Modern Journal of Health and Applied Sciences *(MJHAS)*

E-ISSN 3078-2791; P-ISSN 3078-2783

Journal homepage: https://mucjournals.muc.edu.ps

Gray X-Ray medical images encryption and decryption by chaotic algorithm

Kawther H. Al-khafaji [1], *and Hanan A. Al-Haidari* [1*]

[1] Kufa University, Faculty of Education for Girls, Kufa Iraq

ARTICLE INFO

Received: 23th July 2024
Received in revised form: 02nd September 2024
Accepted:06th September 2024
Published: 15th March 2025

***Corresponding Author:**
Hanan A. Al-Haidari
E-mail:
hanana.alhaida@student.uokufa.edu.iq

Citation: Al-khafaji , K. H. Al-Haidari, A. H., & (2025). Gray X-Ray medical images encryption and decryption by chaotic algorithm. *Modern Journal of Health and Applied Sciences*, 2(1), 1–11.

DOI: https://doi.org/10.70411/MJHAS.2.1.2025143

ABSTRACT

The procedure for securely transferring encrypted images over the network so that an unauthorized user cannot decrypt them is by implementing strong algorithms that cannot be decrypted. There are different methods and multiple algorithms for encrypting and decrypting images. The most common way to encrypt images is the Chaotic Image System. The encryption key and decryption key are called the “symmetric key." In this research, a medical researcher found that the chaotic logistic encryption algorithm has a better effect on encrypting medical X-ray image information and hides the statistical properties of the original medical encryption. Several standards were used to measure image quality during and after encryption, and a comparison was made between them to obtain optimal values for encrypting the X-ray image. The correlation relationship between the adjacent pixels of both the original and the encrypted image was also measured at both values of the initial coefficients. The correlation relationship for the adjacent pixels in the original image was found to be strong. However, in the case of the encrypted image, it is sparse and has little correlation. Finally, in the case of the image in which encryption does not occur, the correlation relationship between adjacent pixels is similar to the original image. Several measurements were used in the research, such as Encryption Time (ET), Decryption Time (DT), and Information Entropy for the Original image (Eo).

Keywords: X-Ray Image Encryption, Decryption, Chaotic Logistic Encryption Algorithm, Histogram.

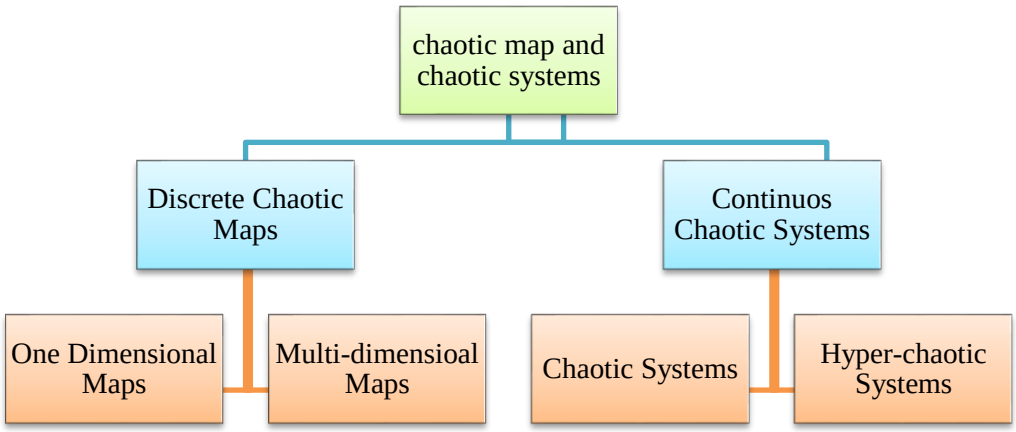
1. Introduction

Digital image processing is today the world's most significant and prominent domain. The web database integrates user data (Abu-Ein, 2023), including text and images. Improving security approaches and developing new algorithms are necessary for secure picture storage and transmission across networks. Cryptography aims to provide secure data transfer, ensuring information anonymity even in hostile environments. The field of cryptography has embraced a variety of strategies to counter assaults. This work presents an essential and efficient cryptography implementation. Chaos theory has significantly strengthened encryption techniques. This paper discusses chaotic cryptography (Ahmed, Hammood, Chisab, Al-Naji, et al., 2023; Ahmed, Hammood, Chisab, & Ismail, 2023; Masood et al., 2022). Telemedicine is an emerging domain that involves the remote delivery of medical services to patients, in which neither the patient nor the healthcare provider is physically collocated. 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 in the world. Most 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 developing 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 employing encryption schemes that render the images unusable for users who do not possess the corresponding encryption information (Bose et al., 2021; Mohamed, 2022; Zhang & Liu, 2023; Zhang et al., 2020). Decryption pertains to the inverse procedure through which encrypted data is regenerated into plain text, whereas encryption involves converting unencrypted data to encrypted data. The four primary objectives of cryptography are information authentication, confidentiality, integrity, and non-repudiation (Asgari-Chenaghlu et al., 2019; Mohsen et al., 2024). Before transmission over public networks, the raw data transforms into a representation devoid of additional information that renders it meaningless. Encryption is repeatedly recommended to guarantee the security of medical images within the healthcare sector. According to this scheme, the initial image is converted into a cypher image, thereby restricting access to its contents to authorized users only. Unauthorized users are thereby thwarted from accessing the data. Cryptography is widely utilized due to its substantial security advantages (Asgari-Chenaghlu et al., 2019).Images utilized in the medical domain are considered 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, researchers have proposed numerous image encryption algorithms. 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 utilized to encrypt images highly efficiently (Raman, 2016). Researchers encounter numerous obstacles when attempting to develop techniques that are impervious to assaults and practical. To accomplish this, sophisticated mathematical models and novel algorithms are implemented. Chaos refers to an unpredictable and pseudo-random motion that arises within a deterministic dynamical system due to its susceptibility to initial values and parameters. The investigation of chaos theory emerged from H. Poincare's 1913 examination of the three-body problem (Kumari et al., 2017). After extensive investigations, 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 (Rajoriya et al., 2018). In their 1975 paper "Period Three Implies Chaos," Tienyien Li and James A. Yorke coined the term "chaos" to denote this phenomenon (Hua & Zhou, 2017). Extensive research has been conducted in the years that followed on chaos-based cryptography, which has also entered the stage of practical application (Zhou et al., 2014). Chaotic systems demonstrate various captivating characteristics, such as their exactness, periodicity, and sensitivity to initial conditions and control parameters. Certain prerequisites for pseudo-random coding (i.e., chaotic) and cryptography apply to virtually any property (Mitra et al., 2006). A logistic map consisting of one and two dimensions generated the chaotic matrix. The encrypted image undergoes an XOR operation at each iteration, achieved via two-phase confusion and diffusion. Moreover, a color image derived from chaotic maps was presented. The aforementioned function is employed to produce pseudo-random sequences, which are subsequently utilized in an encryption

procedure comprising three distinct phases: "permutation," "diffusion," and "substitution." By modifying the values of image pixels during this phase, the position of the image's pixels is scrambled, and the connection between the encrypted and original image is confused (Özkaynak, 2015). The objective of this paper is thus to propose an image encryption algorithm based on chaos.

2. Chaotic Encryption and Decryption Process

Based on their temporal evolution, chaotic systems can be categorized as either discrete chaotic maps or continuous chaotic systems. A continuous chaotic system is characterized by a state that undergoes a continuous evolution over time, and its dynamical equations generally consist of a collection of differential equations. In contrast, a discrete chaotic map denotes a system in which the evolution of its state occurs discretely over time, and its dynamical equation is typically an iterative equation. (Faisal & Ameer, 2020; Hua & Zhou, 2017; Zhang & Liu, 2023).



.

Figure 1. Chaotic maps and systems classification (Zhang & Liu, 2023)

A discrete chaotic map represents a dynamic system characterized by time-varying discrete state variables. The discrete chaotic map is distinguished by its nonlinearity, sensitivity to initial conditions and parameters, and period multiplication (Zhang & Liu, 2023), demonstrating unpredictable and complex behavior over time. The evolution of state variables over time is typically governed by a set of ordinary or partial differential equations that characterize these systems. The state variables comprise physical attributes intrinsic to the investigated system (Zhang & Liu, 2023).

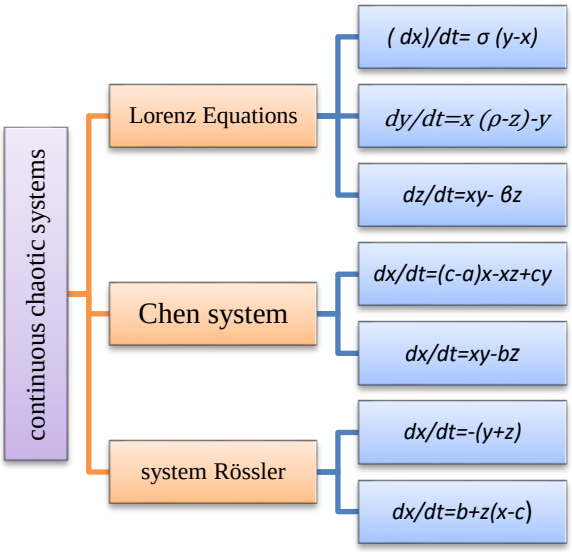


Figure 2. Examples of continuous chaotic systems and their mathematical define (Zhang & Liu, 2023)

A typical nonlinear iterative equation is as follows it ions:

$$X_{(K+1)} = U \times X_K \times (1 - X_K) \quad (1)$$

It is called the control parameter of logistic mapping for any k, where k is the iteration time step. Logistic mapping's dynamic behavior is highly dependent on the control parameter u. The system exhibits.

3. Proposed Algorithms

As illustrated in **Figures 3** and **4,** we proposed an encryption and decryption algorithm in this paper based on the logistic map and the chaotic system.

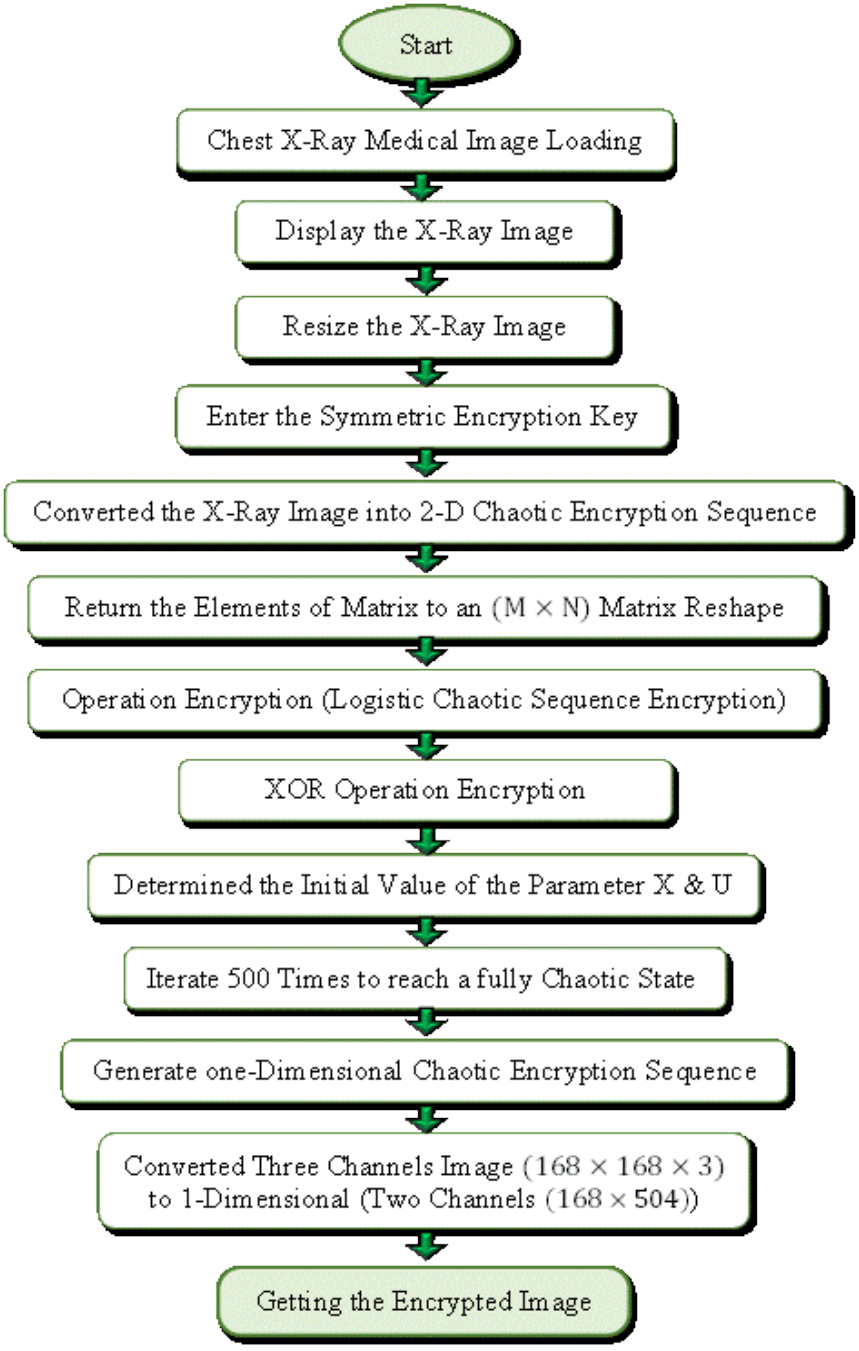


Figure 3. The Algorithm for image encryption

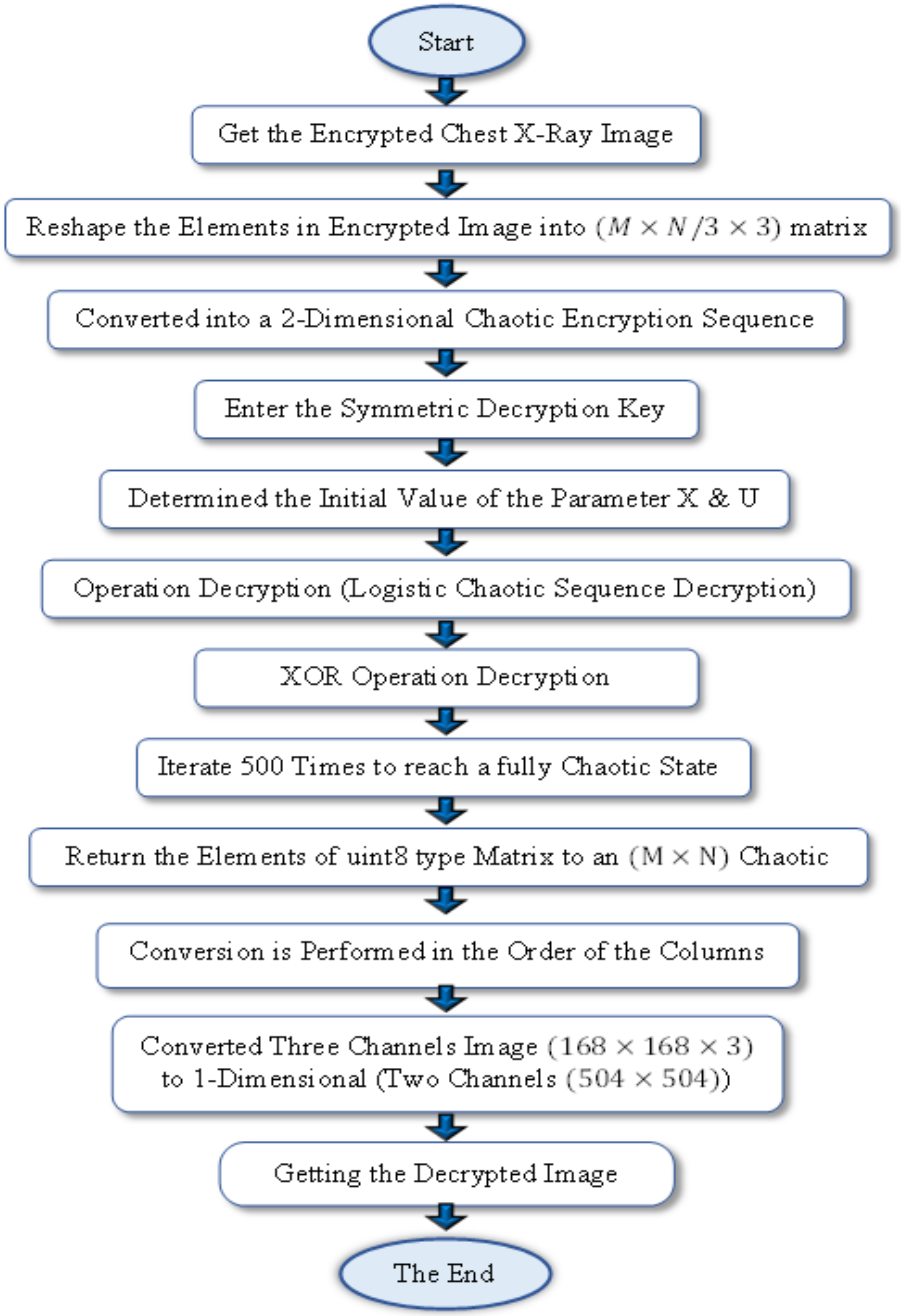


Figure 4. The Algorithm for image decryption

4. Image Acquisition

X-ray medical pictures make up the dataset of images utilized in the experiment. The pictures were provided by the Chest Diseases Center at Al-Hakim Hospital in Najaf and the Radiology Department of Al-Shamiya General Hospital in Diwaniyah. The dimensions picture (168 x 168) was used in our database. The data and numerical simulations were completed utilizing the MATLAB 2021a environment to confirm and demonstrate the viability and security of the suggested optical image encryption scheme. Using an Acer PC laptop running Windows 10 Pro 64-bit, including an Intel(R) Core (i5)-500U processor clocked at 2.5 GHz and 8.0GB of RAM.

Figure 5. X-ray original image

5. The Experiential Results 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: $p1 = 0.1, p2 = 0$. The encrypted X-ray image is depicted.

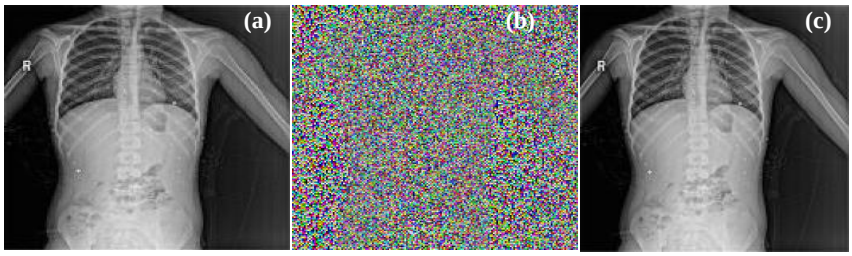


Figure 6. Medical image X-ray encryption using the chaotic method when X= 0.1; U = 4: (a) Original X-ray Image, (b) Encrypted X-ray Image, and (c) Decrypted X-ray Image

According to the outcomes of the investigations, the encrypted X-ray image differs significantly from the original. The encrypted and decrypted X-ray images do not disclose any information regarding the original X-ray image, as in **Figure 6**. In addition, the distribution of the encrypted X-ray image is uniform in the histogram. **Figure 8** demonstrates that the proposed encryption algorithm can effectively withstand statistical attacks.

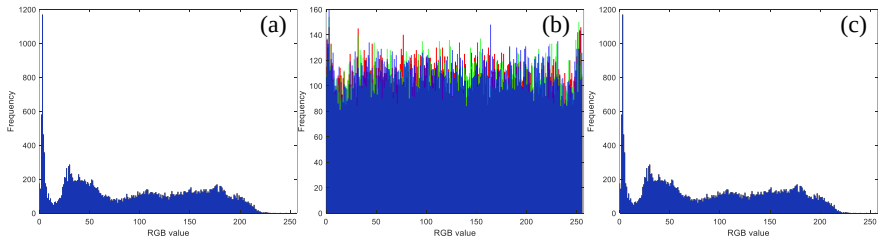


Figure 7. X-Ray Medical Image Histogram X= 0.1; U = 4: (a) Original X-Ray Medical Image Histogram, (b) Encrypted X-Ray Medical Image Histogram, and (c) Decrypted X-Ray Medical Image Histogram

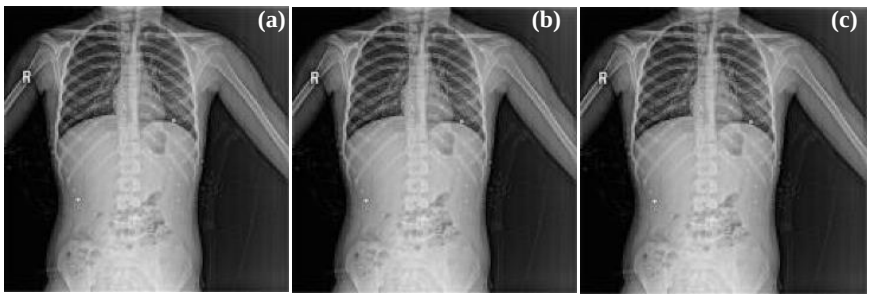


Figure 8. Medical image X-ray encryption using the chaotic method when X= 1; U = 1: (a) Original X-Ray Image, (b) Encrypted X-Ray Image, and (c) Decrypted X-Ray Image

According to the results of the investigations, the encrypted X-ray image does not differ from the original image. The encrypted X-ray images reveal any information related to the original X-ray image, as shown in **Figure 8**. The reason is that chaotic encryption works within a specific range represented by $(1 \leq U \leq 3.5699456)$ and $(0 < X \leq 1)$. In addition, the distribution of the encoded X-ray image is similar in histogram to the histogram of the original and recovered image. As shown in **Figure 9**, the proposed encryption algorithm can thus effectively resist statistical attacks within a specified range.

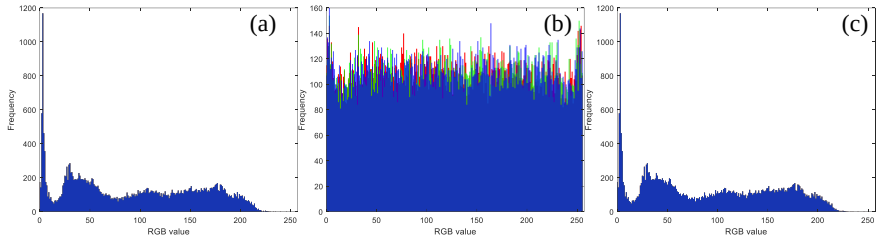


Figure 9. X-Ray Medical Image Histogram when X= 1; U = 1: (a) Original X-Ray Medical Image Histogram, (b) Encrypted X-Ray Medical Image Histogram, and (c) Decrypted X-ray Medical Image Histogram

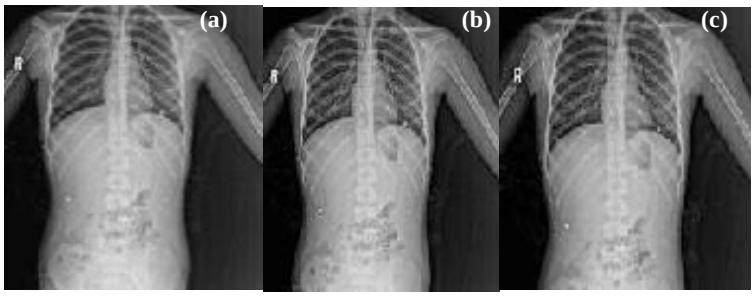


Figure 10. Gray Medical X-Ray Image with X= 0.1; U = 1: (a) Original X-Ray image, (b) Encrypted X-Ray image, and (c) Decrypted X-Ray image

According to the results of the investigations, the encrypted X-ray image does not differ from the original image. The encrypted X-ray images reveal any information related to the original X-ray image, as shown in **Figure 10**. The reason is that chaotic encryption works within a specific range represented by $(1 \leq U \leq 3.5699456)$ and $(0 < X \leq 1)$. In addition, the distribution of the encoded X-ray image is similar in histogram to the histogram of the original and recovered image. As shown in **Figure 11**, the proposed encryption algorithm can thus effectively resist statistical attacks within a specified range.

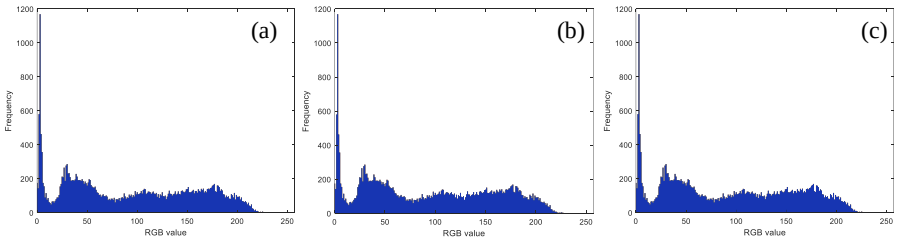


Figure 11. Gray Medical X-Ray Image histogram with X= 0.1; U = 1: (a) Original X-Ray image histogram, (b) Encrypted X-Ray image histogram, and (c) Decrypted X-Ray image histogram

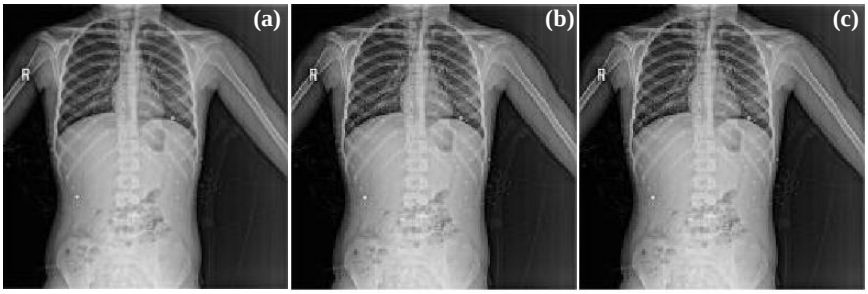


Figure 12. Gray Medical X-Ray Image with X= 1; U = 1: (a) Original X-Ray image, (b) Encrypted X-Ray image, and (c) Decrypted X-Ray image

According to the results of the investigations, the encrypted X-ray image does not differ from the original image. The encrypted X-ray images reveal any information related to the original X-ray image, as shown in **Figure 12**. The reason is that chaotic encryption works within a specific range represented by $(1 \leq U \leq 3.5699456)$ and $(0 < X \leq 1)$. In addition, the distribution of the encoded X-ray image is similar in histogram to the histogram of the original and recovered image. As shown in **Figure 13**, the proposed encryption algorithm can thus effectively resist statistical attacks within a specified range.

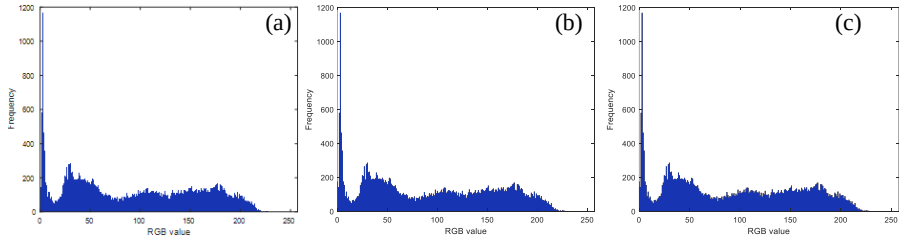


Figure 13. Gray Medical X-Ray Image histogram with X= 0.1; U = 1: (a) Original X-Ray image histogram, (b) Encrypted X-Ray image histogram, and (c) Decrypted X-Ray image histogram

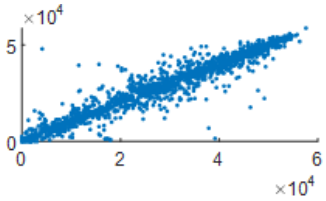
6. Results and Conclusions

This subsection provides an in-depth examination of the empirical analysis. As shown in **Table 1**, the X-ray image was encrypted using the chaotic encryption equation, and values were also used for the initial parameters outside the encryption range. The quality of the proposed algorithm was evaluated using the following image quality metrics:

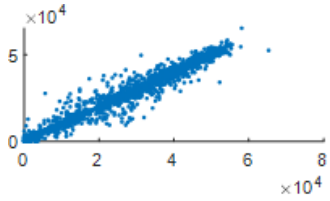
Table 1. Show some IQM values in two different values of X and U for medical images.

NO.	IQM	X=0.1, U=4	X=1,U=1	X=0.1,U=1	X=1, U=4	NO.	IQM	X=0.1, U=4	X=1, U=1	X=0.1,U=1	X=1, U=4
1.	ET	12.08	4.245	7.98	4.245	**10.**	CC1	1	1	1	1
2.	DT	7.599	3.624	8.079	3.624	**11.**	CC2	0.0067	1	1	1
3.	Eo	7.568828	7.56888	7.5688	7.568	**12.**	SNR1	37.857	37.85	37.85	37.8
4.	Ee	7.991998	7.56882	7.5688	7.568	**13.**	SNR2	37.857	37.85	37.85	37.8
5.	Ed	7.568828	7.56882	7.5688	7.568	**14.**	MD1	0	0	0	0
6.	NPCR	0.971	0	**0**	0	**15.**	MD2	227	0	0	0
7.	AV1	93.0489	93.0489	93.048	93	**16.**	EOD	0	0	0	0
8.	AV2	126.58822	93.0489	93.048	93	**17.**	EOE	1.37635	0	0	0
9.	AV3	93.0489	93.0489	93.048	93	**18.**	EDE	1.37635	0	0	0

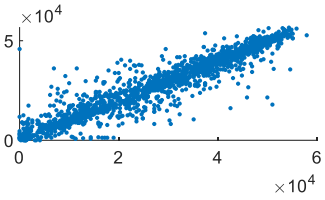
The correlation coefficients between the original and encrypted X-ray images are computed and presented in **Table 1**. The correlation coefficients for the original X-ray image are approximately one. In contrast, they approach zero for the encrypted X-ray image generated by the proposed algorithm, as in the following figures:



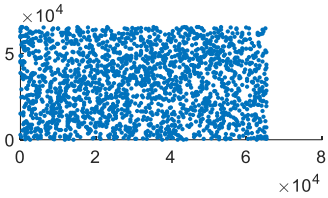
a. Horizontal correlation plot of two neighbouring pixels from the original X-ray picture



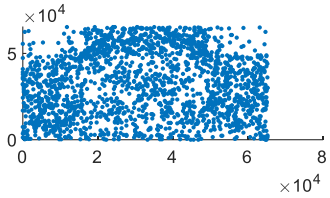
b. A vertical correlation map of two nearby X-ray original picture pixels



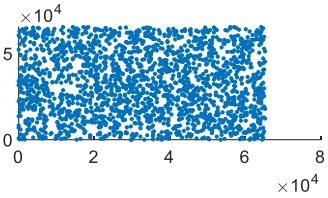
c. A diagonal correlation plot of two nearby X-ray original picture pixels



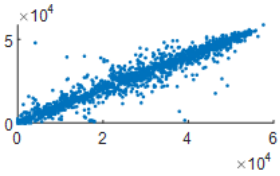
d. A horizontal correlation plot of two neighbouring X-ray encryption picture pixels $X = 0.1., U = 4$



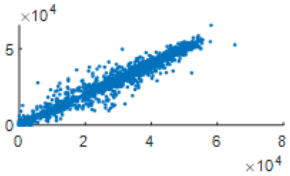
e. A Vertical correlation plot of two neighbouring X-ray encryption picture pixels $X = 0.1, U = 4$



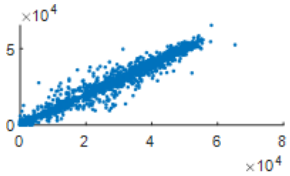
f. A diagonal correlation plot of two neighbouring X-ray encryption picture pixels $X = 0.1, U = 4$



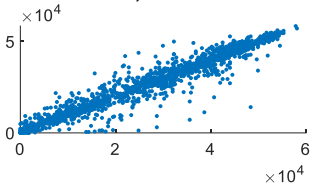
g. A horizontal correlation plot of two neighbouring X-ray encryption picture pixels $X = 1, U = 1$



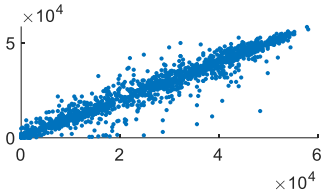
h. A Vertical correlation plot of two neighbouring X-ray encryption picture pixels $X = 1, U = 1$



i. A diagonal correlation plot of two neighbouring X-ray encryption picture pixels $X = 1, U = 1$

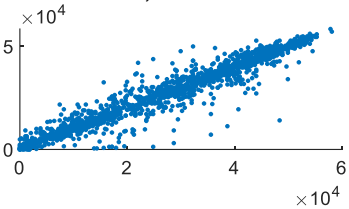


j. A horizontal correlation plot of two neighbouring X-ray encryption picture pixels $X = 0.1, U = 1$

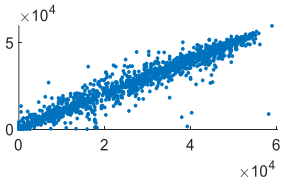


k. A Vertical correlation plot of two neighboring X-ray encryption picture pixels $X = 0.1, U = 1$

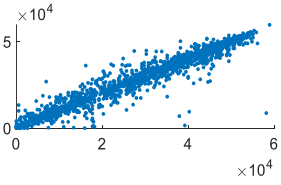
l.



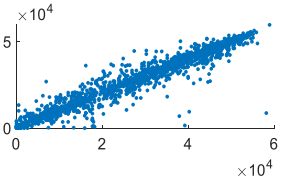
m. A diagonal correlation plot of two neighbouring X-ray encryption picture pixels $X = 0.1, U = 1$



n. A horizontal correlation plot of two neighbouring X-ray encryption picture pixels $X = 1, U = 4$



o. A horizontal correlation plot of two neighbouring X-ray encryption picture pixels $X = 1, U = 4$



p. A horizontal correlation plot of two neighbouring X-ray encryption picture pixels $X = 1, U = 4$

Figure 14. Plotting the correlation between two nearby X-ray medical images

7. Conclusion

More and more data will be accessible for research as medical image analysis techniques and imaging technologies develop. Therefore, it is vital to safeguard such photos. X-ray medical pictures are encrypted using a technique based on the chaotic logistic algorithm. Chaotic is among the most effective mathematical instruments for image analysis and cryptography because it possesses a particular structure. The capability of the chaotic is integrated with additional mathematical instruments. It can be inferred that image encryption and decryption techniques are highly secure and algorithmically chaotic. From **Table 1,** we notice that the value of Encryption time (ET), Decryption time (DT), Information Entropy for encryption image (E_e), Number of Pixel Change Rate (NPCR), Average Value of encryption image (AV2), Maximum Difference Index for encryption image (MD2), Entropy Differences (EOE, EDE) decreases when the values of the primary parameters move from the encoding range to outside the encryption range. At the same time, Correlation Coefficient Analysis (CC2) increases when the values move from the encryption range to outside the encryption range, and finally, Information Entropy (E_d), Average Value of the original image (AV1), Average Value of decryption image (AV3), Coefficient Analysis (CC1), Signal to Noise Ratio Index (SNR), Maximum Difference Index ($MD1$), Entropy Differences (EOD) that remain constant and do not change with any change. Initial parameter values from encryption range to out-of-range. It can be concluded that image encryption and decryption technology are very secure and algorithmically chaotic within the limits of chaotic encryption.

From **Figure 10**, we notice that in the encrypted image, the correlation between adjacent pixels is very weak, as the drawing is scattered, and this makes it impossible to know the information for the encrypted image, as the correlation coefficients are very weak, while in the original image, the pixels have a strong relationship, as they all share a single extension of the coefficient link. While the drawing of the Histogram shows the mismatch of the frequencies of the pixel values between the encrypted image and the original, and this indicates the efficiency of the encryption algorithm, the recovered image is identical to the original histogram image, and this is evidence of the success of the decryption algorithm.

Conflict of Interest

On behalf of all authors, the corresponding author states that there is no conflict of interest.

Data Availability

No data was used for the research described in the article.

References

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

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.

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.

Asgari-Chenaghlu, M., Balafar, M.-A., & Feizi-Derakhshi, M.-R. (2019). A novel image encryption algorithm based on polynomial combination of chaotic maps and dynamic function generation. *Signal Processing*, *157*, 1-13.

Bose, B., Dey, D., Sengupta, A., Mulchandani, N., & Patra, A. (2021). A novel medical image encryption using cyclic coding in Covid-19 pandemic situation. Journal of Physics: Conference Series,

Faisal, Z., & Ameer, E. H. A. (2020). Encryption Image by Using RC6 and Hybrid Chaotic Map. *Webology*, *17*(2), 189-199.

Hua, Z., & Zhou, Y. (2017). Design of image cipher using block-based scrambling and image filtering. *Information sciences*, *396*, 97-113.

Kumari, M., Gupta, S., & Sardana, P. (2017). A survey of image encryption algorithms. *3D Research*, *8*, 1-35.

Masood, F., Driss, M., Boulila, W., Ahmad, J., Rehman, S. U., Jan, S. U., Qayyum, A., & Buchanan, W. J. (2022). A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations. *Wireless personal communications*, *127*(2), 1405-1432.

Mitra, A., Rao, Y. S., & Prasanna, S. (2006). A new image encryption approach using combinational permutation techniques. *International Journal of Computer Science*, *1*(2), 127-131.

Mohamed, K. (2022). Chaos Based Image Encryption.

Mohsen, M., Manisi, Y., Bouzreda, H. M., & Youniss, F. (2024). Evolution of computed tomography techniques. *Modern Journal of Health and Applied Sciences*, *1*(1), 49-58.

Özkaynak, F. (2015). A novel method to improve the performance of chaos based evolutionary algorithms. *Optik*, *126*(24), 5434-5438.

Rajoriya, R., Patidar, K., & Chouhan, S. (2018). A survey and analysis on color image encryption algorithms. *ACCENTS Transactions on Information Security*, *3*(9), 2455-7196.

Raman, A. (2016). *Parallel processing of chaos-based image encryption algorithms*. University of California, Irvine.

Zhang, B., & Liu, L. (2023). Chaos-based image encryption: Review, application, and challenges. *Mathematics*, *11*(11), 2585.

Zhang, G., Ding, W., & Li, L. (2020). Image encryption algorithm based on tent delay-sine cascade with logistic map. *Symmetry*, *12*(3), 355.

Zhou, Y., Hua, Z., Pun, C.-M., & Chen, C. P. (2014). Cascade chaotic system with applications. *IEEE transactions on cybernetics*, *45*(9), 2001-2012.