A Hybrid Domain Medical Image Encryption Scheme Using URUK and WAM Chaotic Maps with Wavelet – Fourier Transforms

Ali Akram Abdul-Kareem[1,*] and
Waleed Ameen Mahmoud Al-Jawher[2]

[1] *Iraqi Commission for Computers and Informatics, Informatics Institute for Postgraduate Studies, Baghdad, Iraq*
[2] *Uruk University, Baghdad, Iraq*
E-mail: phd202020559@iips.icci.edu.iq; profwaleed54@gmail.com
[*] *Corresponding Author*

Received 29 November 2022; Accepted 24 February 2023;
Publication 21 June 2023

Abstract

Image encryption is one of the most important techniques to maintain data confidentiality against illegal access and fraudulent usage. In this study, a new medical image encryption technique was developed by combining the discrete wavelet transform, the fast Fourier transform, the Arnold transform, and two multidimensional chaotic systems. The medical image is subjected to a discrete wavelet transform before the magic square shuffles the image subbands. Confusion operations are performed on each scrambled subdomain using the Uruk 4D chaotic system. To increase randomness and unpredictability, a second stage of confusion is implemented in the domain of the Fast Fourier transform using the Arnold transform. The final encrypted image is obtained utilizing secret keys derived from the WAM 3D chaotic system.

Journal of Cyber Security and Mobility, Vol. 12_4, 435–464.
doi: 10.13052/jcsm2245-1439.1241

In particular, the initial conditions for chaotic systems are derived from grayscale values, thereby increasing the algorithm's sensitivity to the input image. The results of the tests and the security analysis indicate that the proposed algorithm is exceptionally reliable and secure.

Keywords: Cryptographic algorithms, encoding, chaos, Arnold transform, magic square.

1 Introduction

As a result of the social distancing experienced by the global population in recent years, telemedicine has attracted the attention of researchers and those interested in the field, and many research efforts have been devoted to providing medical care to patients far from medical care providers. Diagnostics and decision-making rely on sensitive medical data stored as digital images. X-rays, ultrasounds, Computerized Tomography (CT) scans, brain images, and Magnetic resonance imaging (MRIs) are examples of images that contain confidential and vital information for patients and health centers. These images are shared between the patient and the health center via open public channels; however, these channels are susceptible to cyber-attacks, especially when they are not designed with security standards in mind. In addition to vulnerabilities in the private storage systems of hospitals or medical centers, these images are susceptible to illegal access by attackers who use them for non-diagnostic purposes. Encryption algorithms have been adopted to provide direct protection for images by transforming them into an unintelligible format for unauthorized users. Chaos-based medical image encryption is a fascinating field that uses chaos to generate secret keys with distinctive properties, including sensitivity to initial conditions, independence, long-range, high randomness, and the ability to develop them with low mathematical complexity. On the other hand, encryption techniques in the frequency domain demonstrate unrivaled performance, particularly in terms of the effect of encrypted wave coefficients on the pixel values of completely reconstructed images and the reduction of statistical correlation between pixels via confusion processes [1–6]. Using chaotic encryption keys, it is possible to design a robust encryption system that encrypts images in the frequency domain. Initially, the image is converted into the frequency domain using an appropriate transformation model. Then confusion and diffusion operations are performed on the parameters of the transformation model, resulting in a robust cipher system [6, 7]. D. Ravichandran et al. [8] proposed an algorithm for encrypting medical images based on the combination of three chaotic maps, namely logistic, tent, and pocket maps. Based on chaotic key streams generated by a one-dimensional Combined Logistic-Tent (CLT) system, permutation is implemented. The pixels are then subjected to a crossover process similar to bio-crossover. Before the mutation takes place, the image's pixels are decomposed into two images with a reduced bit depth. The process of XOR is then carried out using a one-dimensional Combined Logistic-Sin (CLS). Using 4D hyper digital chaos maps and dynamic deoxyribonucleic acid processes, M. Guan et al. [9] proposed an algorithm for encoding images in the frequency domain. This algorithm achieves excellent results, but it is severely hampered by the approximation risks of the Fourier transform. S. Kumar et al. [10] reported a scheme for ensuring medical image confidentiality that employs a chaotic function to perform confusion and diffusion operations on the fractional discrete cosine transform (FrDCT) coefficients for medical images. A. Banu S et al. [11] proposed a DICOM (Digital Imaging and Communications in Medicine) image coding technique that generates pseudo-random keys using 3D Lorenz attractors and a logistic map. The medical images are encrypted in the frequency domain using the Integer Wavelet Transform (IWT) and deoxyribonucleic acid (DNA) sequences. The algorithm consists of subsequent phases: permutation, substitution, encoding, complementary, and decryption. S. Jeevitha et al. [12] proposed a medical image encryption algorithm based on the Discrete Wavelet Transform (DWT) and edge maps extracted from the source image. The DWT is applied to the input image to obtain different sub-bands and frequencies. The edge map sequences are generated with the same DWT bit-scales, and all DWT parameters are scrambled to isolate the pixels and weaken the strong correlation between neighboring units. D. Ravichandran et al. [13] proposed a technique for securing digital medical images based on the Integer Wavelet Transform (IWT) combined with deoxyribo nucleic acid (DNA) and chaos. W. El-Shafai et al. [14] developed an algorithm for direct encryption of medical image pixels using logistic maps, piecewise linear chaotic map (PWLCM), and de-oxyribo nucleic acid (DNA) coding. X. Meng et al. [15] proposed an encryption algorithm based on a one-dimensional e^{λ}-cos-cot Map for a region of interest in medical DICOM (Digital Imaging and Communications in Medicine). Adaptive thresholding is used to isolate the region of interest from the medical image. The final encoded image is then produced by executing the confusion and diffusion operations in the spatial domain. According to the aforementioned literature, the majority of frequency domain medical image encryption algorithms rely on specific types of transforms, such as the fractional discrete cosine transform (FrDCT) that generates only real coefficients and the Integer Wavelet Transform (IWT), to avoid encountering the risks of rounding, which is crucial for medical image encryption because it affects image data and negatively impacts the diagnostic process. Other algorithms, on the other hand, encrypt only the most significant portions of the image in the spatial domain or by employing a transformation model, resulting in faster execution and less encryption depth. In the context of execution speed, some cryptographic algorithms have employed chaotic low-dimensional maps, which raises concerns regarding the short-term degradation of chaotic behavior. Multidimensional chaotic maps are unquestionably advantageous for cryptographic systems due to their inherent properties. Nonetheless, the inevitability of chaotic systems has recently sparked widespread debate about their resilience in the face of the rapid development of penetration systems. Discrete Wavelet Transform (DWT), Discrete Fourier Transform (DFT), Arnold Transform (AT), and two chaotic systems are used to present a new medical image encryption algorithm in this paper. The encrypting procedure consists of several operations distributed between the frequency and spatial domains, including Magic Square shuffling, Uruk chaotic system confusion, Arnold scrambling, and WAM chaotic diffusion. The initial conditions for chaotic maps are derived from the input image to increase the algorithm's resistance to known plaintext and chosen plaintext attacks. The proposed algorithm utilized two real-value transformations: the Discrete Fourier Transform (DFT), which generates real and imaginary coefficients, and the Discrete Wavelet Transform (DWT), which produces four sub-bands, which posed a significant challenge in retrieving images following the encoding and decoding procedure. Therefore, the contributions of this study are listed below:

- The outcome of executing a medical image encryption algorithm based on chaotic maps in the spatial domain, discrete Fourier domain, and discrete wavelet transform domain has yet to be investigated.
- The proposed algorithm employs two real-value transformations as opposed to a single transformation, which provides a greater depth of confusion processes and thereby improves encryption efficiency while maintaining decryption image quality.
- The proposed algorithm minimizes the impact of chaotic systems' determinism through random selection during generating chaotic systems' initial conditions.

- Random selection increases the sensitivity of the encryption algorithm to the input image and the sensitivity of the algorithm's implementation process, as a completely different image is produced each time the algorithm is executed on the same input image.
- A novel algorithm is proposed for encoding medical images based on multiple keys derived from chaotic multidimensional systems.

The remaining sections of this study are as follows: In Section 2, the discrete wavelet transform, the Arnold transform, and chaos theory are discussed. The objective of Section 3 is to provide a comprehensive description of the proposed medical image encryption algorithm's phases. The outcomes of the proposed method's security tests and analyses are reported and discussed in Sections 4 and 5. The sixth section discusses methodology and outcomes, while Section 7 extracts the study's conclusion.

2 The Related Knowledges

2.1 Discrete Wavelet Transform

Wavelet transformations are a relatively new phenomenon that has captivated researchers in the physical and mathematical sciences with their diverse application potential. Due to connections with multi-rate filtering, quadrature mirror filters, and sub-band coding, wavelet application fields have expanded rapidly over the past few years. It has been utilized by the digital signal processing community to eliminate noisy signals and compress data and images. One of the primary reasons for detecting waveforms and wavelet transforms is that the Fourier transform analysis lacks local information about the signals. Therefore, the Fourier transform cannot be used to analyze signals in the time and frequency domain. As the wavelet transform computes the internal products of a signal with a family of wavelets, a wealth of new mathematical results has been produced. Notable is that the discrete wavelet transform produces very high resolution at low frequencies and low resolution at high frequencies, where low resolution represents a signal's summary, and high resolution means the signal's precise details, both of which are required for signal analysis and representation [16, 17]. In this study, the discrete wavelet transform (DWT) is employed to convert the image to the frequency domain and analyze it into various sub-bands.

2.2 Chaos Theory

A chaotic system is a deterministic system with similar dynamics to a noise signal and is reproduced using nonlinear equations.

2.2.1 URUK chaotic system

Uruk, a chaotic system, has been used to create confusion sequences. Equations (1)–(4) provide the nonlinear equations that characterize the system:

$$\mathrm{X}_{(\mathrm{n}+1)} = 1 - (\mathrm{X_n} \times \mathrm{Y_n} \times \mathrm{Z_n} \times \mathrm{W_n}) - \mathrm{X_n^2} - \mathrm{Y_n^2} - \mathrm{a} \times \tan(\mathrm{Z_n^2}) - \mathrm{W_n^2} \tag{1}$$

$$\mathrm{Y}_{(\mathrm{n}+1)} = \mathrm{X_n} - \mathrm{b} \times \tan(\mathrm{Z_n}) \tag{2}$$

$$\mathrm{Z}_{(\mathrm{n}+1)} = \mathrm{Y_n} - \mathrm{c} \times \tan(\mathrm{Z_n}) \tag{3}$$

$$\mathrm{W}_{(\mathrm{n}+1)} = \mathrm{X_n} - \mathrm{d} \times \mathrm{W_n} \tag{4}$$

Note that a, b, c, and d represent the control parameters; $\mathrm{X_n}$, $\mathrm{Y_n}$, $\mathrm{Z_n}$, and $\mathrm{W_n}$ represent the initial system states of the n-th chaotic iteration; and $\mathrm{X_{n+1}}$, $\mathrm{Y_{n+1}}$, $\mathrm{Z_{n+1}}$, and $\mathrm{W_{n+1}}$ represent the chaotic sequences generated by the URUK system. The presence of trigonometric functions and nonlinear terms in the aforementioned equations has increased the randomness of the discrete Uruk chaotic map, making it ideal for cryptographic and communication security applications [18]. The Uruk system is repeated $\frac{image\ size}{4}$ times to generate four chaotic sequences for performing confusion on the discrete transform wavelet coefficients.

2.2.2 WAM chaotic system

The WAM chaotic system is a 3D map defined as:

$$\mathrm{X_{n+1}} = 1 - \mathrm{a} \times \mathrm{X_n} \times \mathrm{Y_n} - \mathrm{X_n^2} - \mathrm{Y_n^2} - \mathrm{b} \times \sin(\mathrm{Z_n^2}) \tag{5}$$

$$\mathrm{Y_{n+1}} = \mathrm{X_n} \tag{6}$$

$$\mathrm{Z_{n+1}} = \pi - \mathrm{Y_n} - \mathrm{c} \times \sin(\mathrm{Z_n}) \tag{7}$$

$\mathrm{X_n}$, $\mathrm{Y_n}$, and $\mathrm{Z_n}$ represent the initial values of the n-th chaotic iteration, where a, b, and c are the control parameters. Since WAM is a 3D chaotic map, it can reach the chaotic situation efficiently and quickly [19]. This study employs the WAM chaotic map to generate diffusion sequences.

2.2.3 Arnold transform

In 1968, the mathematician V. I. Arnold introduced the Arnold transform (AT), also known as Arnold's cat map. It has been widely implemented in chaos-based image encryption algorithms, where it is used to scramble the original image's pixel positions. Similarly, AT can be expressed as:

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x_i \\ y_i \end{pmatrix} \text{mod (N)} \tag{8}$$

The definition of the inverse Arnold scrambling is:

$$\begin{pmatrix} x_i \\ y_i \end{pmatrix} = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} \text{mod (N)} \tag{9}$$

Where the original image's pixel positions are $(\mathrm{X_i}, \mathrm{Y_i})$ and the scrambled image's pixel coordinates are (X, Y) with a size of $\mathrm{N} \times \mathrm{N}$. After several repetitions, the image will become garbled. The number of iterations depends on the size of the image and is known as the Arnold period [20, 21].

2.3 Magic Square

In mathematics, the magic square is a square matrix containing positive integers. The constant sum is referred to as the magic constant if the sum of the numbers in each row, column, and diagonal is identical [22]. The 16-order magic square utilized in this study is shown in Table 1.

Table 1 16 × 16 magic square

256	2	3	253	252	6	7	249	248	10	11	245	244	14	15	241
17	239	238	20	21	235	234	24	25	231	230	28	29	227	226	32
33	223	222	36	37	219	218	40	41	215	214	44	45	211	210	48
208	50	51	205	204	54	55	201	200	58	59	197	196	62	63	193
192	66	67	189	188	70	71	185	184	74	75	181	180	78	79	177
81	175	174	84	85	171	170	88	89	167	166	92	93	163	162	96
97	159	158	100	101	155	154	104	105	151	150	108	109	147	146	112
144	114	115	141	140	118	119	137	136	122	123	133	132	126	127	129
128	130	131	125	124	134	135	121	120	138	139	117	116	142	143	113
145	111	110	148	149	107	106	152	153	103	102	156	157	99	98	160
161	95	94	164	165	91	90	168	169	87	86	172	173	83	82	176
80	178	179	77	76	182	183	73	72	186	187	69	68	190	191	65
64	194	195	61	60	198	199	57	56	202	203	53	52	206	207	49
209	47	46	212	213	43	42	216	217	39	38	220	221	35	34	224
225	31	30	228	229	27	26	232	233	23	22	236	237	19	18	240
16	242	243	13	12	246	247	9	8	250	251	5	4	254	255	1

3 Medical Image Encryption Algorithm Design

The proposed algorithm employs nested encryption stages to increase the image's resistance to various attacks. This algorithm uses the Discrete Wavelet Transform (DWT) and Discrete Fourier Transform, as well as multiple phases of confusion and diffusion, to encode medical images. The confusion and diffusion phases are based on the keys obtained from two chaotic systems: Uruk and WAM, in addition to two confusion phases based on the Magic Square and Arnold Transform. Multiple confusion stages assist in reducing the close relationship between image elements and enhancing contrast, which positively reflects the image's resistance to statistical attacks. Notably, the parameters of the chaotic Uruk and WAM systems are derived from the grayscale values of the original image, which improves the proposed scheme's sensitivity to the plaintext image.

3.1 Compute Chaos Parameter Values

The proposed medical image encryption algorithm uses randomly chosen pixel values from the original image to generate control parameters for both the WAM and Uruk systems. This process adds a layer of security because the encryption keys change each time the algorithm is executed. Figure 1 depicts the process of dividing the input image into four equal parts prior to the random selection of pixels from each section. The calculation of control parameters includes the subsequent steps:

1. Divides the original image into four equal portions.
2. Randomly selects a single element from each region of the image.
3. Create a one-dimensional vector $\mathrm{P_i}$ from the selected pixels: $\mathrm{P_i} = [\mathrm{P_1}, \mathrm{P_2}, \mathrm{P_3}, \mathrm{P_4}]$

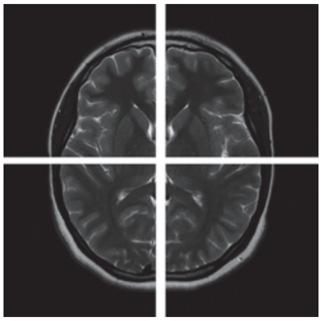


Figure 1 Demonstrates how the original image was divided into four parts.

4. Each value in the P_i vector should be converted to an 8-bit binary representation to obtain P_i'.
5. Creates the 32-bit string b by rearranging the binary values in the vector P'_i.
6. Creates a single decimal number by converting the string b to its decimal representation, as illustrated by the following Equation (10):

$$(b_1 \times 2^0 + b_2 \times 2^1 + b_3 \times 2^2 + \dots) \times 2^{32} \tag{10}$$

7. To obtain the final control parameters, normalize the number obtained from step 6, as shown in Equation (11).

$$\text{Control Parameters} = ub + (lb - ub) \times \sin(R/2^{32}) \tag{11}$$

Where lb is the lower limit of acceptable control parameters for each chaotic system and ub is the upper limit. R is the solution to the expression (10).

3.2 Description of the Proposed Medical Image Encryption Mechanism

Doctors diagnose diseases and make decisions based on medical data; typically, the medical data consists of medical images sent by patients to therapists over a public and open network; therefore, it is crucial to have algorithms that adhere to confidentiality standards. This section describes the proposed encryption algorithm's procedures, illustrated in Figure 2.

Figure 2 summarizes the procedures of the proposed medical image encryption algorithm, which consists of three encryption stages. The first two encryption stages involve implementing confusion operations in two distinct

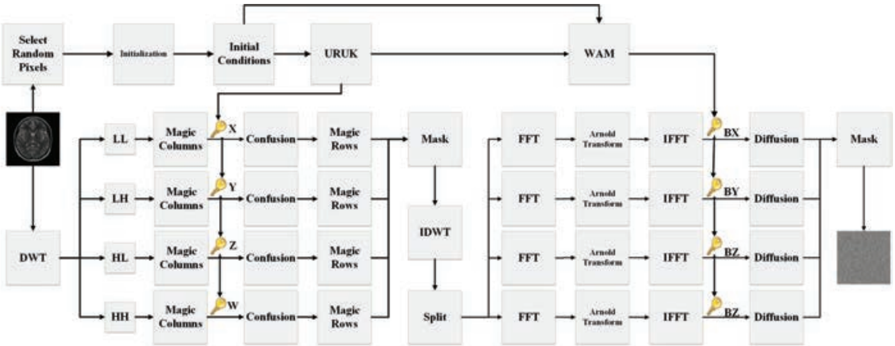


Figure 2 Depicts the proposed medical image encryption algorithm as a block diagram.

domains. The third stage requires diffusion in the spatial domain to provide a high level of security and deterrence against brute force attacks. Initially, the discrete wavelet transform (DWT) is used to separate the sub-bands of the original image, namely [LL, LH, HL, HH]. Then three scrambling operations are performed utilizing the 16×16 magic square shown in Table 1 and the Uruk chaotic system. The frequencies are combined with a custom-made mask, and the inverse discrete wavelet transform (IDWT) is applied. For the second stage of the algorithm, the image is divided into four equal sections in the spatial domain, and each section is transformed into the frequency domain using the Fourier transform. The Fourier coefficients are then shuffled using the Arnold transform; the inverse Fourier transform returns each part to the spatial domain. The algorithm concludes with the propagation process utilizing the bit stream obtained from the WAM system. A mask is used to assemble the four encoded segments into the final encrypted image. Here is a comprehensive description of the recommended encryption method:

1. Input a grayscale medical image A that has the dimensions N × N.
2. Calculate the Uruk and WAM system parameters utilizing the procedure outlined in Section 5.1.
3. The grayscale medical image is decomposed into multiple sub-bands [LL, LH, HL, and HH] by employing the discrete wavelet transform (DWT).
4. Transform the magic square matrix presented in Table 1 into the vector denoted as (q).
5. According to the q vector index, swap the pixel positions in the j^{th} column of each band [LL, LH, HL, and HH] to obtain [LL_1, LH_1, HL_1, and HH_1].
6. The chaotic system 4D-Uruk is iterated $\mathrm{N}/2 \times \mathrm{N}/2 + 1$ times to generate the chaotic sequences [X, Y, Z, and W]. To ensure that the secret key is as random as possible, system parameters are not considered within chaotic sequences.
7. Using chaotic sequences [X, Y, Z, and W] for the confusing process. To generate [X', Y', Z', and W'] index sequences, [X, Y, Z and W] sequences are sorted ascendingly. The vectors [LL_1, LH_1, HL_1, and HH_1] are rearranged using the index sequences [X', Y', Z', and W'] in order to obtain the confused vectors [LL_2, LH_2, HL_2, and HH_2].
8. Swap the pixel positions in the i^{th} row of each band [LL_2, LH_2, HL_2, and HH_2] based on the q vector index to obtain [LL_3, LH_3, HL_3, and HH_3].

9. Using a custom-made mask, combine blended sub-bands to preserve pixel positions.
10. The inverse discrete wavelet transform (IDWT) is used to transform the coefficients resulting from step (9) into the spatial domain.
11. Divides the image produced in step (10) into four equal parts [a, b, c, and d].
12. Each part is converted to the frequency domain using the Fast Fourier Transform (FFT).
13. Using the FFT, each component [a, b, c and d] is transformed into the frequency domain to yield [FA, FB, FC, and FD].
14. Each component of [FA, FB, FC, and FD] is scrambled with a different number of iterations using the Arnold transform to obtain [FA′, FB′, FC′, and FD′].
15. Inverse Fast Fourier Transform (IFFT) is used to transform [FA′, FB′, FC′, and FD′] to the spatial domain, yielding [a′, b′, c′, and d′].
16. The chaotic system 3D-WAM is iterated N/2 × N/2 + 1 times to generate the chaotic bit-stream [BX, BY, and BZ]. To ensure that the secret key is as random as possible, system parameters are not considered within chaotic sequences.
17. To easily implement the diffusion phase, quantify the [a′, b′, c′, and d′] matrices with Equation (12) to obtain the [a'_1, b'_1, c'_1, and d'_1] matrices with elements between (0 and 255).

$$a'_1 = \mathrm{round}\left(255 \times \frac{a' - \min}{\max - \min}\right) \tag{12}$$

18. The elements of the [a′1, b′1, c′1, and d′1] matrices are diffused via XOR computation using WAM’s secret key to produce the [a'_2, b'_2, c'_2, and d'_2] matrices.
19. Using a mask, combine [a'_2, b'_2, c'_2, and d'_2] to produce encrypted image A_2.
20. Output: Encrypted Image A_2.

The mechanism of the proposed image encryption algorithm is depicted in Figure 3.

3.3 Description of the Mechanism for Decryption

Using an inverted implementation of the proposed algorithm, the image is decrypted. First, the WAM and Uruk systems are iterated to generate chaotic sequences and bitstreams based on the encryption system parameters, and the

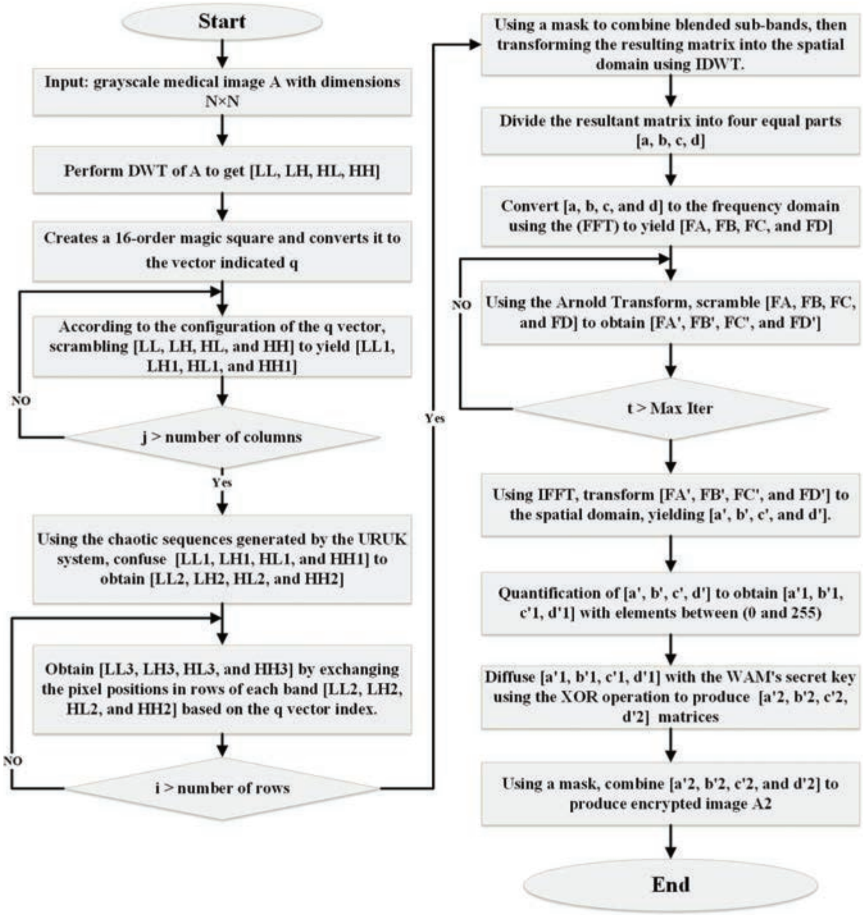

Start
Input: grayscale medical image A with dimensions N×N
Perform DWT of A to get [LL, LH, HL, HH]
Creates a 16-order magic square and converts it to the vector indicated q
According to the configuration of the q vector, scrambling [LL, LH, HL, and HH] to yield [LL1, LH1, HL1, and HH1]
NO
j > number of columns
Yes
Using the chaotic sequences generated by the URUK system, confuse [LL1, LH1, HL1, and HH1] to obtain [LL2, LH2, HL2, and HH2]
Obtain [LL3, LH3, HL3, and HH3] by exchanging the pixel positions in rows of each band [LL2, LH2, HL2, and HH2] based on the q vector index.
NO
i > number of rows
Yes
Using a mask to combine blended sub-bands, then transforming the resulting matrix into the spatial domain using IDWT.
Divide the resultant matrix into four equal parts [a, b, c, d]
Convert [a, b, c, and d] to the frequency domain using the (FFT) to yield [FA, FB, FC, and FD]
NO
Using the Arnold Transform, scramble [FA, FB, FC, and FD] to obtain [FA', FB', FC', and FD']
t > Max Iter
Using IFFT, transform [FA', FB', FC', and FD'] to the spatial domain, yielding [a', b', c', and d'].
Quantification of [a', b', c', d'] to obtain [a'1, b'1, c'1, d'1] with elements between (0 and 255)
Diffuse [a'1, b'1, c'1, d'1] with the WAM's secret key using the XOR operation to produce [a'2, b'2, c'2, d'2] matrices
Using a mask, combine [a'2, b'2, c'2, and d'2] to produce encrypted image A2
End

Figure 3 Depicts the mechanism of the proposed medical image encryption algorithm.

image is then divided into four equal parts. Second, diffusion in the opposite direction is performed separately for each component. Using the Fast Fourier transform, the resulting matrices are converted to the frequency domain, and then the inverse Arnold transform is performed. After performing the Inverse Fast Fourier Transform on the four matrices, they are concatenated into a single matrix and converted back to the frequency domain using the discrete wavelet transform. Using the secret key derived from the Uruk system and the magic square, confusion operations are then performed in reverse. The four matrices are grouped and transformed into the spatial domain using the Inverse Discrete Wavelet Transform to produce the final decoded image.

4 Encryption Quality

Focusing on the quality of the decoded image is crucial in the field of medical image coding due to the fact that coding in the frequency domain can affect image quality, so the appearance of any unwanted sign on the image can lead to a false diagnosis, putting human life at risk.

4.1 Mean Squared Error (MSE)

MSE is calculated to evaluate the differences between the original and decrypted images. MSE should be as low as possible, and slight variations indicate decrypted image quality and the efficacy of the encryption algorithm. The MSE is determined as (13).

$$MSE = \frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left[f(x,y)_r - f(x,y)_p\right]^2 \tag{13}$$

Where $f(x, y)_r$ is the decrypted image and $f(x, y)_p$ is the input image. M and N represent the dimensions of the images, while x and y represent pixel coordinates [23, 24].

4.2 The Root Means Square Error (RMSE)

RMSE is also referred to as the root mean square deviation (RMSD). It provides information regarding the efficacy of encryption algorithms in restoring image quality following decoding. The low result indicates the model's high performance [25]. Calculating the RMSE is as follows (14):

$$\text{RMSE} = \sqrt{\frac{1}{M \times N} \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} \left[f(x,y)_r - f(x,y)_p\right]^2} \tag{14}$$

$$\text{RMSE} = \sqrt{MSE} \tag{15}$$

4.3 Peak Signal to Noise Ratio (PSNR)

By validating the degree of similarity between the input image and the decrypted image, PSNR is widely utilized as a metric for measuring the performance of encryption algorithms. Notably, the higher the PSNR level, the greater the similarity between the original and decoded images

[11, 23, 26–28]. It is mathematically expressed by Equation (16):

$$PSNR = 10 \times log_{10}\left(\frac{255^2}{MSE}\right) \tag{16}$$

The PSNR test results in Table 2 indicate that the proposed encryption algorithm is highly efficient.

4.4 The Mean Structural Similarity Index (MSSIM)

MSSIM is one of the essential metrics for assessing the performance of an image encryption algorithm, as it measures the degree of similarity between the original and decrypted images based on contrast, brightness, and resolution. The closer the MSSIM value is to 1, the greater the similarity between images, indicating a successful decoding effect. In contrast, the MSSIM value approaches zero for images with higher contrast [28–31]. Table 2 displays the MSSIM test results on both the proposed algorithm's input and decrypted images, demonstrating competitive performance and results.

5 Security Analysis of the Proposed Algorithm

Several experimental analyses were performed on a standard 512 × 512 images downloaded from the Medical Image Dataset (Brain Tumor MRI Dataset) using the link https://www.kaggle.com/datasets/masoudnickparvar/brain-tumor-mri-dataset?select=Training. The proposed image encryption scheme's primary feature is its compatibility with various digital image formats (medical, non-medical, and grayscale).

5.1 Evaluation of Image Entropy

In 1949, Claude E. Shannon, a mathematician, announced a mathematical formula for assessing the effectiveness of an image coding algorithm. Its resistance to entropy attacks is determined by the amount of randomness within the encrypted image. The entropy value of the encrypted image ranges from 0 to 8 because the maximum value of a pixel, as described by its 8-bit binary representation, is 255. Close test results to 8 indicate the efficacy of the encryption algorithm and the image's high level of randomness [7, 19, 32–34]. Entropy can be calculated using the (17) mathematical equation:

$$IE(S) = -\sum P(S) \times Log_2\, P(S) \tag{17}$$

Table 2 Information entropy results for the medical image encryption algorithm

Image Name	Entropy	PSNR	MSE	RMSE	MSSIM
Brain	7.9994	40.7593	5.2791	2.2976	0.9883
No Tumor 1	7.9993	53.4262	0	0	0.9911
No Tumor 2	7.9993	55.4189	0	0	0.9963
Glioma Tumor 1	7.9993	54.2255	0	0	0.9984
Glioma Tumor 2	7.9993	58.2924	0	0	0.9991
Meningioma 1	7.9994	55.3736	0	0	0.9972
Meningioma 2	7.9993	56.4462	0	0	0.9972
Pituitary Tumor 1	7.9993	56.6548	0	0	0.9984
Pituitary Tumor 2	7.9993	55.8948	0	0	0.9989
Colon	7.9993	54.0273	0	0	0.9913
Chest	7.9994	53.3395	0	0	0.9981

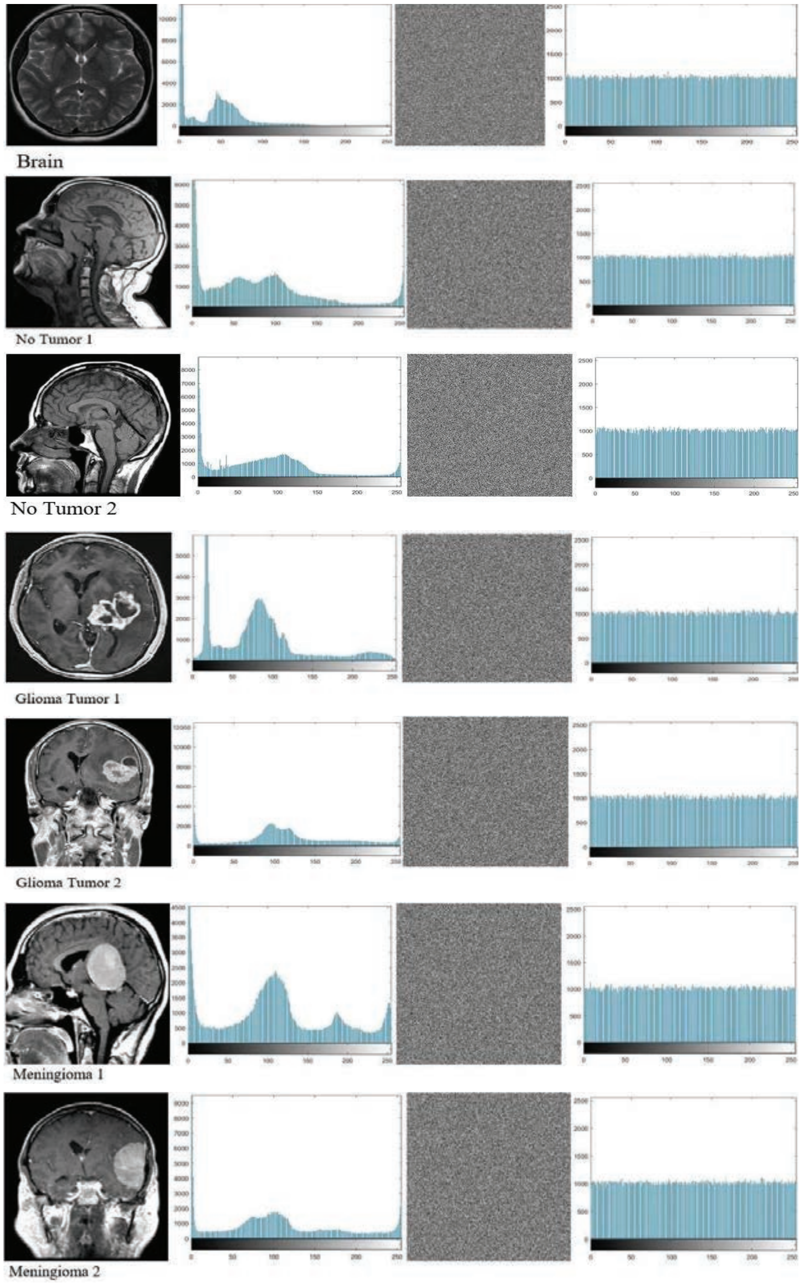
Table 3 The proposed algorithm's entropy test is compared to others

Image	Ref. [1]	Ref. [11]	Ref. [14]	Ref. [35]	Ref. [36]	Ref. [37]	Proposed
Colon	–	7.9979	–	7.9944	–	–	7.9993
Chest	7.9995	–	–	–	7.9987	–	7.9994
NoTumor2	–	–	–	–	7.9987	–	7.9993
Average	7.9991	7.9972	7.9974	7.9877	7.9986	7.9955	7.9993

The results presented in Table 2 indicate that the proposed algorithm has a robust cipher effect and that encrypted images can withstand an entropy attack. Table 3 compares the entropy test results of the proposed algorithm to those of other algorithms.

5.2 Histogram Analysis

A histogram is an analytical tool that represents grayscale levels on the horizontal axis and pixel density on the vertical axis to provide a comprehensive statistical description of an image's content. Notably, histogram columns for encrypted images tend to have a uniform distribution to prevent attackers from discerning the encrypted content, as opposed to the different headers of histogram columns describing normal image content [19, 21, 24, 38, 39]. Figure 4 illustrates the effect of the proposed encryption algorithm on the test images, where the regularity of the graph columns of the encrypted images indicates the algorithm's resistance to statistical attacks.



Brain

No Tumor 1

No Tumor 2

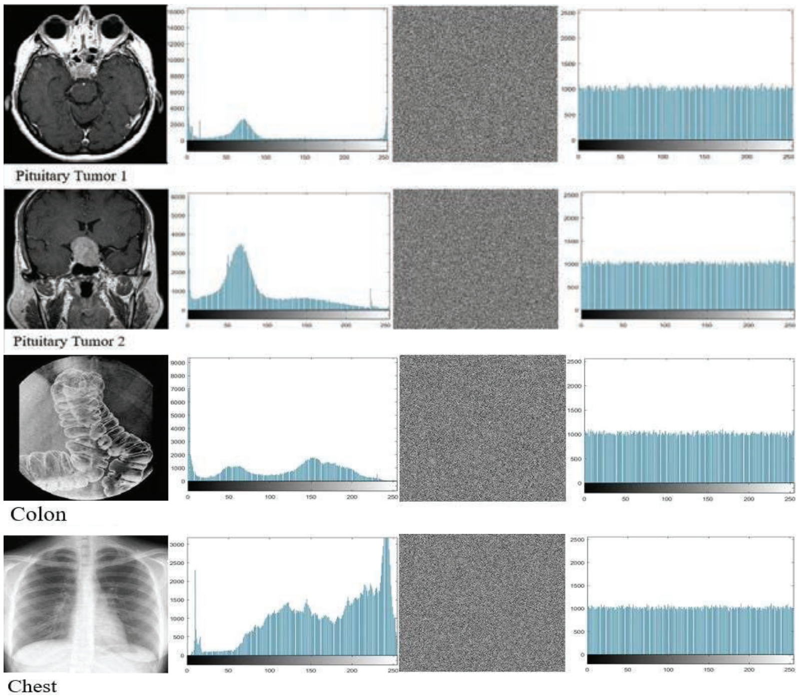
Glioma Tumor 1

Glioma Tumor 2

Meningioma 1

Meningioma 2

Figure 4 Continued


Pituitary Tumor 1

Pituitary Tumor 2

Colon

Chest

Figure 4 Histograms accompany both the unencrypted and encrypted images.

5.3 Security Analysis of Correlation Between Adjacent Pixels

The statistical dependence between adjacent pixels is one of the inherent properties of meaningful images, as the value of any pixel can be predicted based on the value of its neighbors. The decoherence of the encoded image's pixels demonstrates the effect of the confusion phase of the encryption algorithm. In order to resist statistical attacks, an effective encryption algorithm must achieve a correlation coefficient close to zero between adjacent pixels of the encrypted image [1, 5, 40, 41]. The statistical relationship between image pixels before and after encryption is depicted in Figures 5 and 6. In the original images, certain regions contain blocks of pixels, indicating a strong correlation between image elements. In the encoded image, pixels are dispersed throughout the expressive graphic, indicating that the statistical correlation between adjacent pixels has been severely disrupted. In addition, Table 4 summarizes the findings of the correlation coefficient test in all directions for plaintext and encoded images, which were compared to the correlation coefficient tests of other algorithms given in Table 5.

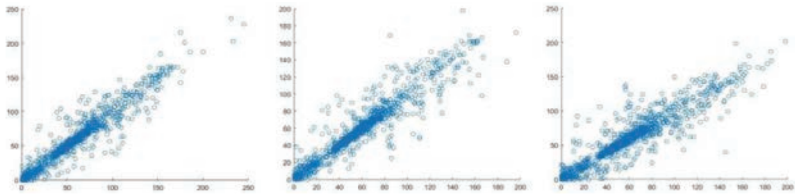


Figure 5 Displays the correlation coefficients for 3000 randomly selected pixels in the plaintext brain image's vertical, horizontal, and diagonal directions, respectively.

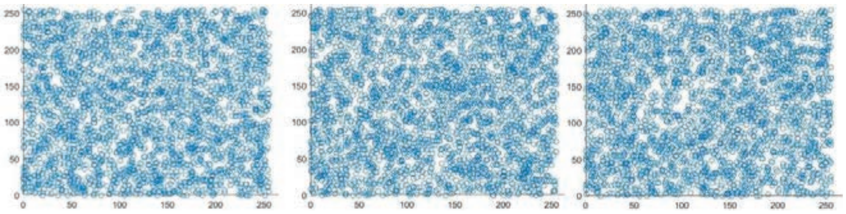


Figure 6 Represents the correlation coefficients for 3000 randomly selected pixels in the encrypted brain image's vertical, horizontal, and diagonal directions, respectively.

Table 4 Correlation Coefficients test results for plain and encrypted images

Direction	Vertical		Horizontal		Diagonal	
Image Type	Plain	Cipher	Plain	Cipher	Plain	Cipher
Brain	0.9808	−0.0098	0.9756	−0.0062	0.9644	−0.0023
No Tumor 1	0.9880	−0.0111	0.9886	−0.0197	0.9756	0.0018
No Tumor 2	0.9842	−0.0390	0.9811	−0.0036	0.9634	0.0051
Glioma Tumor 1	0.9813	−0.0378	0.9826	−0.0235	0.9621	0.0038
Glioma Tumor 2	0.9883	−0.0410	0.9888	−0.0378	0.9830	−0.0015
Meningioma 1	0.9901	0.0070	0.9891	−0.0145	0.9812	−0.0184
Meningioma 2	0.9950	−0.0038	0.9952	−0.0073	0.9918	−0.0171
Pituitary Tumor 1	0.9900	−0.0143	0.9881	0.0018	0.9785	−0.0025
Pituitary Tumor 2	0.9532	−0.0224	0.9471	0.0080	0.9240	−0.0218
Colon	0.9933	0.0002	0.9939	0.0054	0.9870	−0.0065
Chest	0.9977	0.0077	0.9969	0.0065	0.9960	−0.0035

Tests and comparisons revealed that the proposed encryption algorithm is extraordinarily effective at thwarting the statistical correlation.

5.4 Robustness Against Differential Attack

The Number of Pixel Change Rate (NPCR) and the Unified Average Changing Intensity (UACI) are widely utilized metrics for evaluating the sensitivity

Table 5 Compares the Correlation Coefficients test results of the proposed encryption algorithm with those of other algorithms

Image	Ref.	Vertical	Horizontal	Diagonal
Colon	**Ref. [35]**	0.0016	−0.0032	−0.0029
	Ref. [11]	0.0053	0.0069	0.0030
	Proposed	0.0002	0.0054	−0.0065
Chest	**Ref. [36]**	0.0092	0.0182	0.0051
	Ref. [1]	0.0007	0.0023	−0.0008
	Proposed	0.0077	0.0065	−0.0035
No Tumor 2	**Ref. [36]**	0.0104	0.0128	0.0095
	Proposed	−0.0390	−0.0036	0.0051
Average	**Ref. [10]**	0.002396	0.08596	0.02038
	Ref. [12]	−0.00004	−0.00028	−0.00128
	Ref. [14]	0.009783	0.0136	−0.00333
	Ref. [37]	0.000113	−0.0012	−0.00702
	Proposed	−0.01494	−0.00826	−0.00572

of an encryption algorithm to minor changes in a plaintext image. A differential attack is when an attacker attempts to determine the secret key and the cryptographic system by tracing the relationships between the plaintext and encrypted images. Therefore, one of the most critical objectives of practical encryption algorithms is to produce a significant change in the encrypted image in response to a slight change in the original image [19, 21, 23, 34, 42, 43]. The mathematical formulas (18) and (19) respectively determine the resistance of the encryption algorithm to differential attacks.

$$\mathrm{NPCR} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \mathrm{image(i,j)} \times 100\% \tag{18}$$

$$\mathrm{UACI} = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{\mathrm{Encrypted1} - \mathrm{Encrypted2}}{255} \times 100\% \tag{19}$$

The outcomes of the robustness test of the proposed algorithm, NPCR, and UACI, are displayed in Table 6. These results indicate that the proposed encryption model can resist differential attacks.

5.5 Key Sensitivity Analysis

The proposed algorithm's derivation of secret keys is based on two chaotic systems, WAM and Uruk. Due to the extreme sensitivity of both chaotic

Table 6 Number of pixels change rate and unified average changing intensity data

Image Type	NPCR	UACI
Brain	99.62	33.41
No Tumor 1	99.61	33.50
No Tumor 2	99.61	33.38
Glioma Tumor 1	99.60	33.38
Glioma Tumor 2	99.59	33.42
Meningioma 1	99.61	33.39
Meningioma 2	99.62	33.53
Pituitary Tumor 1	99.61	33.51
Pituitary Tumor 2	99.60	33.58
Colon	99.61	33.48
Chest	99.63	33.47

Table 7 Provides a comparison of the NPCR and UACI values of the proposed method with those of other algorithms

	Colon		Chest		Average	
Image	NPCR	UACI	NPCR	UACI	NPCR	UACI
Ref. [1]	–	–	99.62	33.65	99.61	33.51
Ref. [11]	99.58	33.42	–	–	99.61	33.43
Ref. [10]	–	–	–	–	99.14	32.54
Ref. [12]	–	–	–	–	99.59	34.27
Ref. [14]	–	–	–	–	99.61	32.05
Ref. [35]	99.13	33.68	–	–	99.60	33.47
Ref. [37]					99.61	33.48
Proposed	99.61	33.48	99.63	33.47	99.61	33.46

systems to the control parameters, it is anticipated that different secret keys will be generated in response to a slight change in initial conditions. In order to assess the sensitivity of chaotic sequences on the performance of the proposed model, the decryption key was derived by modifying the tenth order after sorting for one of the prime values in each chaotic system. Figure 7 depicts the outcomes of two attempts to decrypt the brain image using a key derived from the WAM and Uruk systems, with initial values slightly modified.

5.6 Evaluation of Robustness Against Noise Attack

Due to the fact that medical images are transmitted via open public channels, they are susceptible to various forms of noise pollution. The 512 × 512

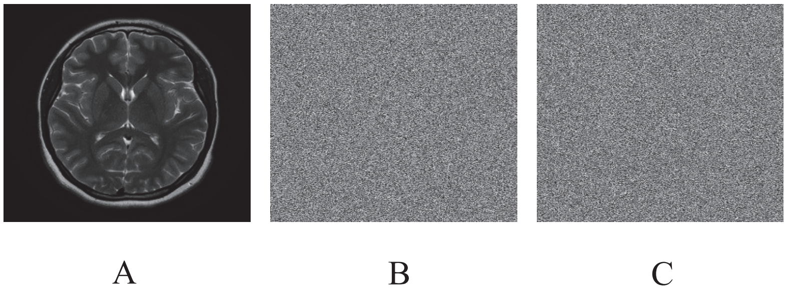


Figure 7 Illustrates an unsuccessful attempt to decrypt a 512 × 512 Brain image with a different encryption key derived from modified control parameters (a) A standard image, (b) decrypting the image with the modified Uruk initial condition, and (c) decrypting image with the modified WAM initial condition.

Table 8 Presents the PSNR and noise intensity added to images of Brain and Meningioma1

Noise	Image	Original	0.000001	0.000003	0.000005	0.000007
Salt and pepper	Brain	40.7593	39.5010	38.6669	38.6247	38.6225
	Meningioma1	55.3736	55.3400	55.2699	54.5283	52.1292
Noise	Image	Original	0.000001	0.000002	0.000003	0.000004
Speckle	Brain	40.7593	39.9507	39.1674	36.0300	34.6427
	Meningioma1	55.3736	55.3603	47.2576	38.9835	36.6367

Brain test image was utilized to evaluate the algorithm's security performance against Salt and Pepper Noise (SPN) and Speckle Noise (SN) attacks. On the basis of the PSNR and noise intensity values presented in Table 8, it can be concluded that the model is resistant to noise pollution attacks. In contrast, as depicted in Figure 8, the images obtained after decoding remain distinct and recognizable by the human eye despite the assaults of noise pollution.

5.7 Examination of Robustness Against Occlusion Attack

An efficient encryption algorithm must be highly resistant to Occlusion attacks in order to avoid their detrimental effects on the image content during decryption. To evaluate the algorithm's resistance to Occlusion attacks, it was assumed that a 512-by-512 brain image was subjected to Occlusion attacks of varying intensities and that the image used for decryption contained missing data. Figure 9 demonstrates the ability of the proposed encryption algorithm to thwart the Occlusion attack and mitigate its negative impact, as slight effects of the blockage attack can be seen on the decrypted images. Still, they remain legible to the human eye.

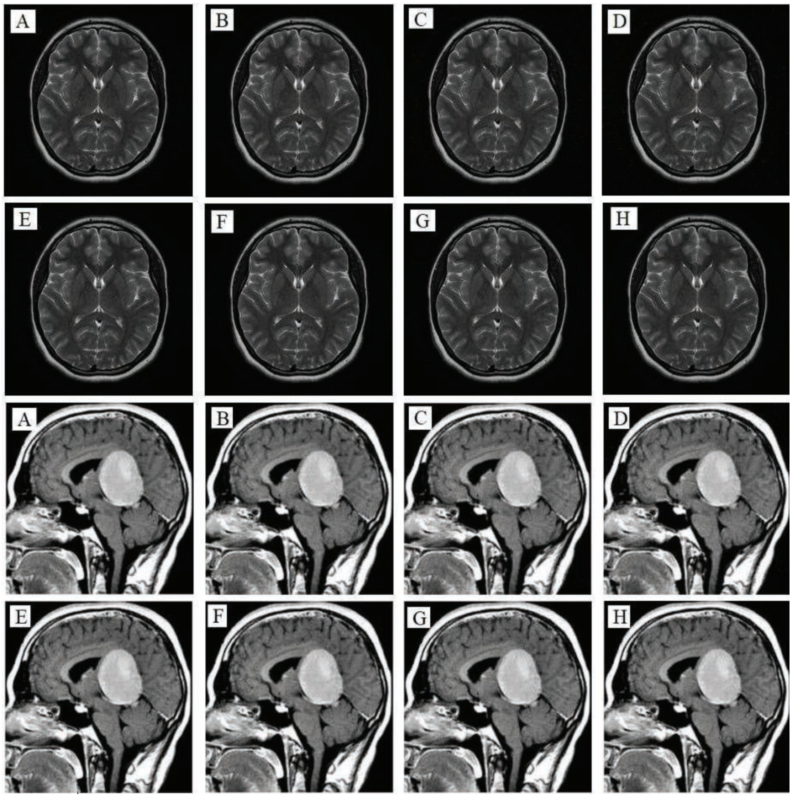


Figure 8 Depicts the outcome of the noise attacks test on Brain, and Meningioma 1 images, where (A)–(D) are the decrypted images after adding Speckle Noise with intensities of 0.000001, 0.000002, 0.000003, and 0.000004, respectively, and (E)–(H) are the decrypted images after adding Salt and Pepper Noise with intensities of 0.00001, 0.00003, 0.0005, and 0.0007, respectively.

5.8 Evaluate the Execution Time

As depicted in Figure 2, the proposed algorithm comprises three stages: the confusion stage in the domain of discrete wavelet transform, the scrambling stage in the domain of fast Fourier transform, and the diffusion stage in the spatial domain. A 512 × 512 brain image was used as a test image to determine the execution time. The generation of secret keys and execution of the initial stage consume 0.43 seconds, or 4.20% of the total execution time. While the second stage of implementing the Arnold transform in the domain of the Fast Fourier Transform consumes the most time, as it requires 8.10 seconds or 79.26% of the overall execution time. In contrast, the diffusion

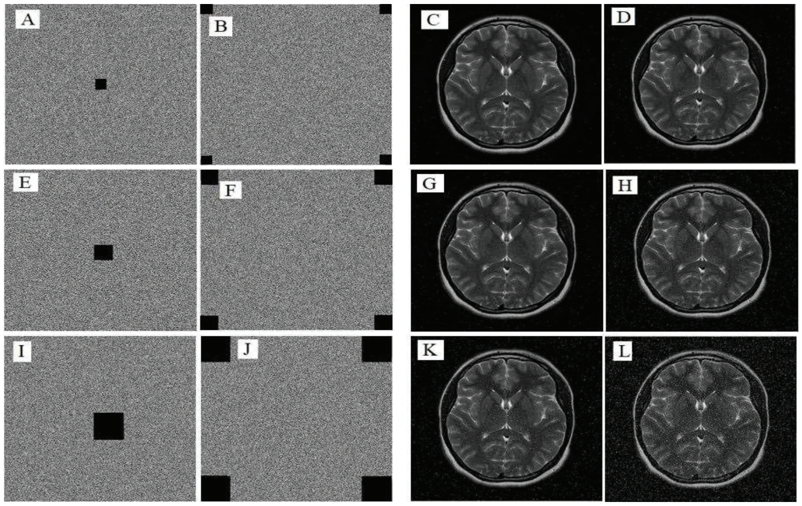


Figure 9 Depicts the outcomes of occlusion attacks on the medical brain image, where (A, B) are encrypted images with loss data sizes 16 × 16 pixels per square, (C, D) are the decrypted images with PSNR of 34.0479 and 29.3971, respectively, (E, F) are encrypted images with loss data sizes 32 × 32 pixel per square, (G, H) are the decrypted images with PSNR of 29.2848 and 23.9673, respectively, (I, J) are encrypted images with loss data sizes 64 × 64 pixel per square, and (K, L) are the decrypted images with PSNR of 23.7947 and 17.9201, respectively.

phase and the quantifying values up to the final encrypted image take up only 1.69 seconds or 16.54% of the total time. Therefore, the total execution time of the proposed algorithm is 10.22 seconds.

6 Discussion of Methods and Results

All Performance Evaluations were conducted under identical conditions with the same hardware, Lenovo Windows 10 Pro; Intel(R) Core (TM) i7-10750H CPU @ 2.60GHz 2.59GHz, RAM: 16GB. To increase the encrypted image's resistance to potential attacks, sub-operations of the proposed encryption algorithm were implemented in the Discrete Wavelet Transform domain, the Fast Fourier Transform domain, and the spatial domain. Extensive security analyses and performance tests demonstrate that the proposed model is highly secure, provides excellent encryption efficiency and that the decrypted images closely resemble the input images. The statistical correlation coefficient test between neighboring pixels also demonstrated the efficacy of the proposed algorithm's encryption effect, as the majority of results were very close to zero, the ideal value for this test, indicating the destruction of the correlation between the image's components. Due to the regularity and flatness of its columns, histogram analysis revealed that the attacker's ability to benefit from statistical information was diminished in addition to the entropy test results, which were extremely close to the ideal value. The noise pollution tests and the analysis of occlusion attacks revealed that the proposed algorithm could recover the image's fine details despite a certain percentage of noise or data loss. Moreover, comparisons with other algorithms revealed the proposed encryption algorithm's remarkable superiority. Therefore, it is anticipated that this algorithm will satisfy the requirements of real-world applications.

7 Conclusion

This paper proposes a medical image encryption model based on the Discrete Wavelet Transform domain, the Fast Fourier Transform domain, and the spatial domain to provide efficient transmission security for medical images. For specific encryption operations, Uruk and magic square maps were used to confuse the image in the DWT domain based on the secret keys used in each sub-band. Next, the Arnold transform was applied to scramble the image in the FFT domain, and finally, the WAM map was implemented to generate a bit stream that was used to diffuse the scrambled image. Experiments demonstrate that the proposed algorithm can withstand common attacks, adhere to security standards, and generate high-quality images following decryption operations. Despite the complexity of the frequency domain encryption procedure, the proposed scheme has the benefits of rapid implementation, enhanced security, and high encryption efficiency. At the same time, comparing the proposed algorithm's performance to other algorithms revealed its marked superiority. In addition, control parameters for chaotic systems are derived using random pixels from the input image, which reduces the influence of chaotic system determinism and increases the algorithm's resistance to known plaintext and chosen plaintext attacks.

Acknowledgments

In conclusion, the authors would like to express their gratitude and appreciation to the reviewers and editors for their insightful comments and suggestions, which significantly enhanced the research

Availability of Data and Materials

This section is irrelevant to this study.

Competing Interests

The authors declare that they have no personal or financial relationships that could have influenced the research presented in this article.

Funding

Financial support is irrelevant to this paper.

Authors' Contributions

Prof. Waleed Ameen Mahmoud Al-Jawher	Supervisor
Ali Akram Abdul-Kareem	PhD Student

References

[1] F. Masood, M. Driss, W. Boulila, J. Ahmad, S. U. Rehman, S. U. Jan, A. Qayyum, W. J. Buchanan. "A Lightweight Chaos-Based Medical Image Encryption Scheme Using Random Shuffling and XOR Operations," *Wireless Personal Communications*, May 2021, **Published**, doi: 10.1007/s11277-021-08584-z.

[2] W. El-Shafai, F. Khallaf, E.-S. M. El-Rabaie, and F. E. A. El-Samie, "Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 10, pp. 9007–9035, Mar. 2021, doi: 10.1007/s12652-020-02597-5.

[3] M. Boussif, N. Aloui, and A. Cherif, "Securing DICOM images by a new encryption algorithm using Arnold transform and Vigenère cipher," *IET Image Processing*, vol. 14, no. 6, pp. 1209–1216, Apr. 2020, doi: 10.1049/iet-ipr.2019.0042.

[4] A. Pourjabbar Kari, A. Habibizad Navin, A. M. Bidgoli, and M. Mirnia, "A new image encryption scheme based on hybrid chaotic maps," *Multimedia Tools and Applications*, vol. 80, no. 2, pp. 2753–2772, Sep. 2020, doi: 10.1007/s11042-020-09648-1.

[5] H. A. Abdullah, H. N. Abdullah, and W. A. Mahmoud Al-Jawher, "A hybrid chaotic map for communication security applications," *International Journal of Communication Systems*, vol. 33, no. 4, p. e4236, Nov. 2019, doi: 10.1002/dac.4236.

[6] A. B. Joshi, D. Kumar, D. C. Mishra, and V. Guleria, "Colour-image encryption based on 2D discrete wavelet transform and 3D logistic chaotic map," *Journal of Modern Optics*, vol. 67, no. 10, pp. 933–949, Jun. 2020, doi: 10.1080/09500340.2020.1789233.

[7] A. Shafique, J. Ahmed, M. U. Rehman, and M. M. Hazzazi, "Noise-Resistant Image Encryption Scheme for Medical Images in the Chaos and Wavelet Domain," *IEEE Access*, vol. 9, pp. 59108–59130, 2021, doi: 10.1109/access.2021.3071535.

[8] D. Ravichandran, P. Praveenkumar, J. B. Balaguru Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing DICOM image," *Computers in Biology and Medicine*, vol. 72, pp. 170–184, May 2016, doi: 10.1016/j.compbiomed.2016.03.020.

[9] M. Guan, X. Yang, and W. Hu, "Chaotic image encryption algorithm using frequency-domain DNA encoding," *IET Image Processing*, vol. 13, no. 9, pp. 1535–1539, Jun. 2019, doi: 10.1049/iet-ipr.2019.0051.

[10] S. Kumar, B. Panna, and R. K. Jha, "Medical image encryption using fractional discrete cosine transform with chaotic function," *Medical & Biological Engineering & Computing*, vol. 57, no. 11, pp. 2517–2533, Sep. 2019, doi: 10.1007/s11517-019-02037-3.

[11] A. Banu S and R. Amirtharajan, "A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach," *Medical & Biological Engineering & Computing*, vol. 58, no. 7, pp. 1445–1458, Apr. 2020, doi: 10.1007/s11517-020-02178-w.

[12] S. Jeevitha and N. Amutha Prabha, "Novel medical image encryption using DWT block-based scrambling and edge maps," *Journal of Ambient Intelligence and Humanized Computing*, vol. 12, no. 3, pp. 3373–3388, Aug. 2020, doi: 10.1007/s12652-020-02399-9.

[13] D. Ravichandran, A. Banu S, B. K. Murthy, V. Balasubramanian, S. Fathima, and R. Amirtharajan, "An efficient medical image encryption using hybrid DNA computing and chaos in transform domain," *Medical & Biological Engineering & Computing*, vol. 59, no. 3, pp. 589–605, Feb. 2021, doi: 10.1007/s11517-021-02328-8.

[14] W. El-Shafai, F. Khallaf, E.-S. M. El-Rabaie, and F. E. A. El-Samie, "Robust medical image encryption based on DNA-chaos cryptosystem for secure telemedicine and healthcare applications," *Journal of Ambient*

Intelligence and Humanized Computing, vol. 12, no. 10, pp. 9007–9035, Mar. 2021, doi: 10.1007/s12652-020-02597-5.

[15] X. Meng, J. Li, X. Di, Y. Sheng, and D. Jiang, "An Encryption Algorithm for Region of Interest in Medical DICOM Based on One-Dimensional eλ-cos-cot Map," *Entropy*, vol. 24, no. 7, p. 901, Jun. 2022, doi: 10.3390/e24070901.

[16] L. Debnath and F. A. Shah, "Lecture Notes on Wavelet Transforms," *Compact Textbooks in Mathematics*, 2017, **Published**, doi: 10.1007/978-3-319-59433-0.

[17] Brunton, S., & Kutz, J. "Fourier and Wavelet Transforms," *Data-Driven Science and Engineering*, pp. 47–83, Jan. 2019, doi: 10.1017/9781108380690.003.

[18] A. A. Abdul-Kareem and W. A. Mahmoud Al-Jawher, "URUK 4D Discrete Chaotic Map for Secure Communication Applications," *Journal Port Science Research*, vol. 5, no. 3, pp. 131–142, Oct. 2022, doi: 10.36371/port.2022.3.2.

[19] Ali Akram Abdul-Kareem, Prof. Waleed Ameen Mahmoud Al-Jawher (2022) "WAM 3D Discrete Chaotic Map for Secure Communication Applications", International Laser Technology and Optics Symposium 2022 (iLATOS2022) that will be held on 21st and 22nd of September 2022.

[20] W.-W. Hu, R.-G. Zhou, J. Luo, S.-X. Jiang, and G.-F. Luo, "Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms," *Quantum Information Processing*, vol. 19, no. 3, Jan. 2020, doi: 10.1007/s11128-020-2579-9.

[21] V. Guleria, S. Sabir, and D. C. Mishra, "Security of multiple RGB images by RSA cryptosystem combined with FrDCT and Arnold transform," *Journal of Information Security and Applications*, vol. 54, p. 102524, Oct. 2020, doi: 10.1016/j.jisa.2020.102524.

[22] J. Wang and L. Liu, "A Novel Chaos-Based Image Encryption Using Magic Square Scrambling and Octree Diffusing," *Mathematics*, vol. 10, no. 3, p. 457, Jan. 2022, doi: 10.3390/math10030457.

[23] Z. Bashir, N. Iqbal, and M. Hanif, "A novel gray scale image encryption scheme based on pixels' swapping operations," *Multimedia Tools and Applications*, vol. 80, no. 1, pp. 1029–1054, Sep. 2020, doi: 10.1007/s11042-020-09695-8.

[24] L. S. Khan, M. M. Hazzazi, M. Khan, and S. S. Jamal, "A novel image encryption based on rossler map diffusion and particle swarm optimization generated highly non-linear substitution boxes,"

Chinese Journal of Physics, vol. 72, pp. 558–574, Aug. 2021, doi: 10.1016/j.cjph.2021.03.029.

[25] O. A. Kozhemyak and O. V. Stukach, “Reducing the Root-Mean-Square Error at Signal Restoration using Discrete and Random Changes in the Sampling Rate for the Compressed Sensing Problem,” *2021 International Siberian Conference on Control and Communications (SIBCON)*, May 2021, **Published**, doi: 10.1109/sibcon50419.2021.9438937.

[26] N. Khalil, A. Sarhan, and M. A. M. Alshewimy, “An efficient color/grayscale image encryption scheme based on hybrid chaotic maps,” *Optics & Laser Technology*, vol. 143, p. 107326, Nov. 2021, doi: 10.1016/j.optlastec.2021.107326.

[27] M. Ghazvini, M. Mirzadi, and N. Parvar, “A modified method for image encryption based on chaotic map and genetic algorithm,” *Multimedia Tools and Applications*, vol. 79, no. 37–38, pp. 26927–26950, Jun. 2020, doi: 10.1007/s11042-020-09058-3.

[28] Y. Luo, Y. Liang, S. Zhang, J. Liu, and F. Wang, “An image encryption scheme based on block compressed sensing and Chen system?,” May 2022, **Published**, doi: 10.21203/rs.3.rs-1604114/v1.

[29] Q. Xu, K. Sun, C. Cao, and C. Zhu, “A fast image encryption algorithm based on compressive sensing and hyperchaotic map,” *Optics and Lasers in Engineering*, vol. 121, pp. 203–214, Oct. 2019, doi: 10.1016/j.optlaseng.2019.04.011.

[30] H. Hu, Y. Cao, J. Xu, C. Ma, and H. Yan, “An Image Compression and Encryption Algorithm Based on the Fractional-Order Simplest Chaotic Circuit,” *IEEE Access*, vol. 9, pp. 22141–22155, 2021, doi: 10.1109/access.2021.3054842.

[31] K. Wang, X. Wu, and T. Gao, “Double color images compression–encryption via compressive sensing,” *Neural Computing and Applications*, vol. 33, no. 19, pp. 12755–12776, Jun. 2021, doi: 10.1007/s00521-021-05921-y.

[32] M. U. Rehman, A. Shafique, S. Khalid, and I. Hussain, “Dynamic Substitution and Confusion-Diffusion-Based Noise-Resistive Image Encryption Using Multiple Chaotic Maps,” *IEEE Access*, vol. 9, pp. 52277–52291, 2021, doi: 10.1109/access.2021.3069591.

[33] M. Hanif, R. A. Naqvi, S. Abbas, M. A. Khan, and N. Iqbal, “A Novel and Efficient 3D Multiple Images Encryption Scheme Based on Chaotic Systems and Swapping Operations,” *IEEE Access*, vol. 8, pp. 123536–123555, 2020, doi: 10.1109/access.2020.3004536.

[34] S. Patel, V. Thanikaiselvan, D. Pelusi, B. Nagaraj, R. Arunkumar, and R. Amirtharajan, “Colour image encryption based on customized neural

network and DNA encoding," *Neural Computing and Applications*, vol. 33, no. 21, pp. 14533–14550, May 2021, doi: 10.1007/s00521-021-06096-2.

[35] J. Chandrasekaran and S. J. Thiruvengadam, "A Hybrid Chaotic and Number Theoretic Approach for Securing DICOM Images," *Security and Communication Networks*, vol. 2017, pp. 1–12, 2017, doi: 10.1155/2017/6729896.

[36] H. Nematzadeh, R. Enayatifar, H. Motameni, F. G. Guimarães, and V. N. Coelho, "Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices," *Optics and Lasers in Engineering*, vol. 110, pp. 24–32, Nov. 2018, doi: 10.1016/j.optlaseng.2018.05.009.

[37] K. N. Singh, O. P. Singh, A. K. Singh, and A. K. Agrawal, "EiMOL: A Secure Medical Image Encryption Algorithm based on Optimization and the Lorenz System," *ACM Transactions on Multimedia Computing, Communications, and Applications*, Sep. 2022, **Published**, doi: 10.1145/3561513.

[38] Y. Pourasad, R. Ranjbarzadeh, and A. Mardani, "A New Algorithm for Digital Image Encryption Based on Chaos Theory," *Entropy*, vol. 23, no. 3, p. 341, Mar. 2021, https://doi:10.3390/e23030341.

[39] X. Wang, N. Guan, and J. Yang, "Image encryption algorithm with random scrambling based on one-dimensional logistic self-embedding chaotic map," *Chaos, Solitons & Fractals*, vol. 150, p. 111117, Sep. 2021, doi: 10.1016/j.chaos.2021.111117.

[40] A. Shafique and F. Ahmed, "Image Encryption Using Dynamic S-Box Substitution in the Wavelet Domain," *Wireless Personal Communications*, vol. 115, no. 3, pp. 2243–2268, Aug. 2020, doi: 10.1007/s11277-020-07680-w.

[41] H. Wen et al., "Design and Embedded Implementation of Secure Image Encryption Scheme Using DWT and 2D-LASM," *Entropy*, vol. 24, no. 10, p. 1332, Sep. 2022, doi: 10.3390/e24101332.

[42] A. Momeni Asl, A. Broumandnia, and S. J. Mirabedini, "Scale Invariant Digital Color Image Encryption Using a 3D Modular Chaotic Map," *IEEE Access*, vol. 9, pp. 102433–102449, 2021, doi: 10.1109/access.2021.3096224.

[43] Ö. Kasim, "Secure medical image encryption with Walsh–Hadamard transform and lightweight cryptography algorithm," *Medical & Biological Engineering & Computing*, vol. 60, no. 6, pp. 1585–1594, Apr. 2022, doi: 10.1007/s11517-022-02565-5.

Biographies

Ali Akram Abdul-Kareem earned a Bachelor from Middle Technical University in Baghdad, Iraq, in 2011 and a Master of Science in Computer Science from Middle East University in Amman, Jordan, in 2016. Currently, he is a Ph.D. candidate at the Iraqi Commission for Computers and Informatics, Information Institute for Postgraduate Studies in Baghdad, Iraq, and a Computer Programmer at Al Rafidain Bank in Baghdad, Iraq. He has more than ten years of experience implementing banking information systems projects. His research interests are image encryption, chaos, compressive sensing, and optimization algorithms.

Waleed Ameen Mahmoud Al-Jawher: President Assistance for scientific Affairs, University of Uruk, Iraq. He received a School of Research in Digital Signal Processing (2005). He received his Ph.D. in Digital Signal Processing from University of Wales, United Kingdom (1986). He has a teaching experience in Computer Science and Communication engineering for 44 years. A total of (15) National Awards. He Published over (290) papers, Supervised more than (210) MSc and PhD Students. He was the First professor Award of University of Baghdad, Iraq. His present areas of research interest are the field of Digital Signal Processing and their applications.