A Robust Chaos-Based Medical Image Cryptosystem

SAMIRA DIB[1], ASMA BENCHIHEB[2], FADILA BENMEDDOUR[3]
[1]Department of Electronics
University of Jijel
BP 98 O. Aissa, Jijel 18000
ALGERIA
[2]Faculty of Medicine
University of Constantine 3
Constantine 25000
ALGERIA
[3]Department of Electronic Engineering
University of M'Sila
M'Sila 28000
ALGERIA
samiradib@yahoo.fr

Abstract: - In In this paper, we propose an efficient cryptosystem for medical images. While the confusion stage is ensured by an Arnold's cat map allowing the permutation of pixels; the diffusion stage is alleviated by an improved logistic map used by the chaotic key-based algorithm (CKBA).
The simulation results attest that the proposed algorithm has superior security and enables efficient encryption/decryption of medical images. Performances were evaluated by several security analyses: the NPCR and UACI are improved over 99.60% and 33.46% respectively, and entropy is reported close to 7.8. What makes this new cipher much stronger security.

1 Introduction

In recent years, telemedicine systems have been introduced in hospitals and medical centers with the aim of establishing communication bridges offering good medical services between specialists and patients. For reasons of patient incapacity or the remoteness or scarcity of certain specialties, physicians may interact among themselves or with their patients to diagnose a disease or prescribe a treatment. They use clinical data such as images and medical signals.

Various patient medical information and specialist diagnoses are confidential and must be secure during transfer over different communication networks in a highly computerized and interconnected world. In order to reinforce the security of this information, several approaches are used, the most important of which are cryptographic techniques. The goal of any image encryption method is to obtain a higher quality image in order to keep the information secret and safe.

Because of their sensitivity to changes in initial conditions, chaotic systems are one of the best approaches to protect the information in secure communications. It represents one of the most powerful classes of cryptography by their resistance to external attacks. Much research has been conducted in this area over the past two decades [3–20] and references therein.

The chaotic key-based algorithm (CKBA) for image encryption is originally proposed by Yen and Guo [3] and claiming strong security for image encryption. This statement is challenged showing that the complexity of a ciphertext attack against the CKBA is much lower than originally announced, and chosen/known text attacks can be applied effectively. Since then, research work has been carried out to improve the safety of the CKBA. Another technique, presented in [4] and based on the chaotic logistic map, provides high security for gray images. The method proposed in [5] is secure against brute force attacks, sensitive to the key and is efficient even in terms of speed. However, the success of this method may be limited due to the common operations it uses. This makes external attacks vulnerable. Despite these developments, even faster and more secure cryptosystems are

needed. Further, many efforts have been focused on the use of the chaotic cryptography for medical data encryption [19–27].

In this paper, a medical image encryption scheme using a modified logistic (ML) map is presented. The initial condition x_0 of the chaotic ML system is considered as the secret key of our proposed encryption algorithm. Furthermore, the parameters of cat map, p and q, are used as confusion key parameters.

To test the feasibility of the proposed algorithm, a variety of standard reference images were used including X-ray, ultrasound, MRI and CT scanner images. Additionally, to accurately verify the performance of this method, several parameters were calculated, including histogram analysis, correlation, differential attack, PSNR, SSIM and information entropy. The results reveal that the proposed technique offers good results and can therefore be adopted in a telemedicine system.

The organization of the paper is as follows: Section 2 is devoted to the definitions of the logistic map and the modified map of the chaotic system. The proposed encryption method is presented in Section 3. Section 4 is devoted to the discussion of the obtained results. Finally, conclusions are presented in section 5.

2 Logistic Map and Modified Map

The logistic map is typically used in most chaos-based cryptosystems, especially in secure communication systems.

2.1 Logistic Map

Logistic map is one-dimensional map which is explained by a recursive function as follows:

$$x_{n+1} = L(r, x_n) = r . x_n . (1 - x_n) \tag{1}$$

Where r is its parameter that lies in interval [0, 4] and $x_n \in [0,1]$.

2.2 Modified Logistic Map (ML)

In order to expand chaotic region of Logistic map and make it suitable for cryptography, we will approach a modification to the Logistic map and use that one proposed in [11]:

$$x_{n+1} = \frac{4 . s . x_n . (1 - x_n) - s}{\alpha} + \frac{s + \alpha}{2s} \tag{2}$$

Where n is a time index, x_0 is the initial value, $x_n \in \left[\frac{s-\alpha}{2s}, \frac{s+\alpha}{2s} \right]$ and the control parameters are α and s used as key parameters for the proposed cryptosystem. They are related by the following equation:

$$\alpha = s - x_0 \tag{3}$$

Here, the parameter s must always be greater than α, for the x_n values to appear inside the interval (0,1). Moreover, the closer the value α is to s, the wider the interval of x_n.

In order to explain the performance of Equations (1) and (2), Bifurcation diagram and Lyapunov exponents are calculated and plotted with respect to respective control parameters 'r' and 's' in Figure 1, for the Logistic map and the Modified Logistic Map (ML).

Regarding Fig.1, Logistic map is chaotic when parameter "r" lies in interval [3.6, 4] and ML map is chaotic when parameter 's' lies in interval [0.1, 20]. Therefore, the chaotic range of ML is more than the others. As shown in the figure, there are no free white spaces and the entire area is almost covered. More importantly, all values of s can be used to build the key space. This property extends the key space of the proposed cryptosystem.
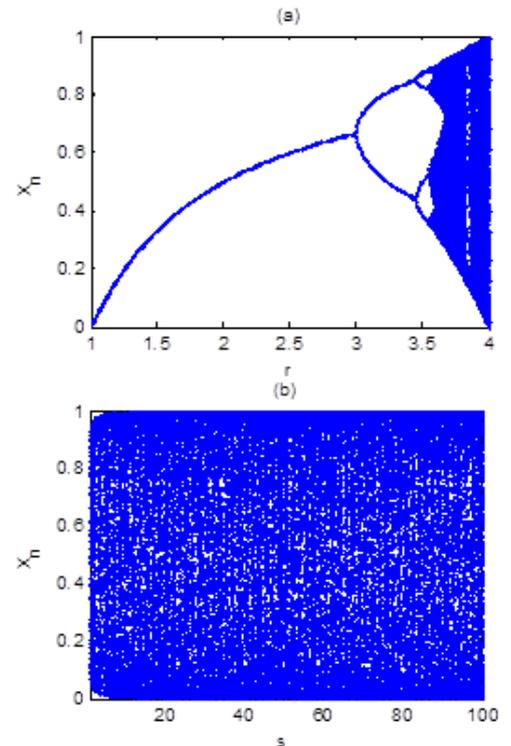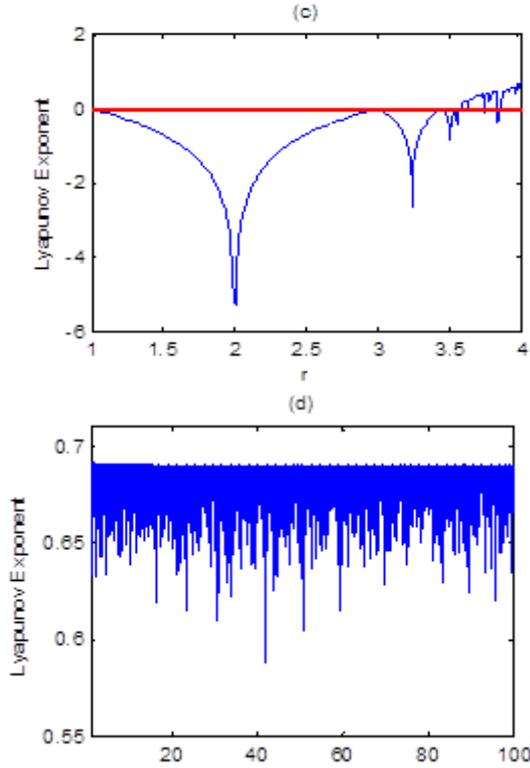
Fig. 1. (a) Bifurcation diagram of logistic map ; (b) Bifurcation diagram of ML map ; (c) Lyapunov Exponent of Logistic map ; (d) Lyapunov exponent of ML map.

3 Proposed Cryptosystem

In general, chaos-based image encryption systems are applied in two steps: replacing pixels called confusion and changing pixel values called diffusion.

It is known that an ordinary image has a strong correlation of adjacent pixels which must be broken before any encryption procedure. Several ways of ensuring this decorrelation are used in the literature. Within the framework of this paper, we propose the application of Arnold Cat Map (ACM). It is a discrete invertible system which allows a good reorganization of the pixels' positions of the original image. It is represented by

$$\begin{bmatrix} x' \\ y' \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \qquad (4)$$

where (x,y) are the pixel position of the plain image with a size of N×N and (x', y') is the corresponding pixel position. Control parameters of the ACM are p and q, which are positive integers and will be used as confusion key parameters:

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x' \\ y' \end{bmatrix} \bmod N \qquad (5)$$

ACM effectively changes all pixel positions as only linear transformation with simple mod function need to be performed. Furthermore, it has a characteristic of area-preserving which means that if it is iterated enough times, original image reappears. Shortly, ACM can be considered as a permutation method that focuses on the pixel position not the pixel value of the plain image. Hence, the cryptosystem requires a diffusion process to enhance the security.

This stage is ensured by the CKBA algorithm using the modified logistic map which offers a large key space.

Modified CKBA algorithm

In order to protect medical images transferred on public roads and in order to fortify their security, we proposed in this paper a modified algorithm based on chaotic keys (CKBA) by the use of the traditional architecture given in [3]. The modification is made using the modified map (ML) given in eqt(2) rather than the logistic map eqt(1).

The encryption process is described as follows:

Step 1 : Assume that the size of the original image (Img) is M×N.

Step 2 : Select different parameters keys namely :
- p and q and a number of iteration, to apply Arnold's cat map to change the pixels position.
- Two bytes key1 and key2 (8 bits) and the initial condition x0 of the ML chaotic system as the secret keys of the encryption system.

Not all secret keys can make well disorderly cipher-images, the basic criterion to select key1 and key2 should be satisfied: $\sum_{i=0}^{7}(a_i \oplus d_i) = 4$, where key1 $= \sum_{i=0}^{7} a_i \times 2^i$ and key2 $= \sum_{i=0}^{7} d_i \times 2^i$

Step 3 : Run the chaotic system to make a chaotic sequence $\{x(i)\}_{i=0}^{\frac{MN}{8}-1}$

Step 4 : Generate a pseudo-random binary sequence (PRBS) $\{b(i)\}_{i=0}^{2MN-1}$ from the 16-bit binary representation of $x(i) = 0.b(16i+0)b(16i+1)\dots b(16i+15)$. Once $\{b(i)\}$ is generated, the encryption can start.

- For the plain-pixel f(x,y) $(0 \leq x \leq M - 1 , 0 \leq y \leq N-1)$, the corresponding cipher-pixel f'(x,y) is determined by the following rule :

$$f'(x,y) = \begin{cases} f(x,y) \text{XOR} \ \ key1, b'(x,y) = 3 \\ f(x,y) \text{XNOR} \ key1, b'(x,y) = 2 \\ f(x,y) \text{XOR} \ \ \ key2, b'(x,y) = 1 \\ f(x,y) \text{XNOR} \ key2, b'(x,y) = 0 \end{cases} \quad (6)$$

Where $b'(x,y) = 2.b(l) + b(l+1)$ and $l = x.N + y$.

Step 5 : The decryption procedure is just like the encryption since XOR and XNOR are both involutive operations.

4 Performance analysis

In order to evaluate the proposed cryptographic method, multiple medical images have been adopted, including X-Ray, ultrasound, MRI and CT scanner images which are retrieved from open databases [29, 30].

4.1. Histogram Analysis

In image processing, histogram is the graphical representation of the pixel values' distribution in an image by plotting the number of pixels at each gray level. The randomness of the proposed algorithm can be validated by a flat and uniformly distributed histogram of the encrypted images.

A good cipher image has a uniform frequency distribution of the pixel values. Fig. 2 shows histograms of the plain and cipher images with the studied algorithm. As can be seen, the cipher images are so boisterous in a way that any data from them cannot be obtained, so the proposed scheme is powerful against histogram attacks.

4.2. Correlation Analysis

Correlation distributions and correlation coefficients play a crucial role in the analysis of encrypted images. It is well known that the correlation between adjacent pixels of an informative image is high in any direction. Whereas for the encrypted image, the correlation must be very weak in order to be able to withstand the various statistical attacks.

In this section, the correlations of the adjacent pixels in the original image and encrypted image are analysed and compared by choosing 20 000 pairs of adjacent pixels in horizontal, vertical, and diagonal directions from the original image and its encrypted image. To calculate the correlation coefficient of adjacent pixels, Eq. 7 can be adopted [28]:

$$r_{ab} = \frac{cov(a.b)}{\sqrt{D(a)}\sqrt{D(b)}}$$
$$D(a) = \frac{1}{M} \sum_{i=1}^{M} \sum_{i=1}^{M} (a - E(a_i))^2 \quad (7)$$
$$E(a) = \frac{1}{M} \sum_{i=1}^{M} a_i$$
$$cov(a.b) = \frac{1}{M} \sum_{i=1}^{M} (a_i - E(a))(b_i - E(b))$$

Where a and b are values of 2 adjoining pixels, E(a) and E(b) is the mean of a and b respectively, and M is the number of adjoining pixels of the image.

If the correlation coefficient is 1, it means that the original image and its encrypted image are highly dependent. However, if this coefficient is 0, then the encrypted image and the original image are not correlated. Table 1 demonstrates the results obtained. Indeed, it is clear that two adjacent pixels of the original image, in the three directions, are strongly correlated. However, for adjacent pixels of the encrypted image, the correlation is is very small or negligible. Therefore, the proposed algorithm has good permutation and substitution properties.

On the other hand, the graphical representation of the correlation is a visual inspection of the pixel dependence of the image, where the horizontal axis represents the intensity value of the pixel and the vertical axis represents the value of the neighbouring pixel, horizontal, vertical or diagonal. For an informative image, the graph is expected to show a strong pattern on a 45 degree line; the denser this line, the more the tested image is correlated. In the encrypted image, the expected graph should have points in the whole plane since most neighbours of any pixel have different intensity values with respect to that pixel.

The graphical representation of the correlation analysis is performed by plotting the pixel gray values between adjacent pixels in the different directions for 1024 randomly selected adjacent pixels pairs for both the original and the encrypted image. It is clearly shown from Fig. 3 (a)–(d) that the strong correlation between adjacent pixels is completely broken in all directions after applying the proposed encryption process.
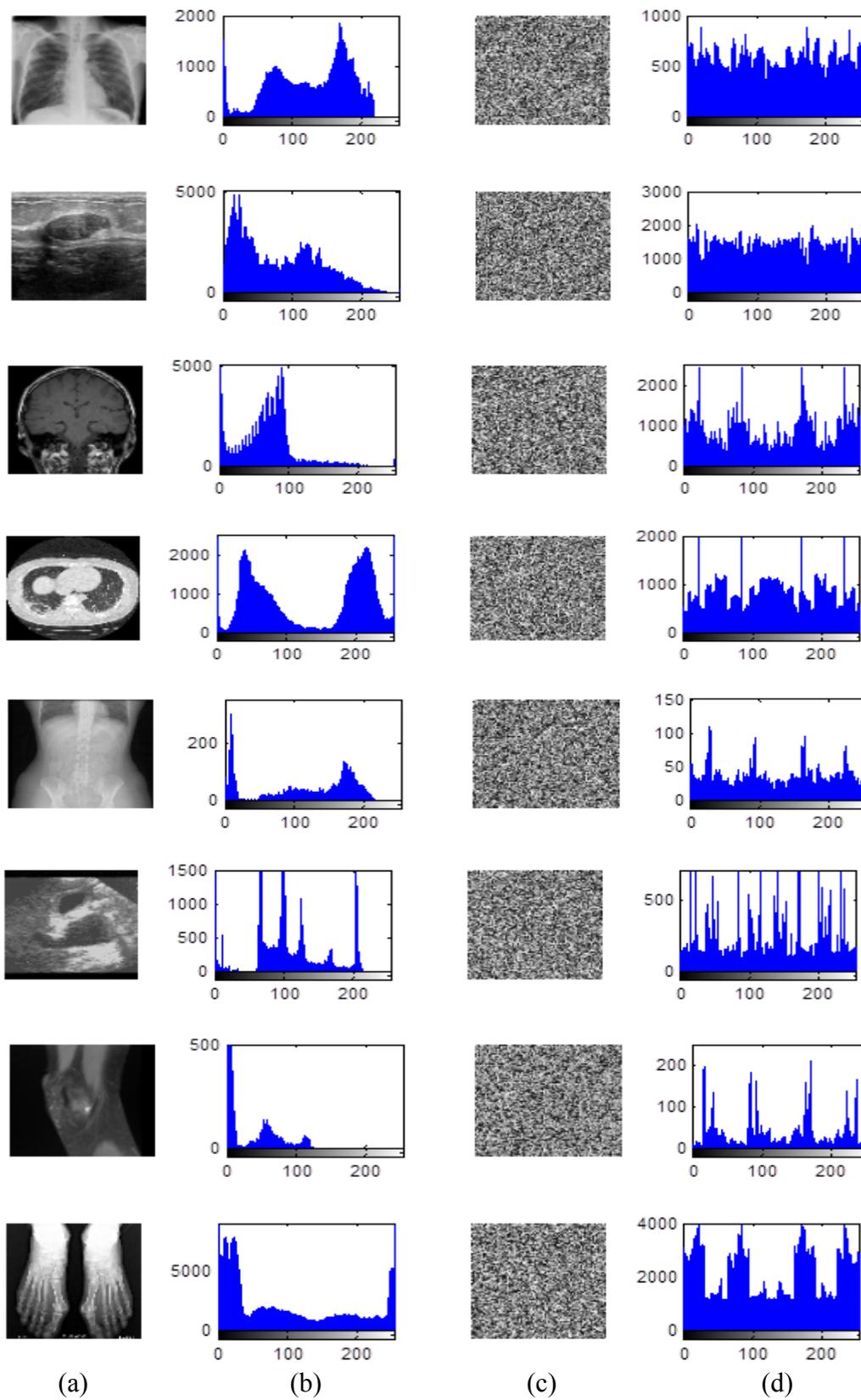
(a)   (b)   (c)   (d)

Fig. 2. Simulation results: (a) Original images. (b) Histograms of the original images. (c) Encrypted images. (d) Histograms of the encrypted images.

Table 1. Correlation between adjacent pixels of original and encrypted images.

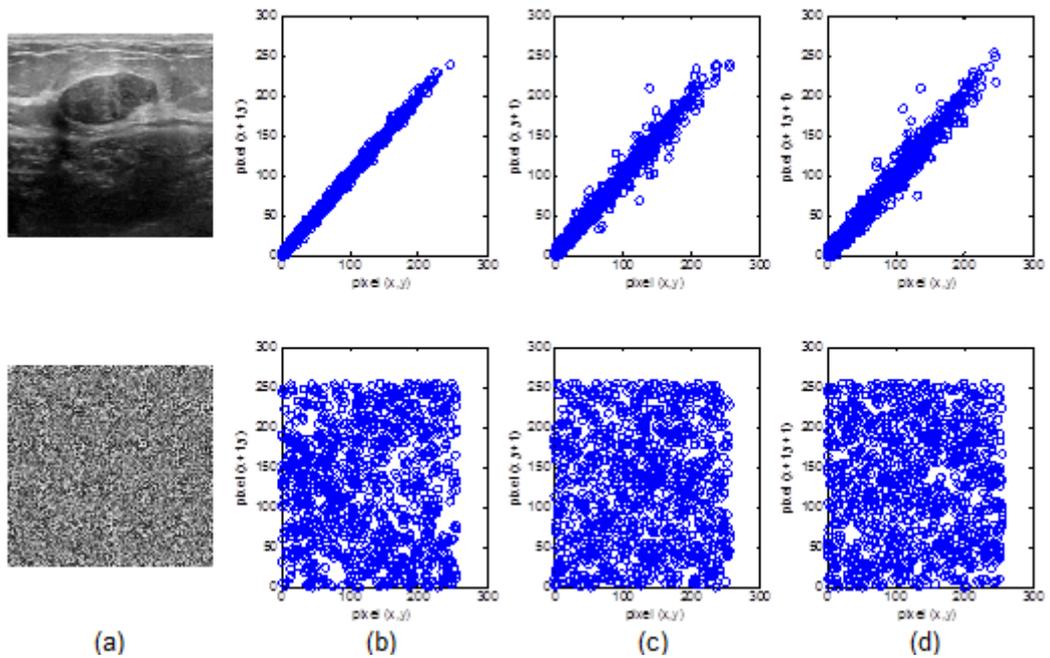| Directions of adjacent pixels	Horizontal		Vertical		Diagonal	
Image	Original	Encrypted	Original	Encrypted	Original	Encrypted
	0.9956	0.0231	0.9971	-0.0034	0.9933	-0.0005
	0.9836	-0.00706	0.9744	0.000201	0.9677	0.0093
	0.9880	0.00005	0.9931	-0.0013	0.9828	-0.0087
	0.9805	0.0422	0.9832	-0.0013	0.9664	-0.0015
	0.9981	-0.0002	0.9899	-0.0034	0.9883	0.0081
	0.9812	0.0250	0.9511	0.0134	0.9418	0.0003
	0.9904	0.0051	0.9943	0.0044	0.9870	-0.0006
	0.9737	0.0477	0.9905	0.00351	0.9714	0.00006

Fig. 3. Correlation distribution of adjacent pixels in different directions: (a) Original and encrypted images. (b) Diagonal direction. (c) Vertical direction. (b) Horizontal direction.

4.3. Information Entropy analysis

The pixel values of a cipher image should be randomly distributed that they do not hold any relation with the plain image. Entropy denotes the degree of randomness and it is calculated using logarithm over a probability distribution.
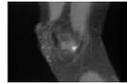
$$H(x) = -\sum_{i-1}^{N} P(x_i)\log_2 P(x_i) \qquad (8)$$

where, $P(x_i)$ is the probability mass function.

Generally, we expect from a good image encryption scheme that the entropy of the encrypted image is close to the ideal case. For an image data given in the form of a byte, the maximum entropy value is 8. Thus, the entropy value close to 8 denotes higher randomness; else if this entropy value is lesser then there is a possibility of attack which can reduce the security of image transmission. In Table 2, the entropy after encryption is compared to that before encryption for various images. According to the obtained values, the average entropy of all encrypted images is very close to the theoretical value (≈ 7.7). This means that the proposed algorithm is much efficient and is highly secure. So we can conclude that the main objectives of image encryption are ensured, namely, illegibility and indeterminacy.

Table 2 The information entropy of different images.

Images								
Plain images	7.516	7.574	6.097	0.642	6.701	6.017	6.361	7.530
Cipher	7.977	7.9819	7.214	7.879	7.404	7.429	7.446	7.8412

4.4. Differential Attack Analysis
4.4.1. NPCR and UACI tests

Number of Pixel Change Rate (NPCR) and Unified Average Change in Intensity (UACI) are the two most important parameters to measure the resistance of developed algorithm against differential attacks. This analysis can be made by observing the relationship between two cipher images, one obtained from the normal image and another from single pixel changed plain image. NPCR measures the minimum number of pixels altered and UACI measures the average difference between the two cipher images. The NPCR and UACI are evaluated by Eqs. (9) and (10) [28] :

$$NPCR = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M} D(i,j)}{N \times M} \times 100 \qquad (9)$$

$$UACI = \frac{\sum_{i=1}^{N}\sum_{j=1}^{M}|E_2(i,j) - E_2(i,j)|}{255 \times N \times M} \times 100 \qquad (10)$$

Subject to :

$$D(i,j) = \begin{cases} 0 \ if \ E_2(i,j) = E_2 = (i,j) \\ 1 \ if \ E_2(i,j) \neq E_2 = (i,j) \end{cases}$$

where E_1 and E_2 are the encrypted images.

Evaluation of encrypted images by NPCR and UACI parameters is depicted in Table 3. The results reveal that a swift change in the original images leads to a change in the cipher ones. This signifies that the proposed scheme has a high ability to resist differential attack and the image encryption schema has a high sensitivity to a minor change in the original images.

The average values of NPCR and UACI for images are estimated as 99.60 % and 33.47% respectively.

4.4.2. SSIM and PSNR

An encryption method achieves successful performance when the encrypted image has a low PSNR and SSIM values. Indeed, two same images have PSNR value as 1 and perfectly similar images have SSIM value as 1(one).

To determinate the change in the pixel values of encrypted image from original image and accuracy of decrypted image from original image, peak signal-to-noise ratio (PSNR) and structural similarity (SSIM) value are calculated using the following equations [28]:

$$PSNR = 20 \times \log 10 \frac{MAX}{\sqrt{MSE}} \qquad (11)$$

$$MSE = \frac{1}{M \times N} \sum_{i=0}^{m-1} \sum_{i=0}^{n-1} [I(i,j) - K(i,j)]^2 \qquad (12)$$

$$SSIM(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \qquad (13)$$

Where :

MAX: Maximum supported pixel value, MSE: Mean squared error, $M \times N$: Size of the image, $I(i,j)$: Original image pixel value at location (i, j), and $K(i,j)$: Received image pixel value at location (i, j).

In medical image, it is important that the decrypted image is exactly the same as the original one. Table 4 shows the PSNR and SSIM values for both crypted and decrypted image with respect to the original image. These results indicate that the PSNR is less than 10 dB and the SSIM is close to 0 for all encrypted images. In addition, all the images have been well reconstructed. Indeed, the SSIM is close to 1 and the PSNR is very high and tends to ∞.
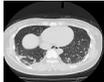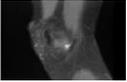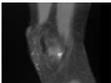
Table 3. NPCR and UCAI images

NPCR (%)	99.55	99.61	99.61	99.57	99.61	99.56	99.61	99.61
UACI (%)	33.48	33.46	33.46	33.48	33.46	33.48	33.46	33.46

Table 4. The SSIM and PSNR values for encrypted/decrypted images

PSNR (dB)	Encrypted	8.77	7.86	6.81	8.14	6.91	6.81	8.46	6.58
	Decrypted	∞	43.26	∞	28.42	∞	41.34	∞	∞
SSIM	Encrypted	0.02	0.04	0.03	0.00	0.04	0.02	0.02	0.06
	Decrypted	1	1	1	0.97	1	0.96	1	1

4.5. Key Sensitivity Analysis

For the encryption of medical images, the sensitivity of the keys is a very important index for building any cryptosystem and evaluating the quality of an encryption algorithm. An image cannot be properly decrypted if the key is changed slightly, indicating that the encryption method has high performance. On the contrary, if the key changes significantly, the image may still be partially decrypted, indicating that the encryption performance of the encryption method is poor.

Key sensitivity analysis can be observed in two aspects: (i) if slightly different keys are applied to encrypt the same images, then completely different cipher images should be produced; (ii) if a small

difference exists in decryption key, then the cipher image could not be decrypted correctly.

For the first key sensitivity analysis, a test plain of X-Ray image is encrypted with a randomly chosen key of $s=97.5678910,\ x_0=0.1234567$. Then a slight change 10^{-7} is applied to the one of the parameters with the other remains same, and repeats the encryption. The corresponding cipher images and the differential images are shown in Fig. 4. The correlation coefficients between the cipher images are calculated and given in Table 5. Small key changes will lead to incorrect decryption results. This also shows that the security performance of this method is very high. Fig .4 illustrates that the decrypted images with incorrect secret key are quite different from the original image, which demonstrates that the proposed scheme is highly sensitive to the slightest changes in secret keys.

The proposed cryptosystem should also be sensitive to Cat map stage p, q and n parameters. Cipher images produced by slightly different keys are shown in Fig. 5 and the correlation coefficients for the corresponding cipher images are given in Table 6. It is clear from these results that a very small difference for all encryption keys results in completely different encryption images.

In the second case, the encrypted image could not be properly decrypted, using a slightly different key than the one used in the decryption. As an example, the scanner CT image of Fig. 2(c) was used and the result is shown in Fig. 6.

We conclude that the proposed cryptosystem is quite sensitive to all keys and can resist differential attacks effectively.
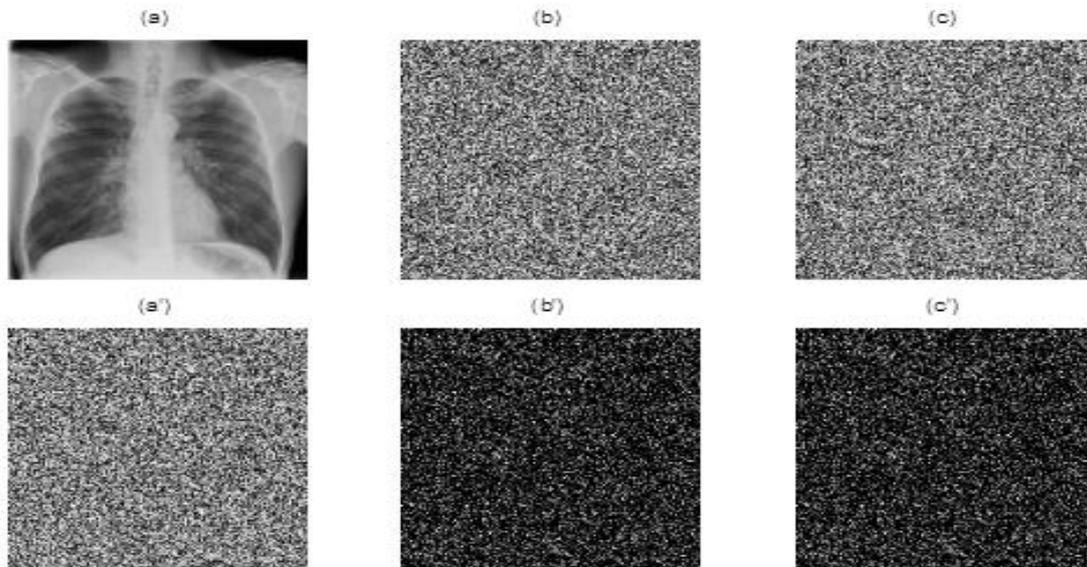

Fig. 4. Key sensitivity in the first case: (a) Plain image; (a') Cipher image with $s=97.5678910,\ x_0 = 0.1234567$; (b) Cipher image with $s=97.5678911,\ x_0 = 0.1234567$; (c) Cipher image with $s = 97.5678910$; $x_0 = 0.1234568$; (d) Differential image between (a') and (b); (c') Differential image between (a') and (c).

Table 5. Correlation coefficients between cipher images produced by slightly different keys.

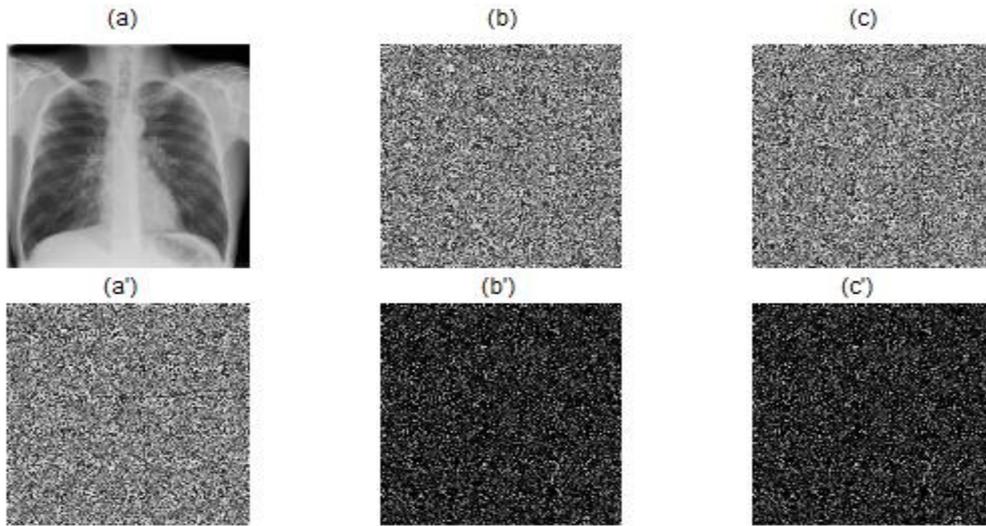| Figure 4	Key		Correlation coefficient
	s	x_0	
(a') - (b)	97.5678911	0.1234567	-0.0019
(a') - (c)	97.5678910	0.1234568	0.0054

Fig. 5. Key sensitivity in the first case: (a') Cipher image with $p = 7$, $q = 5$, $n = 10$; (b) Cipher image with $p=6$, $q = 3$, $n = 10$; (c) Cipher image with $p = 5$, $q = 3$, $n = 7$.

Table 6. Correlation coefficients between cipher X-Ray images produced by slightly different keys.

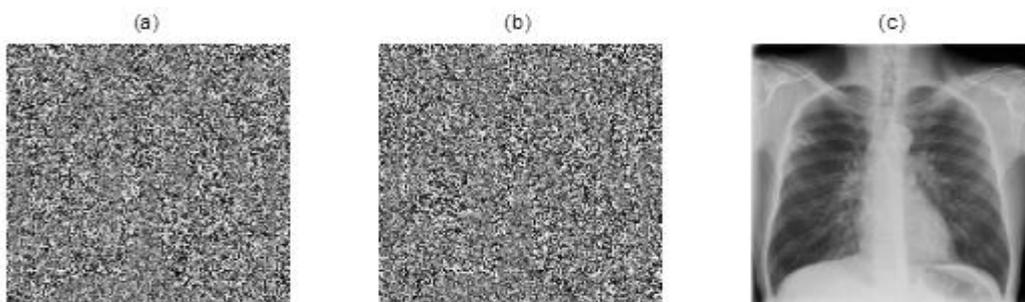| Figures	Keys			Differential Figures	Correlation coefficient
	p	q	n		
3(b)	6	4	10		
5(a')	7	5	10	3(b)-5(a')	0.0097
5(b)	6	3	10	3(b)-5(b)	0.0076
5(c)	5	3	7	3(b)-5(c)	0.0016

Fig. 6. Key sensitivity in the second case: (a) Wrong decrypted image with $s = 97.5678911$, $x_0 = 0.1234567$; (b) Wrong decrypted image with $s = 97.5678910$, $x_0 = 0.1234568$; (c) Correct decrypted image with $s = 97.5678910$, $x_0 = 0.1234567$

4.6. Data Loss and Noise Attack Analysis

During transmission, the image is subject to data loss. A powerful image cryptosystem must withstand this loss. Cropping attack and noise attack analysis is performed to find how the algorithm is stronger against a loss of data when an image is sent over the public channel.

Fig. 7 shows examples simulation of the data loss attack. A CT scan and ultrasound test images are first encrypted using the proposed algorithm. Next, a 60x60 data slice of the encrypted images is performed. According to the obtained result, the decrypted images contain most of the original information. Even after cropping, the intended receiver will be able to retrieve the plain images to some extent, hence against this cropping its robustness is been proved.

Moreover, the ability of defending the noise attacks is measured by adding different types of noise. In this test, the salt and pepper noise are added in cipher image of ultrasound and MRI with the density of 1% and 2%, which are given in Fig. 8. The Gaussian noise influences the cipher image with the intensity of 0.0001 and 0.0002 are shown in Fig.9.

From these Figures, it is concluded that the proposed method has good robustness to defend the noise attacks. It is demonstrates that the proposed method can still succeeds in recovering the image when the cipher image subjects to different noise attacks.
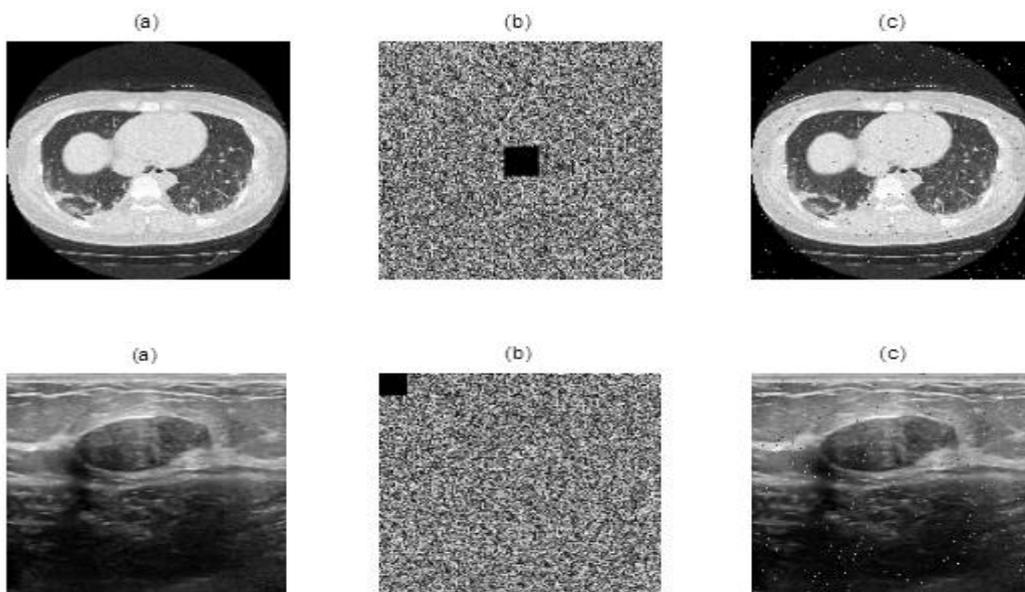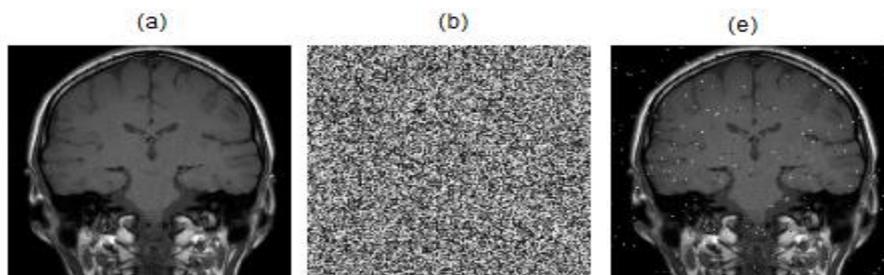

Fig. 7. Data loss analysis: (a) Original Ultrasound and CT scanner images;

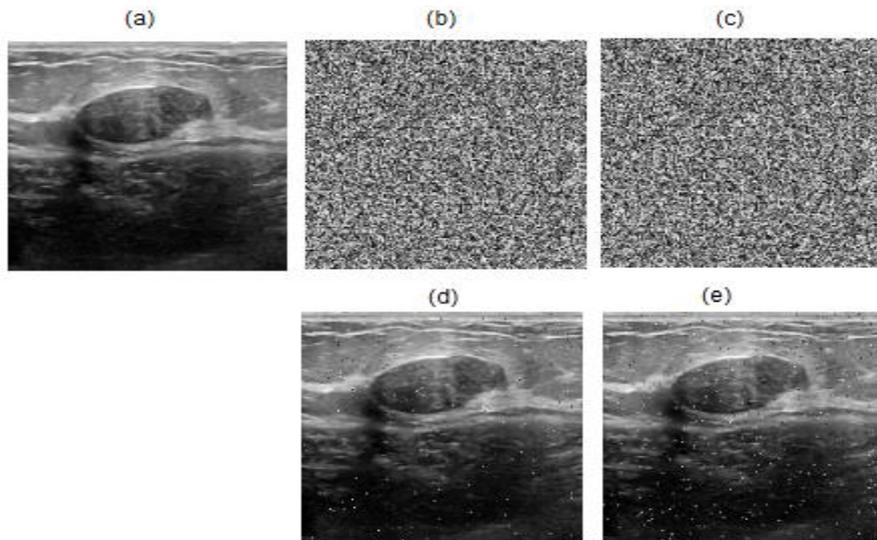(b) Cipher image with 60×60 data cut; (c) Decrypted image of (b).

Fig. 8. Noise attack analysis: (a) Original Ultrasound and MRI images; (b)-(c) Cipher images added with 1% "salt & pepper" and 2% "salt & pepper" noise ; (d)-(e) Decrypted images.
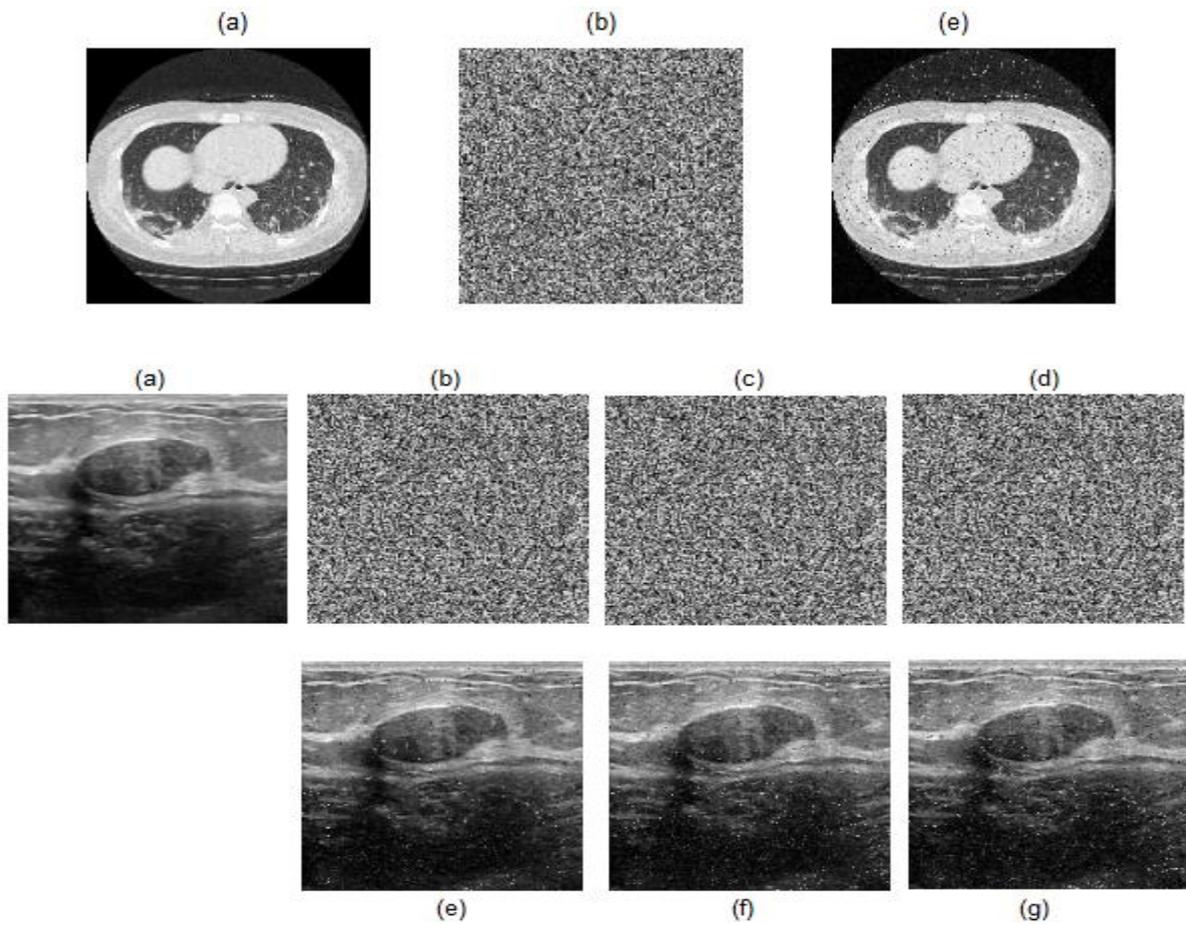

Fig.9. Noise attack analysis: (a) Original CT and Ultrasound images; (b)-(d) Cipher images under Gaussian noise with the degree of Mean=0, Variance=0.0001, 0.0002 and 0.0003; (e)-(g) Decrypted images.

5. Conclusion

To contribute to the security of medical image encryption, this paper proposes an efficient chaos-based cryptosystem is proposed for medical images. The system uses the CKBA with a modified logistics (ML) map that provides a wide range of the key space due to the unlimited value of the command parameter. Various criteria were used to analyze and validate the security and performance of the developed algorithm.

A small change in the simple image or in any cryptosystem setting will provide totally different keys even if the same encryption key is used. The experimental results proved the robustness of this algorithm achieving desirable protection for real-time medical image security applications. Further key sensitivity evaluation proves that the method in this paper is very sensitive to the small changes of the keys, and the encryption security is high. The results of plaintext sensitivity evaluation show that the NPCR average value of all encrypted images is as 99.60%.

For future work, we suggest implementing the presented method for other file types such as video and color 3D images very often encountered in ultrasound and scanner techniques.

References:
[1] S. Dutta, K. Saini, Securing Data, A Study on Different Transform Domain Techniques, *WSEAS Transactions on Systems and Control*, Vol.16, 2021, pp. 110–120.

[2] S. M. Rathnam, G.S. Koteswara Rao, A Novel Deep Learning Architecture for Image Hiding, *WSEAS Transactions on Signal Processing*, Vol.16, 2020, pp. 206–210.

[3] J.-C. Yen and J.-I. Guo, A new chaotic key-based design for image encryption and decryption, *In Proceedings of 2000 IEEE International Conference on Circuits and Systems*, Vol. 4, 2000, pp. 49-52.

[4] Borujeni, S. Etemadi, and M. S. Ehsani, Modified logistic maps for cryptographic application, *Applied Mathematics* Vol. 6.05, 2015, 773.

[5] A.U. Rehman, J.S. Khan, J. Ahmad, S.O. Hwang, A new image encryption scheme based on dynamic s-boxes and chaotic maps, *3D Research*, Vol. 7, 2016, pp. 1-8.

[6] A. Sambas, M. Mamat, S. Vaidyanathan, M. A. Mohamed, W.S.M. Sanjaya, Mujiarto, A Novel Chaotic Hidden Attractor, its Synchronization and Circuit Implementation, *WSEAS Transactions on Systems and Control*, Vol. 13, 2018, pp. 345 – 352.

[7] F. Chong, Z.F. Chen, W. Zhao, H. Jiang, A New Fast Color Image Encryption Scheme Using Chen Chaotic System, *18th IEEE conference*, 2017, pp. 121–126.

[8] F.M. Mursi, A.H. Abd El-Aziem, Applications of Chaotic Maps and Coding for Secure Transmission of Images over Wireless Channels, *WSEAS Transactions on Computer and Resaerch*, Vol. 4, 2016, pp. 86 – 95.

[9] F.-G. Jeng, W.-L.Huang and T.-H. Chen, Cryptanalysis and Improvement of Two Hyper-Chaos-Based Image Encryption Schemes, *Signal Processing*, Vol. 34, 2015, pp. 45-51.

[10] H. Xue, S. Wang, X. Meng, Study on One Modified Chaotic System Based on Logistic Map, *Research Journal of Applied Sciences, Engineering and Technology*, Vol. 5, 2013, pp. 898-904.

[11] H. Oğraş, M. Türk, A Robust Chao-Based Image Cryptosystem with an Improved Key Generator and Plain Image Sensitivity Mechanism, *Journal of Information Security*, Vol.8, 2017, pp. 23-41.

[12] S. Liua, L. Liub and M. Pang, Encryption method and security analysis of medical images based on stream cipher enhanced logical mapping, *Technology and Health Care*, Vol. 29, 2021, pp. 185–193.

[13] X. Wang, C. Tu , A chaos-based medical image encryption method, *Indonesian J. of Elec. Eng. & Comp. Sci*, Vol. 19, 2020, pp. 1316-1324.

[14] Y. Dai, H.Wang and Y. Wang, Chaotic Medical Image Encryption Algorithm Based on Bit-Plane Decomposition, *Int. J. Patt. Recogn. Artif. Intell*, Vol. 30, 2016, pp. 1657001–1657015.

[15] C. Fu, Y.-F. Shan, M.-Y. He, Z.-Y. Yu and H.-L. Wu, A new medical image encryption algorithm using multiple 1-D chaotic maps, *IEEE Inter. Conf. on Syst. Man, & Cyber*, 2018, Miyazaki, Japan, pp. 2055–2060.

[16] X. Chen and C.-J. Hu, Adaptive medical image encryption algorithm based on multiple chaotic mapping, *Saudi J. of Bio. Sci*, Vol. 24(8), 2017, pp. 1821–1827.

[17] Y. Chen, C. Tang and R. Ye, Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive

diffusion, *Signal Processing*, Vol. 167, 2020, 107286.

[18] SM. Ismail, LA. Said, AG. Radwan, Generalized double-humped logistic map-based medical image encryption, *Journal of Advanced Research*, Vol. 29(5), 2018, pp. 232-239.

[19] C. Fu, G.-y. Zhang, O. Bian, W.-m. Lei, and H.-f. Ma, A novel medical image protection scheme using a 3-dimensional chaotic system, *PloS One*, Vol. 9, 2014, pp. 1–25.

[20] K. A. Kumari, B. Akshaya, B.Umamaheswari, K.Thenmozhi, R. Amirtharajan and P.Praveenkumar, 3D Lorenz Map Governs DNA Rule in Encrypting DICOM Images, *Biomedical & Pharmacology Journal*, Vol. 11(2), 2018, pp. 897-906.

[21] U. Verma and N. Sharma, Security Analysis of Medical Images using ECC over RSA, *Journal of University of Shanghai for Science and Technology*, Vol. 23(5), 2021, pp. 356-367.

[22] L. D. Singh, K. M. Singh, Medical image encryption based on improved ElGamal encryption technique, *Optik*, Vol. 147, 2017.

[23] Q.A. Kesr, L. Nana, A. C. Pascu, S. Gire, J. M. Eghan, N. N. Quaynor, A cryptographic technique for security of medical images in health information systems, *Procedia Computer Sciences*, Vol. 58, 2015, pp. 538 – 543.

[24] E. A. Adedokun, J. B. Akan, H. Bello-Salau, I. J. Umoh, Nwosu R. I, and Y. Ibrahim, A Secure Chaotic Framework for Medical Image Encryption using a 3D Logistic Map, *Applications of Modelling and Simulation*, Vol. 4, 2020, pp. 141-148.

[25] BS. Aashiq, R. Amirtharajan, A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach, *Medical & Biological Engineering & Computing*, Vol. 22(3), 2020, pp.102-110.

[26] G. Mathur, A Survey on Medical Image Encryption, *Intern. J. of Comp. Sci & Eng.*, 2019.

[27] R. Dib, Active Contours with Term of Smouthing: Application in Medical Imaging, *WSEAS Transactions on Signal Processing*, Vol.16, 2020, pp. 108–117.

[28] W. Zhou, C.B. Alan, R.S.Hamid and P.S. Eero, Image Quality Assessment: From Error Visibility to Structural Similarity, *IEEE Trans. on Image Proc.*, Vol. 13, 2004, pp. 600-612.

[29] W. Al-Dhabyani, M. Gomaa, H. Khaled, A. Fahmy, Dataset of breast ultrasound images, *Data in Brief*, 2020, Feb;28:104863.

[30] T. Preston-Werner and C. Wanstrath, Github, https://github.com/ieee8023/covid-chestxray-dataset/tree/master/images.com, accessed September 2020.