TELKOMNIKA Telecommunication Computing Electronics and Control
Vol. 23, No. 6, December 2025, pp. 1743~1754
ISSN: 1693-6930, DOI: 10.12928/TELKOMNIKA.v23i6.27135

Adaptive DICOM images encryption using quadtree and lightweight ITUBee algorithm

Muntaha Abdulzahra Hatem[1], Balsam Abdulkadhim Hameedi[2], Jamal Nasir Hasoon[3], Fahad Ghalib Abdulkadhum[4]
[1]Department of Missions and Cultural Relations, Ministry of Higher Education and Scientific Research, Baghdad, Iraq
[2]Palestine High School for Excellence, Ministry of Education, Baghdad, Iraq
[3]Department of Computer Sciences, Faculty of Science, University of Mustansiriyah, Baghdad, Iraq
[4]Department of Computer Sciences, Faculty of Computer Sciences and Mathematics, Kufa University, Najaf, Iraq

Article Info

Article history:

Received Apr 18, 2025
Revised Oct 8, 2025
Accepted Oct 19, 2025

Keywords:

DICOM image
Henon map
ITUBee
Lightweight encryption
Medical image
Quadtree

ABSTRACT

The encryption of medical images protects the privacy of patient information transmitted over networks and communications. In this paper, a lightweight encryption method for medical images is proposed, combining a quadtree-based segmentation and a modified ITUBee algorithm for encryption. A digital imaging and communications in medicine (DICOM) image is divided into variable-size blocks using the quadtree technique, and the key is generated through a two-dimensional Henon map; the first dimension is used in the confusion process (bit permutation) of the pixel values, and the second sequence is used to generate the key schedule through the application round function. Different numbers of rounds are applied to the ITUBee method based on the size of the segments in the quadtree, making the algorithm adaptive by increasing the round number when the block size is reduced. The method is used as a lightweight encryption method for encrypting all blocks, utilizing different round numbers for each block size to balance the degree of complexity with the total time consumption of the DICOM image. The result reinforces the proposed method, which produced a high mean squared error (MSE) between the DICOM image and the Encrypted One, and a lower peak signal-to-noise ratio (PSNR). The proposed generated numbers were also tested using national institute of standards and technology (NIST) to evaluate the randomness.

Corresponding Author:

Muntaha Abdulzahra Hatem
Department of Missions and Cultural Relations, Ministry of Higher Education and Scientific Research
Al-Rusafa-Baghdad, Iraq
Email: muntaha.hatem@scrd.gate-gov.iq

1. INTRODUCTION

Medical imaging, encompassing computed tomography (CT), magnetic resonance imaging (MRI), ultrasound, and X-rays, plays a pivotal part in diagnosing a diverse spectrum of diseases. The rapid advancement of internet technology has made it easier to share and move large amounts of medical data quickly and easily. This is particularly important for the growth of telemedicine services, such as teleconsultation and telesurgery [1]. Secure communication channels are necessary for doctors, patients, and scanning centers to share medical images so that patients' private information is not leaked during transmission [2]. Attackers may tamper with transmitted medical images, leading to incorrect diagnoses, which underscores the challenge of maintaining confidentiality and integrity during image transmission [3], [4]. Transfer of medical images over public networks is critical, so it requires extra attention, and standard

methods (cryptography, steganography, and watermarking) are used for this. The field is rapidly evolving as medical companies consistently introduce more medical imaging devices and new technologies [5]. A diverse range of medical imaging technologies worldwide enables physicians to obtain high-quality images, which are critical for accurate disease diagnosis [5], [6]. However, the accessibility of this medical information without owner approval poses several concerns, including security, proof of ownership, and copyright protection.

Medical images have a lot more sensitive and important information than regular images [7]. Every pixel in these pictures is very important for diagnosis, and changing any of them could lead to wrong diagnoses [8]. It is hard to keep these images safe because they do not like being changed as much as less sensitive images do. Medical images typically comprise two parts: the region of no interest (RONI) and the region of interest (ROI) [9]-[11]. The ROI, which has important and sensitive data that is needed for diagnosis, must not be changed. The RONI, on the other hand, shows the background of the image and does not have any important information, so it can be changed.

The medical diagnosis process is essential for determining the type of future treatment, which often depends on the transmitted medical images [12], especially if the presented case originates from geographically distant places, making it necessary to transmit it digitally. Therefore, it must be protected from manipulation and forgery. These aspects are considered (purely medical), and we do not ignore the legal aspect that requires doctors and health departments to maintain the confidentiality of information [13]. From this standpoint, the information (images) must be protected during the transmission process to comply with the relevant regulations and laws [14]. Many images are exposed to many risks through their transfer between different networks and communications systems, intentionally, such as hacking operations, or unintentionally, such as glitches in transmission processes or loss of data during transmission [15]. Therefore, these images must be protected in ways that limit the risks of loss or piracy when transmitted. Encryption [16] is one of the most important ways to keep these images safe.

This paper examines the combination of quadtree decomposition with the novel ITUBee encryption algorithm as a promising method for enhancing the security of medical images in digital contexts. This method aims to make sure that sensitive medical data stored or sent electronically is better protected by using quadtree's ability to divide images into hierarchical structures and ITUBee's strong encryption features. quadtree's ability to efficiently organize image data hierarchically works well with ITUBee's ability to encrypt data, which improves the integrity and confidentiality of medical images. This combined method not only makes sure that medical images are stored and sent securely, but it also meets the important need for strong encryption methods in healthcare data management.

2. RELATED WORKS

The most important scholarly work about our research is covered in this section. By including a secure tampering detection and lossless recovery mechanism, the paper in [17] suggests a way to safeguard medical images transmitted to the cloud. The method utilizes a binary number system arranged in a specific order. It first finds the ROI in the medical image and then breaks it up into blocks that do not overlap. JPEG-LS compression is used to encode the pictures in these blocks. This method works especially well for medical images.

Zheng *et al*. [18], tackled the issue of storing large amounts of medical image data by using deoxyribonucleic acid (DNA) as an effective way to store data. It presents an innovative DNA-based compression and encryption algorithm specifically designed for medical images. The algorithm uses the fact that medical images have homogeneous pixels, especially in their bit-plane decompositions, to get rid of redundancy during compression. The proposed DNA-based quadtree decomposition algorithm transforms the entire image into a sequence of four DNA nucleotides, facilitating the retrieval of the original image through decoding. The DNA-based advanced encryption standard (AES) algorithm in cipher block chaining (CBC) mode encrypts the sequences that come from the compression process to make them safer from bad use.

Revanna and Keshavamurthy [19], discusses the difficulty of securely managing healthcare data that is stored in the cloud because more and more people are using smart eHealthcare, which is made possible by IoT and big data technology. Healthcare facilities are concerned about sensitive data leaks, even though the cloud is a fantastic way to store and share a lot of healthcare data. They encrypt this data before transferring it to the cloud to protect it. However, traditional encryption makes it difficult for sophisticated applications, such as similarity range queries, to work with encrypted data stored in the cloud. To address this limitation, the paper introduces an efficient privacy-preserving similarity range query (EPSim) scheme. In order to provide selective security, the scheme begins by introducing a modified asymmetric scalar-product-preserving encryption (ASPE) technique. After that, it uses a quadtree representation for the data and comes up with an algorithm based on a filtration condition to do efficient similarity range queries on this tree

structure. The EPSim scheme ultimately combines the modified ASPE method and the Quadsector tree to make it possible to safely and quickly search for similar ranges in encrypted cloud-stored healthcare data. A thorough security analysis of the proposed EPSim scheme shows that it is strong.

The study's recommended approach in [20] is predicated on encrypting grayscale document images using both full and partial encryption techniques. The image is first divided into blocks using a Quad-tree decomposition based on block variance to perform partial encryption. While some blocks with uniform pixel levels are considered trivial, others are considered substantial. A 1D Skew tent chaotic map is used to permute the pixels of the important blocks. To improve security, a 2D Henon map is used for additional permutation, creating input for total encryption.

The study in [21] details the creation of a specialized ontology that makes it possible to classify objects in medical images using a multilayer neural network. In order to process large datasets as efficiently as possible and enable faster image processing, the study uses the MapReduce paradigm in a cloud environment. Additionally, to streamline Cloud node communication and reduce pre-processing time, a data compression method based on deduplication is proposed. The suggested remedy undergoes testing in a multisite cloud environment, showcasing improved data transfer optimization, with an average time enhancement of 27%.

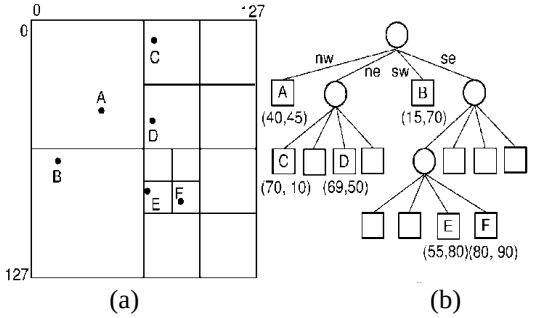
Padmavati and Meshram [21], focus on the problem of sending large medical images over the internet, especially when bandwidth is limited. We use image compression methods to fix this problem, with a focus on fractal image compression. Fractal image compression uses the idea of self-similarity in images to greatly speed up transmission rates, even when bandwidth is limited. However, although they decode rapidly, conventional techniques for compressing fractal images frequently take seconds to complete the encoding process. The paper presents an architecture created especially for fractal image compression in order to get around this restriction. The design is put into action using an field-programmable gate array (FPGA) board called Xilinx Spartan-6 and evaluated with the use of medical imaging data.

Fang *et al*. [22], addressed the growing concerns of patient information leakage and image tampering in cloud-based medical systems. To address these challenges, a new zero-watermarking algorithm named Bandelet-DCT, based on Bandelet and discrete cosine transform, is introduced for medical images. The proposed approach involves several key steps. To start, the scale invariant feature transform (SIFT) is used to get features from an image as a first step. Then, a chaotic system tent map is used to encrypt the watermark that contains the patients' information. After that, the medical images are used to get visual feature vectors with Bandelet-DCT. Lastly, the algorithm employs both zero-watermarking and cryptographic techniques to add and remove the watermark securely.

The studies in the collection looked at different ways to make cloud-based medical image management safer and more efficient. The main goal of these studies was to find answers to problems with medical image security, compression, storage, and data transfer. Each study presented innovative methodologies aimed at tackling specific aspects of medical image management in cloud environments. There is still a lot to do in this area.

3. IMAGE SEGMENTATION USING QUADTREE

A quadtree data structure divides a two-dimensional space into four equal parts, called quadrants, by using a process that repeats itself. The image segmentation method uses a hierarchical data structure called a quadtree to divide an image into parts or areas. A quadtree divides a two-dimensional space into four quadrants over and over again until certain conditions are met [23]. A portion of the image is represented by each node in the quadtree, as explained in Figure 1(a) represented the block partitioning and Figure 1(b) represented the quadtree structure.



(a) (b)

Figure 1. Quadtree structure: (a) the segmentation process and (b) tree structure

This structure is much better for storing and showing spatial data like points, lines, and polygons than a regular list or array. Each node in a quadtree can only have a maximum of four children. The entire two-dimensional space, split into four equal halves, is shown by the root node. A child node of the root represents each quadrant. If the child nodes have more than one point, they can additionally be further separated into four quadrants. This loop keeps going until every point is contained in a separate leaf of the tree. A quadtree is a method for structuring two-dimensional space by recursively subdividing it into smaller segments. The process begins by partitioning the space into four equal quadrants, subsequently subdividing each quadrant into four additional quadrants until all subdivisions satisfy specific criteria.

4. LIGHTWEIGHT CRYPTOGRAPHY (ITUBee)

The length of the key and the size of the ITUBee block are 80 bits. The encryption utilizes a Feistel structure composed of 20 rounds, with main whitening layers located at the top and bottom of the encryption, as depicted in Figure 2. The fact that ITUBee manages memory and energy consumption while maintaining a respectable level of security is encouraging.

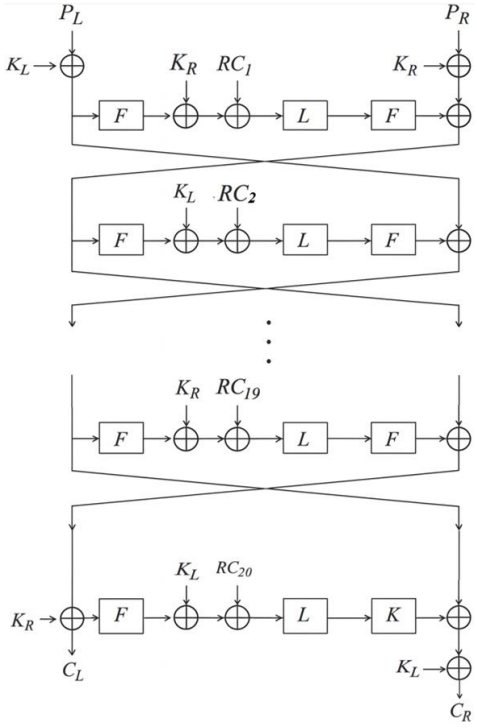


Figure 2. ITUBee framework

5. METHODOLOGY

The suggested method calls for gathering medical images so they can be moved and prepared. quadtrees divide these images into smaller parts so that they are easier to manage and analyze. We make primary keys for these parts of the collected images, and we use these keys later on in the encryption process. Pixels in images are replaced in specific proportions according to these generated tasks. Random keys are selected from among those generated previously, and the original pixels in the images are replaced with the values associated with these keys. After the coding is done, the medical images that are needed for the research are collected. These pictures are read and pre-processed so that they can be put together in the best way possible. The quadtree algorithm then splits them up into square areas, and each area is encoded in a way that fits its own needs. The goal of these operations is to achieve an optimal balance between processing speed and confidentiality. Encrypting areas accomplishes this in multiple ways, according to their nature and importance, which provides advanced protection for medical images and their associated data without compromising the speed and effectiveness of searching and the rapid use of these images. The general framework of the proposed method is explained in Figure 3.

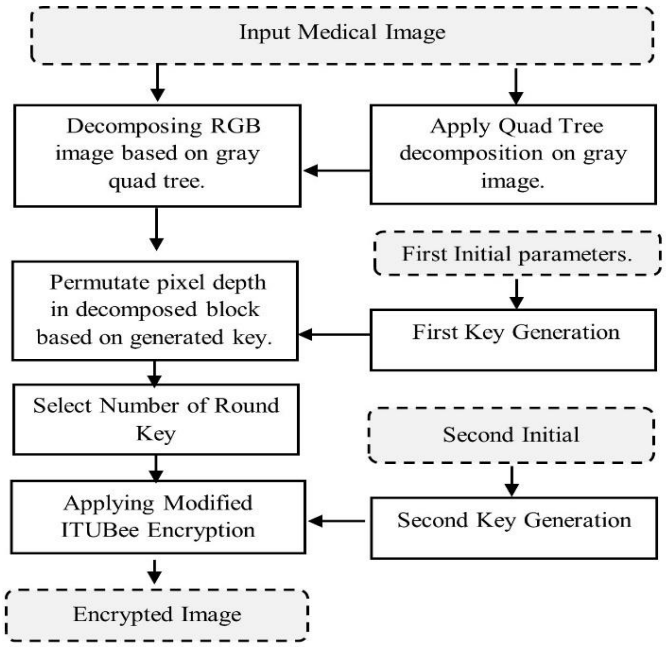


Figure 3. The framework of the proposed method

5.1. Apply quadtree decomposition

The initial phase of the proposed system involves applying the segmentation process to medical images using the quadtree technique, which is applied to the input image (medical image) after it has been converted to grayscale, as illustrated in Figure 4. This technique identifies the most significant areas in the image. It isolates them from the less important areas through a specific threshold that depends on the variance value in the region. Whenever the variance value is high, the region is divided into four other parts until the smallest possible piece is reached. The size of the block is large and undivided, indicating that this region is less significant and lacks many details.

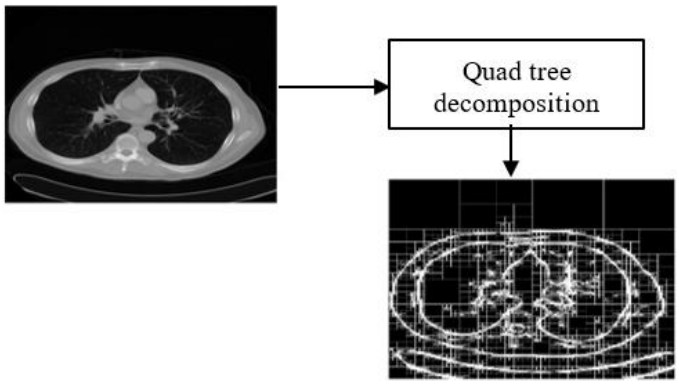
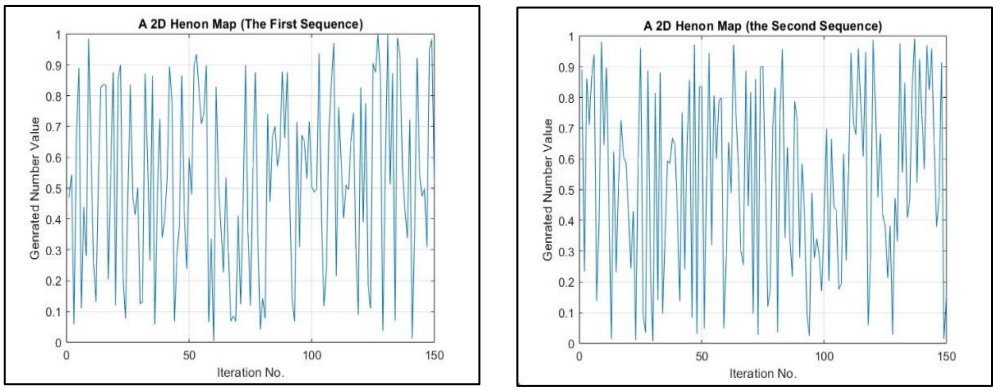


Figure 4. DICOM quadtree decomposition

5.2. Key generation

The number generating (key generation) depends on a two-dimensional chaotic map (Henon map). The first-dimension sequence is used in the process of redistributing the bits (permutation) for each pixel in the existing block, as different initial values are created for each block size. Thus, each block is completed (the two sequence samples are visualized in Figure 5). Figure 5(a) shows the first sequence, which is used in the bit-permutation process for each pixel within the block. Figure 5(b) shows the second sequence, which is used to generate the key schedule for the modified ITUBee encryption algorithm. There is a process of redistributing the bits, differing in size from the other block. Thus, we have a fermentation process.

The second number generation process is carried out by generating private keys for the proposed lightweight encryption algorithm ITUBee. For each specific block size, there is a different key generation process (i.e., a different initial state). This increases the complexity of the method, which gives strength to the proposed method.



(a) (b)

Figure 5. Visualization of generated numbers: (a) first sequence and (b) second sequence

5.3. Select the number of round keys

The number of rounds is now obtained for each distinct block size. The number of rounds decreases as the block size increases. Because of this, there are more rounds in the larger, less detailed blocks, and more rounds in the smaller, more detailed blocks. This makes the encryption process more complex in this area, which in turn creates a balance between the degree of encryption and the value of the information, as well as between the time it takes to complete the encryption process.

5.4. Applying modified ITUBee encryption

The lightweight encryption algorithm applied is a modified ITUBee encryption method, which involves changing the number of rounds for each block size, as illustrated in Figure 6. The number of rounds controls the degree of complexity (time-consuming) and the information value in each region, serving the adaptation. The encryption process is done differently for each block size, as the number of rounds for each block is chosen. The larger the block size, the fewer the number of rounds, thus achieving a balance between the complexity of the region and the encryption, with completely different results. The results of encrypting the same input message with varying numbers of rounds, as well as the time required for encryption in each specified round. Finally, the decryption process used the same process in reverse order.

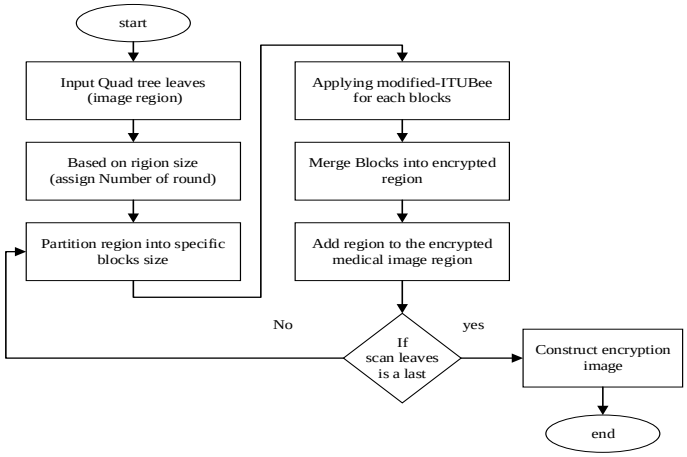


Figure 6. Region encryption using the proposed method

5.5. Modified ITUBee encryption algorithm

The proposed encryption algorithm is represented by partitioning the main image into sub-images. The sub-image is partitioned into 80-bit blocks, each of which is input to the proposed method to produce the encrypted blocks, as explained in Algorithm 1. The number of blocks is varied depending on the segment size, which makes it variable in time-consuming.

```
Algorithm 1: Modified ITUBee encryption algorithm
Input: GeneratedMaster_key, plainBlock (80-bit), No.of rounds,  RC// round constant
Output: Ec\\EncryptedBlock
Steps:
1:  Master key is expanded into round keys (80-bit sub-keys).
2: assigned  pL←MSB(plainBlock) //first 40-bit
3: assigned  pR←LSB(plainBlock) // last 40-bit
4: assignd    kL←MSB(SubKey0) //first 40-bit
5: assigned  kR←LSB(SubKey0) // last 40-bit
6: Initialized Xo←pL□kL and X1←pR□kR
7: for i←1 to No.of rounds
         If reminder(i,2)=1 then
             RK←  kR
         Else
             RK← kL
         End if
         Xi+1 ← Xi+1 □ Fun(L(RK□RCi □ Fun(Xi)))
     End for
8: EcL←Xn □ KR  EcR←Xn+1 □ KL
9: Ec←merge(EcL,EcR)
10: return Ec
End algorithm
```

5.6. Modified ITUBee decryption algorithm

The decryption process is the reverse of the encryption process. The same generated key is used with the same initial values in reverse order. The encryption algorithm of the proposal is represented by the same steps in forward steps (encryption steps) in reverse order, with the same subkeys from bottom to top for reconstructing the plain block.

6. EXPERIMENTAL RESULTS

The proposed method was tested using a set of DICOM images as medical images with a (512×512) size and a 16-bit depth. The first process applied is segmentation using the quadtree method of the dataset of the DICOM image, and its decomposition is explained in Figure 7. The encryption process of medical images is explained, considering the safety and security of patient information. The application of the proposed method yielded images with no correlated information, as illustrated in Figure 8.

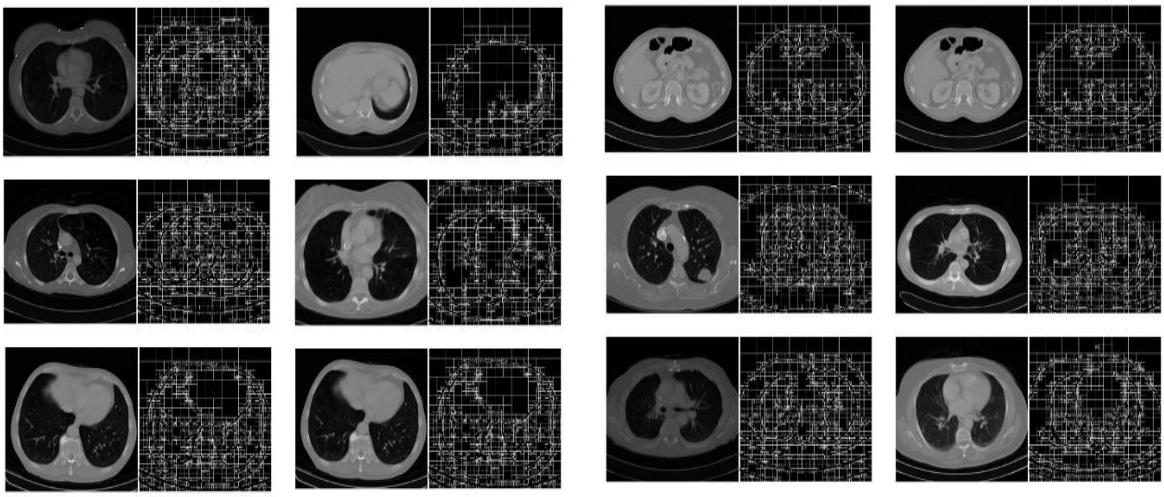


Figure 7. The DICOM dataset and its decomposition are using a quadtree

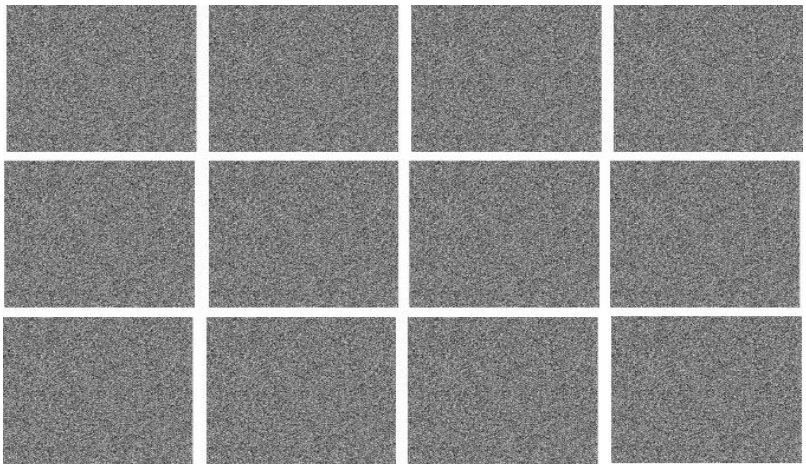


Figure 8. Medical image encryption

The permutation process example is explained in Table 1 based on the generated numbers of the Henon map. This permutation illustrates how the first-dimension chaotic values reorder the pixel bits before encryption, ensuring initial confusion at the bit level. The sample of rounds number that is based on block size is illustrated in Table 2. It further details how different block sizes produced by the quadtree segmentation are assigned different numbers of encryption rounds. Since smaller blocks contain more detailed information, they are assigned higher round counts. From the previous Table 2, each block size will take its corresponding time as explained in Table 3. It summarizes the encryption time corresponding to each round number, showing how increasing the number of rounds increases processing time in a predictable manner. Together, these tables demonstrate the adaptive nature of the proposed method, which balances encryption strength with computational cost.

Table 1. The permutation process in the pixel bits example

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	0	0	0	1	0	0	1	1	0	0	0	0	0	1
6	3	16	11	7	14	8	5	15	1	2	4	13	9	10	12
1	0	1	0	0	0	0	0	0	0	0	0	0	1	1	0

Table 2. Specifying the number of rounds of each block size

Block size	256×256	128×128	64×64	32×32	16×16	8×8	4×4
No. of rounds	4	6	8	10	12	16	20

Table 3. The encryption time of each specifies the number of rounds

	Hex. sample is ‘0123456789ABCDEF1234’	
No. of rounds	Hex. encryption	Elapsed time of the block
8	‘E77A363E6A3CAB7EF0ED’	0.006148
10	‘6F6797CC63DDB9B91DA8’	0.008538
12	‘5D0E527293D60AFDDB6D’	0.009984
14	‘00F97F11CEA7C0E5FC6B’	0.010321
16	‘965262DE7D6955473A84’	0.011493
18	‘4CDD5B300131676B2174’	0.012994
20	‘AA80646BA3DD40111C38’	0.013456

The first experiment, which applies the proposed method, aims to determine the mean squared error and peak signal-to-noise ratio of the encrypted image compared to the reference image [24], as outlined in Table 4. It reports the MSE and PSNR values for all encrypted DICOM images. The results show consistently high MSE and low PSNR values, indicating a significant visual difference between the original and encrypted images. These findings confirm that the proposed encryption method effectively eliminates meaningful visual information from the image.

Table 4. Image quality test for DICOM data set using a proposed encryption algorithm

#	MSE	PSNR	#	MSE	PSNR
1	1.47673E+09	4.17799	7	1.32177E+09	4.74633
2	1.45964E+09	4.50808	8	1.49467E+09	4.51080
3	1.44328E+09	4.30537	9	1.40513E+09	4.75164
4	1.42249E+09	4.79935	10	1.29731E+09	4.20836
5	1.43539E+09	4.68879	11	1.45673E+09	3.92338
6	1.43813E+09	4.35392	12	1.31446E+09	4.00027

From Table 4, the values of MSE and PSNR indicate significant differences between the reference images and the encrypted images. The correlation check results for each image are presented in Table 5, which includes the images used to evaluate the outcomes [25]. With these images, the correlation between the photographs taken before and after the encryption procedure was examined. Before encryption, it was observed that the images exhibited a strong correlation (almost one). However, this correlation was disrupted, resulting in values that are now close to zero or negative in all directions.

Table 5. The correlation test of all the DICOM image datasets

#	Correlation	#	Correlation
1	-0.125874701	7	-0.058546451
2	-0.177125325	8	-0.064530225
3	-0.191786396	9	-0.057387054
4	-0.030737911	10	-0.163069082
5	-0.07364085	11	-0.031394577
6	-0.128256232	12	-0.172050538
	Av.		-0.106199945

NIST tests are employed, which are exemplified by a standard test [26]. Every test was conducted on sequences of the key generation using the Henon map. According to Table 6, the p-values of all tests are more significant than 0.1, indicating that all the results exceed the threshold value. The differential attack on images, to assess how resilient picture encryption techniques are to differential assaults, number of pixel change rate (NPCR), and unified confusion–avalanche indicator (UCAI), is crucial. While low numbers may indicate flaws that could be exploited, high values in both metrics indicate a secure encryption method. The UCAI and NPCR are explained in Table 7.

The time consumption for each DICOM image is recorded to evaluate the algorithm's success. The time needed to utilize the recommended algorithm for the encryption and decryption of the 512×512 DICOM image sizes is explained and measured in Table 8, which compares the results obtained by applying the AES algorithm to the same DICOM images. According to Table 8, the average time consumption is 5.66957 seconds for encryption. In comparison, 5.02541 seconds are required for the decryption process, which is less than the time consumption of the same DICIM using the AES standard algorithm.

Table 6. The NIST test results of the proposed system

#	Test	P-value	Status	#	Test	P-value	Status
1	Run test	0.56904	Pass	8	Maurer's universal test	0.969577	Pass
2	Serial test	0.80773	Pass	9	The longest run of one	0.906531	Pass
3	Random excursion variant test	0.808941	Pass	10	Linear complexity test	0.598968	Pass
4	Random excursion test	0.725053	Pass	11	Frequency test within a block test	0.875782	Pass
5	Overlapping template matching test	0.94472	Pass	12	Discrete fourier transform test	0.633792	Pass
6	Non-overlapping template matching test	0.963372	Pass	13	Cumulative sums test	0.971584	Pass
7	Frequency monobit test	0.939911	Pass				

Table 7. The differential test (UCAI and PCNR)

#	UCAI	NPCR	#	UCAI	NPCR
1	32.63281	98.21255	7	32.12302	99.03974
2	32.22455	98.1759	8	33.72373	98.45148
3	32.22355	98.45941	9	32.56731	98.776
4	33.79175	98.63678	10	31.97207	98.4049
5	32.93441	98.04097	11	33.19228	98.44132
6	33.0684	98.17463	12	34.2298	99.16332

Table 8. Comparison of the time consumption of the proposed method with the AES algorithm

	Proposed method			AES method	
#	Encryption time	Decryption time	#	Encryption time	Decryption time
1	5.973	5.072	1	8.865	6.105
2	5.222	4.697	2	7.602	6.298
3	6.145	5.387	3	8.093	7.388
4	5.779	4.909	4	8.551	6.168
5	5.041	4.344	5	6.726	5.996
6	5.936	5.849	6	8.712	7.484
7	6.005	5.058	7	8.211	6.080
8	5.274	4.698	8	7.443	6.384
9	6.053	5.253	9	8.489	6.936
10	5.692	4.730	10	7.410	6.146
11	4.840	4.428	11	6.298	6.167
12	6.074	5.881	12	8.087	7.233

7. CONCLUSION

The encryption technique that works well for medical facilities that offer electronic services and medical systems has become crucial. The suggested technique relies on a lightweight encryption of DICOM images, based on a specific decomposition technique called the quadtree technique, which splits the image into blocks of varying sizes. The Henon map (2D function) is used to generate the keys. The first set of generated numbers is used in the permutation of the pixel values' bits, and the second set is employed in the suggested encryption technique. The experiments, which explain the high MSE and low PSNR, indicate significant differences between the input and output DICOM images, as well as the randomness of the generated key, and are tested using a standard test (NIST test). The correlations of encrypted images are very low, indicating that there is no correlation between pixels in the encrypted images. , and the differential attacks tested (NPCR and UCAI), which are approximately 33.3% and 99.5%, respectively, denoting high resistance to differential attacks. The proposed method could be developed to encrypt other types of media, such as audio or video, in an efficient manner.

ACKNOWLEDGMENTS

The authors would like to thank the University of Diyala (UOD), particularly Ali Hussein Fadhil, for providing the time and facilities necessary to complete this study.

FUNDING INFORMATION

This study was self-funded by the authors.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Muntaha Abdulzahra Hatem	✓	✓		✓			✓		✓					
Balsam Abdulkadhim Hameedi		✓			✓			✓		✓		✓		
Jamal Nasir Hasoon	✓	✓	✓				✓		✓				✓	
Fahad Ghalib Abdulkadhum		✓			✓					✓	✓	✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

We have obtained informed consent from all individuals included in this study.

DATA AVAILABILITY

In this paper, no new data were created.

REFERENCES

[1] F. Abbasi and N. A. Memon, "Reversible watermarking for the security of medical image databases," in *2018 21st Saudi Computer Society National Computer Conference (NCC)*, IEEE, Apr. 2018, pp. 1–6, doi: 10.1109/NCG.2018.8593009.

[2] I. Aouissaoui, T. Bakir, and A. Sakly, "Robustly correlated key-medical image for DNA-chaos based encryption," *IET Image Processing*, vol. 15, no. 12, pp. 2770–2786, Oct. 2021, doi: 10.1049/ipr2.12261.

[3] W. Wu, L. Zhang, and W. Zhang, "Improved impossible differential cryptanalysis of reduced-round Camellia," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 5381 LNCS, 2009, pp. 442–456, doi: 10.1007/978-3-642-04159-4_29.

[4] 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, Oct. 2021, doi: 10.1007/s12652-020-02597-5.

[5] S. Gupta, R. Baraskar, and S. Agrawal, "A survey on reversible watermarking techniques for image security," *International Research Journal of Engineering and Technology (IRJET)*, vol. 6, no. 8, pp. 826–836, 2019.

[6] O. Kara, "Reflection cryptanalysis of some ciphers," in *Progress in Cryptology - INDOCRYPT 2008, 9th International Conference on Cryptology in India, Kharagpur, India*, vol. 5365 LNCS, 2008, pp. 294–307, doi: 10.1007/978-3-540-89754-5_23.

[7] F. Huma, M. Jahan, I. B. Rashid, and M. A. Yousuf, "Wavelet and LSB-based encrypted watermarking approach to hide patient's information in medical image," in *Proceedings of International Joint Conference on Advances in Computational Intelligence. Algorithms for Intelligent Systems*, 2021, pp. 89–104, doi: 10.1007/978-981-16-0586-4_8.

[8] J. Liu, J. Ma, J. Li, M. Huang, N. Sadiq, and Y. Ai, "Robust watermarking algorithm for medical volume data in internet of medical things," *IEEE Access*, vol. 8, pp. 93939–93961, 2020, doi: 10.1109/ACCESS.2020.2995015.

[9] S. Shen, L. Huang, and Q. Tian, "A novel data hiding for color images based on pixel value difference and modulus function," *Multimedia Tools and Applications*, vol. 74, no. 3, pp. 707–728, Feb. 2015, doi: 10.1007/s11042-014-2016-0.

[10] F. N. Thakkar and V. K. Srivastava, "A blind medical image watermarking: DWT-SVD based robust and secure approach for telemedicine applications," *Multimedia Tools and Applications*, vol. 76, no. 3, pp. 3669–3697, Feb. 2017, doi: 10.1007/s11042-016-3928-7.

[11] R. Obuchowicz, M. Strzelecki, and A. Piórkowski, "Clinical applications of artificial intelligence in medical imaging and image processing—a review," *Cancers*, vol. 16, no. 10, p. 1870, May 2024, doi: 10.3390/cancers16101870.

[12] E. Isibor, "Regulation of healthcare data security: legal obligations in a digital age," *SSRN*, 2024.

[13] S. Shivshankar, N. Makhija, and P. Mathusudhanan, "Digital imaging and communication in medicine (DICOM): Biomedical and health informatics: imaging and interoperability using HL7 and DICOM," in *Smart Healthcare and Machine Learning. Advanced Technologies and Societal Change*, Eds., Singapore: Springer, 2024, pp. 299–317, doi: 10.1007/978-981-97-3312-5_20.

[14] K. Hussain, A. R. Rahmatyar, B. Riskhan, M. A. U. Sheikh, and S. R. Sindiramutty, "Threats and vulnerabilities of wireless networks in the Internet of Things (IoT)," in *2024 IEEE 1st Karachi Section Humanitarian Technology Conference (KHI-HTC)*, IEEE, Jan. 2024, pp. 1–8, doi: 10.1109/KHI-HTC60760.2024.10482197.

[15] H. Gao and T. Gao, "A secure lossless recovery for medical images based on image encoding and data self-embedding," *Cluster Computing*, vol. 25, no. 1, pp. 707–725, Feb. 2022, doi: 10.1007/s10586-021-03446-6.

[16] C. Bhaya, M. S. Obaidat, A. K. Pal, and S. H. Islam, "Encrypted medical image storage in DNA domain," in *ICC 2021 - IEEE International Conference on Communications*, IEEE, Jun. 2021, pp. 1–7, doi: 10.1109/ICC42927.2021.9500718.

[17] S. D. Mahmood, F. Drira, H. Falih Mahdi, and A. M. Alimi, "Secure medical image sharing: Technologies, watermarking insights, and open issues," *IEEE Access*, vol. 13, pp. 103995–104026, 2025, doi: 10.1109/ACCESS.2025.3574477.

[18] Y. Zheng, R. Lu, Y. Guan, J. Shao, and H. Zhu, "Efficient privacy-preserving similarity range query with quadsector tree in eHealthcare," *IEEE Transactions on Services Computing*, vol. 15, no. 5, pp. 2742–2754, Sep. 2022, doi: 10.1109/TSC.2021.3081350.

[19] C. R. Revanna and C. Keshavamurthy, "A new partial image encryption method for document images using variance based quad tree decomposition," *International Journal of Electrical and Computer Engineering*, vol. 10, no. 1, pp. 786–800, 2020, doi: 10.11591/ijece.v10i1.pp786-800.

[20] E.-S. Apostol and C.-O. Truică, "Advanced medical image representation for efficient processing and transfer in multisite clouds," *Prepr. arXiv. 2305.15411*, 2023.

[21] S. Padmavati and V. Meshram, "A hardware implementation of fractal quadtree compression for medical images," in *Integrated Intelligent Computing, Communication and Security*, vol. 771, Eds., Singapore: Springer, 2019, pp. 547–555, doi: 10.1007/978-981-10-8797-4_55.

[22] Y. Fang *et al.*, "Robust zero-watermarking algorithm for medical images based on SIFT and Bandelet-DCT," *Multimedia Tools and Applications*, vol. 81, no. 12, pp. 16863–16879, 2022, doi: 10.1007/s11042-022-12592-x.

[23] U. Sara, M. Akter, and M. S. Uddin, "Image quality assessment through FSIM, SSIM, MSE and PSNR—a comparative study," *Journal of Computer and Communications*, vol. 7, no. 3, pp. 8–18, 2019, doi: 10.4236/jcc.2019.73002.

[24] S. Yoon, H.-J. Jung, J. C. Knowles, and H.-H. Lee, "Digital image correlation in dental materials and related research: A review," *Dental Materials*, vol. 37, no. 5, pp. 758–771, May 2021, doi: 10.1016/j.dental.2021.02.024.

[25] Z. Mengdi, Z. Xiaojuan, Z. Yayun, and M. Siwei, "Overview of randomness test on cryptographic algorithms," *Journal of Physics: Conference Series*, vol. 1861, no. 1, Mar. 2021, doi: 10.1088/1742-6596/1861/1/012009.

[26] L. Li, "A novel chaotic map application in image encryption algorithm," *Expert Systems with Applications*, vol. 252, Oct. 2024, doi: 10.1016/j.eswa.2024.124316.

BIOGRAPHIES OF AUTHORS

Muntaha Abdulzahra Hatem received the Master and B.Sc. degree in Computer Science (Mustansiriyah University, Iraq) in 2020 and 2009 respectively. Her research interests include networks, information security, and artificial intelligence algorithms. She can be contacted at email: muntaha.hatem@scrdiraq.gov.iq.

Balsam Abdulkadhim Hameedi received a Master's degree from the University of Mustansiriyah, Baghdad, Iraq, College of Education, Computer Science Department in 2022. She received her B.Sc. degree in Computer Science in 2000 from the University of Mustansiriyah, Baghdad, Iraq/College of Education, Computer Science Department. His research focuses on information security. She works in the Ministry of Education. She can be contacted at email: Balsam119@res-rus2.edu.iq.

Jamal Nasir Hasoon received the Ph.D. degree in Computer Science (University of Technology, Iraq) in 2020 and finished his Master and B.Sc. degree in (Mustansiriyah University, Iraq) in 2014 and 2006 respectively. His research interests include machine learning, computer vision, pattern recognition, and information security. He can be contacted at email: jamal.hasoon@uomustansiriyah.edu.iq.

Fahad Ghalib Abdulkadhum Department of Computer Sciences Faculty of Computer Sciences and Mathematics. Master of Software Engineering and PhD in Networks and Informatics from Northwestern Polytechnical University. He can be contacted at email: ahadg.abdulkadhim@uokufa.edu.iq