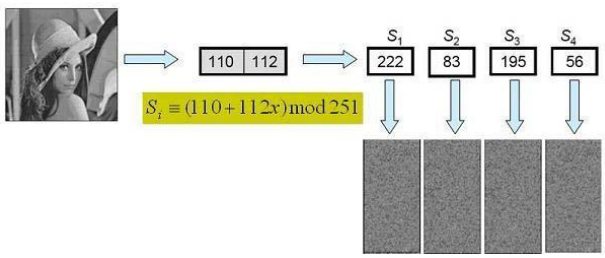

Figure 1. Thien and Lin's secret sharing scheme [31]

In the proposed system, use (n, n) secret image sharing with n=8 to generate eight shares as cipher output for the block of eight bytes.

3.2 The hyperchaotic system

The Hyperchaotic System employed in this study is derived from the dynamic system proposed by Natiq et al. [32], which is an enhancement of the system introduced by Liu et al. [33]. The key modification in this hyperchaotic system involves substituting the original cubic nonlinearity nonlinearity with a hyperbolic sine nonlinearity nonlinearity. This change is motivated by the desire to streamline the practical design of electronic circuits, as the hyperbolic sine nonlinearity can be easily implemented using two diodes connected antiparallel. In contrast, cubic nonlinearity nonlinearity requires analogue multipliers, which can introduce complexities and challenges in circuit realization.

The mathematical representation of this hyperchaotic system is as follows:

$$\left\{\begin{array}{c} x_1 = -\beta_1 \left(x_2 + 0.2(x_1 - \varepsilon \sinh(x_1))\right) \\ x_2 = \beta_2 * x_1 - x_2 + x_3 + x_4 \\ x_3 = \beta_3 * x_2 - x_4 \\ x_4 = -\beta_4 * x_1 \end{array}\right\} \quad (7)$$

In the equations above, x_1, x_2, x_3, and x_4 represent the system's state variables, while β_1, β_2, β_3, and β_4 are positive parameters. Notably, the complex behaviour exhibited by this hyperchaotic system is primarily associated with the state variable $x1$, which is linked to the hyperbolic sine nonlinearity.

This modified hyperchaotic system offers a more feasible approach to implementing chaotic behaviour in practical electronic circuits by introducing the hyperbolic sine nonlinearity and its relatively simple realization through diodes. This trade-off between theoretical complexity and practicality is a common consideration in chaos-based research, ensuring that chaotic systems can be effectively harnessed for real-world applications such as secure communication and encryption.

3.3 Morton scan

Morton scan, also known as the Z-order curve, is a method used to traverse and index multi-dimensional data in a linear, one-dimensional sequence. It is beneficial for dividing a 2D space into smaller sub-blocks and then scanning through those sub-blocks in a manner that preserves spatial locality. This is achieved by interleaving the bits of the 2D coordinates of each point to create a single index that reflects the spatial relationship. Coordinates to Index Conversion: Consider a 2D grid where each cell has an X and Y coordinate. To convert these coordinates into a Morton index, you interleave the bits of the X and Y coordinates. This means you take the least significant bit of the X coordinate, then the least significant bit of the Y coordinate, then the second least significant bit of X, the second least significant bit of Y, and so on, until you have used all the bits of both coordinates. This interleaved bit sequence forms the Morton index. Spatial Locality: The essential advantage of the Morton scan is that nearby points in 2D space are likely to have similar Morton indices, which preserves their spatial proximity even in the one-dimensional index space. Sub-Block Division: When applying the Morton

scan to sub-blocks, you divide the 2D space into smaller rectangular regions (sub-blocks). Then, you convert each sub-blocks top-left corner coordinates into a Morton index. By scanning through these Morton indices, you traverse through the sub-blocks in a way that maintains their spatial relationship. In your context of applying the Morton scan for each sub-block, you are to use this technique for indexing or accessing data stored in a grid or a 2D structure. Using the Morton scan, you can improve cache utilization and data locality when accessing neighbouring sub-blocks, which can be especially useful in image processing, spatial databases, and similar applications, as illustrated in Figure 2.

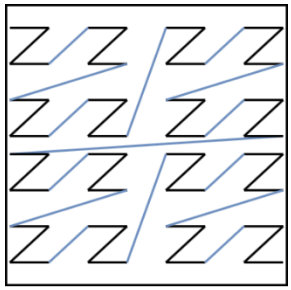

Figure 2. Z-order curve "Morton Scan"

3.4 Feistel network

The Feistel cipher takes Horst Feistel's name and utilizes a symmetric key architecture. It reverses the critical application using nearly the same encryption and decryption procedure. Figure 3 shows a Feistel round function. Figure 3 splits an n-bit block into two parts, *L* (left) and *R* (right). The right half is next subjected to a function F(*R*, *K*), and the outcome is XORed with the left half (this is the first involution):

$$\begin{aligned} L_{i+1} &= R_i \\ R_{i+1} &= L_i \oplus \mathrm{F}(K_i, R_i) \end{aligned} \tag{8}$$

The round subkey, or *K*, generated by the key scheduling algorithm may change from one round to the next. After that, the procedure is repeated with the halves switched (the second involution). The function (F) applied need not be reversible [34].

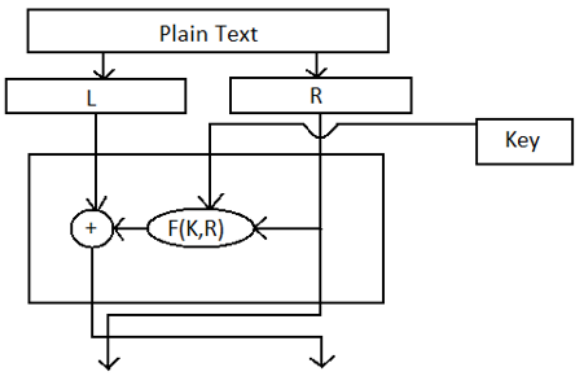

Figure 3. Feistel cipher structure

The Feistel network is used in the proposed system to cypher 16 bytes, i.e., (4×4) bytes as input, which is split into two parts of 8 bytes, *L* and *R*. The F function is performed (8,8) secret image sharing based on polynomials. The Key K_i is supplied from key generation steps based on hyperchaotic maps.

3.5 Linear system

The system proposed in reference [35] uses a set of linear equations to generate shares. Each share comprises a secret set of k integer numbers, denoted as a_{ij}, where *i* ranges from 1 to n and j ranges from 1 to k. Here, n represents the total number of shares, and k denotes the minimum number that can be used to recover the image data. To put it simply, given a block of image data {Vj| j=1… k}, the i^{th} share is calculated using the following linear equations:

$$S_i = \sum_{j=1}^{k} a_{ij} V_J \; mod \; 256 \tag{9}$$

This passage refers to retrieving data from a block using shares generated from the block. In this process, S_i represents the i^{th} generated share for the block V(). The coefficient represents the i^{th} coefficient belonging to the linear equation representing the share. By collecting k shares from n the total shares (i.e., $\{S_i|\ i=1...k\}$), the inverse matrix of A=$\{a_{ij}|\ i, j=1...k\}$ the method mentioned above can be employed to retrieve the values of V precisely ().ensuring accurate reconstruction of the original data.

$$V = \mathrm{A}^{-1} S \tag{10}$$

The range of shared values, S_i, is confined within [0..255]. Consequently, the equation mentioned above can be expressed as follows:

$$\sum_{i=1}^{k} a_{ij} V_j = S_i + 256 p_i \tag{11}$$

During retrieval, share values are adjusted based on specific integer division rules. Here, p_i represents an integer value that does not contribute to the shared values.

Algorithm (1): (*k*, *n*)-Threshold Reveal Phase

Input:
k: denoted the number of allied shares.
k shares: An array consisting of k bytes.

Output:
V: An array containing secret bytes retrieved.

Step 1: Select the shares that correspond to indexes {n1, n2, ..., nk}, ensuring only one secret byte value is get from each chosen share (i.e., {Sm| m=1, 2, …}).

Step 2: Create the coefficients matrix, A'(), for the linear equations, where

$$a'_{ml} = a_{n_{ml}}$$

where, $a'_{ml} \in \mathrm{A}'$ and $a_{n_{ml}} \in \mathrm{A}$ *m*=1, 2, ..., *k* and *l*=1, 2, ..., *k*.

Step 3: To compute the determinant value of matrix A, we can use the formula D = det(A). Once we have obtained the determinant value, we can derive the complementary matrix C. The condition must be met for all values of j that fall within the range of 1 to *k*.

$$\sum_{i=1}^{k} a_{ij} C_{ij} = \sum_{j=1}^{k} a_{ij} C_{ij} = D \tag{12}$$

where, C_{ij} equals the determinant of the reduced matrix C (with the ith row and column removed), multiplied by $(-1)^{i+j}$.

Step 4: Determine the values of the retrieved secret bytes $\{V'_j | j=1, ..., k\}$ using:

$$V'_j = \frac{1}{D}\{(\sum_{i=1}^{k} C_{ij} S_{ni}) + w_j\} \quad (13)$$

w_j is an integer value is multiples of 256 as:

$$w_j = 256 \sum_{i=1}^{k} C_{ij} p_i \quad (14)$$

4. PROPOSED ALGORITHM

The proposed system consists of tumor segmentation (i.e., ROI) and ROI Encryption. The details of the two stages are illustrated in the following sub-sections.

4.1 Segmentation of region of interest (ROI)

This study uses U-Net architecture to present an automatic brain tumor segmentation on magnetic resonance imaging. The tumor segmentation block diagram based on U-Net is shown in Figure 4.

Figure 5 shows the original images, their masks, and predication images.

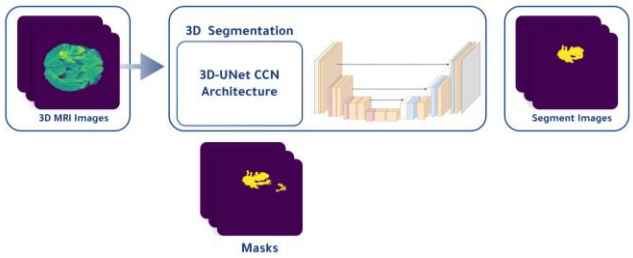

Figure 4. Tumor segmentation based on U-Net

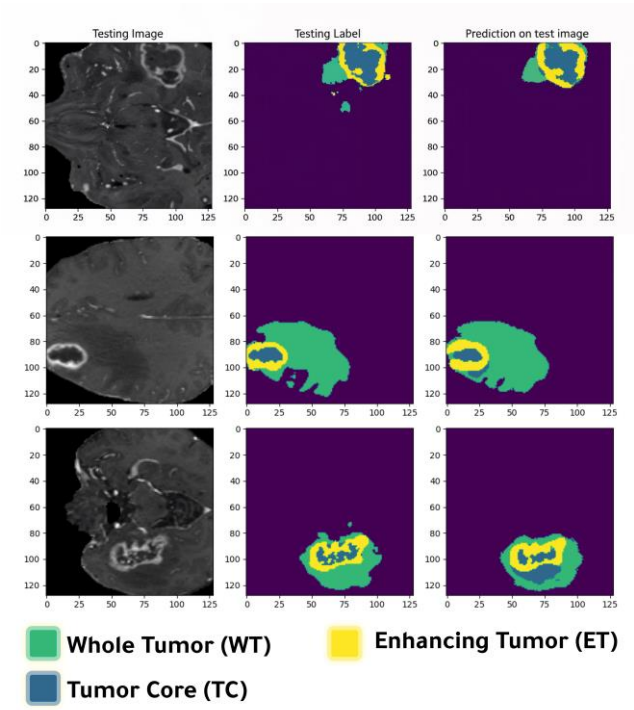

Figure 5. Examples of brain tumor segmentation

4.2 Proposed partial image encryption

The proposed algorithm for partial image encryption is a selective and partial method for encrypting medical images. The algorithm uses the Integer Discrete Wavelet Transform (IDWT), a chaotic system, and secret image sharing. This method helps to address security concerns arising from high inter-pixel correlation and large data capacity when encrypting an image. A suitable encryption technique should diminish this correlation, obscure positions of pixels, and render the original image cryptic and disorderly, thereby haphazardly randomizing and disarranging pixel locations. In the presented diffusion approach, the image is perturbed through a linear system by generating random variables to displace the positions of all pixels in the plaintext image. The IDWT is applied to the perturbed image, wherein the low-frequency coefficients can be utilized to construct a blurred approximation of the original image.

In contrast, the high-frequency coefficients solely contribute to the finer image details. Therefore, encrypting only the low-frequency components might be of interest. The proposed image encryption process encompasses key generation, image permutation based on a chaotic map, and image diffusion using secret image sharing.

4.3 Key generation

The process of generating keys uses both hash coding and a hyperchaotic map. Specifically, the hash function takes features from the area of interest using SHA-512, resulting in a 512-bit hash value [36]. As SHA-512 is permanent, it resists various attacks, including plaintext attacks. The algorithm for generating keys in the encryption scheme using SHA-512 is outlined in Algorithm 2. High-dimensional hyperchaotic systems have a more complex structure than low-dimensional chaotic systems, resulting in more robust randomness of the generated sequence, making them ideal for image encryption. In this encryption method, the secret keys comprise the initial values and parameters of the hyperchaotic system. Using pixels within the region of interest (ROI) as the primary private key source enhances security.

Algorithm (2): Proposed Key Generation

Input:

ROI,

S_{key} // Secret encryption key

Output:

k_i i=1,..,n // n is the number of sub-blocks

Step 1: Calculate SHA-512 of ROI to generate a vector with a 512-bit hash value.

hash=SHA-512 (ROI)

hash=$\{h_1, h_2, ..., h_{32}\}$ (15)

It should be noted that when extracting features, even minor changes can significantly impact the outcome. For instance, a one-bit change in the Region of Interest (ROI) can cause hash values to change drastically. To mitigate this issue, four values are produced using the XOR operation ($\oplus$) on the hash values, as shown in the equations below:

$S_1 = h_1 \oplus h_2 \oplus \ldots \oplus h_8$

$S_2 = h_9 \oplus h_{10} \oplus \ldots \oplus h_{16}$

$$S_3=h_{17} \oplus h_{18} \oplus \ldots \oplus h_{24}$$
$$S_4=h_{25} \oplus h_{10} \oplus \ldots \oplus h_{32} \quad (16)$$

Step 2: Suppose the initial keys x_1, x_2, x_3, and x_4 and positive parameters are β_1, β_2, β_3, and β_4. are randomly chosen for the hyperchaotic system in Eq. (1). After that, the first keys are updated affording to the plain image pixel value as follows:

$$X'=(x_1 \bmod S_1)/256$$
$$Y'=(x_2 \bmod S_2)/256$$
$$Z'=(x_3 \bmod S_3)/256$$
$$W'=(x_4 \bmod S_4)/256 \quad (17)$$

Step 3: Normalize the four variables X', Y', Z', and W' to the range [0, 1].
Step 4: The hyperchaotic system is firstly iterated (100 times) to generate four chaotic sequences, denoted as X', Y', Z', and W', respectively; the first 100 elements of each sequence are discarded. This practice enhances the sensitivity of the initial values and parameters of the map, effectively mitigating transient effects.
Step 5: Afterward, the chaotic sequences X' and Y' are generated. Then, a key extension method is performed by multiplying X' (8, 1) and Y' (1, 8), and a chaotic matrix *Chaotic1* (8, 8) is obtained.
Step 6: Repeat step 5 with Z' *and* W' to obtain *Chaotic2* (8, 8).
Step 7: The chaotic matrix *Chaotic1 and Chaotic2* are handled together with *UserKey* to construct a chaotic matrix k_1 and k_2 of size 8×8 (as expressed in Eqs. (18) and (19).

$$k_1=((Chaotic1\times 1000)\times UserKey) \bmod 256 \quad (18)$$

$$k_2=((Chaotic2\times 1000)\times UserKey) \bmod 256 \quad (19)$$

where, *UserKey* is a user secret key with size 8×8.
Step 8: Repeat steps from step 2 to step 6 to generate k_i i=1, ..., n. For each value of *UserKey,* a unique chaotic sequence of *Chaotic* is generated.

4.4 Image diffusion phase

The proposed diffusion phase employs a set of linear equations with n=2 and k=2. The linear transformation presented in Eq. (20) can detach a high pixel correlation.

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} mod\ N = \begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} mod\ N \quad (20)$$

where, (x, y) represents the original pixel position, (x', y') denotes the transformed pixel position, and both (x', y') and (x, y) belong to the range [1, N]×[1, N]. The image is divided into N sub-blocks, and the x_1, x_2, x_3, and x_4 are hyperchaotic system variables generated by Eq. (7) as secret keys. The ROI is first rearranged in a symmetric matrix as input to the diffusion phase.

Besides using linear equations, modular algebra controls the increasing index size. According to Eq. (15), the range of indices values $\begin{bmatrix} x' \\ y' \end{bmatrix}$ is [0... N].

$$\begin{bmatrix} x_1 & x_2 \\ x_3 & x_4 \end{bmatrix} \times \begin{bmatrix} x \\ y \end{bmatrix} mod\ N = \begin{bmatrix} x' + p_i \\ y' + p_i \end{bmatrix} \quad (21)$$

P_i is an integer value that will not be included in the index values. During retrieval, its values will be adjusted according to specific integer division rules. Figure 6 shows an example of the proposed image diffusion.

Example 1:

Let A an is 8×8 image; the number of 2×2 subblocks is 16 and N=7. Let x_1=13, x_2=29, x_3=53, and x_4=31. Let x=5 and y=1. According to the Eq. (8):

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} mod\ 7 = \begin{bmatrix} 13 & 29 \\ 53 & 31 \end{bmatrix} \times \begin{bmatrix} 5 \\ 1 \end{bmatrix} mod\ 7$$
$$13\times5+29\times1=\text{mod } 7=3$$
$$53\times5+31\times1=\text{mod } 7=3$$
$$X'=3,\ y'=3.$$

Let x=7 and y=5. According to the Eq. (1):

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = A \begin{bmatrix} x \\ y \end{bmatrix} mod\ 7 = \begin{bmatrix} 13 & 29 \\ 53 & 31 \end{bmatrix} \times \begin{bmatrix} 7 \\ 5 \end{bmatrix} mod\ 7$$
$$13\times7+29\times5=\text{mod } 7=5$$
$$53\times7+31\times5=\text{mod } 7=1$$
$$x'=5,\ Y'=1.$$

As a result, the pixel at location (5,1) is placed at location (3,3), and the pixel at location (7,5) is placed at location (5,1).

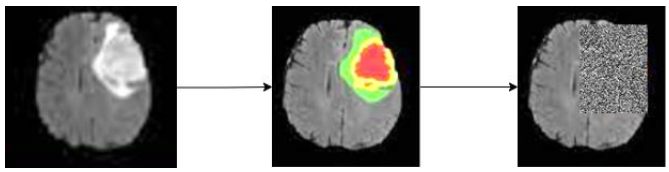

Figure 6. Example of the proposed diffusion phase

4.5 Image confusion phase

In this phase, selective and partial image encryption is used. The ROI is divided into 8×8 sub-blocks, and IDWT is applied for each block. The low-frequency coefficients *LL* of size 4×4 are only encrypted using (n,n) polynomial-based secret image sharing. The *LL* band for each block is passed to the Feistel Network FN, and then the inverse of IDWT is applied to the encrypted *LL'* bands to generate C_i, i=1, ..., n, where n is the number of subblocks. The high-frequency *LH*, *HL*, and *HH* are diffused using the Morton scan to swap coefficient positions and then confused based on the chaotic map. The block diagram of the proposed image confusion phase is shown in Figure 7.

The Feistel network is used in the proposed system to cipher 16 bytes, i.e., (4×4) bytes as input, split into two parts of 8, *L*, and *R*. The F function performs (8,8) secret image sharing based on polynomials. The Key K_i is supplied from key generation steps based on hyperchaotic maps. The Feistel network performs two secret image-sharing rounds (8,8), as illustrated in Figure 8.

Algorithm (3): Proposed Confusion Phase
Input
ROI,
k_i i=1, ..., n // n is the number of sub-blocks,
Width, Height, blocks divided by 8
Output
EROI

Step 1: Divide the *ROI* into subblocks of size 64 bits (8×8).
Step 2:
For i=1 to Width
For j=1 to Height
Get sub-block Blk
Apply IDWT on the Blk.
Pass LL band to FN to construct polynomials to calculate the encrypted coefficients such as the following:

$$c_1 = ll_1k_{11} + ll_2k_{12} + ll_3k_{14} + ll_4k_{14} + ll_5k_{15} + ll_6k_{16} + ll_7k_{17} + ll_8k_{18} \; mod \; 251$$
$$c_2 = ll_1k_{21} + ll_2k_{22} + ll_3k_{24} + ll_4k_{24} + ll_5k_{25} + ll_6k_{26} + ll_7k_{27} + ll_8k_{28} \; mod 251$$
$$\vdots$$
$$c_8 = ll_1k_{81} + ll_2k_{82} + ll_3k_{84} + ll_4k_{84} + ll_5k_{85} + ll_6k_{86} + ll_7k_{87} + ll_8k_{88} \; mod \; 251$$

Rearranged the encrypted coefficients in *LL'*
To generate vector S, apply a Morton scan to each sub-block with the remaining coefficients of *the LH, HL, and HH* bands.
Apply confusion on the *S* vector based on the chaotic sequence *X'* to generate *the S'* vector.
Rearranged the *S'* vector into *LH', HL'* and *HH'*. bands
Apply the inverse of IDWT to generate *Cll.*
Put the subblock *Cll* in the *EROI.*
EndFor j
EndFor i
Step 3: The output is the *EROI*.

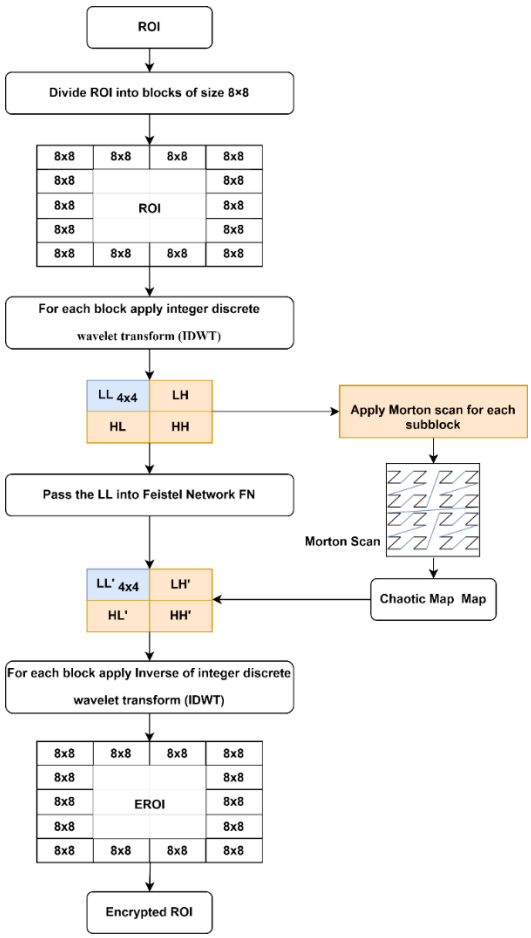

Figure 7. Block diagram of the proposed confusion phase

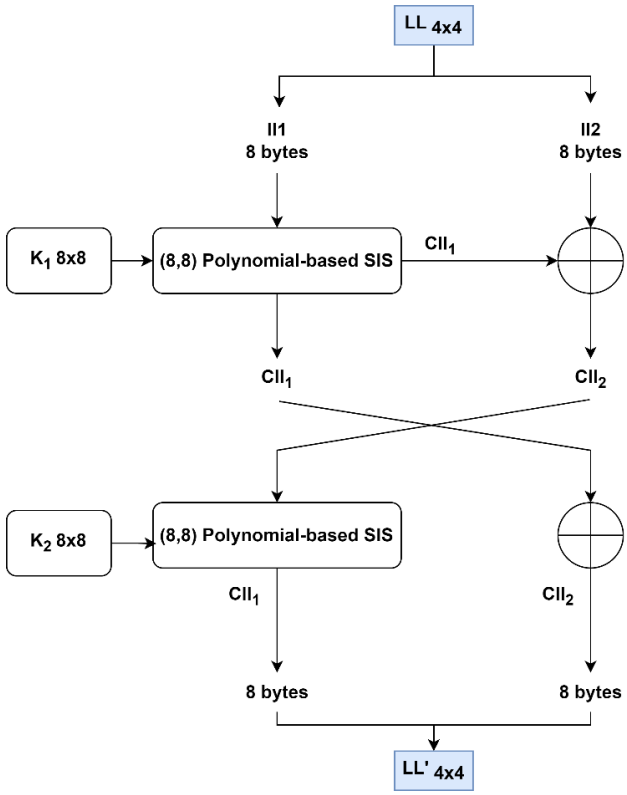

Figure 8. Block diagram of the proposed Feistel network

Example to show the (8,8) Polynomial-based SIS.
Let *b* be a block from diffused image *DiffROI* of size 8 bytes, as shown below:

Band *LL*

ll_1	ll_2	Ll_3	ll_4	ll_5	ll_6	ll_7	ll_8

Let *k* be a secret key block of size 8×8 (i.e., 512 bits).

Key k_1

k_{11}	k_{12}	k_{13}	k_{14}	k_{15}	k_{16}	k_{17}	k_{18}
k_{21}	k_{22}	k_{23}	k_{24}	k_{25}	k_{26}	k_{27}	k_{28}
k_{41}	k_{42}	k_{43}	k_{44}	k_{45}	k_{46}	k_{47}	k_{48}
k_{41}	k_{42}	k_{43}	k_{44}	k_{45}	k_{46}	k_{47}	k_{48}
k_{51}	k_{52}	k_{53}	k_{54}	k_{55}	k_{56}	k_{57}	k_{58}
k_{61}	k_{62}	k_{63}	k_{64}	k_{65}	k_{66}	k_{67}	k_{68}
k_{71}	k_{72}	k_{73}	k_{74}	k_{75}	k_{76}	k_{77}	k_{78}
k_{81}	k_{82}	k_{83}	k_{84}	k_{85}	k_{86}	k_{87}	k_{88}

Construct (8,8) Polynomial-based SIS for each subblock $\{ll_j | j=1 \ldots, 8\}$ to generate 8 bytes in encrypted block $\{cll_j | j=1 \ldots, 8\}$; utilize the following polynomials to compute the encrypted first row:

$$c_1 = ll_1k_{11} + ll_2k_{12} + ll_3k_{14} + ll_4k_{14} + ll_5k_{15} + ll_6k_{16} + ll_7k_{17} + ll_8k_{18}$$
$$c_2 = ll_1k_{21} + ll_2k_{22} + ll_3k_{24} + ll_4k_{24} + ll_5k_{25} + ll_6k_{26} + ll_7k_{27} + ll_8k_{28}$$
$$\vdots$$
$$c_8 = ll_1k_{81} + ll_2k_{82} + ll_3k_{84} + ll_4k_{84} + ll_5k_{85} + ll_6k_{86} + ll_7k_{87} + ll_8k_{88}$$

Cipher band *LL'*

cll_{11}	cll_{12}	cll_{13}	cll_{14}	cll_{15}	cll_{16}	cll_{17}	cll_{18}

5. EXPERIMENTAL RESULT

This section uses various validation metrics to conduct performance and security analyses.

5.1 Security analysis

The main focus of the design philosophy behind this work was to provide a high level of security. Therefore, we designed the proposed cipher with substantial security aspects. It has been created based on the theory of provable security, which protects against brute-force attacks, matching plaintext-ciphertext, differential cryptanalysis and linear cryptanalysis.

The only way to make a block cipher withstand a brute-force attack is to choose input key k so large that a brute-force attack becomes practically infeasible. The key length k of the proposed algorithm is 2^{1628}, as computed in the next section. On the other hand, the length block size of 512 bits is long enough to resist the matching plaintext-ciphertext

The frequency domain has numerous benefits for encryption. Finding the crucial areas that need to be encrypted is simpler. Connecting between spatial domain pixel values and frequency domain values is challenging. As a result, the image is safe from numerous assaults, including known plaintext attacks and ciphertext-only attacks.

The security analysis has shown that the Linear system possesses a security property. According to this property, "Any k-1 or fewer shadows cannot obtain enough information to reveal the secret image." In our scheme, for a secret colour image of size 512×512, there are a certain number of possibilities to correctly guess the combined coefficients a_{ij} (where i∈[1, n] and j∈[1, k], with n representing the total number of shares and k being the minimum number required to retrieve the image data), along with a block of image data $\{V_j|j=1, ..., k\}$.

$$BrutForce = (8 \times k)^{Q} \log_2(R(a_{ij}))^{k} \quad (22)$$

where,

$$Q = \frac{width \times hight}{k} \quad (23)$$

R: Range of a's

Example: Let the size of the secret colour image is 512×512, then the probability of guessing the right block of image data $\{V_j|j=1...k\}$ when k=2 is:

$$(8\times2)^{(512\times512)/2}=2^{524288}$$

Moreover, the probability of guessing the right combined coefficients a_{ij} when $R(a_{ij})$=256 is:

$$\log_2((256)^2) = \log_2(2^{16})=16.$$

It is essential to understand that the likelihood of guessing the combined coefficients a_{ij} is much lower compared to the probability of correctly guessing a block of image data. This probability is affected by the size of the image and the value of k, while the coefficients a_{ij} are distinct for each share throughout the entire image.

In addition to using the image diffusion phase to decorrelate pixels prior to applying the (n, n) secret image sharing scheme, Discrete Wavelet Transformation (DWT) is utilized to process a secret image. After applying a transform to the data, a combination procedure decorrelates the transform coefficients and improves security.

Regarding polynomial-based image secret sharing, recovering a secret image involves using Lagrange's interpolation to reconstruct the polynomial and obtain the grayscale values of the original secret image. However, retrieving every pixel of the secret image requires solving multiple linear systems, which can be computationally intensive and time-consuming due to the large number of secret image pixels and the significant amount of data involved.

Key-dependent permutation operations enhance the proposed algorithm's security. This involves exchanging input bits under the control of subkeys to destroy the additive difference and protect it against linear and differential cryptanalysis. Each algorithm phase depends on its key, which prevents fixed output and increases its nonlinearity.

5.2 Key space analysis

The key space is fundamental to any encryption scheme, providing vital resistance against brute force attacks. The proposed system utilizes eight independent variables, consisting of four secret initial values (x_1, x_2, x_3, and x_4) along with four positive parameters (β_1, β_2, β_3, and β_4). Consequently, these symbols collectively constitute the key space [37]. However, due to the utilization of double-precision numbers for these variables, the count of distinct values surpasses 10^{14}. The proposed approach employs the hyperchaotic system thrice, each incorporating diverse initial and parameter values, thereby establishing a key space of $((10^{14})^8)^3 = 10^{336} \approx 2^{1116}$ for a single block. Furthermore, the proposed algorithm adopts a user key spanning 512 bits, resulting in a total key space of $2^{1116} \times 2^{512} = 2^{1628}$. Table 2 offers a comparative analysis of the key space between the proposed system and other relevant methodologies.

Notably, the employed algorithm exhibits a larger key space than most algorithms under comparison. This outcome signifies that the scheme has a robust capability to thwart brute-force attacks effectively. Moreover, incorporating a nonlinear chaotic system to generate the input sequence within this algorithm enhances its resilience. The inherent nonlinearity, unpredictability, and pseudo-random characteristics of chaotic systems contribute significantly to countering linear attacks.

Table 2. Key space comparison between the proposed scheme and other schemes

Algorithm	Key Space
Proposed system	2^{1628}
[21]	2^{465}
[38]	2^{348}
[39]	2^{197}
[40]	2^{425}
[41]	2^{298}
[42]	2^{197}
[43]	2^{199}

5.3 Statistical analysis

The application of statistical analysis emerges as a critical metric within the domain of image encryption technology. Researchers have carried out two distinct categories of tests: histogram analysis and correlation coefficient analysis.

5.3.1 Histogram analysis

The histogram of a given image illustrates the distribution of pixel intensity values. In the case of an unencrypted image, the histogram typically exhibits slanting bars, a characteristic that could potentially be exploited by malicious parties to glean information about the image. To counter such statistical attacks, an encryption scheme must possess the ability to transform these slanting bars into well-organized bars with a distribution that closely resembles the original. By doing so, the scheme prevents hackers from extracting meaningful information. The histograms of both the unencrypted and encrypted images of Lena are depicted in Figure 9. In particular, Figure 9(e) displays the curved slanting bars in the histogram of the unencrypted and encrypted Lena image. The histogram transformed into a well-organized, evenly distributed plain bar in the encrypted counterpart. These organized plain bars offer robust resilience against histogram attacks, underscoring the efficiency of the proposed encryption scheme.

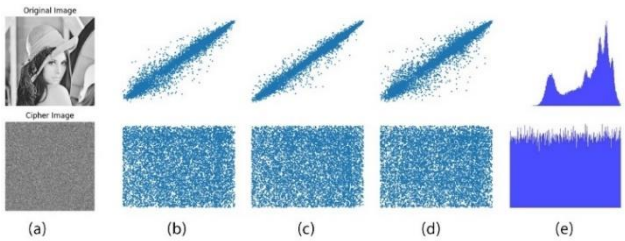

Figure 9. (a) Original & encrypted images, (b) horizontal, (c) vertical, (d) diagonal correlations of original & encrypted images, (e) Histogram of original & Encrypted images

Furthermore, the proposed algorithm was applied to several images of brain scans, specifically after extracting the region of interest (ROI) from each image. This process is illustrated in Figure 10.

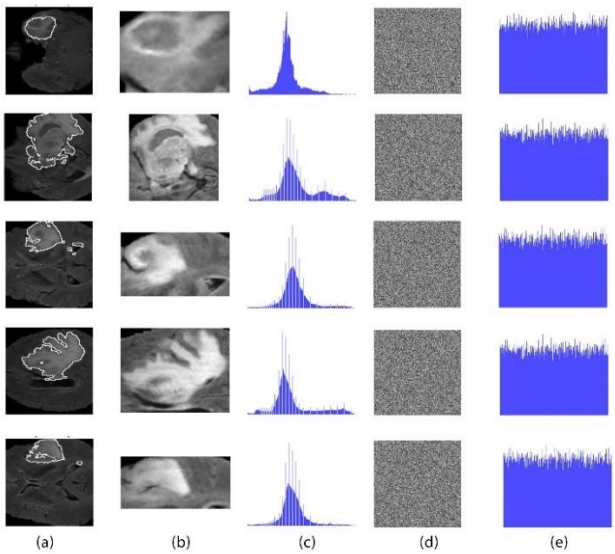

Figure 10. (a) Original image, (b) ROI, (c) Histogram of ROI, (d) Encrypted image, (e) Histogram of the encrypted image

5.3.2 Analysis of the correlation coefficient

For natural and unencrypted images, pixel arrangement follows systematic patterns, with neighbouring pixels exhibiting solid correlations. The correlation coefficient (CC) serves as a crucial security parameter, quantifying the inter-pixel correlation within an image. These adjacent pixels can be aligned vertically, diagonally or horizontally. Image encryption methods are designed to disrupt these patterns of adjacent pixels. To evaluate the correlation coefficient (CC) within the proposed encryption scheme, 10,000 pairs of consecutive pixels were randomly selected from the encrypted and original images. CC was computed using the following equation:

$$CC = \frac{A\sum_{l=1}^{A}(x_1 \times y_1) - \sum_{l=1}^{A} x_1 \times \sum_{l=1}^{A} y_1}{\sqrt{\left(A\sum_{l=1}^{A} x_1^2 - \left(\sum_{l=1}^{A} x_1^2\right)\right)\left(A\sum_{l=1}^{A} y_1^2 - \left(\sum_{l=1}^{A} y_1^2\right)\right)}}$$

where, A denotes the number of pixels; the neighbouring pixels are called x and y.

The fully encrypted image showed correlation coefficients approaching zero in all directions. Furthermore, the partially encrypted image's correlation coefficients fell from 0 to 1. This observation underscores the algorithm's resilience against geometric attacks.

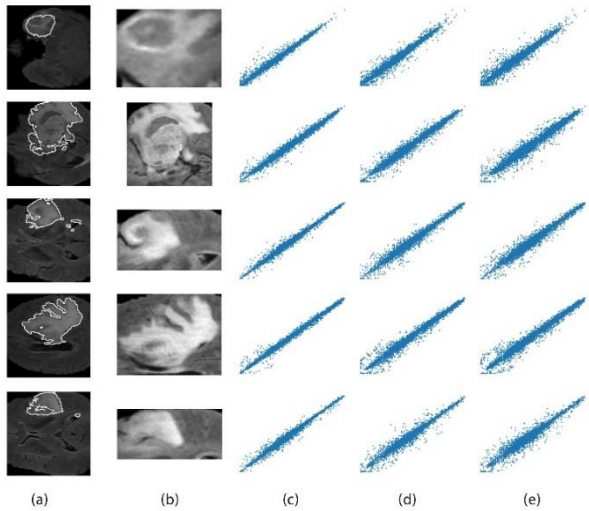

Figure 11. Correlation coefficients were calculated for the original medical images using the proposed algorithm, including (a) Original image, (b) Region of interest (ROI), (c) Horizontal correlations, (d) Vertical correlations, and (e) Diagonal correlations

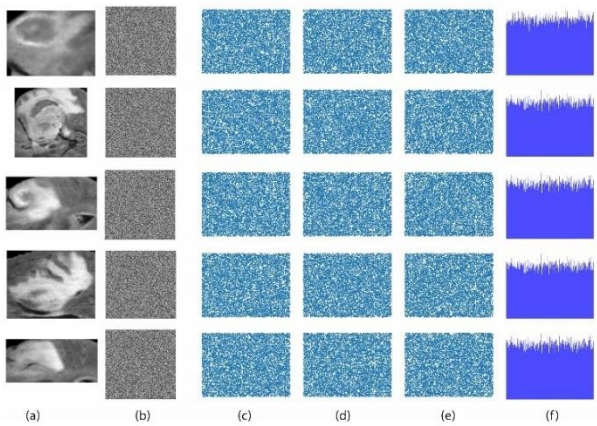

Figure 12. Correlation coefficients for the encrypted medical images utilizing the proposed algorithm (a) ROI, (b) Encrypted image, (c) horizontal, (d) vertical, (e) diagonal correlations

However, the correlation coefficients for the encrypted and original images were analyzed in three directions to provide a comprehensive understanding. The graphical representations of these correlation coefficients can be found in Figure 11 and Figure 12.

5.3.3 Entropy

Entropy serves as a means to assess the degree of randomness or unpredictability exhibited by pixel values within an image. It aids in quantifying the level of disorder present in a cryptogram, thereby providing insight into the effectiveness of diffusion and confusion processes within encryption. Mathematically, entropy could be calculated using the equation below [44]:

$$E = \sum_{i=0}^{n} p_i \, log_2(p_i)$$

where, p_i represents the probability of the occurrence of pixel value i in the image.

A cryptogram approaching a value of 8 or equaling it signifies a more robust implementation of diffusion and confusion, rendering it more resilient to entropy attacks. This heightened level of randomness within the cryptograms enhances their security by making them inherently more challenging to predict or decipher. Furthermore, as illustrated in Table 3, the results of entropy analysis provide insights into the security and strength of encryption methods.

Table 3. The entropy of the original and encrypted images has been calculated using the proposed algorithm

Image	Original Image	Encryption Image
1st Image	5.2350	7.9970
2nd Image	5.7419	7.9967
3rd Image	5.5482	7.9973
4th Image	5.3695	7.9969
5th Image	6.5444	7.9966
6th Image	6.8078	7.9975
7th Image	6.5210	7.9965
8th Image	6.3950	7.9965

Table 3 presents the entropy values for eight images before and after encryption. The entropy values were computed to evaluate the images' degree of randomness and disorder. This analysis provides a comprehensive understanding of how encryption processes impact the entropy of the images, shedding light on the effectiveness of the encryption scheme in preserving security and minimizing predictability.

The table demonstrates the impact of encryption on the entropy values, with post-encryption values consistently approaching or reaching the desirable value of 8. This result highlights the efficacy of the encryption method in improving the randomness and security of the encrypted images.

5.3.4 NPCR (Number of Pixel Change Rate)

The Normalized Pixel Change Rate (NPCR) is a metric that measures how effective an encryption algorithm is in preventing differential attacks. It calculates the percentage of changes in pixel locations between two images. A high NPCR value, close to 100%, indicates a significant difference between the two images, implying that they have undergone substantial transformation due to encryption. This increased level of variation enhances the security against differential attacks, as it becomes increasingly difficult for attackers to extract significant information from encrypted data. A near-100% NPCR value indicates the encryption's effectiveness in introducing significant alterations to image pixel positions, thereby enhancing security. Table 4 presents the analysis of NPCR results for eight tested images below. It was found that the NPCR rate for all images was 99%, indicating that the encryption process significantly altered the locations of the pixels. This result confirms that the encryption scheme is robust against differential attacks, which enhances the system's overall security.

5.3.5 UACI (Unified Average Changed Intensity)

The average is calculated from the differences in pixel intensity between the two images. The expected outcome is that this calculation yields a result greater than 33%. Normalized Unified Average Change Intensity (UACI) and Pixel Change Rate (NPCR) were computed using two cryptograms with nearly identical keys, except for a slight alteration in the least significant decimal digit. The NPCR values obtained exceeded 99%, while the UACI values surpassed 33%. This implies that the proposed system generates a significantly distinct cryptogram when provided with a plain image and a minor alteration. The findings are summarized in Table 4.

The proposed method's effectiveness was evaluated on a standard image (Lena), using different parameters such as entropy, correlation analysis, unified average change intensity (UACI), and normalized pixel change rate (NPCR) in Table 4. The results of this evaluation are presented, where the histogram and correlation coefficient distributions of the proposed method demonstrate positive outcomes. The UACI and NPCR values obtained through this method are comparable to those obtained through polynomial-based secret image sharing and chaotic maps encryption approaches. One significant achievement of this method is that the information entropy value obtained is also very close to the ideal value. Moreover, all tests were completed successfully, which supports the claim that the suggested approach is reliable and secure.

Table 4. The entropy of the original and encrypted images using the proposed algorithm

Image	NPCR	UACI
1st Image	99.6292	37.3938
2nd Image	99.6002	35.7715
3rd Image	99.5972	35.4818
4th Image	99.6460	34.0463
5th Image	99.6384	32.5668
6th Image	99.6292	31.7352
7th Image	99.6414	29.0743
8th Image	99.6490	28.7795

Table 5. Comparison of the suggested algorithm with alternative techniques for the "Lena" image

Correlation		
Horizontal	Vertical	Diagonal
-0.0028	0.0171	0.0022
-0.0359	0.0020	0.0019
/	/	/
0.0020	0.0105	0.0019
0.0023	0.0019	0.0011
0.0030	0.0024	0.0034
-0.0016	0.0028	-0.0006
-0.0008	0.0064	-0.0223

Table 6. The time required for both the ROI and complete image encryption

Image	Size (Original Image) (KB)	Size (ROI) (KB)	Time of ROI (sec)	Time of Localization	Time of Encrypt Original Image (sec)
1st Image	71.9	8.09	0.10384	0.026	2.3737
2nd Image	59.6	20.4	0.35629	0.053	2.2707
3rd Image	64.4	11.3	0.23348	0.029	2.3045
4th Image	73.1	17.8	0.33749	0.033	2.4280
5th Image	56.5	10.6	0.15459	0.027	2.2364

5.3.6 Time complexity

Selective image encryption is a crucial aspect of medical imaging as it helps to reduce both time and cost. Many current encryption methods are complex and rely on traditional techniques. The proposed algorithm ensured the privacy of the ROI; there is a trade-off between time complexity and security requirements compared with full image encryption. Selective image encryption presents several advantages compared to the network transform method. However, it still faces security challenges since only specific parts of an image receive sufficient protection. The level of security provided by encryption depends on the intended application and meeting the necessary criteria. Delve into the critical aspect of time complexity concerning implementing Partial Image Encryption. Time complexity plays a pivotal role in evaluating the efficiency of cryptographic algorithms. In this context, it explicitly addresses how execution time was optimized by applying Partial Image Encryption techniques. The empirical results of these optimizations are meticulously presented in Table 5 for comprehensive analysis.

Table 6 provides a detailed comparison of the execution times for the ROI and the encryption of the original image. The results indicate a significant decrease in execution time when using the Partial Image Encryption technique compared to encrypting the original image. This achievement is highly practical and efficient in real-world scenarios. The reduction in execution time is due to the selective encryption of specific regions of interest (ROI) within the image, resulting in a streamlined process that maintains security and efficiency. This optimization enhances the overall user experience and holds promise for applications that require fast encryption and decryption, such as real-time image transmission and secure data storage.

6. CONCLUSIONS

This study has addressed the formidable challenge of securing medical images, which often encompass sensitive patient and diagnostic data that traverse public networks. Conventional cryptographic methods have proven inadequate due to the unique attributes of digital images, including their substantial size, inherent redundancy, and pixel correlation. To confront this challenge, an innovative approach to image encryption was introduced, amalgamating multiple techniques to bolster security. The proposed method optimizes security and efficiency by selectively encrypting specific segments of the confidential image. An encryption mechanism was crafted using the principles of chaotic systems, maps, and attractors, imparting high levels of randomness and unpredictability. The integration of polynomial-based secret image sharing, coupled with partial encryption, further enhances the resilience of the proposed approach against potential attacks.

Furthermore, the power of transform domain encryption was harnessed, capitalizing on techniques like discrete wavelet transform to enhance security without introducing undue algorithmic complexity. A symmetric encryption algorithm strengthens the overall security architecture while ensuring practical implementation. This paper has introduced a pragmatic image encryption model customized for medical images, introducing an efficient diffusion model based on a linear system and chaotic map. This study effectively mitigated the computational overhead of sizeable digital image sizes by incorporating partial encryption and pixel rearrangement within the Region of Interest (ROI).

REFERENCES

[1] Ahmed, S.T., Hammood, D.A., Chisab, R.F., Al-Naji, A., Chahl, J. (2023). Medical image encryption: A comprehensive review. Computers, 12(8): 160. https://doi.org/10.3390/computers12080160

[2] Natha, S., Laila, U., Gashim, I.A., Mahboob, K., Saeed, M.N., Noaman, K.M. (2024). Automated brain tumor identification in biomedical radiology images: A multi-model ensemble deep learning approach. Applied Sciences, 14(5): 2210. https://doi.org/10.3390/app14052210

[3] Sayed, W.S., Roshdy, M., Said, L.A., Radwan, A.G. (2021). Design and FPGA verification of custom-shaped chaotic attractors using rotation, offset boosting and amplitude control. IEEE Transactions on Circuits and Systems II: Express Briefs, 68(11): 3466-3470. https://doi.org/10.1109/TCSII.2021.3082271

[4] Nosov, V.R., Meda Campana, J.A., Gomez Mancilla, J.C. (2019). Method and algorithm to construct a quasi-chaotic sequence. IEEE Latin America Transactions, 17(01): 31-36. https://doi.org/10.1109/TLA.2019.8826692

[5] Zhang, L., Zhu, Y., Ren, W., Wang, Y., Choo, K.K.R., Xiong, N.N. (2021). An energy-efficient authentication scheme based on Chebyshev chaotic map for smart grid environments. IEEE Internet of Things Journal, 8(23): 17120-17130. https://doi.org/10.1109/JIOT.2021.3078175

[6] Rao, N., Xu, X.J., Li, S.Q. (2004). Hybrid chaotic sequence for QS-CDMA system with RAKE receiver. Journal of Systems Engineering and Electronics, 15(3): 278-282.

[7] Preishuber, M., Hutter, T., Katzenbeisser, S., Uhl, A. (2018). Depreciating motivation and empirical security analysis of chaos-based image and video encryption. IEEE Transactions on Information Forensics and Security, 13(9): 2137-2150. https://doi.org/10.1109/TIFS.2018.2812080

[8] Lin, C.M., Pham, D.H., Huynh, T.T. (2022). Encryption and decryption of audio signal and image secure communications using chaotic system synchronization control by TSK fuzzy brain emotional learning

controllers. IEEE Transactions on Cybernetics, 52(12): 13684-13698. https://doi.org/10.1109/TCYB.2021.3134245

[9] Li, X., Zeng, J., Ding, Q., Fan, C. (2022). A novel color image encryption algorithm based on 5-D hyperchaotic system and DNA sequence. Entropy, 24(9): 1270. https://doi.org/10.3390/e24091270

[10] Liu, W., Sun, K., Zhu, C. (2016). A fast image encryption algorithm based on chaotic map. Optics and Lasers in Engineering, 84: 26-36. https://doi.org/10.1016/j.optlaseng.2016.03.019

[11] Wang, X., Wei, N., Zhang, D. (2015). A novel image encryption algorithm based on chaotic system and improved gravity model. Optics Communications, 338: 209-217. https://doi.org/10.1016/j.optcom.2014.10.042

[12] Xu, X., Wang, Y., Chen, S. (2016). Medical image fusion using discrete fractional wavelet transform. Biomedical Signal Processing and Control, 27: 103-111. https://doi.org/10.1016/j.bspc.2016.02.008

[13] Jain, K., Aji, A., Krishnan, P. (2021). Medical image encryption scheme using multiple chaotic maps. Pattern Recognition Letters, 152: 356-364. https://doi.org/10.1016/j.patrec.2021.10.033

[14] Yepdia, L.M.H., Tiedeu, A. (2021). Secure transmission of medical image for telemedicine. Sensors and Imaging, 22(1): 17. https://doi.org/10.1007/s11220-021-00340-8

[15] Masood, F., Driss, M., Boulila, W., Ahmad, J., Rehman, S.U., Jan, S.U., Qayyum, A., Buchanan, W.J. (2022). A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. Wireless Personal Communications, 127(2): 1405-1432. https://doi.org/10.1007/s11277-021-08584-z

[16] Li, J., Zhang, Z., Li, S., Benton, R., Huang, Y., Kasukurthi, M.V., Li, D., Lin, J., Borchert, G.M., Tan, S.B., Li, G., Ma, B., Yang, M., Huang, J. (2020). A partial encryption algorithm for medical images based on quick response code and reversible data hiding technology. BMC Medical Informatics and Decision Making, 20(S14): 297. https://doi.org/10.1186/s12911-020-01328-2

[17] Yan, X., Sun, L., Lu, Y., Yang, G. (2020). Adaptive partial image secret sharing. Symmetry, 12(5): 703. https://doi.org/10.3390/sym12050703

[18] George, L.E., Hassan, E.Kh., Mohammed, S.G., Mohammed, F.G. (2020). Selective image encryption based on DCT, hybrid shift coding and randomly generated secret key. Iraqi Journal of Science, 61(4): 920-935. https://doi.org/10.24996/ijs.2020.61.4.25

[19] Noori Ghanim, Z., Raheem Khoja, S.A. (2022). A partial image encryption scheme based on DWT and texture segmentation. Cogent Engineering, 9(1). https://doi.org/10.1080/23311916.2022.2026555

[20] Yousif, N.A., Mahdi, G.S., Hashim, A.T. (2022). Medical image encryption based on frequency domain and chaotic map. International Journal of Safety and Security Engineering, 12(4): 467-473. https://doi.org/10.18280/ijsse.120407

[21] Salman, L.A., Hashim, A.T., Hasan, A.M. (2022). Selective medical image encryption using polynomial-based secret image sharing and chaotic map. International Journal of Safety and Security Engineering, 12(3): 357-369. https://doi.org/10.18280/ijsse.120310

[22] Kiran, P., Parameshachari, B.D. (2022). Resource optimized selective image encryption of medical images using multiple chaotic systems. Microprocessors and Microsystems, 91: 104546. https://doi.org/10.1016/j.micpro.2022.104546

[23] Natsheh, Q., Sălăgean, A., Zhou, D., Edirisinghe, E. (2023). Automatic selective encryption of DICOM images. Applied Sciences, 13(8). https://doi.org/10.3390/app13084779

[24] Al-Barzinji, S.M., Abd Abrahim Mosslah, R.H.M. (2023). Partial image encryption using DCT image-based DES algorithm. Journal of Southwest Jiaotong University, 58(1). https://doi.org/10.35741/issn.0258-2724.58.1.49

[25] Harshitha, M., Rupa, Ch., Sai, K.P., Pravallika, A., Sowmya, V.K. (2021). Secure medical data using symmetric cipher based chaotic logistic mapping. In 2021 7th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, pp. 476-481. https://doi.org/10.1109/ICACCS51430.2021.9441836

[26] El-Shafai, W., Khallaf, F., El-Rabaie, E.S.M., El-Samie, F.E.A. (2021). Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications. Journal of Ambient Intelligence and Humanized Computing, 12(10): 9007-9035. https://doi.org/10.1007/s12652-020-02597-5

[27] Gan, Z., Song, S., Zhou, L., Han, D., Fu, J., Chai, X. (2022). Exploiting compressed sensing and polynomial-based progressive secret image sharing for visually secure image selection encryption with authentication. Journal of King Saud University - Computer and Information Sciences, 34(10): 9252-9272. https://doi.org/10.1016/j.jksuci.2022.09.006

[28] Thien, C.C., Lin, J.C. (2002). Secret image sharing. Computers & Graphics, 26(5): 765-770. https://doi.org/10.1016/S0097-8493(02)00131-0

[29] Shamir, A. (1979). How to share a secret. Communications of the ACM, 22(11): 612-613. https://doi.org/10.1145/359168.359176

[30] Wang, B., Qin, J., Lv, L., Cheng, M., Li, L., Xia, D., Wang, S. (2023). MLKCA-Unet: Multiscale large-kernel convolution and attention in Unet for spine MRI segmentation. Optik, 272: 170277. https://doi.org/10.1016/j.ijleo.2022.170277

[31] Bai, L., Biswas, S., Ortiz, A., Dalessandro, D. (2006). An image secret sharing method. In 2006 9th International Conference on Information Fusion, Florence, Italy, pp. 1-6. https://doi.org/10.1109/ICIF.2006.301805

[32] Natiq, H., Al-Saidi, N.M.G., Said, M.R.M., Kilicman, A. (2018). A new hyperchaotic map and its application for image encryption. The European Physical Journal Plus, 133(1): 6. https://doi.org/10.1140/epjp/i2018-11834-2

[33] Liu, L., Hao, S., Lin, J., Wang, Z., Hu, X., Miao, S. (2018). Image block encryption algorithm based on chaotic maps. IET Signal Processing, 12(1): 22-30. https://doi.org/10.1049/iet-spr.2016.0584

[34] Biryukov, A. (2011). Feistel cipher. In Encyclopedia of Cryptography and Security, Springer US, pp. 455-455. https://doi.org/10.1007/978-1-4419-5906-5_577

[35] Hashim, A.T., George, L.E. (2014). Secret image sharing based on discrete cosine transform. International Journal of Computers & Technology, 12(7): 3697-3711. https://doi.org/10.24297/ijct.v12i7.3100

[36] Wen, W., Wei, K., Zhang, Y., Fang, Y., Li, M. (2020). Colour light field image encryption based on DNA

sequences and chaotic systems. Nonlinear Dynamics, 99(2): 1587-1600. https://doi.org/10.1007/s11071-019-05378-8

[37] Hashim, A.T., Jabbar, A.K., Hassan, Q.F. (2021). Medical image encryption based on hybrid AES with chaotic map. Journal of Physics: Conference Series, 1973(1): 012037. https://doi.org/10.1088/1742-6596/1973/1/012037

[38] Iqbal, N., Hanif, M., Abbas, S., Khan, M.A., Almotiri, S.H., Al Ghamdi, M.A. (2020). DNA strands level scrambling based color image encryption scheme. IEEE Access, 8: 178167-178182. https://doi.org/10.1109/ACCESS.2020.3025241

[39] Chai, X., Gan, Z., Zhang, M. (2017). A fast chaos-based image encryption scheme with a novel plain image-related swapping block permutation and block diffusion. Multimedia Tools and Applications, 76(14): 15561-15585. https://doi.org/10.1007/s11042-016-3858-4

[40] Ye, R., Xi, Y., Ma, Y. (2016). A chaotic image encryption scheme using swapping based confusion approach. In 2016 First IEEE International Conference on Computer Communication and the Internet (ICCCI), Wuhan, China, pp. 374-377. https://doi.org/10.1109/CCI.2016.7778946

[41] Fu, C., Zhao, G., Gao, M., Ma, H. (2013). A chaotic symmetric image cipher using a pixel-swapping based permutation. In 2013 IEEE International Conference of IEEE Region 10 (TENCON 2013), Xi'an, China, pp. 1-6. https://doi.org/10.1109/TENCON.2013.6718798

[42] Chen, J., Zhu, Z., Fu, C., Yu, H. (2013). An improved permutation-diffusion type image cipher with a chaotic orbit perturbing mechanism. Optics Express, 21(23): 27873. https://doi.org/10.1364/OE.21.027873

[43] Chen, J., Zhu, Z., Fu, C., Yu, H. (2014). A fast image encryption scheme with a novel pixel swapping-based confusion approach. Nonlinear Dynamics, 77(4): 1191-1207. https://doi.org/10.1007/s11071-014-1370-9

[44] Hashim, A.T., Jassem, A.H., Ali, S.A. (2021). A novel design of blowfish algorithm for image security. Journal of Physics: Conference Series, 1818(1): 012085. https://doi.org/10.1088/1742-6596/1818/1/012085