SEBHA UNIVERSITY CONFERENCE PROCEEDINGS, VOL.03 NO. 2 2024
DOI: 10.51984/SUCP.V3I2.3293

وقائع مؤتمرات جامعة سبها
Sebha University Conference Proceedings

Confrence Proceeeding homepage: http://www.sebhau.edu.ly/journal/CAS

Studying the Effect of the Primary Coefficients (X, U) of the Logistic Chaotic Encryption Algorithm Equation on the Performance of X-Ray Medical Image Encryption

*Hanan Ahmed Sahib, Kawther H. Al-khafaji

Faculty of Education for Girls, Kufa University, Kufa, Iraq

Keywords:
Chaotic
Logistic
Decryption
Encryption
X-Ray Image

ABSTRACT

An image encryption method based on the chaotic logistic encryption algorithm was applied on X-ray medical image, using the histogram of the X-ray image and the plot showing the correlation between adjacent pixels to verify the encryption effect of this encryption algorithm. In order to reflect the effect of the algorithm in encrypting image information, use MATLAB to display the encryption. Subsequent image and histogram analysis can intuitively find that the chaotic logistic encryption algorithm has a better effect on encrypting image information, and the statistical data well hides the characteristics of the original image, which can effectively resist statistical attacks based on image pixel values. Image encryption effect and multiple image quality metrics are applied to verify the encryption effect of this encryption algorithm, this method was applied to medical images of the type of X-ray Through the application of a number of image quality standards, the extent of the influence of the parameter X.

دراسة تأثير المعاملات الأولية (X، U) لمعادلة خوارزمية التشفير الفوضوي اللوجستي على أداء تشفير الصور الطبية السينية

*حنان احمد صاحب الحيدري و كوثر حسن صاحب الخفاجي

كلية التربية للبنات ،جامعة الكوفة، الكوفة، العراق

الكلمات المفتاحية:
التشفير
صورة الاشعة السينية
فوضوية
فك التشفير
لوجستية

الملخص

تم تطبيق طريقة تشفير الصور المعتمدة على خوارزمية التشفير اللوجستي الفوضوي على صورة الأشعة السينية الطبية، وذلك باستخدام الرسم البياني لصورة الأشعة السينية والمؤامرة التي توضح الارتباط بين وحدات البكسل المجاورة للتحقق من تأثير التشفير لخوارزمية التشفير هذه. لكي يعكس تأثير الخوارزمية في تشفير معلومات الصورة، استخدم MATLAB لعرض التشفير. يمكن لتحليل الصور والرسم البياني اللاحق أن يجد بشكل بديهي أن خوارزمية التشفير اللوجستي الفوضوي لها تأثير أفضل على تشفير معلومات الصورة، وأن البيانات الإحصائية تخفي جيدًا خصائص الصورة الأصلية، والتي يمكنها مقاومة الهجمات الإحصائية بشكل فعال بناءً على قيم بكسل الصورة. تم تطبيق تأثير تشفير الصور ومقاييس جودة الصورة المتعددة للتحقق من تأثير تشفير خوارزمية التشفير هذه، وتم تطبيق هذه الطريقة على الصور الطبية من نوع الأشعة السينية من خلال تطبيق عدد من معايير جودة الصورة، ومدى تأثيرها المعلمة X.

1. Introduction

Telemedicine is an emerging domain that involves the remote delivery of medical services to patients, in which neither the patient nor the healthcare provider are physically co-located. Confidential patient information, including medical images, is transmitted via Internet or cellular network communication channels. An advanced healthcare system necessitates a streamlined framework that can securely store medical images, ensuring that only authorized users have access to them regardless of their location on the geological surface. The majority of the researchers' efforts have been devoted to developing computer-based approaches to enhance patient care. However, there has been a certain degree of latency in the development of methods to attain the intended level of security for sensitive data in both storage systems and communication channels. One approach to safeguarding medical images in this circumstance is by employing encryption schemes that render the images unusable for users who do not possess the corresponding encryption information. [4]

Decryption pertains to the inverse procedure through which encrypted data is regenerated into plain text, whereas encryption involves the conversion of unencrypted data to encrypted data. The four primary objectives of cryptography are information authentication,

*Corresponding author:
E-mail addresses: hanana.alhaida@student.uokufa.edu.iq, (K. H. Al-khafaji) Kutherh.kafajy@uokufa.edu.iq

Article History : Received 06 June 2024 - Received in revised form 24 August 2024 - Accepted 06 October 2024

confidentiality, integrity, and non-repudiation [3]. Prior to transmission over public networks, the raw data undergoes a transformation into a representation devoid of any additional information that renders it meaningless.

Encryption is repeatedly recommended as a means to guarantee the security of medical images within the healthcare sector. The initial image is converted into a cypher image according to this scheme, thereby restricting access to its contents to authorized users only. Unauthorised users are thereby thwarted from accessing the data. Presently, cryptography is widely utilised due to the substantial security advantages it offers. [2]

Images utilised in the medical domain are typically regarded as sensitive data within bio information systems. In order to transmit images of this nature over a network, a secure encryption algorithm is indispensable. Over the past few decades, numerous image encryption algorithms have been proposed by researchers. The Data Encryption Standard algorithm is the earliest algorithm in use for encryption, and its cost computations require the least amount of time. Either symmetric or asymmetric algorithms can be utilised to encrypt images in a highly efficient manner. [7]

Researchers encounter numerous obstacles when attempting to develop techniques that are impervious to assaults and practical in nature. To accomplish this, sophisticated mathematical models and novel algorithms are implemented. The objective of this paper is thus to propose an image encryption algorithm based on chaos. [6]

Chaos refers to an unpredictable and pseudo-random motion that arises within a deterministic dynamical system as a result of its susceptibility to initial values and parameters. The investigation of chaos theory emerged from H. Poincare's 1913 examination of the three-body problem. E. N. Lorenz introduced the Lorenz equation in 1963, the initial instance of a chaotic solution arising from a deterministic equation in a dissipative system, subsequent to an extensive series of investigations. In their 1975 paper "Period Three Implies Chaos," Tienyien Li and James A. Yorke coined the term "chaos" to denote this phenomenon.

The Logistic map, initially introduced by Robert M. May in a 1976 article, underwent extensive examination by M.J. Feigenbaum, who in 1978 postulated on its universal applicability. Since then, there has been significant progress in the study of pandemonium.

1989 saw the explicit proposal of the "chaotic encryption" algorithm by Robert Matthews. Subsequently, scholars have investigated the transition of systems from structured to disordered states, as well as the characteristics of chaotic systems. Extensive research has been conducted in the years that followed on chaos-based cryptography, which has also entered the stage of practical application. [5] Chaotic systems demonstrate an assortment of captivating characteristics, such as their exactness, ergodicity, and sensitivity to initial conditions and control parameters. Certain prerequisites for pseudo-random coding (i.e., chaotic) and cryptography are applicable to virtually any property. [1]

2. Chaotic Logistic Map Theory

1975 saw the publication of the article "Period 3 Means Chaos" by American mathematician York and Chinese-American Li Tianyan. In it, they introduced the term "chaos" and provided its first mathematical definition, which has had a profound impact on the field of chaos studies and has since inspired extensive research on the subject. Chaos denotes the capricious and uncertain movement that arises within a deterministic dynamic system as a result of its sensitivity to initial values. The formula for logistic mapping represents a typical nonlinear iterative Equation.

$$X_{k+1} = U X_k(1 - X_k) \mathrm{k} = 0,1,\dots \mathrm{n} \ , \mathrm{X_k} \in (0,1) \qquad (1)$$

Where;

$(X_{(k+1)})$ referred to as the control parameter of logistic mapping,

k represents the time increment of the iteration.

U The system parameter.

X The initial value

Logistic mapping's dynamic behaviour is highly dependent on the control parameter U. The characteristics of the system vary depending on the value of u; for instance, as (k) approaches infinity, the change in X_k will be distinct. one of them According to research, logistic mapping is characterized by two primary parameters: the initial value (X) and the system parameter (U). Logistic demonstrates periodicity when ($0<U\leq 3.5699456$) conversely, it enters a chaotic state when the mapping equation fulfills the conditions ($0<X<1$) and ($3.5699456<U\leq 4$). In other words, it is in a state of disorder, unpredictability, chaos, and untouchability. The generated sequence is aperiodic, non-convergent, and sensitive to initial conditions for a given initial value (X).[5,8]

3. Chaotic maps and systems classification

A map that demonstrates chaotic behavior is said to be a chaotic map. A discrete-time or continuous-time parameter can be used to parameterize a map. Discrete maps are usually the iterated functions. Chaotic maps are frequently occurs in the study of dynamical systems. [9] Chaotic maps can be classified as discrete one dimensional or multi-dimensional maps and Continuous systems. Whereas continuous maps(systems) are parameterized by a continuous time parameter; they are governed by differential equations. [9, 10]

The low-dimensional chaotic map is a discrete iterative dynamic system. Al-though its model is simple, it embodies very complicated dynamic behavior. Commonly used low-dimensional chaotic system are like logistic map and tent map. High-dimensional chaotic maps are mainly continuous chaotic system and hyper chaotic system. A significant characteristic of hyper chaotic system is that they have at least two positive Lyapunov exponents. A hyper chaotic system is meant to create more complex nonlinear dynamic behavior.

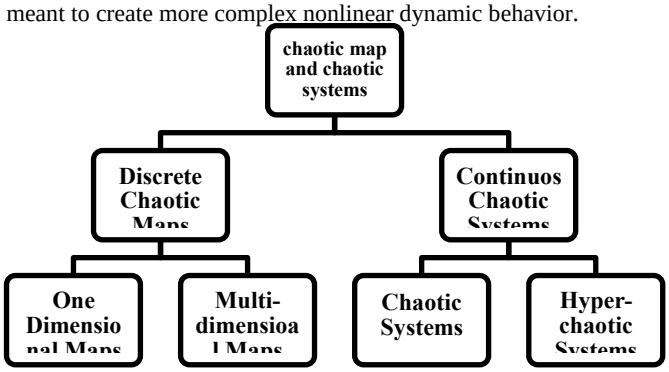


Fig .1: Chaotic maps and systems classification

A discrete chaotic map represents a dynamic system characterized by time-varying discrete state variables. Among other qualities, the discrete chaotic map is distinguished by its nonlinearity, sensitivity to initial conditions and parameters, and period multiplication [5].

Table 1: Some mathematically defined examples of discrete chaotic maps

Logistic map	$X_{k+1} = f_l(X_n) = U X_k(1 - X_k$	*(2)*
Tent map	$X_{k+1} = f_t(X_n) = \begin{cases} uX_k & , X_k < \frac{1}{2} \\ u(1 - X_k), & \frac{1}{2} \leq X_k \end{cases}$	*(3)*
Arnold Cat map	$\begin{cases} X_{k+1} = (2X_k + Y_k) \\ Y_{k+1} = X_t + Y_t \end{cases}$	*(4)*
Henon map	$\begin{cases} X_{k+1} = 1 - aX_k^2 + Y_k \\ Y_{k+1} = bX_k \end{cases}$	*(5)*

4. Proposed Algorithms

As shown in the figure, in this research we proposed an encryption and decryption algorithm based on the logistic map and the chaotic system by changing the initial parameters.

4.1 The Algorithm For Image Encryption

Step1: loading the original chest X-Ray image from the system.

Step2: Resize the input X-Ray image and Converted into a two-dimensional chaotic encryption sequence.

Step3:Converted intoa two-dimensional chaotic encryption sequence.

Step4: Return the elements of matrix to an (M×N)matrix reshape(Img), where Img is a chaotic matrix.

Step5: Operation encryption (Logistic chaotic sequence encryption)

Step6: Enter the symmetric encryption key

Step7: Determined the initial value of the parameter X and parameter U

Step8: Converting the image to uint8, the image will become two-dimensional, the original X-Ray image is (168×168×3) three channels

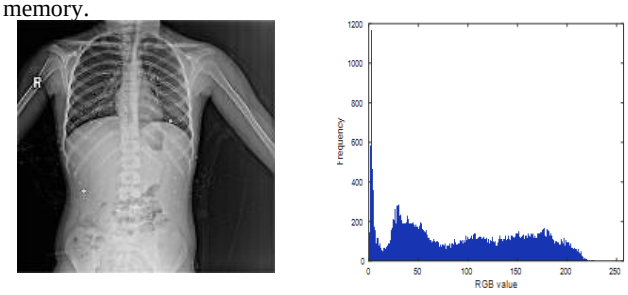
and then converted to (168×504).
Step9: Reshape the elements in encrypted image into an (M×N/3×3) matrix.

4.2 The Algorithm For Image Decryption

Step1: Resize the input image and Converted into a two-dimensional chaotic encryption sequence.
Step2: Enter the symmetric decryption key
Step3: Converted into a two-dimensional chaotic encryption sequence.
Step4: Return the elements of uint8 type matrix to an (M×N) matrix Img, where Img is a chaotic matrix.
Step5: Conversion is performed in the order of the columns, that is, the first column is read, the second column is read, and the column is stored.
Step6: Operation encryption (Logistic chaotic sequence encryption)
Step7:- converting the image to uint8, the image will become two-dimensional, the original picture is (168×168×3) three channels and then converted to (168×504).
Step8:- Reshape the elements in encrypted image into an (M×N/3×3) matrix.
Step9:- Getting the decrypted image .

5 Image Acquisition

The dataset of images that are used for the experimental purposes is chest x-ray medical images. The images were obtained from the Chest Diseases Centre at Al-Hakim Hospital in Najaf. The image of dimensions (168 x 168) was used in our database. To verify and prove the feasibility and security of the proposed image encryption system, all the data and numerical simulations were carried out using the MATLAB 2021a environment, have been conducted. on a laptop running Windows 10 Pro 64-bit, System Model: Lenovo PC, with a core Processor: Intel(R) Core (i5)-500U, 2.5 GHz, and 8.0GB memory.



(a) **(b)**

Fig. 2: a. X-ray original image , b. . X-ray original image histogram

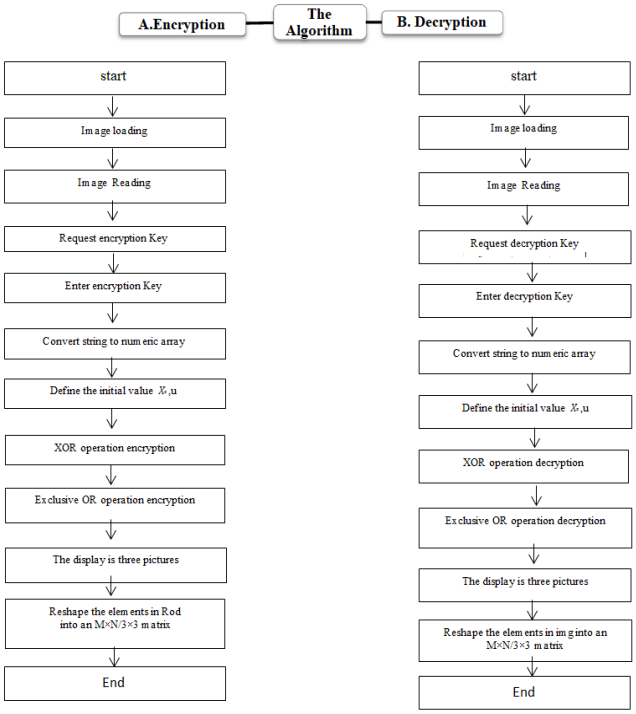


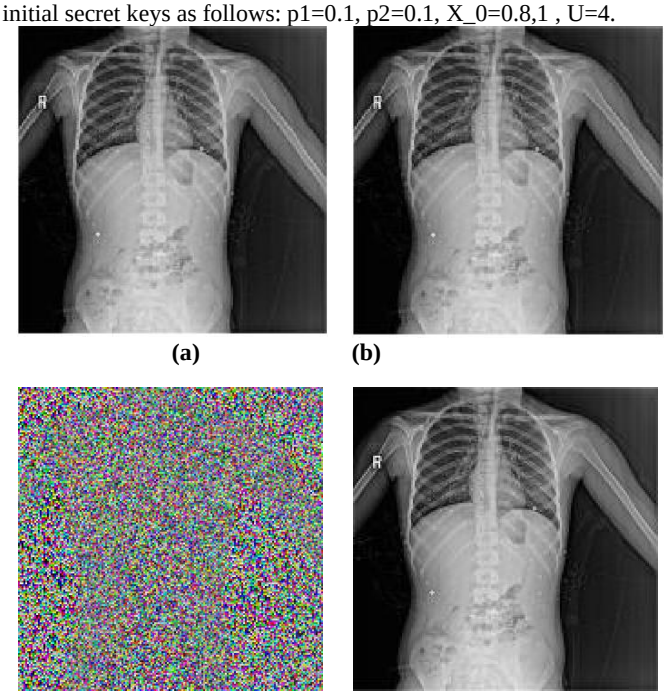
Fig. 3: Encryption and Decryption Algorithm Using Chaotic Maps

6 Encryption-Decryption Results

This section mainly introduces the overall process of our proposed method, gives some evaluation metrics to evaluate the quality of medical image encryption.

6.1 The Effect of changing (X) value and Histogram Analysis

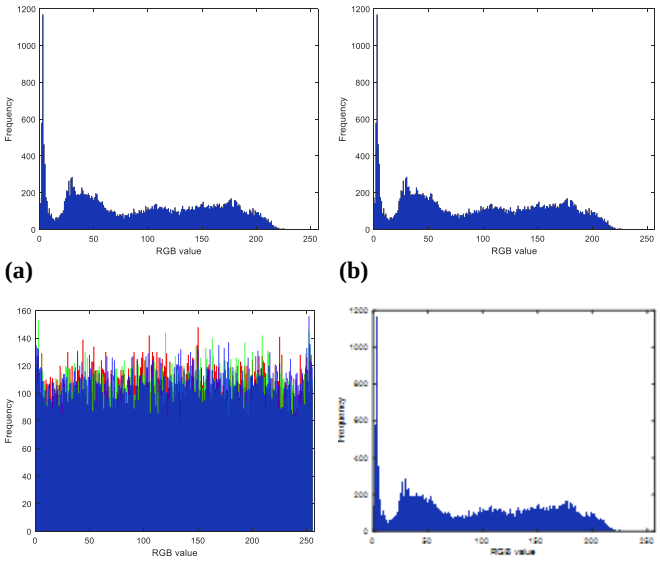
In order to simulate the proposed algorithm in MATLAB, a 168 x 168 standard grayscale x-ray image is selected as the basic image, Set the initial secret keys as follows: p1=0.1, p2=0.1, X_0=0.8,1 , U=4.



(a) **(b)**

(c) **(d)**

Fig. 4: The results display of the encrypted image (a ,c) and decrypted image (b, d) with(X=1 ,0.8 ,U=4) respectively



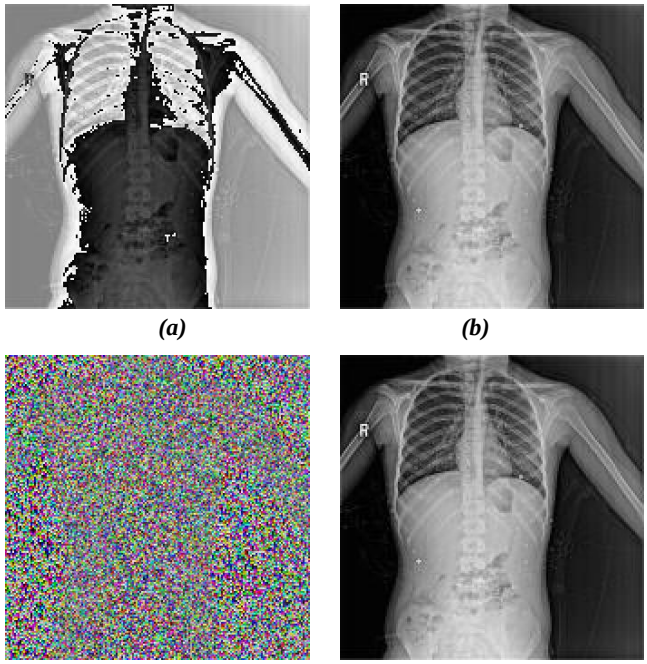
(a) **(b)**

(c) **(d)**

Fig. 5: the Encrypted image histogram (a, c) and decrypted image histogram (b, d) with(X=1 ,0.8 ,U=4) respectively

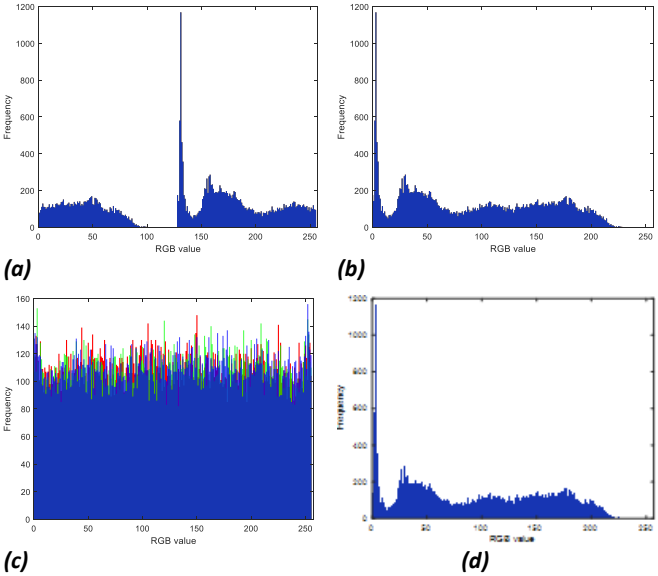
6.2 The Effect of changing (U) value and Histogram Analysis

In order to simulate the proposed algorithm in MATLAB, a 168 x 168 standard grayscale x-ray image is selected as the basic image, Set the initial secret keys as follows: p1=0.1, p2=0.1, X_0=0.1 , U= 2, 4.



(a) *(b)* *(c)* *(d)*

Fig. 6: The results display of the encrypted image (a ,c) and decrypted image (b ,d) with(U=2,4 ,X=0.1) respectively



(a) *(b)* *(c)* *(d)*

Fig. 7: the Encrypted image histogram (a, c) and decrypted image histogram (b, d) with(U=2,4 ,X=0.1) respectively

6.3 Tests Results and Pixel Correlation

This subsection provides an in-depth examination of experimental analysis. As demonstrated in the table (2), the X-ray image was encrypted using the chaotic encryption equation, and the quality of the proposed algorithm was assessed using the following image quality metrics:

Table 2 : show some IQM value in the coefficients (X , U)

IQM	X=1 U=4	X=0.8 U=4	X=0.1 U=2	X=0.1 U=4
ET	4.24	8.07	12	12.08
DT	3.62	8.20	11.96	7.59
UACI	0	0.31	0.501	0.30
NPCR	0	0.9714	1	0.9710
CC1	1	1	1	1
CC2	1	-0.003	-0.53	0.006
SNR1	37.85	37.85	1	37.85
SNR2	37.85	37.85	37.85	37.85
PSNR1	99	99	37.85	99
PSNR2	99	29.33	28.63	29.29
MSNR1	99	99	99	99
MSNR2	99	2.96	2.5243	2.94
MSE1	0	0	Inf	0
MSE2	0	75.71	4.08	76
RMSE1	0	0	0	0
RMSE2	0	8.7	89.02	8.74
LMSE1	0	0	0	0
LMSE2	0	106.1	21.8	107.5

Encryption time(ET) refers to the duration required to employ a particular technique of image encryption. It is the product of the time required to compile and execute. The encryption time for images should be kept to an absolute minimum for practical implementations. It is commonly denoted in minutes, milliseconds, or seconds.

The decryption time(DT) refers to the duration required to employ a particular procedure for decrypting an image. It is the product of the time required to compile and execute. In order to create a meaningful image, the correlation(CC) between adjacent pixels is invariably high due to the close proximity of their values. A effective encryption algorithm, on the other hand, reduces correlation and induces effect diffusion.

The subsequent procedures are executed in order to examine the disorientation effect of the encryption and assess the correlation: The following equation is used to determine the value of two pixels that are diagonally adjacent, two pixels that are adjacent vertically, and two pixels that are adjacent horizontally.

$$CC = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}(I_0 - \grave{I}_0)(I_E - \grave{I}_E)}{\sqrt{(\sum_{i=1}^{M}\sum_{j=1}^{N}(I_0 - \grave{I}_0)^2)(\sum_{i=1}^{M}\sum_{j=1}^{N}(I_E - \grave{I}_E)^2)}} \quad (6)$$

The ratio between the desired information or signal strength and the unwanted signal or background noise strength (SNR) was calculated according to the equation:[12]

$$SNR = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I_O(i,j)\right)^2}{\sum_{i=1}^{M}\sum_{j=1}^{N}\left(I_O(i,j) - I_D(i,j)\right)^2} \quad (7)$$

The quality(PSNR) was calculated between the original images and the decrypted images, as well as between the encrypted and the decrypted image [11], where the level of deterioration of the normal image after the encryption and decryption process was shown. It was measured according to the following equation:

$$PSNR(dB) = 10 \times \log_{10}\frac{(2^n - 1)^2}{MSE} \quad (8)$$

The ratio of the original signal power to the noise power (error) (MSNR)has been calculated [12]. According to the equation below:

$$MSNR = \frac{\frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N} I_O(I,j)^2}{MSE} \quad (9)$$

The comparison was made according to the degree of similarity (MSE)between the two images, according to the following equation [12]:

$$MSE = \frac{1}{M \times N}\sum_{i=1}^{M}\sum_{j=1}^{N}|I_O(I,j) - I_D(I,j)|^2 \quad (10)$$

The frequency of differences between values (sample values) predicted by the model or estimator and observed values was measured. RMSE can be calculated as follows [12]:

$$RMSE = \sqrt{\frac{\sum_{i=1}^{M}\sum_{j=1}^{N}|I_O(i,j) - I_D(i,j)|^2}{(M \times N)}} \quad (11)$$

Calculate the mean square error of Laplace based on the Laplace value of the predicted and obtained data which depends on the importance of measuring edges. LMSE is defined as follows [12]:

$$LMSE = \frac{\sum_{i=1}^{M-1}\sum_{j=1}^{N-1}[O\{I_O(I,j)\} - O\{I_D(I,j)\}]^2}{\sum_{i=1}^{M-1}\sum_{j=1}^{N-1}[O\{I_O(I,j)\}]^2} \quad (12)$$

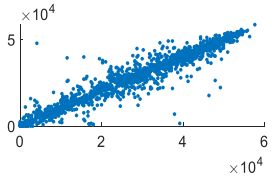


Fig. 30 :a. An neighboring pair's correlation plot x-ray original image pixels in horizontal direction**.**

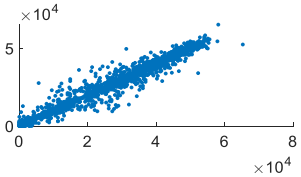


Fig .30: b. An neighboring pair's correlation plot x-ray original image pixels in Vertical direction

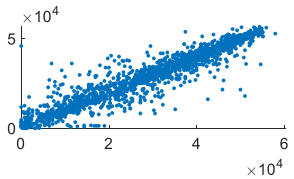


Fig .30:c. An neighboring pair's correlation plot x-ray original image pixels in diagonal direction

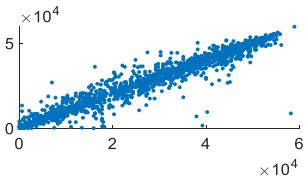


Fig .31: a. An neighboring pair's correlation plot x-ray encryption image pixels in horizontal direction with $X = 1, U = 4$

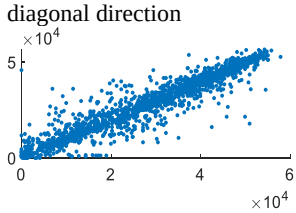


Fig .31: b .An neighboring pair's correlation plot x-ray encryption image pixels in Vertical direction with $X = 1, U = 4$

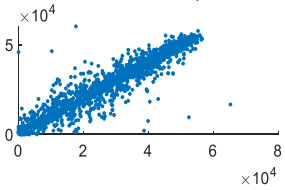


Fig .31: c An neighboring pair's correlation plot x-ray encryption image pixels in diagonal direction with $X = 1, U = 4$

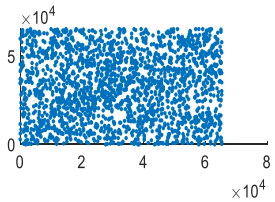


Fig .32: a. An neighboring pair's correlation plot x-ray encryption image pixels in horizontal direction with $X = 0.8, U = 4$

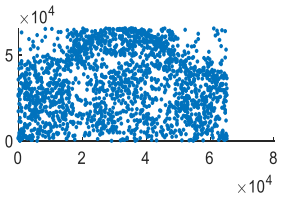


Fig .32: b An neighboring pair's correlation plot x-ray encryption image pixels in Vertical direction with $X = 0.8, U = 4$

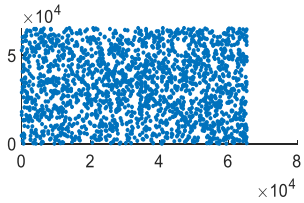


Fig 32:c.An neighboring pair's correlation plot x-ray encryption image pixels in diagonal direction with $X = 0.8, U = 4$

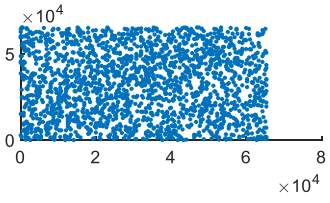


Fig .33: a An neighboring pair's correlation plot x-ray encryption image pixels in horizontal direction with $X = 0.1, U = 4$

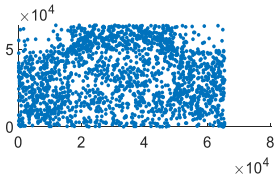


Fig .33: b. An neighboring pair's correlation plot x-ray encryption image pixels in Vertical direction with $X = 0.1, U = 4$

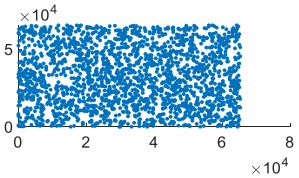


Fig .33:c. An neighboring pair's correlation plot x-ray encryption image pixels in diagonal direction with $X = 0.1, U = 4$

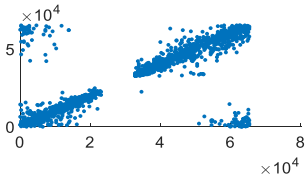


Fig .34:a. An neighboring pair's correlation plot x-ray encryption image pixels in horizontal direction with $X = 0.1, U = 2$

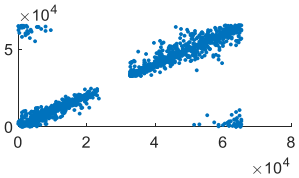


Fig .34:b. An neighboring pair's correlation plot x-ray encryption image pixels in Vertical direction with $X = 0.1, U = 2$

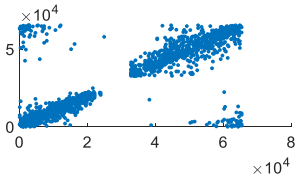


Fig .34:c An neighboring pair's correlation plot x-ray encryption image pixels in diagonal direction with $X = 0.1, U = 2$

7 Conclusion

New developments in e-health systems include both positive and negative aspects. Despite offering cutting-edge healthcare services, there are growing worries about the security of e-health data, which is very sensitive.

In this paper, a robust image encryption scheme based on a binary chaotic logistic map is proposed. In the proposed image encryption system, in order to make the picture more secure, a symmetric key was used., and the quality comparison was made for the encrypted image, the normal image, and the recovered image.

The main advantage of this algorithm is that it is easily implementable and therefore more suitable for image encryption applications. The chaos 0based image encryption algorithm has four stages: decomposition, shuffling, propagation, and merging Decomposition is the process of breaking down an original picture into its component parts. The mixing and propagation stages are essential for the security of the entire encryption algorithm. The mixing phase hides the original organization of the pixels and the propagation phase hides the original values of the pixels. One of them has no effect on how the image's pixels are distributed statistically. The latter performs the probability distribution of pixels into a uniform distribution.

Multidimensional logistic map is one of the best mathematical tools used in image encryption and analysis. Because it has a specific structure. This technology has the potential to be combined with other sports tools.

In this research, different initial parameters (belonging to the conditions of chaotic encryption and not belonging to the conditions of chaotic encryption) were used to transform the original image into an unclear image using image encryption and decryption techniques. We conclude that both encryption and chaotic decryption techniques for these images using the logistic map are secure within cryptographic conditions ,

The experimental results show that the logistic map model has achieved good application results in encoding medical images, that is, they all have a small horizontal, vertical and diagonal correlation coefficient whose value ranges from (1, -0.003, -0.53, 0.006), which indicates that our method works best when (X= 0.8, U=4) in medical image encryption.

This paper's medical picture encryption approach is more secure, resilient, and timely than competing methods, and it shows promise for use in real-world image encryption tasks.

To address the current issues with medical image encryption, we are thinking of merging images of varying sizes and encrypting them all at once. We are also thinking about ways to improve and smooth X-ray medical images before encryption, and we want to generalize the model so it works better with different kinds of medical images, protecting patients' privacy even more effectively. as well as medical records.

The MATLAB program used has a feature that shows the efficiency of the algorithms used, as efficient algorithms consume a little time to implement, unlike algorithms that take days to implement, and through the short encryption and decryption time shown in Table 2, we prove the efficiency of the algorithms, as they are fast and smooth.

Figure *4* shows how encryption occurs at the relevant limits of encryption, where the image is distorted and completely different from the original. Note C, but when encryption does not occur, the image is identical to the original image, as in Figure A. Figures B, D represent the recovered image after decryption, and we notice the amount of similarity. Between the two images, this proves the quality of the decryption algorithm. Likewise, for Hostgram, note Figure 5. Since U is the controlling parameter in the logistic map equation, when it is chosen for other values, the case becomes partially encrypted, as in Figure 6, and the graph in Figure 7 shows this.

Through the correlation relationship between adjacent pixels, we notice the relationship of pixels in the original image, Figure 30. The correlation relationship of adjacent pixels is similar to the image in which no encryption occurs, as in Figure 31, But it is not similar to the correlation relationship of adjacent pixels in the image in which complete or partial encryption occurs, as in Figure 32, 33, 34.

8 Abbreviations

No.	The Parameter Description
I_o : Original image	I_E : Encrypted image I_D : Decrypted image
1.	Execution time (ET) of images encryption and decryption in seconds
2.	Number of Pixel Change Rate ($NPCR$) between I_o and I_E
3.	Unified Average Changed Intensity ($UACI$) between I_o and I_E
4.	Correlation Coefficient Analysis (CC)
	CC1 between I_o and I_D CC2 between I_o and I_E
5.	Universal Image Quality Index (UIQI)
	UIQI1 between I_o and I_D UIQI2 between I_o and I_E
6.	Signal to Noise Ratio Index (SNR)
	SNR1 between I_o and I_D SNR2 between I_o and I_E
7.	Peak Signal to Noise Ratio Index (PSNR)
	PSNR1 between I_o and I_D PSNR2 between I_o and I_E
8.	Mean Signal to Noise Ratio Index (MSNR)
	MSNR1 between I_o and I_D MSNR2 between I_o and I_E
10.	Mean Square Error Index (MSE)
	MSE1between I_o and I_D MSE2 between I_o and I_E
11.	Root Mean Square Error Index ($RMSE$)
	$RMSE1$ between I_o and I_D $RMSE2$ between I_o and I_E
12.	Laplacian Mean Square Error ($LMSE$)
	$LMSE1$ between I_o and I_D $LMSE2$ between I_o and I_E

9 Acknowledgement

I would like to thank my teachers who did not burden me with any effort or information, and I would often turn to them and find help with open arms, and I thank the staff at Al-Hakim Hospital in Najaf for providing me with a set of medical images

References

[1]- Abu-Ein, A. A. (2023). An Effective Chaotic Image Encryption Algorithm Based on Piecewise Non-linear Chaotic Map. Inf. Sci. Lett. Nat, 12, 1173-1181.

[2]- Ahmed, S. T., Hammood, D. A., Chisab, R. F., Al-Naji, A., & Chahl, J. (2023). Medical Image Encryption: A Comprehensive Review. Computers, 12(8), 160.

[3]- Ahmed, S. T., Hammood, D. A., Chisab, R. F., & Ismail, N. B. H. (2023). Medical Image Encryption and Decryption Based on DNA: A Survey. Journal of Techniques, 5(3), 116-128.

[4]- Masood, F., Driss, M., Boulila, W., Ahmad, J., Rehman, S. U., Jan, S. U., ... &;ZX Buchanan, W. J. (2022). "A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations". Wireless Personal Communications, 127(2), pp.(1405-1432)

[5]- Zhang, B., & Liu, L. (2023). Chaos-Based Image Encryption: Review, Application, and Challenges. Mathematics, 11(11), 2585.

[6]- Mohamed, K. (2022). Chaos Based Image Encryption.

[7]- Bose, B., Dey, D., Sengupta, A., Mulchandani, N., & Patra, A. (2021, February). A novel medical image encryption using cyclic coding in Covid-19 pandemic situation. In Journal of Physics: Conference Series (Vol. 1797, No. 1, p. 012035). IOP Publishing.

[8]- Patel, S., & Muthu, R. K. (2020). Image encryption decryption using chaotic logistic mapping and dna encoding. arXiv preprint arXiv:2003.06616.

[9]- Ye, G., Pan, C., Huang, X., Zhao, Z., & He, J. (2018). A chaotic image encryption algorithm based on information entropy. International Journal of Bifurcation and Chaos, 28(01), 1850010.

[10]- Mohamed, K. (2022). Chaos Based Image Encryption.

[11]- Kaur, M., & Kumar, V. ," A comprehensive review on image encryption techniques". Archives of Computational Methods in Engineering, Vol.27, No.1, pp.15-43,2020.

[12]- Al-Hilo, E.," Speeding-up Fractal Colored Image Compression using Moments Features, PHD Theses,2007.