

Medical image encryption using multi chaotic maps

Abbas Zamil Hussain, Maisa'a Abid Ali Khodher

Department of Computer Science, University of Technology, Baghdad, Iraq

Article Info

Article history:

Received Jul 28, 2022

Revised Nov 05, 2022

Accepted Dec 28, 2022

Keywords:

3DES

Chaotic maps

Cryptography

Medical images

TCP/IP

ABSTRACT

Over the last twenty years, chaos-based encryption has been an increasingly popular way to encrypt and decrypt data using nonlinear dynamics and deterministic chaos. Discrete chaotic systems based on iterative maps have gotten a lot of interest because of their simplicity and speed. In this paper, three kinds of chaotic maps are utilized to build a digital image encryption strategy depending on a chaotic system. These chaotic maps are the logistic map, Arnold Cat's map, and Baker's map. In addition to using the triple data encryption standard (3DES) encryption scheme with the chaotic maps mentioned. The results of the experiments revealed that the suggested digital image encryption technique is both efficient and secure, making it ideal for usage in insecure networks. The transmission control protocol (TCP)/internet protocol (IP) protocol was used for the purpose of transferring data from server to client through the network and vice versa.

This is an open access article under the [CC BY-SA](https://creativecommons.org/licenses/by-sa/4.0/) license.



Corresponding Author:

Abbas Zamil Hussain

Department of Computer Science, University of Technology

Baghdad, Iraq

Email: cs.20.34@grad.uotechnology.edu.iq

1. INTRODUCTION

Chaos theory has expanded and changed several disciplines, since its discovery in the 1960s, it has been used in a variety of fields, such as physics, engineering, computer programming, economics, and biology. Academics didn't discover there were intimate links and analogies connecting chaos theory and encryption until the 1990s, and ever since, chaos has begun to infiltrate into current cryptography [1]. As illustrated in Figure 1, any property of chaotic systems has a corresponding counterpart in traditional cryptosystems [2].

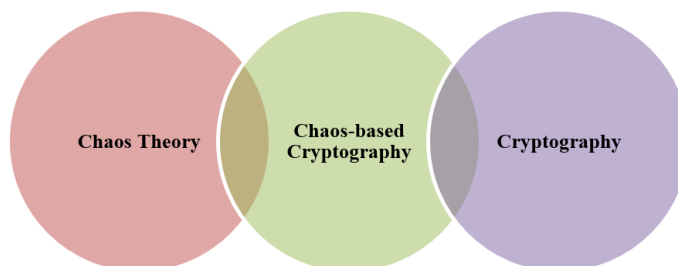


Figure 1. Chaos-based cryptography [2]

Despite the fact that chaotic systems are deterministic, their unique traits make them relevant to secure multimedia communications (i.e., confusion and diffusion, unpredictability properties, and sensitivity to initial conditions and parameters) [3]. Each of these characteristics can be linked to the standard cryptographic qualities of a good cipher, such as confusion and diffusion, for the purpose of with standing statistical analysis assaults. As a result, the commonalities between chaotic systems and crypto systems make collaboration appealing [4].

Many academics have pointed out that chaos and cryptography have a significant relationship. The most significant advantage of a chaotic system over a noisy one is that it is predictable, allowing the recovery of a message with perfect knowledge of initial conditions and system characteristics. The concept of chaotic cryptography was first proposed by Alghafis *et al.* [5]. This paper is partitioned into sections as: in section 2, we looked at some of the related works. Section 3 went through the theoretical foundation in greater depth. In section 4, the proposed scheme architecture was provided. Section 5 contains the experimental results as well as security evaluations. In section 6, we look at several algorithm comparisons from the literature, section 6 has the conclusion.

2. RELATED WORKS

Several chaos-based image encryption algorithms have recently been proposed. In this section, some be arranged in chronological order from oldest to newest. Gupta *et al.* [6] proposed a method that is robust, efficient, secure, and rapid, as evidenced by the results of many parameters. The cat map and chaotic function have been successfully and effectively applied to a variety of images. The simulation results show that the new approach reduces the risk of a brute force decryption assault and is fast enough for real image encryption.

Gashim and Hussein [7] integrated two logistic maps to create the key. The created key is employed in the stages of confusion and dissemination. The image's pixel is permuted in the confusion stage, while the value of each pixel is modified in the diffusion step. These approaches' security and performance were extremely precise and quick.

Balaska *et al.* [8] merged the Grain-128a stream cipher technique with a 2D Zaslavsky chaotic map to increase sensitivity and security in the initial parameter selection. Then, to generate the chaotic map's needed parameters, a 256-bit secret key with a fixed length is used. The sequences will then be used to encrypt the image using a diffusion approach and some confusion. The simulated experiments demonstrated that the proposed approach for encrypting images of any type or format is incredibly dependable and effective.

Guodong *et al.* [9] used the cryptosystem to produce the initial parameters for the fundamental quantum logistic map. Discrete cosine transform (DCT), on the other hand, transfers images to the frequency domain. Substitution-permutation network (SPN) with five rounds offers effective protection against differential-like assaults. In comparison to asymmetric-based images, encryption requires procedures with reduced computational complexity.

Kari *et al.* [10] proposed a set of innovative chaotic maps depending on discret wavelet transform (DWT) and the double chaotic function to increase encryption quality and execution. The proposed map was commonly hyper-chaotic, with great sensitivity and complexity, as determined by dynamical analysis and sample entropy techniques. As a result, the suggested chaos-based picture cipher could be a valuable tool for a variety of applications.

Alhumyani [11] created an image cipher that makes advantage of the DCT chaotic Baker map (BM). Before rearranging the DCT coefficients of the original plain image with the BM, the proposed DCT-based BM image cipher's module DCTs the plain image. The proposed DCT-based BM image cipher's superiority in terms of sensitivity, statistics, noise immunity, and differential was demonstrated through a number of experiments.

Ibrahim *et al.* [12] introduced a broad medical image encryption system depending on a novel combination of two extremely efficient structures: dynamic substitution boxes (S-boxes) and chaotic maps. Experiments have shown that the suggested architecture, regardless of implementation, passes all security tests. Any chaotic map can be created, as well as any key-dependent dynamic S-box construction method.

Elghandour *et al.* [13] proposed the chaotic sequences are generated via a two-dimensional piecewise smooth nonlinear chaotic map. These sequences are then converted to numbers between 0 and 255. Ultimately, the chaotic sequences are employed to mask the image that has been jumbled (diffusion). Their method was secure, quick, and resistant to numerous assaults.

Guodong *et al.* [14] developed a novel asymmetric image encryption system. The starting values for a quantum logistic map are generated first using the asymmetric public key Rivest-Shamir Adleman (RSA) technique. On the plain image, the Arnold scrambling process is used to accomplish the basic concealment of visual information. Finally, exclusive-OR (XOR) diffusion is applied to each row and column of the image as separate units. Then, Arnold's map parameters are calculated. The experimental testing show better distribution of pixel values uniformly minimizes high correlation and can withstand various assaults.

Ankita *et al.* [15] proposed dividing the color images into red, green, and blue channels, transposing them from the pixel plane to the bit-plane, and then scrambling the matrix using the Arnold cat map (ACM). The new system is more sensitive to differential assaults, more secure, and more resilient to brute-force attacks. The performance and security metrics histogram, correlation distribution, correlation coefficient, entropy, number of pixel change rate, and unified averaged changed intensity are calculated to show the potential of the proposed encryption technique.

3. RESEARCH METHOD

In this section, the technologies utilized in the suggested medical image encryption model are discussed. A brief description of each algorithm or technique used in the proposed system is given. It includes the types of encryptions and the concept of chaos theory and its types in addition to clarifying the protocol used to transmit medical images through the network from sender to receiver.

3.1. Introduction to cryptography

Cryptography is a technique for assuring data security. It encrypts sensitive data to protect it from being captured by attackers, hackers, or the public in general, and therefore only authorized transmitters or users are able to accurately decrypt the data. Both encryption and decryption methods are depicted in Figure 2. The private message is written in plaintext. Encryption is a method of hiding the true message in plaintext using a secret key and then displaying the ciphertext. During the decryption procedure, only the proper secret key will decrypt the ciphertext and retrieve the plaintext [16].

There are two main cryptography kinds are symmetric and asymmetric cryptography, which are determined by the encryption key. Symmetric cryptography uses only one key for encryption and decryption. Asymmetric cryptography employs two pairing keys (public key) and a private key that is never exchanged over the network. This type of cryptography takes longer and is more complicated than symmetric cryptography [17]. The 3DES is an example of symmetric cryptography, in this section, we will explain it briefly [18].

Triple DES (3DES): the development of 3DES is based on a double DES approach for enhancing DES security that was previously available. Three keys are needed for both encryption and decryption in the 3DES technique. The same key is used in symmetric cryptography to encode and decode data. For contemporary use, 3DES encryption with two or three distinct keys is reliable. The flowchart of 3DES rounds presents in Figure 3.

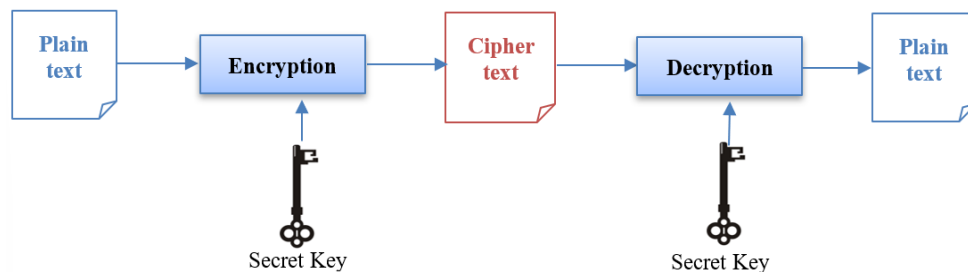


Figure 2. Encryption and decryption [16]

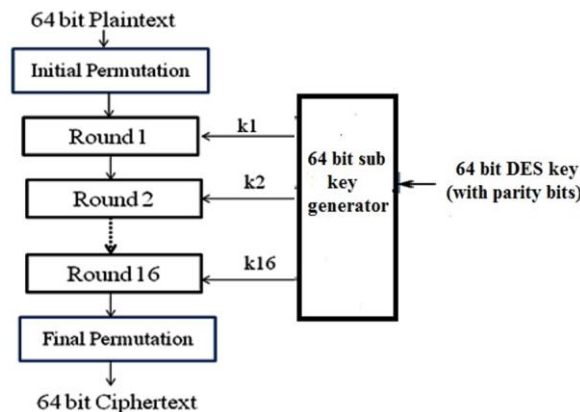


Figure 3. Diagram of triple-DES [18]

3.2. Image processing and image encryption terminologies

An image that has been digitally encoded is called a digital image. A digital image is arranged in a rectangular pattern in a 2-dimensional grid. A raster image or a bit-mapped picture is the numerical representation of a two-dimensional image. The brightness of an image at every position (x, y) is represented by the value of “ f ” [19]. The process of transforming an original image into a coded image is known as image encryption. Image decryption is a reversible encryption method that allows you to restore an encrypted image to its original state. It protects the image while it is being transmitted over a public network. Using the secret keys and decryption technique, only an authorized person can acquire the original image in this procedure [20].

3.3. Chaos theory

The science of unexpected events is known as chaos. dynamic systems with nonlinear and unpredictable behavior are involved. Turbulence, weather, the stock market, mental states, and other unpredictable behaviors are addressed by chaos theory. Chaos theory gives us a starting point for a better understanding of chaotic and fractal phenomena [21]. A chaotic map is defined as one that exhibits chaotic behavior. In the following subsections, some chaotic systems will be introduced: the logistic map, Arnold’s cat map, and Baker’s map.

a) Logistic map

It is an American ecologist who developed the logistic equation. In 1976, it was planned. The logistic equation was utilized to investigate the link between insect populations and environmental conditions. It was a one-dimensional non-linear equation that was both simple and important. The following are the items on the logistic map as in (1).

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

Where $y_0 \in (0, 1)$ represents the starting state of the chaotic system at any time n and $\mu \in (0, 4)$, is the system parameter also called the bifurcation parameter as shown in Figure 3. The next stage of the system is expressed by y_{n+1} , where n shows the discrete time. The behavior of the logistic map highly depends on the value of the control parameter μ [22].

b) Arnold cat map

Vladimir Arnold’s Arnold cat map is a two-dimensional chaotic system. The transformation procedure is built by converting an image to an $N \times N$ matrix. It’s a straightforward demonstration of Chaos Theory, Vladimir Arnold’s theory of chaos. Each pixel’s coordinates are given by an ordered pair of (X, Y) in the real range $[0, 1]$, which is represented by two independent (2) and (3).

$$X_{n+1} = X_n + Ay_n \pmod{N} \quad (2)$$

$$Y_{n+1} = BX_n + AY_n \pmod{N} \quad (3)$$

Where X_n, Y_n are the sample positions in the $N \times N$ matrix, $n = 1, 2, 3, \dots, N - 1$, and X_{n+1}, Y_{n+1} are the transformed positions after cat map, and A, B are two control parameters that are positive integers. The encryption procedure is carried out via cat map iteration; after M iterations, there exist T positive integers such that $(X_{n+1}, Y_{n+1}) = (X_n, Y_n)$. The period T is determined by the parameters A and B , as well as the size of the sample’s matrix ($N \times N$ matrix) [23].

c) Baker map

The chaotic Baker map is a well-known encryption technique in the image processing domain. It’s a permutation-based tool that uses a secret key to change the pixel positions in a square matrix of dimensions $N \times N$. In a bijective mode, it assigns a pixel to another pixel position. The discretized Baker map is a useful tool for generating random numbers in a square matrix. The discretized map is denoted by $B(n_1, \dots, n_k)$, where the vector $[n_1, \dots, n_k]$ represents the secret key as S_{key} . The secret key is chosen so that each integer n_i divides N , and $n_1 + \dots + n_k = N$, using N as the number of data items in one row. Allow $N_i = n_1 + \dots + n_i$. The indices (r, s) data item is relocated to the indices as shown in (4).

$$B(r, s) = \left[\frac{N}{n_i}(r - N_i) + s \pmod{\left(\frac{N}{n_i}\right)} \cdot \frac{n_i}{N} \left(s - s \left(\frac{N}{n_i}\right) \right) + N_i \right] \quad (4)$$

The chaotic permutation is carried out in the following steps:

- N rectangles of width n_i and the number of components N are divided into a square matrix of $N \times N$.
- Each rectangle’s elements are organized into a row in the permuted rectangle. From left to right, upper rectangles are taken first, followed by lower rectangles.

The scan begins at the bottom left corner of each rectangle and works its way up. Chaos systems is a sophisticated nonlinear sequence that is hard to understand and predict. For such an “a word a secret” encryption system, the chaotic sequence is a suitable key sequence. Chaotic sequences have a number of cryptographic advantages over normal ciphers, including the fact that they are difficult to attack and crack [24].

3.4. Overview of TCP/IP protocol

Two of the most important protocols in the TCP/IP protocol suite are transmission control protocol (TCP) and Internet protocol (IP). TCP/IP is organized in layers, just like other networking software. Along with its tiered structure, the term protocol stack denotes the stack of layers in the protocol suite. To connect with all those above and below them, layers use basic interfaces. In this way, a layer can both serve the layer above it and use the services of the layer below it [25]. Figure 4 illustrates the TCP/IP protocol stack.

4. THE PROPOSED MODEL

In this work, a set of chaotic maps with a 3DES algorithm were used for the purpose of encoding medical images. First, a set of preprocessing is performed on the image, then the image is encoded using 3DES, then the output is encoded by using one of the chaotic maps, and then the cipher image is sent to the receiver. On the other hand, the receiver decodes the image to get the plain image. Figure 3 explains the overall diagram of the proposed system. As shown in Figure 5, the proposed system is a gray medical image encryption system. The image goes through two encryption stages, the first is encryption using 3DES, and the next stage is encryption. The purpose of the proposed method is to increase data security by using two algorithms that provide high security. Because one of the most important things to consider when sending data through the network as in our proposed system is the issue of data security. After applying the encryption algorithms on the client side and sending the data to the server side, decryption processes are applied in reverse for the purpose of retrieving the original image. The TCP/IP protocol was used for data transmission. Algorithm (1) explains all the processes that take place within the network between the sender side and the receiver side.

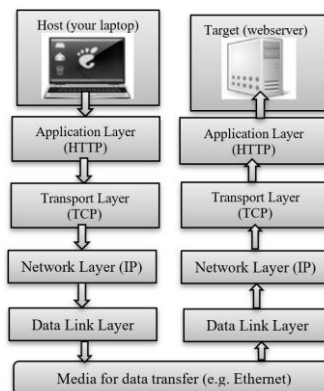


Figure 4. Conceptual model of the TCP/IP protocol stack [26]

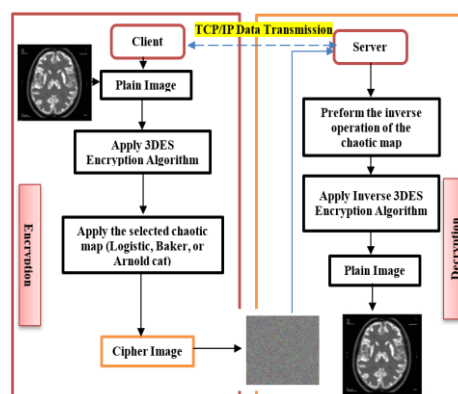


Figure 5. An overall diagram of the proposed method

Algorithm 1. The proposed method

Input: plain image on the client-side

Output: cipher image on server-side, plain image on client-side

Begin

- 1) Define a thread that will use a TCP connection socket to serve a client the behavior of the thread
- 2) Make a TCP socket that listens
- 3) While (true)

Begin

- Wait for a client to establish a connection
- Establish a new thread that will serve the client using the newly formed TCP connection socket
- Go to 4

End while

- 4) Read the input plain image then do:
 - If the input image is a color image convert it to grayscale, then go to 5
 - Else
 - Go to 5
 - End if

5) Apply the 3DES encryption algorithm

6) Select the chaotic map form (Logistic or Arnold cat or Baker) map

7) Send the cipher image to the server-side

8) After receiving the image on the server-side do:

9) Perform the inverse operation of the chaotic map that was selected on the client-side

10) Apply the 3DES decryption algorithm to the cipher image

11) Return the plain image

End

On client-side

On server-side

5. RESULTS AND ANALYSIS

In this section, the results of the encryption system based on chaotic maps are presented and discussed. Several metrics were used to test the proposed system in the encryption and decryption operations. These metrics are illustrated.

5.1. Encryption performance metrics

This set of metrics assesses encryption performance; they include [26].

a) Mean square error (MSE)

The difference between the plain and encrypted images is measured by utilizing the MSE. A large MSE score indicates a large disparity between plain and encrypted images. It can take the form of an (5).

$$MSE = \frac{\sum_{i=1}^M \sum_{j=1}^N [P(i,j) - C(i,j)]^2}{MN} \quad (5)$$

Where M and N are the height and width of the image respectively. $P(i,j)$ is the $(i,j)^{th}$ pixel value of the original image, and $C(i,j)$ is the $(i,j)^{th}$ pixel value of the decrypted image.

b) Peak signal to noise ratio (PSNR)

It can be used to determine an image's quality. A decent picture encryption method should result in encrypted images with a low PSNR value. PSNR is calculated using the (6).

$$PSNR = \frac{10 \log_{10}(2^{2n}-1)^2}{MSE} \quad (6)$$

c) Information entropy analysis

Information entropy is a mathematical concept that may be used to explain how random or uncertain signals are. Using (7), the following information entropy for the image is calculated:

$$Entropy = -\sum_{i=0}^{2^n-1} P(m_i) \log_2[P(m_i)] \quad (7)$$

Where $P(m_i)$ denotes the occurrence probability of the gray level i , and $i = 0, 1, 2, \dots, 2^n$. The 2^n is an image's number of grayscale levels.

5.2. Experimental tests

For testing, grayscale and color photos are obtained. The simulations are run on MATLAB R2021b with a Windows 10 operating system and 8 GB of memory. The test images are shown in Figure 6(a) to Figure 6(f). As a result, these cipher images provide no relevant information about the plain image. The plain images retrieve as it is after the decryption process. As we can see, our scheme can be implemented quickly.

Table 1 shows the results of evaluation metrics between input and cipher image and time of encryption. Table 2 shows the results of evaluation metrics between the input image and retrieved image and the time of decryption. The tables display the results of the encryption and decryption of each image using three chaotic maps, to compare these results later and to determine the best map in the case of encryption and decryption.

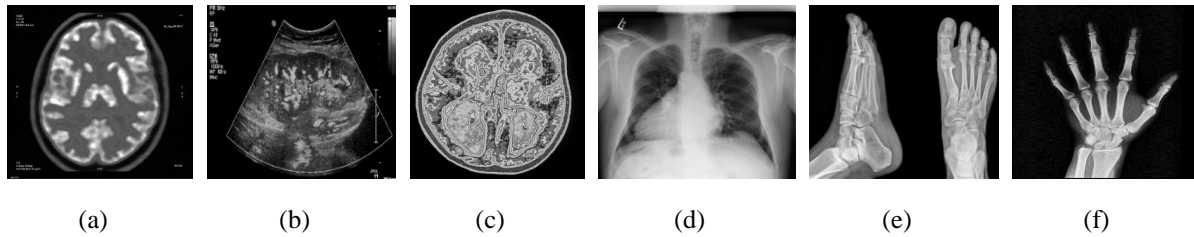


Figure 6. Plain grayscale images with different sizes: (a) 512×512, (b) 600×600, (c) 900×900, (d) 1024×1024, (e) 612×612, and (f) 500×500

Table 1. PSNR, MSE, entropy, and execution time


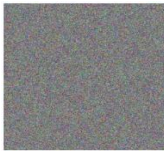
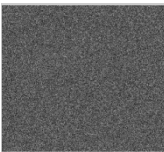
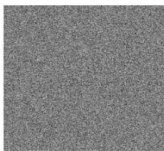

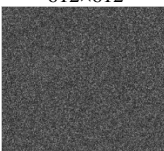
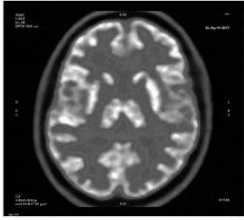

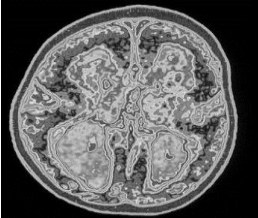



Cipher image	Method	PSNR	MSE	Entropy	Encryption time in sec.
 512×512	Logistic map + 3DES	9.9718	20807	7.9993	5.45657
	Arnold cat map + 3DES	7.9079	23068	7.9994	4.67588
	Baker map + 3DES	13.9898	16384	7.9990	2.87987
 600×600	Logistic map + 3DES	15.9809	19092	7.9998	3.98098
	Arnold cat map + 3DES	11.4982	22778	7.9990	2.76832
	Baker map + 3DES	19.2980	19898	7.9993	3.89797
 900×900	Logistic map + 3DES	11.490	25980	7.9994	4.80980
	Arnold cat map + 3DES	8.8979	17980	7.9998	6.39878
	Baker map + 3DES	9.3675	13897	7.9991	3.99080
 1024×1024	Logistic map + 3DES	11.3780	35980	7.9990	6.39789
	Arnold cat map + 3DES	8.9080	26980	7.9993	3.87990
	Baker map + 3DES	7.8797	24678	7.9995	1.87979
 612×612	Logistic map + 3DES	6.7686	35788	7.9993	5.27238
	Arnold cat map + 3DES	13.879	56980	7.9997	3.34989
	Baker map + 3DES	12.897	25879	7.9993	3.78687
 500×500	Logistic map + 3DES	11.110	12675	7.9990	8.76876
	Arnold cat map + 3DES	8.564	25643	7.9998	9.98983
	Baker map + 3DES	10.786	25249	7.9999	2.87999

Table 2. PSNR, MSE, entropy, and execution time of image decryption

Cipher image	Method	PSNR	MSE	Entropy	Decryption time
 512×512	Logistic map + 3DES	Inf.	0	7.2720	5.59879
	Arnold cat map + 3DES	Inf.	0	7.2973	3.89798
	Baker map + 3DES	Inf.	0	7.8573	2.98080
 600×600	Logistic map + 3DES	Inf.	0	7.2720	6.76867
	Arnold cat map + 3DES	Inf.	0	7.2973	5.78687
	Baker map + 3DES	Inf.	0	7.8573	3.27868
 900×900	Logistic map + 3DES	Inf.	0	7.3897	7.67577
	Arnold cat map + 3DES	Inf.	0	7.3786	7.27868
	Baker map + 3DES	Inf.	0	7.2654	0.37686
 1024×1024	Logistic map + 3DES	Inf.	0	7.3677	3.87989
	Arnold cat map + 3DES	Inf.	0	7.3897	6.87633
	Baker map + 3DES	Inf.	0	7.3256	2.37687
 612×612	Logistic map + 3DES	Inf.	0	7.1342	6.37683
	Arnold cat map + 3DES	Inf.	0	7.2367	3.27863
	Baker map + 3DES	Inf.	0	7.8978	0.26578
 500×500	Logistic map + 3DES	Inf.	0	7.3267	4.97990
	Arnold cat map + 3DES	Inf.	0	7.2357	5.78687
	Baker map + 3DES	Inf.	0	7.8273	1.78689

5.3. Encryption efficiency

The PSNR and MSE of the original and encrypted images are calculated to determine the efficacy of the encryption operation. Lower PSNR and higher MSE values indicate that image encryption is more efficient. The higher value of MSE is better because this means the difference between the plain and encrypted images is high. It is clear from the results that the PSNR values were low, while the sum of the difference between the pixel value in the original image and its value in the encrypted images which is called MSE was very large, and this indicates the efficiency of the used chaotic maps.

5.4. Decryption efficiency

PSNR should be higher and MSE should be lower between the original and decrypted images for better decryption efficiency. The value of MSE is zero in all cases which means that the original image was retrieved as it is. While the value of PSNR, in this case, will be infinity because the value is divided by zero. Therefore, we set a value of 100%, which indicates the optimal value.

5.5. Execution time

In both encryption and decryption processes, the execution time doesn't exceed a few seconds and fractions of a second. Any cryptography algorithm's encryption time is the amount of time it takes to transform plain text into cipher text. The throughput of any encryption process is computed using the encryption time, which is calculated as the total encrypted plaintext (in bytes) divided by the encryption time (in ms).

6. CONCLUSION

By employing efficient cryptographic primitives, the proposed medical image encryption system achieves an exceptional throughput suitable for encryption. The suggested framework's security and efficiency benefits may be applied to any chaotic map, whether classic, modern, or future. The suggested method's most notable features are its amazing sensitivity to even minor changes in the encryption key, as well as its robustness versus data loss due to transmission network issues. 3DES is more reliable and has a larger key length, which avoids several of the attacks that may be used to speed up the process. As a result, chaotic maps provide various advantages, including a large keyspace and good security. In order to reach higher performance for medical image encryption in an ideal time, we proposed a method that takes advantage of the long key and the high security with easy implementation of them. The simulation and performance assessment findings show that the approach is successful and trustworthy in encrypting images of various sorts and sizes, making it suitable for dependable and feasible cryptographic usage. The proposed scheme will be paired with image steganography in the future to allow for secure image transfer utilizing the secret key.





REFERENCES

- [1] J. A. M. -García, A. M. G. -Zapata, E. J. R. -Ramírez, and E. T. -Cuautle, "On the Prediction of Chaotic Time Series using Neural Networks," *Journal of Chaos Theory and Applications*, vol. 4, no. 2, pp. 94-103, 2022, doi: 10.51537/chaos.1116084.
- [2] O. M. Al-Hazameh, M. F. Al-Jamal, N. Alhindawi, and A. Omari, "Image Encryption Algorithm Based on Lorenz Chaotic Map with Dynamic Secret Keys," *Neural Computing and Applications*, vol. 31, pp. 2395–2405, 2019, doi: 10.1007/s00521-017-3195-1.
- [3] Y. Luo, J. Yu, W. Lai, and L. Liu, "A Novel Chaotic Image Encryption Algorithm Based on Improved Baker Map and Logistic Map," *Multimedia Tools Application*, vol. 78, pp. 22023–22043, 2019, doi: 10.1007/s11042-019-7453-3.
- [4] X. Chai, X. Fu, Z. Gan, Y. Zhang, Y. Lu, and Y. Chen, "An Efficient Chaos-Based Image Compression and Encryption Scheme Using Block Compressive Sensing and Elementary Cellular Automata," *Neural Computing and Applications*, vol. 32, pp. 4961–4988, 2020, doi: 10.1007/s00521-018-3913-3.
- [5] A. Alghafis, F. Firdousi, M. Khan, S. I. Batool, and M. Amin, "An Efficient Image Encryption Scheme Based on Chaotic and Deoxyribonucleic Acid Sequencing," *Mathematics and Computers in Simulation*, vol. 177, pp. 441–466, 2020, doi: 10.1016/j.matcom.2020.05.016.
- [6] R. Gupta, R. Pachauri, and A. K. Singh, "An Efficient Way of Medical Image Encryption using Cat Map and Chaotic Logistic Function," *International Journal of Computer Science and Information Security (IJCSIS)*, vol. 15, no. 11, 2017. [Online]. Available: https://www.researchgate.net/publication/322384257_An_Efficient_Way_of_Medical_Image_Encryption_using_Cat_Map_and_Chaotic_Logistic_Function
- [7] L. L. Gashim and K. Q. Hussein, "A New Algorithm of Encryption and Decryption of Image Using Combine Chaotic Mapping," *Iraqi Journal of Information Technology*, vol. 9, no. 2, 2018. [Online]. Available: <https://www.iasj.net/iasj/download/95ac83f87a71d850>
- [8] N. Balaska, Z. Ahmida, A. Belmeguenai, and S. Boumerdassi, "Image Encryption Using a Combination of Grain-128a Algorithm and Zaslavsky Chaotic Map," *The Institution of Engineering and Technology*, vol. 14, no. 6, pp. 1120-1131, 2020, doi: 10.1049/iet-pr.2019.0671.
- [9] G. Ye, K. Jiao, X. Huang, B. -M. Goi, and W. -S. Yap, "An Image Encryption Scheme Based on Public-Key Cryptosystem and Quantum Logistic Map," *Scientific Reports*, vol. 10, no. 21044, 2020, doi: 10.1038/s41598-020-78127-2.
- [10] A. P. Kari, A. H. Navin, A. M. Bidgoli and M. Mirmia, "A New Image Encryption Scheme Based on Hybrid Chaotic Maps," *Multimedia Tools and Applications*, vol. 80, pp. 2753–2772, 2021, doi: 10.1007/s11042-020-09648-1.
- [11] H. Alhumyani, "Efficient Image Cipher Based on Baker Map in the Discrete Cosine Transform," *Cybernetics and Information Technologies*, vol. 20, no. 1, 2020, doi: 10.2478/cait-2020-0005.
- [12] S. Ibrahim *et al.*, "Framework for Efficient Medical Image Encryption Using Dynamic S-Boxes and Chaotic Maps," in *IEEE Access*, vol. 8, pp. 160433-160449, 2020, doi: 10.1109/ACCESS.2020.3020746.
- [13] A. Elghandour, A. Salah, and A. Karawia, "A New Cryptographic Algorithm Via a Two-Dimensional Chaotic Map," *Ain Shams Engineering Journal*, vol. 13, no. 1, 2022, doi: 10.1016/j.asej.2021.05.004.
- [14] G. Ye, H. Wu, K. Jiao, and D. Mei, "Asymmetric Image Encryption Scheme Based on the Quantum Logistic Map and Cyclic Modulo Diffusion," *Mathematical Biosciences and Engineering*, vol. 18, no. 5, pp. 5427-5448, 2021, doi: 10.3934/mbe.2021275.
- [15] A. Bisht, M. Dua, S. Dua, and P. Jaroli, "A Color Image Encryption Technique Based on Bit-Level Permutation and Alternate Logistic Maps," *Journal of Intelligent Systems*, vol. 29, no. 1, 2022, doi: 10.1515/jisys-2018-0365.
- [16] Z. Qiao, "Nonlinear Dynamics, Applications to Chaos-Based Encryption," *PH.D. Thesis, University of Le Havre Normandy*, 2021. [Online]. Available: https://hal.archives-ouvertes.fr/tel-03200707/file/Z_QIAO.pdf
- [17] O. G. Abood and S. K. Guirguis, "A Survey on Cryptography Algorithms," *International Journal of Scientific and Research*





- Publications*, vol. 8, no. 7, 2018, doi: 10.29322/IJSRP.8.7.2018.p7978.
- [18] C. A. Sari, E. H. Rachmawanto, and C. A. Haryanto, "Cryptography Triple Data Encryption Standard (3DES) for Digital Image Security," *Scientific Journal of Informatics*, vol. 5, no. 2, 2018, doi: 10.15294/sji.v5i2.14844.
- [19] S. T. Kamal, K. M. Hosny, T. M. Elgindy, M. M. Darwish and M. M. Fouda, "A New Image Encryption Algorithm for Grey and Color Medical Images," in *IEEE Access*, vol. 9, pp. 37855-37865, 2021, doi: 10.1109/ACCESS.2021.3063237.
- [20] N. S. Noor, D. A. Hammond, A. Al-Naji, and J. Chahl, "A Fast Text-to-Image Encryption-Decryption Algorithm for Secure Network Communication," *Computers*, vol. 11, no. 3, 2022, doi: 10.3390/computers11030039.
- [21] W. -K. Lee, R. C. -W. Phan, W. -S. Yap, and B. -M. Goi, "Spring: A Novel Parallel Chaos-Based Image Encryption Scheme Dynamic," *Nonlinear Dynamic*, vol. 92, pp. 575–593, 2018, doi: 10.1007/s11071-018-4076-6.
- [22] M. J. Rostami, A. Shahba, S. Saryazdi, and H. N. -Pour, "A Novel Parallel Image Encryption with Chaotic Windows Based on Logistic Map," *Computers and Electrical Engineering*, vol. 62, pp. 384–400, 2017, doi: 10.1016/j.compeleceng.2017.04.004.
- [23] D. Elmaci and N. B. Catak, "An Efficient Image Encryption Algorithm for the Period of Arnold's CAT Map," *International Journal of Intelligent Systems and Applications in Engineering*, vol. 6, no. 1, pp. 80-84, 2018, doi: 10.18201/ijisae.2018637935.
- [24] F. Musanna and S. Kumar, "Image Encryption Using Quantum 3-D Baker Map and Generalized Gray Code Coupled with Fractional Chen's Chaotic System," *Quantum Information Processing*, vol. 19, no. 220, 2020, doi: 10.1007/s11128-020-02724-3.
- [25] A. P. Pande and S. R. Devane, "Study and Analysis of Different TCP Variants," *2018 Fourth International Conference on Computing Communication Control and Automation (ICCCUBEA)*, 2018, pp. 1-8, doi: 10.1109/ICCCUBEA.2018.8697750.
- [26] 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.

BIOGRAPHIES OF AUTHORS



Abbas Zamil Hussain     is currently pursuing a master's degree in computer science at the University of Technology in Baghdad. He obtained his Bachelor's Degree in computer science in 2019. His area of interest includes Information Systems, Cryptography, and Image Processing. He can be contacted at email: cs.20.34@grad.uotechnology.edu.iq.



Maisa'a Abid Ali Khodher     obtained her M.Sc. and Ph.D. in 2005 and 2016 from the University of Technology in Iraq, and her M.Sc. in Image Processing, and her Ph.D. in information hiding. Currently, she is Assist. Prof. in Computer Science. Dr. Maisa'a has more than 30 years of experience and she has supervised B.Sc. final year projects. And she has supervised M.Sc. and Ph.D. Her research interests include cryptography, image processing, databases, data security, and linguistic steganography. She can be contacted at email: Maisaa.A.Khodher@uotechnology.edu.iq.