Revue d'Intelligence Artificielle
Vol. 38, No. 1, February, 2024, pp. 313-321
Journal homepage: http://iieta.org/journals/ria

Securing Medical Images Using Chaotic Map Encryption and LSB Steganography

Abbas Zamil Hussain*, Maisa'a Abid Ali Khodher

Computer Science Department, University of Technology, Baghdad 10066, Iraq

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

https://doi.org/10.18280/ria.380133

Received: 8 October 2023
Revised: 6 November 2023
Accepted: 6 December 2023
Available online: 29 February 2024

Keywords:
image encryption, chaotic map, triple data encryption standard (3DES), advanced encryption standard (AES), bat algorithm (BA), least significant bit (LBS)

ABSTRACT

Secure image transfer is a difficult topic in the age of communication technology because millions of people utilize and share images online for personal and professional reasons. Encryption algorithms, such as cipher images, help achieve secure transfer through networks. Despite attackers having decryption keys, they cannot retrieve the original image. To ensure integrity assurance, prevent changes to medical images that could lead to a misdiagnosis, transmit patient medical records in a private and secure manner, and prevent falling victim to cyberattacks, a high-performance, effective method of encrypting medical images must be developed. Encrypting medical images is common in telemedicine, making secure image transfer essential. The medical dataset includes personal data about the health of a patient. All essential information, including medical images, is now kept on picture and communication servers because of the growing interest in inpatient records across the world. In this study, we presented a unique approach to medical picture encryption that combines the Triple data encryption algorithm (3DES) and advanced encryption standard (AES) methods with three chaotic maps (Logistic, Arnold CAT, and Baker). The BAT optimization algorithm is also used to accomplish the task of key generation. Finally, the Least Significant Bit (LBS) is used to hide encrypted medical images before sending them to the server by TCP/IP protocol. The experiments yielded promising results in entropy of 5.92, PSNR of 0.99, and MSE 0.0001.

1. INTRODUCTION

One of the most basic human requirements nowadays is access to the internet [1]. The rapid development and use of new digital communication and network technologies have led to significant promise for improved data storage and electronic data transfer across the Internet [2]. But private data protection is just as important, which is why data integrity and network security have always been top priorities. Scientists have responded by taking the necessary safety precautions to increase visibility and guard against security flaws [3]. Most of the multimedia that is shared and saved online takes the form of images. Therefore, image encryption is used to protect the privacy and veracity of digital images [4]. To protect patients 'private information when sending medical images, these data should be sent over a secure communication network. If an attacker manages to intercept and alter a transmitted medical image, it could result in a false diagnosis [5]. Therefore, maintaining integrity and secrecy in the transfer of medical images became extremely difficult. Thus, greater care must be taken to safeguard medical images sent over open networks. Watermarking, steganography, and cryptography are common methods utilized in medical image security [6].

Cryptography is the study of encrypting data to prevent unauthorized parties from reading it. The reason image cryptography is so popular at the moment is that effective encryption requires some natural feature management. The image's core properties include a considerable correlation of nearby pixels, high redundancy, and big volume [7]. When applied directly to images, several text-based encryption algorithms, such as AES and DES, become less suitable [8]. One of the greatest and most appropriate techniques for photo encryption is a chaotic system. This method encrypts data by employing a pixel randomization scheme. It has various inherent advantages, including susceptibility to control settings and starting conditions, ergodicity, pseudorandomness, and aperiodicity [9]. However, because this way merely the pixel location is scrambled and the image's entropy and even though histogram values do not vary, these two criteria are used to assess the security of picture encryption against statistical assaults [10]. The chaotic system is commonly employed with several methods to increase picture encryption security, including XOR replacement or additional techniques like El Gamal, compressed sensing, an elliptic curve, and DNA coding, and so on [11]. Figure 1 shows the techniques used to encrypt the data, most of which were used in this work.

Based on the findings of earlier research, this study presents a chaotic system, data concealment, and classic cryptography method with certain improvements, such as a BA optimization algorithm for key processing. The fundamental objective is to improve the diffusion and permutation process so that the encryption products are more resistant to different assaults. In addition, the encryption results were assessed using a range of methodologies, including correlation coefficient analysis, histogram analysis, MSE, information entropy, avalanche impact, and PSNR. Researchers constructed an effective encryption and data concealing method for medical images to address the issue of medical picture confidentiality. In light of this, this paper's primary contribution is the provision of many chaotic maps for data encryption and assessment criteria for picture encryption. Lastly, current issues are emphasized, and a variety of possible research directions that could help close the gaps in these fields are indicated, supporting the work of both developers and academics.

The format of the paper is as follows: The related works are presented in Section 2. The suggested strategy, including encryption and decryption methods, is explained in Section 3. Section 4 contains an examination of the implementation findings on medical imagery. Finally, in section 5, the findings are reviewed.

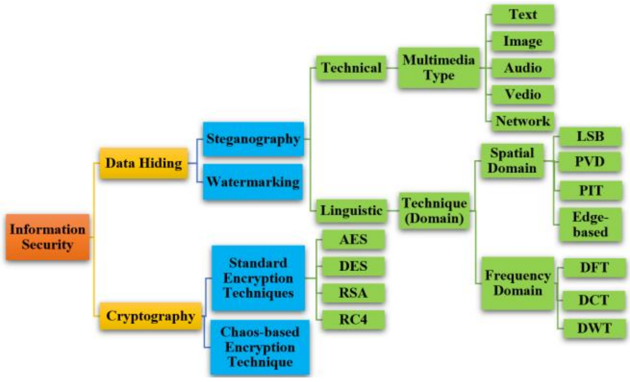


Figure 1. Different information protection mechanisms [12]

2. RELATED WORKS

The most modern chaos-based image encryption techniques are covered in this section. Several picture encryption methods have been put forward, and they differ in terms of resilience and efficacy. This paper presents ways to encode images based on chaos.

Askar et al. [13] used chaotic maps to create a pseudo-number generator to design a color picture encryption decryption technique. To generate the Key, this study combines two Logistic maps. The generated key is used throughout the confusion and propagation stages. The confusion stage permutates the image's pixels, whereas the diffusion step changes the value of each pixel. The data showed that this algorithm performed quite accurately and quickly. Bhogal et al. [14] devised a method that employed a chaotic map in combination with AES and assessed it against AES in its conventional version. They were able to explore how and why the chaotic map affected encryption quality thanks to this comparison. CAT-AES encrypts data by repeatedly iterating over Arnold's cat map, whereas regular AES encryption does not. The findings revealed that the encryption quality has improved. The histograms were more consistent, and the absolute correlation coefficient was near 0 for several of the evaluated images after CAT-AES encryption. Al-Khasawneh et al. [15] suggested a picture encryption technique depending on multi-chaos. Because a multi-chaotic system is the foundation of our proposed method, it can overcome the problems associated with algorithms based on a low-dimensional chaotic map. Permutations at the bit and pixel levels are used to increase the cryptosystem's security. Several tests were conducted to establish the security and sustainability of the proposed picture encryption technology. Gatta and Abd Al-latief [16] presented a method to secure medical images, which play an important part in people's healthcare organizations. The main goal of this work is to develop a robust encryption technique that preserves human treatment and diagnosis while enabling high-quality, information-distortion-free reproduction of the original picture from the encrypted image. The experimental findings demonstrate the efficacy of the suggested method utilizing several statistical metrics and a strong correlation between the original and decrypted photos. Kumar et al. [17] A strong technique for encrypting medical images was put forward. The partial discrete cosine transforms, which is immune to differential, statistical, and brute force attacks, was developed using chaotic maps. The sensitivity of the suggested method is around 1012. In terms of performance, the suggested methodology outperforms several state-of-the-art algorithms due to the large keyspace 1060. The findings lay the framework for a variety of prospective real-time medical services, such as mobile health care and wireless networking for medical image security. Farah et al. [18] offered a new hybrid chaotic map and a fresh way to optimize encryption algorithm performance. In terms of unpredictability and sensitivity, the suggested chaotic map beats current chaotic functions. The unique mathematical function outperforms traditional maps depending on its Lyapunov coefficients and entropy measure. They propose a novel image cipher based on Shannon's confusion/diffusion features. The optimization procedure's purpose is to produce a bijective matrix with a high nonlinearity score. Yin and Li [19] suggested a genetic simulated annealing particle swarm optimization (GSAPSO)-based medical encryption method. The results of the experiments reveal that the encryption system successfully removes the correlation between nearby pixels, and the ciphertext image has a high degree of unpredictability and dispersity. It's impervious to statistical analysis, differential attacks, violent attacks, and other types of attacks. Meanwhile, it can do computational activities and has a high encryption efficiency. Yasser et al. [20] suggested a set of novel chaotic maps that depend on DWT and double chaotic functions to improve encryption quality and execution. As a result, the suggested pipeline avoided numerous existing cryptanalysis approaches and cryptography assaults. The dynamic analysis and sampling entropy methods demonstrated that the suggested map is generally hyperchaotic, with high sensitivity and complexity. Akan et al. [21] offered a better method for medical picture encryption based on a hybrid chaotic permutation approach and a 3D logistic map for ensuring the privacy of patients' medical photographs during transmission and storage. They introduce a combination of bit-level and block-level pixel scrambling in the confusion stage. The technique was also introduced for image pixel shuffling by using the block-level pixel scrambling mechanism first the image sub-blocks are randomly scrambled then each individual pixel contained in each sub-block is shuffled based on the 3D logistic chaotic mapping system. Hashim et al. [22] presented a unique technique for securing these images from AES and chaotic system assaults. The proposed medical image encryption method uses advanced cryptographic primitives to achieve the following: One large keyspace that renders brute force assaults unfeasible. 2) Before using the AES method, medical image scrambling provides more safety than using AES alone. Because the standard picture encryption algorithm is ineffective for utilization in authentication, It is being overtaken by a more efficient technique. In terms of security, the proposed technique outperforms the present AES algorithm. Chaudhary et al. [23] Researchers developed and tested block cipher picture encryption and chaos-based photo encryption techniques. AES is employed as a block cipher scheme, while Arnold cat maps and a logistic map are used as native and hybrid chaotic algorithms, respectively. The Chaos and AES algorithms are used to encrypt photos. According to the study, the hybrid chaotic map is more resistant to differential or chosen plain text assaults since it has higher NPCR and UACI values. Abdallah and Farhan [24] developed a novel way of image encryption depending on the principles of confusion and diffusion. The new S-confusion Box's principle and the diffusion applicator in New IP. These tables depend on a multi-chaotic system. The chaotic system is affected by the initial values. When any value changes, the substation and permutation operations change. In our approach, shuffling operations are employed to enhance the gap between plain and encrypted images. The results in the preceding tables show that the proposed approach is more secure against attackers while attempting to retrieve plain image data. To achieve strong encryption against a variety of attacks, Rachmawanto and Zulfiningrum [25] proposed an image encryption process that combines several techniques. These techniques include block-based substitution, chaotic hash, diffusion with logistic maps, scrambling to achieve the confusion operation, merged hash functions, and dynamic bit shifting based on Josephus sequences. Depending on the test findings, three types of photos were used: normal, special, and medical pictures. It has been shown that the suggested encryption method is impervious to statistical and differential attacks.

3. METHODOLOGY

The proposed system in Figure 2 aims to provide greater security for medical images due to the sensitivity and privacy of the information it contains, so a set of information security techniques such as image cryptography and image hiding were used to achieve this purpose, these techniques will be explained in some detail in this section. No data set was used, but rather a set of random images of different sizes. The client receives a two-dimensional medical image, encrypted using 3DES and LSB algorithms. A key is created using BAT optimization and AES encryption. The image is encrypted using a chaotic map, repeated for N rounds. The secret key created by BAT can influence the number of rounds. TCP/IP protocol transfers data between client and server. All operations are carried out in reverse order on the server. Because medical photographs contain sensitive and private information, the proposed system seeks to increase security for these kinds of photos. In order to do this, a variety of information security strategies were employed, including picture cryptography and image concealing. In this part, these methods will be covered in more detail.

3.1 Generate key using bat optimization algorithm

The bat Algorithm is a population-based metaheuristic influence on the implementation of bat hunting habits. Biosonar is used by bats in the dark to avoid obstructions and discover prey or their roosts, and the echo It can distinguish between several kinds of adjacent objects because to bounces. Bats can discriminate between background obstacles and flies using their echolocation abilities to measure distance. Bats always fly at a random velocity (vi) at a fixed frequency (*fmin*), but with varying wavelengths (λ) and loudness (A0), at a place (^{xi}) to pursue prey. The intensity of a bat's pulse may vary greatly. However, Yang postulated that it fluctuated between a positive large number (A0) and a minimum constant value (Amin). Eqs. (1), (2), and (3) were tuned to produce a different solution in the simulation by adjusting the frequency, loudness, and pulse rate. The new solution is deemed superior to the prior one based on how finely the solutions were tuned by modifying the loudness and pulse rate, which is determined by how close it is to the ideal solution [26].

$$f_i = f_{min} + (f_{max} - f_{min})\beta \tag{1}$$

$$v_i^t = v_i^{t-1} + (x_i^t - x_*)f_i \tag{2}$$

$$x_i^t = x_i^{t-1} + v_i^t \tag{3}$$

where x_g is the location of the best bat in the swarm and β is a random vector distributed in the interval [0,1]. Figure 3 depicts the behavior of the bat [27].

The key that will be used as a key to the 3DES algorithm to encrypt input data is generated randomly every time using the bat algorithm making it very difficult to get the key.

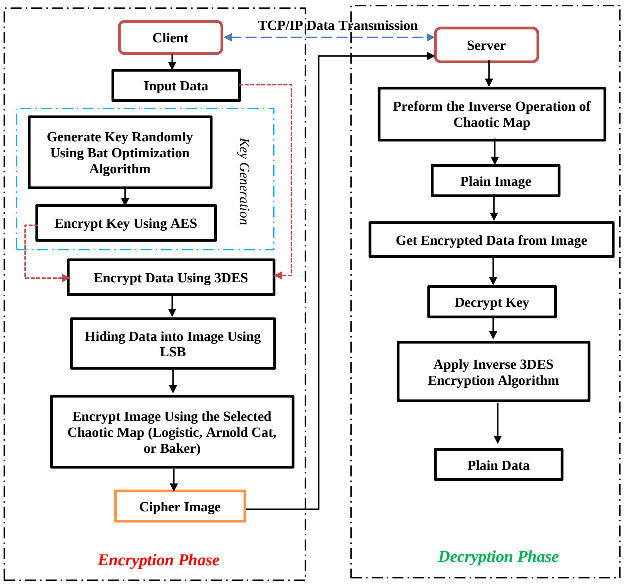

TCP/IP Data Transmission
Client
Input Data
Generate Key Randomly Using Bat Optimization Algorithm
Key Generation
Encrypt Key Using AES
Encrypt Data Using 3DES
Hiding Data into Image Using LSB
Encrypt Image Using the Selected Chaotic Map (Logistic, Arnold Cat, or Baker)
Cipher Image
Encryption Phase
Server
Preform the Inverse Operation of Chaotic Map
Plain Image
Get Encrypted Data from Image
Decrypt Key
Apply Inverse 3DES Encryption Algorithm
Plain Data
Decryption Phase

Figure 2. An overall diagram of the proposed method

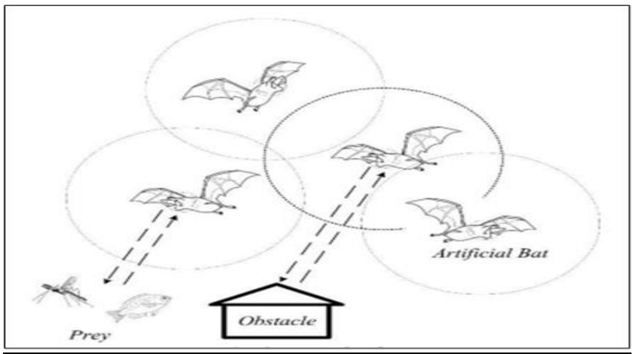


Figure 3. Bat algorithm

3.2 Encrypt key by advanced encryption standard (AES)

NIST suggested the AES as a contemporary ciphering method in 2001 to take on the role of DES. AES may provide any database gathering. Using encryption-decryption, the AES algorithm encodes 10 cycles for 128-bit keys. After 12 rounds for 192-bit keys and 14 rounds for 256-bit keys, the final cipher message is obtained. One 128-bit information length, which may be split into four basic active blocks, is supported by AES. These elements are treated as a line of bytes, which are then combined to create "the state," a 4 by 4 matrix [28]. The key generated using the bat algorithm in the previous step will be used to encrypt the patient's data after it is encrypted using the AES algorithm.

3.3 Encrypt data based on triple data encryption standard (3DES)

It was created to address the weaknesses of DES while retaining the same encryption. The 3DES key size (56-bit). To do this, apply the procedure three times consecutively, using three distinct keys. There are 168 bits in total length. TDEA uses three 64-bit DEA keys (K1, K2, and K3) in the encode-decode-Encode (EDE) stage [29]. At this stage, the keys generated and encrypted in the previous stages are used as keys to the traditional 3DES algorithm where the data entered at this stage of the proposed system is encrypted.

3.4 Encrypt data based on triple data encryption standard (3DES)

In the spatial domain, where a digital photo is built of a matrix of color values and intensity, the LSB technique is the most widely used. The LSB approach's secret message bits instantaneously replace the cover picture pixels with some or all the LSBs. Because changing the LSB of the host pixels results in minimal contrast in the image, the stage photo seems to be like the host image. A grayscale image contains 8 bits per pixel, but a color photograph has 24 bits per pixel, with 8 bits for each color component (RGB) [30]. Data encrypted using LSB technology is concealed in the last phase of the proposed system.

3.5 Encrypt image that contains hiding data by chaotic maps

Three chaotic maps are used to encrypt the image within which the encrypted data is hidden, and the results of these methods are then compared.

3.5.1 Logistic map

Among these, logistic chaotic mapping is one of the models that is used the most. The logistic equation was improved by American ecologist May R. Logistic, often referred to as the wormhole model. In 1976, a proposal was made. At the time, the link between the number of distinct insect populations and environmental conditions was studied using the logistic equation. It was a one-dimensional nonlinear equation that was both important and basic [31]. Eq. (4) is included in the logistical map:

$$y_{n+1}=\mu y_n(1-y_n) \tag{4}$$

where, $y_0\in(0, 1)$ demonstrates the chaotic system's starting condition at any moment and $\mu\in(0, 4)$, is the bifurcation parameter also referred to as the system parameter. The next stage of the system is expressed by y_{n+1}, where n shows the discrete time. The amount of control factor has a significant impact on how the logistic map behaves μ [32].

3.5.2 Arnold cat map

The Arnold cat map, a two-dimensional chaotic system, was suggested by Vladimir Arnold in 1960. An elementary illustration of chaos theory. In order to create an NN matrix, an image must be transformed into the proper number of pixels. In the real range [0, 1), the coordinates of every pixel are represented by an ordered pair of (X, Y), which is determined by two independent equations. (5) and (6) in the following way:

$$X_{n+1}=X_n + Ay_n \ (Mod\ N) \tag{5}$$

$$Y_{n+1}=BX_n+ABY_n \ (Mod\ N) \tag{6}$$

where A, B are two positive integer control parameters, Xn, Yn are the sample locations in the N×N matrix, and n=1, 2, 3, N-1. The transformed positions after the cat map are represented by Xn+1, Yn+1. The encryption technique is implemented by a cat map iteration; after M iterations, there are T positive integers such that (Xn+1, Yn+1)=(Xn, Yn). The parameters A and B, in addition to the sample matrix size (N×N matrix), specify the time T [33, 34].

3.5.3 Baker map

The chaotic Baker map is a popular encryption technique used in image processing. It's a permutation-based tool that modifies pixel coordinates in a N*N-dimensional square matrix by using a secret key. It allots a pixel to a bijective mode-positioned pixel. The discretized Baker map may be used to generate random numbers in a square matrix. B[n1,.., nk] denotes the discretized map, while the vector [n1,..., nk] denotes the secret key, Skey. The secret key is chosen in such a way that N is the number of data items in one row, and each integer ni partitions N, with n1+...+nk=N. Assume that Ni = n1+...,+ni. As shown by Eq (7), the indices (r, s) data item is relocated to the indices [35].

$$B(r.s) = \left[\frac{N}{n_i}(r - N_i) + s\ mod\left(\frac{N}{n_i}\right).\frac{n_i}{N}\left(s - s\left(\frac{N}{n_i}\right)\right) + N_i\right] \tag{7}$$

The following procedures are taken to complete the chaotic permutation:

(1) N rectangles of width n_i are formed, and the N*N square matrix is formed by dividing the number of components N.

(2) In the permuted rectangle, each rectangle's components are arranged in a row. Upper triangles are taken first, then lower rectangles, going from left to right.

Within every rectangle, the scan moves up from the bottom left corner [36].

3.5.4 Sending encrypted image from client to server using TCP/IP protocol

Transmission Control Protocol (TCP) and Internet Protocol (IP) are two of the most significant protocols that are part of the TCP/IP protocol suite. TCP/IP, like other networking software, is arranged in layers. Simple interfaces are used by layers to interact with those both above and below them. A layer utilizes the services offered by the layer below in order to give a solution to the layer from above [37]. Data is sent from the client to the server, where it is processed inversely on the server side to produce encrypted patient data.

3.5.5 Attack types in images

This section introduces some frequent attacks in picture processing [38]:

(1) Ciphertext-only
(2) Known-plaintext
(3) Chosen-plaintext
(4) Brute-force
(5) Differential attack
(6) Noise
(7) Occlusion
(8) Entropy

4. EXPERIMENTAL RESULTS ANALYSIS

The statistical analysis parameters used to assess the efficacy of encryption include Mean Squared Error (MSE), Root Mean Squared Error (RMSE), Normalized Root Mean Squared Error (NRMSE), Peak Signal-to-Noise Ratio (PSNR), Structural Similarity Index (SSIM), Information Entropy (IE), Correlation Coefficient, and Execution Time (ET). Table 1 provides specific measurements for several of them [39, 40].

A set of medical images was utilized to test the suggested system as shown in Table 2.

The Figures 4-9 show the results testing of the three chaotic maps used in this work.

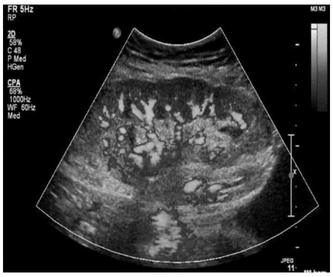
Table 1. A technique for picture encryption evaluation

Metric	Description	Formula	Highlights
Mean Squared Error (MSE)	Error levels that separate the plain picture from the encrypted image are evaluated. MSE Range:0 to ∞	MSE= $\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\ [P(i\ .j)-C(i\ .j)]^2}{MN}$ where M and N stand for the photo's height and breadth, respectively. P (i, j) represents the image's (i. j)th pixel value, whereas C(i, j) represents the decrypted photo's (i. j)th pixel value.	The MSE for good quality photos should be close to zero.
Peak Signal to Noise Ratio (PSNR)	A comparison of the decrypted and unencrypted image quality is presented. Its decibel (dB) value falls within the PSNR range: 0 to ∞	$PSNR=\frac{10\log_{10}(2^n-1)^2}{MSE}$ where n is the number of bits per pixel	When comparing an original picture and decrypted images, the PSNR value should be high.
Structural Similarity Index (SSIM)	determines the homogeneity of unencrypted, connected images. It is a statistic for gauging the quality of encrypted photos. Range of SSIM: -1 to +1	$SSIM\ (x.y)=[l(x.y)]^{\alpha}\cdot[c(x.y)]^{\beta}\cdot[s(x.y)]^{\gamma}$ Here, are the positive constants and α, β, and γ are the positive constants. "l" stands for luminance, which is used to compare brightness between two images; "c" for contrast, which is used to compare the contrast between the brightest and darkest regions of two images; and "s" for structure, which is used to compare the local luminance pattern between two images to find similarities and differences between the images.	SIMM should be one between a plain image and a decrypted image.
Information Entropy (IE)	One uses the average data per bit in a picture to compute it. Every pixel has a unique value. Range of IE: 0 to +8	Entropy $=-\sum_{i=0}^{2^n-1}P(m_i)\log_2[P(m_i)]$ where $P(m_i)$ denotes the occurrence probability of the gray level i, and i=0, 1, 2, ..., 2^n. The 2^n is an image's number of grayscale levels.	For an 8-bit picture, the quantity of IE ought to be close to 8.
Execution Time (ET)	Process of encryption It is an accumulation of run time and compilation time. It is measured in milliseconds, seconds, and minutes.	——	Any encoding method should have a lower ET value.

Table 2. Results of picture encryption evaluation metrics

Pic. No.	Chaotic Map Type	SSIM	PSNR	MSE	RMSE	NRMSE	Entropy	Correlation Coefficient	Encryption Time in Sec.	Decryption Time in Sec.
1	Logistic Map	87.9153	0.9999	0.0001	0.0102	0.0001	5.4102	0.3907	0.107	0.054
	Arnold CAT Map	87.2622	0.9999	0.0001	0.0110	0.0001	5.4102	0.3907	0.112	0.062
	Baker Map	86.0385	0.9999	0.0001	0.0127	0.0001	5.4102	0.3907	0.114	0.054
2	Logistic Map	85.8449	0.9999	0.0001	0.0130	0.0001	5.9251	0.9999	0.48	0.333
	Arnold CAT Map	85.2964	0.9999	0.0001	0.0138	0.0001	5.9251	0.9999	0.439	0.327
	Baker Map	85.4462	0.9999	0.0001	0.0136	0.0001	5.9251	0.9999	0.469	0.338
3	Logistic Map	85.2964	0.9999	0.0001	0.0138	0.0002	3.1338	0.9999	0.103	0.44
	Arnold CAT Map	85.0810	0.9999	0.0001	0.0142	0.0002	3.1339	0.9999	0.106	0.41
	Baker Map	85.2235	0.9999	0.0001	0.0139	0.0002	3.1338	0.9999	0.113	0.39
4	Logistic Map	85.1517	0.9999	0.0001	0.0140	0.0002	3.9733	0.9999	0.452	0.459
	Arnold CAT Map	85.2235	0.9999	0.0001	0.0139	0.0002	3.9733	0.9999	0.432	0.382
	Baker Map	85.2964	0.9999	0.0001	0.0138	0.0002	3.9733	0.9999	0.444	0.386
5	Logistic Map	84.7442	0.9999	0.0001	0.1047	0.0004	2.7972	0.9999	0.209	0.181

	Arnold CAT Map	85.3707	0.9999	0.0001	0.0137	0.0003	2.7970	0.9999	0.223	0.187
	Baker Map	85.4462	0.9999	0.0001	0.0136	0.0003	2.7970	0.9999	0.206	0.179
6	Logistic Map	85.2235	0.9999	0.0001	0.0139	0.0002	2.5655	0.9999	0.398	0.285
	Arnold CAT Map	85.8449	0.9999	0.0001	0.0130	0.0002	2.5653	0.9999	0.39	0.252
	Baker Map	84.7442	0.9999	0.0002	0.0147	0.0002	2.5657	0.9999	0.39	0.27



600×600

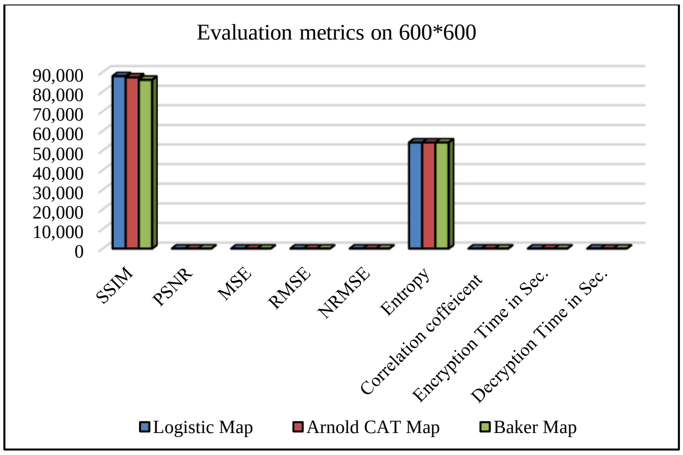
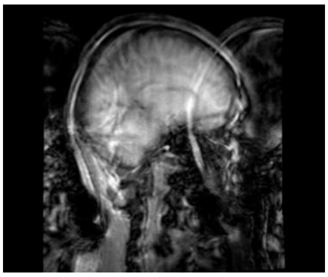


Figure 4. Evaluation metrics on 600*600 image



640×480

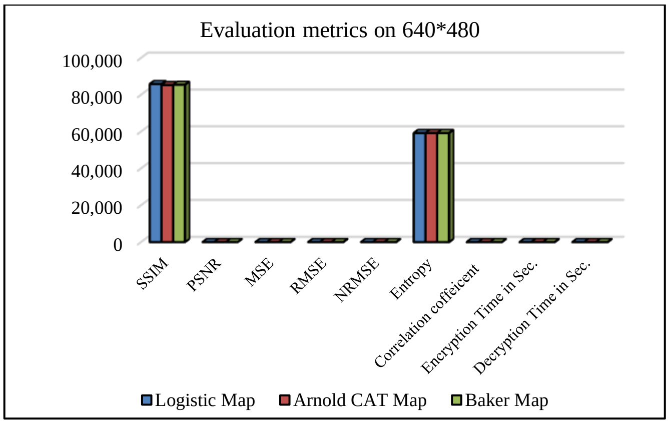
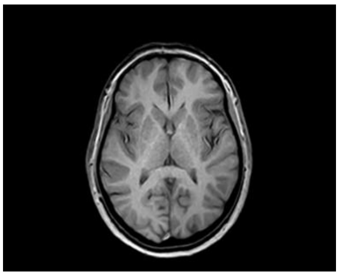


Figure 5. Evaluation metrics on 640*480 image



900×900

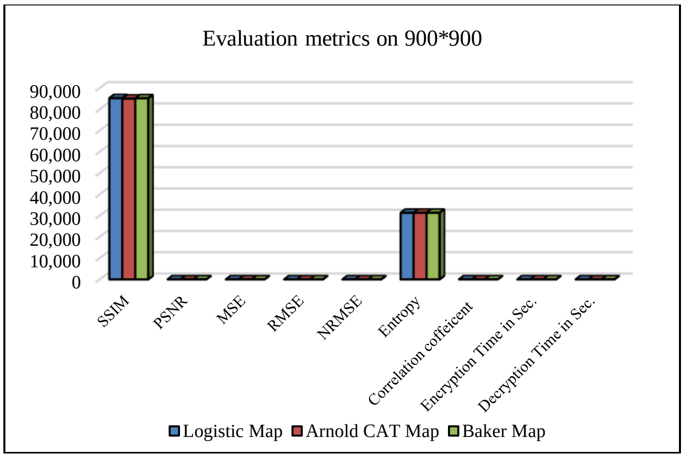
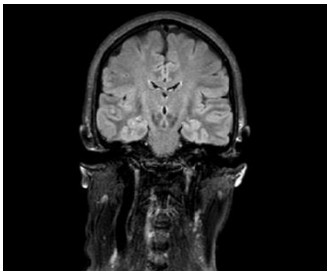


Figure 6. Evaluation metrics on 900*900 image



480×480

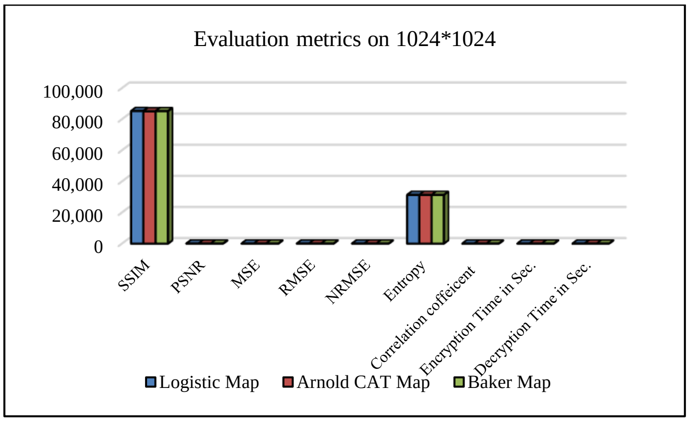


Figure 7. Evaluation metrics on 1024*1024 image

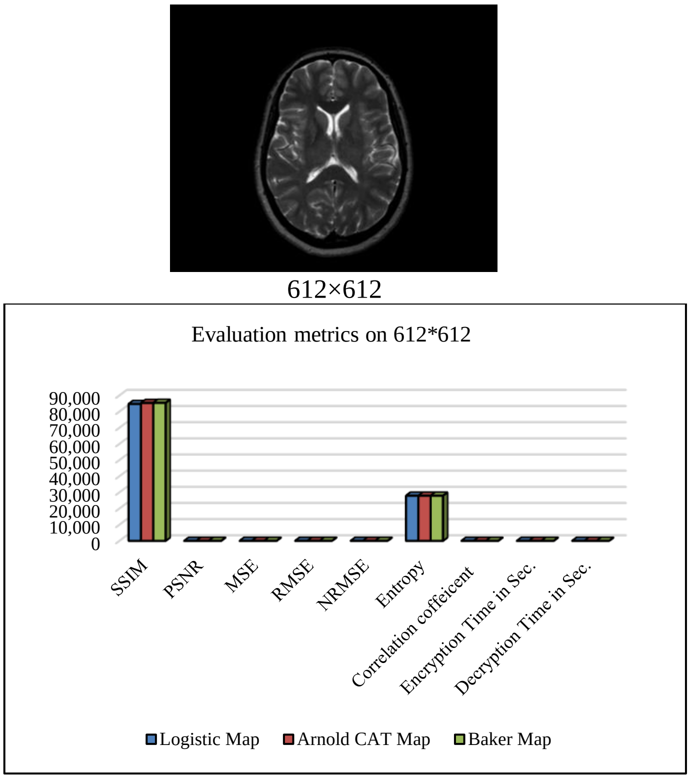


Figure 8. Evaluation metrics on 612*612 image

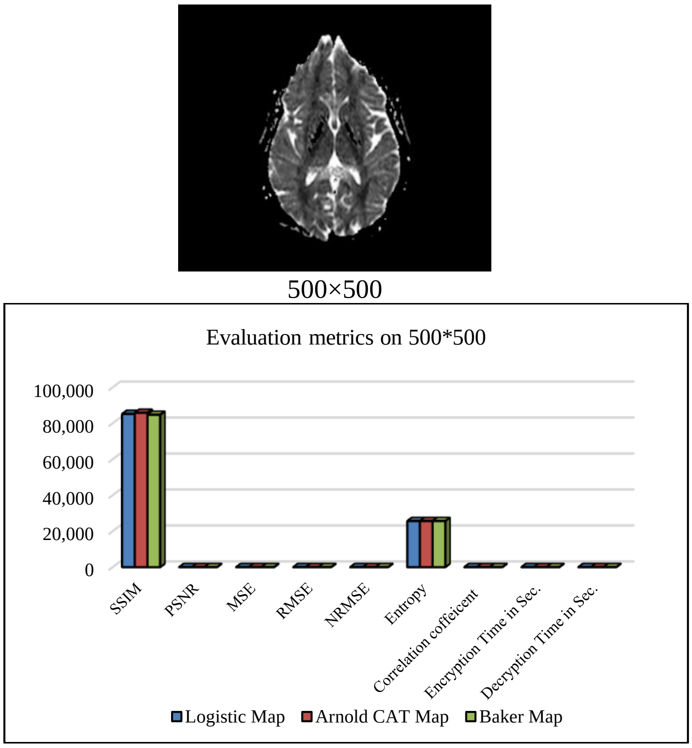


Figure 9. Evaluation metrics on 500*500 image

It is evident from the preceding table and charts that, when employing the three chaotic maps, the scale values are extremely similar and barely differ at all. Using Arnold's cat map, the maximum similarity scale value was 85.8449, while the lowest value was 84.8758. All test results showed a PSNR of 0.9999 and an MSE of 0.0001, indicating that the image was recovered with the lowest feasible error rate following encoding. This holds true for the NRMSE values, which varied from 0.0001 to 0.0002, and the RMSE values, which varied from 0.0136 to 0.0145. These numbers have the same importance as the MSE scale. Lastly, the range of entropy values was 3.1338 to 5.925.

5. CONCLUSIONS

Encrypting medical images might potentially address many different e-health application problems. The issues include identity theft, data security, private data exchange, administration, and storage of e-health data. This study presented a unique technique to medical picture encryption based on three chaotic maps (Logistic, Arnold CAT, and Baker) and the 3DES and AES algorithms. The BAT optimization process is also utilized to perform key creation. Finally, the Least Significant Bit (LBS) is utilized to conceal encrypted medical images before they are sent to the server over the TCP/IP protocol. The experiments produced promising results in MSE, PSNR, and SSIM, demonstrating that the image is returned exactly as it is, with no loss or data loss. In the case of collection, entropy results were within range and did not surpass 8 degrees. In addition, in all situations, the execution time was fractions of a second or less.

For future works, we suggest using another chaotic maps with dataset instead of randomly selected medical images.

ACKNOWLEDGMENT

This work has been prepared for scientific and research purposes only, and to assist researchers in various fields and specializations.

REFERENCES

[1] Alawida, M., Samsudin, A., Teh, J.S., Alkhawaldeh, R.S. (2019). A new hybrid digital chaotic system with applications in image encryption. Signal Processing, 160: 45-58. https://doi.org/10.1155/2020/9597619

[2] Ali, T.S., Ali, R. (2020). A new chaos based color image encryption algorithm using permutation substitution and Boolean operation. Multimedia Tools and Applications, 79(27-28): 19853-19873. https://doi.org/10.1007/s11042-020-08850-5

[3] Arab, A., Rostami, M.J., Ghavami, B. (2019). An image encryption method based on chaos system and AES algorithm. The Journal of Supercomputing, 75: 6663-6682. https://doi.org/10.1007/s11227-019-02878-7

[4] Broumandnia, A. (2019). Designing digital image encryption using 2D and 3D reversible modular chaotic maps. Journal of Information Security and Applications, 47: 188-198. https://doi.org/10.1016/j.jisa.2019.05.004

[5] Ghadirli, H.M., Nodehi, A., Enayatifar, R. (2019). An overview of encryption algorithms in color images. Signal Processing, 164: 163-185. https://doi.org/10.1016/j.sigpro.2019.06.010

[6] Ismail, S.M., Said, L.A., Radwan, A.G., Madian, A.H., Abu-Elyazeed, M.F. (2018). Generalized double-humped logistic map-based medical image encryption. Journal of Advanced Research, 10: 85-98. https://doi.org/10.1016/j.jare.2018.01.009

[7] Kamal, S.T., Hosny, K.M., Elgindy, T.M., Darwish, M.M., Fouda, M.M. (2021). A new image encryption

algorithm for grey and color medical images. IEEE Access, 9: 37855-37865. https://doi.org/10.1109/ACCESS.2021.3063237

[8] Kandar, S., Chaudhuri, D., Bhattacharjee, A., Dhara, B.C. (2019). Image encryption using sequence generated by cyclic group. Journal of Information Security and Applications, 44: 117-129. https://doi.org/10.1016/j.jisa.2018.12.003

[9] Khan, J.S., Kayhan, S.K. (2021). Chaos and compressive sensing based novel image encryption scheme. Journal of Information Security and Applications, 58: 102711. https://doi.org/10.1016/j.jisa.2020.102711

[10] Wang, R., Deng, G.Q., Duan, X.. (2021). An image encryption scheme based on double chaotic cyclic shift and Josephus problem. Journal of Information Security and Applications, 58: 102699. https://doi.org/10.1016/j.jisa.2020.102699

[11] Luo, Y., Ouyang, X., Liu, J., Cao, L. (2019). An image encryption method based on elliptic curve elgamal encryption and chaotic systems. IEEE Access, 7: 38507-38522. https://doi.org/10.1109/ACCESS.2019.2906052

[12] Heo, J., Jeong, J. (2021). Deceptive techniques to hide a compressed video stream for information security. Sensors, 21(21): 7200. https://doi.org/10.3390/s21217200

[13] Askar, S.S., Karawia, A.A., Alshamrani, A. (2015). Image encryption algorithm based on chaotic economic model. Mathematical Problems in Engineering, 2015: 341729. https://doi.org/10.1155/2015/341729

[14] Bhogal, R.S., Li, B., Gale, A., Chen, Y. (2018). Medical image encryption using chaotic map improved advanced encryption standard. IJ Information Technology and Computer Science, 8: 1-10. https://doi.org/10.1155/2022/9363377

[15] Al-Khasawneh, M.A., Shamsuddin, S.M., Hasan, S., Bakar, A.A. (2018). An improved chaotic image encryption algorithm. In 2018 International conference on smart computing and electronic enterprise (ICSCEE), pp. 1-8. https://doi.org/10.1007/s10586-021-03466-2

[16] Gatta, M.T., Abd Al-latief, S.T. (2018). Medical image security using modified chaos-based cryptography approach. In Journal of Physics: Conference Series, 1003(1): 012036. https://doi.org/10.1088/1742-6596/1003/1/012036

[17] Kumar, S., Panna, B., Jha, R.K. (2019). Medical image encryption using fractional discrete cosine transform with chaotic function. Medical & Biological Engineering & Computing, 57: 2517-2533. https://doi.org/10.1007/s11517-019-02037-3

[18] Farah, M.B., Farah, A., Farah, T. (2020). An image encryption scheme based on a new hybrid chaotic map and optimized substitution box. Nonlinear Dynamics, 99(4): 3041-3064. https://doi.org/10.1007/s11071-019-05413-8

[19] Yin, S., Li, H. (2021). GSAPSO-MQC: medical image encryption based on genetic simulated annealing particle swarm optimization and modified quantum chaos system. Evolutionary Intelligence, 14: 1817-1829. https://doi.org/10.1007/s12065-020-00440-6

[20] Yasser, I., Khalifa, F., Mohamed, M.A., Samrah, A.S. (2020). A new image encryption scheme based on hybrid chaotic maps. Complexity, 2020. https://doi.org/10.1155/2020/9597619

[21] Akan, J.B., Adedokun, E.A., Onuh, G., Umar, A., Nwosu, R.I., Ibrahim, Y. (2020). Medical image encryption scheme based on hybrid chaotic permutation. International Journal of Scientific Research in Computer Science and Engineering, 8(4): 97-104.

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

[23] Chaudhary, N., Shahi, T.B., Neupane, A. (2022). Secure image encryption using chaotic, hybrid chaotic and block cipher approach. Journal of Imaging, 8(6): 167. https://doi.org/10.3390/jimaging8060167

[24] Abdallah, A.A., Farhan, A. (2022). A new image encryption algorithm based on multi chaotic system. Iraqi Journal of Science, 63(1): 324-337. https://doi.org/10.24996/ijs.2022.63.1.31

[25] Rachmawanto, E.H., Zulfiningrum, R. (2022). Medical image cryptosystem using dynamic Josephus sequence and chaotic-hash scrambling. Journal of King Saud University-Computer and Information Sciences, 34(9): 6818-6828. https://doi.org/10.1016/j.jksuci.2022.04.002

[26] Umar, S.U., Rashid, T.A. (2021). Critical analysis: bat algorithm-based investigation and application on several domains. World Journal of Engineering, 18(4): 606-620. https://doi.org/10.1108/WJE-10-2020-0495

[27] Zebari, A.Y., Almufti, S.M., Abdulrahman, C.M. (2020). Bat algorithm (BA): review, applications and modifications. International Journal of Scientific World, 8(1): 1-7. https://doi.org/10.14419/ijswv8i1.30120

[28] Smid, M.E. (2021). Development of the advanced encryption standard. Journal of Research of the National Institute of Standards and Technology, 126: 126024. https://doi.org/10.6028/jres.126.024

[29] Sari, C.A., Rachmawanto, E.H., Haryanto, C.A. (2018). Cryptography triple data encryption standard (3DES) for digital image security. Scientific Journal of Informatics, 5(2): 105-117. https://doi.org/10.15294/sjiv5i2.14844

[30] Msallam, M.M. (2020). A development of least significant bit steganography technique. IRAQI Journal of Computers, Communications, Control and Systems Engineering, 20(1): 31-39. https://doi.org/10.33103/uot.ijccce.20.1.4

[31] Rostami, M.J., Shahba, A., Saryazdi, S., Nezamabadi-pour, H. (2017). A novel parallel image encryption with chaotic windows based on logistic map. Computers & Electrical Engineering, 62: 384-400. https://doi.org/10.1016/j.compeleceng.2017.04.004

[32] Ali, T.S., Ali, R. (2022). A novel color image encryption scheme based on a new dynamic compound chaotic map and S-box. Multimedia Tools and Applications, 81(15): 20585-20609. https://doi.org/10.1007/s11042-022-12268-6

[33] Elmacı, D., Baş Çatak, N. (2018). An efficient image encryption algorithm for the period of arnold's CAT map. International Journal of Intelligent Systems and Applications in Engineering, 6(1): 80-84. https://doi.org/10.18201/ijisae.2018637935

[34] Hariyanto, E., Rahim, R. (2016). Arnold's cat map algorithm in digital image encryption. International Journal of Science and Research (IJSR), 5(10): 1363-1365. https://doi.org/10.21275/ART20162488

[35] Alhumyani, H. (2020). Efficient image cipher based on baker map in the discrete cosine transform. Cybernetics and Information Technologies, 20(1): 68-81. https://doi.org/10.2478/cait-2020-0005

[36] Musanna, F., Kumar, S. (2020). Image encryption using quantum 3-D Baker map and generalized gray code coupled with fractional Chen's chaotic system. Quantum Information Processing, 19: 1-31. https://doi.org/10.1007/s11128-020-02724-3

[37] Pande, A.P., Devane, S.R. (2018). Study and analysis of different TCP variants. In 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), pp. 1-8. https://doi.org/10.1109/ICCUBEA.2018.8697750

[38] Kaur, M., Kumar, V. (2020). A comprehensive review on image encryption techniques. Archives of Computational Methods in Engineering, 27: 15-43. https://doi.org/10.1155/2021/5012496

[39] Priyanka, Singh, A.K. (2023). A survey of image encryption for healthcare applications. Evolutionary Intelligence, 16(3): 801-818. https://doi.org/10.1007/s12065-021-00683-x

[40] Talhaoui, M.Z., Wang, X., Midoun, M.A. (2021). Fast image encryption algorithm with high security level using the Bülban chaotic map. Journal of Real-Time Image Processing, 18: 85-98. https://doi.org/10.1007/s11554-020-00948-1