A New 6D Hyperchaos-Based Medical Image Encryption Scheme Using *k*-Fibonacci Numbers

Samira Dib[1,*], Asma Benchiheb[2], and Fadila Benmeddour[3]
[1] Department of Electronics, MSBY University, Jijel, Algeria
[2] Faculty of Medicine, University of Constantine3, Constantine, Algeria
[3] Department of Electronic Engineering, University of M'Sila, M'Sila, Algeria
Email: samiradib@yahoo.fr (S.D.), asmabenchiheb@yahoo.fr (A.B.), benmeddourfadila@yahoo.fr (F.B.)

***Abstract*—In the era of information technology, hospitals, medical centers, doctors and health specialists share millions of images. Securing these images is essential to maintaining patients' privacy. Several cryptographic algorithms are implemented to meet the increasing demands of transmission systems. As a contribution to securing these data, we propose a novel robust and efficient algorithm. We randomly generate numbers from a six-dimensional hyperchaotic system and Arnold's cat map to confuse the original images. The confused images are then diffused using a *k*-Fibonacci matrix. The performance of the proposed algorithm was evaluated using several parameters tested on a set of reference images of different sizes and modalities. The obtained results are conclusive and the performances are excellent, sometimes exceeding those found by other recent algorithms proposed in the literature.**

***Index Terms*—hyperchaotic system, *k*-Fibonacci numbers, cryptography, medical image**

I. Introduction

Recently, the field of health has undergone immense progress, including the development of smart health, e-health, and telemedicine applications. The Covid-19 pandemic has shown us how important e-health is in our daily lives. Indeed, hospitals that use telemedicine systems benefit from high-quality services between specialists and patients. For example, to diagnose diseases or prescribe treatments, doctors and patients can interact with each other, using clinical data such as medical images. However, they are often shared over open networks, such as the internet or cellular networks. Securing these images is a challenging task that has become increasingly important in recent years.

Medical images contain confidential and sensitive information essential for the diagnosis of health conditions. Unauthorized access to these images may result in loss of patient confidentiality. In addition, if these images are modified, it could lead to an erroneous diagnosis that may put patients' lives at risk. One way to protect medical images is to use encryption algorithms. These algorithms make the images useless to anyone who does not have the encryption key. Some proposed security solutions for telemedicine are presented in [1, 2].

Manuscript received August 28, 2023; revised November 18, 2023; accepted December 12, 2023.
*Corresponding author

Chaotic systems are non-periodic and random systems with initial conditions that are very sensitive to any change. This provides them with promising prospects for robust image encryption. During the last few years, much research has been conducted in this field and encouraging results have been obtained. In fact, chaos-based cryptography uses different chaotic maps to generate random sequences that allow correct encryption of images [3, 4]. However, it has been shown that encryption algorithms using chaotic systems with simple random behavior and low ergodicity cannot withstand attacks [5, 6]. Accordingly, many researchers introduced alternative algorithms for image confusion and diffusion, such as elliptical curves developed by Sasikaladevi *et al.* [7], and Fibonacci sequences investigated by Khan et al. [8], and Hosny *et al.* [9]. In addition, Wang *et al.* [10] proposed a hybrid encryption algorithm that introduces permutation and diffusion procedures in one step, which can prevent attackers from knowing the encryption method used. More research has been directed towards manipulating sub-blocks and thus increasing resistance against potential attacks. Specifically, Xian *et al.* [11] proposed a form of image encryption based on chaotic permutation of sub-blocks and digital selection diffusion that requires the hacker to break each algorithm individually in order to obtain a clear text image. Also, Khan *et al.* [12] introduced efficient encryption of block images, based on expanding the dynamic selection of the correlation coefficient for each block, which makes hacking more difficult.

Furthermore, Chai *et al.* [13] mentioned the possibility of classifying chaotic systems in either the low or higher dimension, such as 1D chaotic maps and hyperchaotic systems. Implementation of low-dimensional systems is relatively simple. However, they provide relatively small key spaces and thus a low level of security [14].

On the other hand, securing medical data using chaotic cryptography has attracted the interest of a large number of researchers. In particular, Mathur [15] described trends and provided information for future research. Liu *et al.* [16] applied a hyperchaotic system to encrypt pathological images. In an attempt to improve the level of security for encrypting medical images, Liu *et al.* [17] presented a stream cipher-enhanced logical mapping encryption method in which the key configuration is given by the Chebyshev map while the initial value is set

doi: 10.18178/ijeetc.13.2.148-159

using a series of coding operations. In [18], the authors implemented an improved version of the ElGamal algorithm which solved the data expansion problem as well as improved the execution speed. Hua *et al*. [19] proposed an algorithm based on random data insertion that provides high-speed scrambling and adaptive pixel streaming.

In addition, Chen *et al.* [20] presented an adaptive encryption system based on enhanced chaotic mapping using a logistic-sine map to scramble individual images and a hyper-chaotic system for sub-block diffusing. Fu *et al.* [21] proposed a chaotic 3D Chen system used for both permutation and diffusion. Similarly, a chaotic framework for medical images has been proposed in [22] and [23] that allows good performance. Meanwhile authors in [24] enhanced the security by applying a fourth-dimensional system.

Singh and Singh [25] used elliptic curve cryptography for encryption, decryption, and digital signature of cipher images to give authenticity and integrity. Ali and Ali [26] designed a new medical image encryption scheme reinforced by an elliptic curve with chaotic maps that provides good results in confidentiality, authentication, integrity, unforgeability, forward secrecy, and non-repudiation. Furthermore, Banu and his collaborators [27] recommended a DICOM image encryption based on the combination of frequency and spatial domains. A chaotic 3D Lorenz attractor and a Logistic map are used to generate the keys in the frequency domain combined with a DNA sequence in the spatial domain. Kumar *et al.* [28] used fractional discrete cosine transform with chaotic function to improve the system performance.

Many other researchers focused on DNA coding in medical image cryptography, such as [29, 30]. In the method presented by Belazi *et al.* [31], the key is generated after two encryption cycles. An efficient algorithm has been proposed in [32] using a 3D-chaotic system that allows the generation of a keystream used to accomplish image confusion while diffusion is performed by a key-image generated using the Piecewise Linear Chaotic Map. Kamal *et al*. [33] presented a novel algorithm to encrypt both gray and color medical images based on splitting the image into scrambled blocks using a zigzag pattern, rotation, and random permutation. Diffusion is ensured by a chaotic logistics map offering a high level of security. In [34], the authors proposed a lightweight cryptosystem based on a chaotic Henon map, Brownian motion, and chaotic Chen system to achieve a good level of security regarding confidential medical information. In [35], Lai *et al.* proposed a new 2D Logistic-Gaussian hyperchaotic map based on a simple and high-efficiency cryptographic structure by pixel permutation and diffusion. Wang and Wang [36] presented a Logistic-Tent chaotic system (LTS) to derive the confused image and the diffusion is based on odd–even interleaved points. In order to enhance the security protection of multimedia data, the authors in [37] were interested in the synchronization problem using fractional-order hyperchaotic systems, and the proposed algorithm achieved good performance.

Low-dimensional systems are improved using hyperchaotic methods that allow generating sequences with large keyspace. However, co-encryption algorithms have certain shortcomings, especially in the face of different attacks. For example, the initial conditions of a chaotic map are often unrelated to the original image, which may make the algorithm vulnerable to differential attacks. In addition, some of these algorithms are not resistant to statistical attacks due to the non-uniformity of the histogram of the encrypted image.

To overcome the above limitations, explore the rich properties of chaotic systems, and discover the secret impact of Fibonacci sequences, we suggest a novel, robust, and efficient cryptosystem for secure medical image sharing. We implement a new efficient 6D hyperchaotic system enhanced by Arnold map to ensure the confusion of the plain image. In order to make the algorithm more resistant to differential attacks, we calculated the initial condition from the plain image itself. A matrix generated by *k*-Fibonacci numbers is applied to sub-blocks of the confused image, thus ensuring the diffusion step.

In the following, we will list the main contributions of this work:

- The *k*-Fibonacci matrix is used for the first time in the security of medical images.
- The 6D hyperchaotic system used in this work is more complex than other chaotic systems, which justifies its use in the security of medical image communication.
- The combination of Arnold's map and this new complex 6D system offers a very confusing image.
- The *k*-Fibonacci matrix has demonstrated its superiority over other methods of confusion by generating an encrypted image with a higher level of security.
- The selection of four keys has made it possible to enlarge the key space, providing strong resistance to external attacks. Indeed, the keys are x_1, p, q and n.
- The proposed technique provided very effective results, thus justifying its application for the security of medical data.

The rest of the paper is organized as follows: Section II presents the mathematical concepts of the proposed 6D hyperchaotic system, the *k*-Fibonacci matrix, and the Arnold Cat map. In Section III, we will describe our cryptographic system in detail. Section IV discusses the results obtained. Finally, Section V highlights the main results and contributions.

II. Mathematical Foundations

A. Six-Dimensional Hyperchaotic System

For many years, dynamic chaos generators have been widely used in telecommunication systems, especially in cryptography. In [38] and references therein, Kopp and Kopp developed new systems with hyperchaotic oscillations characterized by wide bandwidth and complexity of the chaotic signal structure, as well as

strong sensitivity to initial conditions. This justifies their use for the secure transmission of information.

A system is said to be hyperchaotic if it has at least four dimensions having at least two positive Lyapunov exponents. In this study, we use the 6D hyperchaotic system developed in [38] as follows:

$$\begin{cases} \dfrac{dx_1}{dt} = -x_1 + Rx_2 - 2x_4 - ax_5 \\ \dfrac{dx_2}{dt} = a(x_1 - x_2 - x_1x_3) \\ \dfrac{dx_3}{dt} = a(bx_3 + x_1x_2) \\ \dfrac{dx_4}{dt} = -x_4 + ax_1 \\ \dfrac{dx_5}{dt} = -x_5 + cx_1 + 2x_6 \\ \dfrac{dx_6}{dt} = -x_6 - dx_4 - ax_5 \end{cases} \quad (1)$$

where x_1, x_2, x_3, x_4, x_5, x_6 are the state variables of the 6D hyperchaotic system and R, a, b, c, d are the system parameters. To ensure that the sum of all exponents is negative, the authors in [38] selected the constant values as R=58; a=0.1; b=–8/3; c=8.21; d=24.65. After some calculations, the Lyapunov exponents are precisely determined as follows:

L_1 = 0.0988591, L_2 = 0.0109865, L_3 = –0.544226, L_4 = –1.00557, L_5 = –1.15581, and L_6 = –1.77091.

It can be seen that L_1 and L_2 are positive, and the sum of all terms is negative.

Compared to various chaotic systems, the new system in (1) proves to be very complex. This justifies our motivation to apply it for the security of image communication.

Fig. 1 shows the corresponding phase portraits of the hyperchaotic system (1) using the aforementioned system parameters, providing a visual window into the intricate dynamics of the used attractor. The figure reveals a captivating complexity, characteristic of chaotic systems. Furthermore, a striking resemblance to a butterfly emerges, adding a layer of visual intrigue to the system's fascinating behavior. We also confirmed the dynamic behavior of the hyperchaotic system (1) by varying the system parameter R. Fig. 2 depicts the bifurcation diagram of system (1) with the aforementioned parameter values. The diagram reveals a captivating progression of system behavior as R increases. Notably, the system trajectory transitions from a stable fixed point to a period-doubling bifurcation, ultimately leading to a chaotic attractor. This captivating sequence underscores the intricate interplay between parameter values and system dynamics.

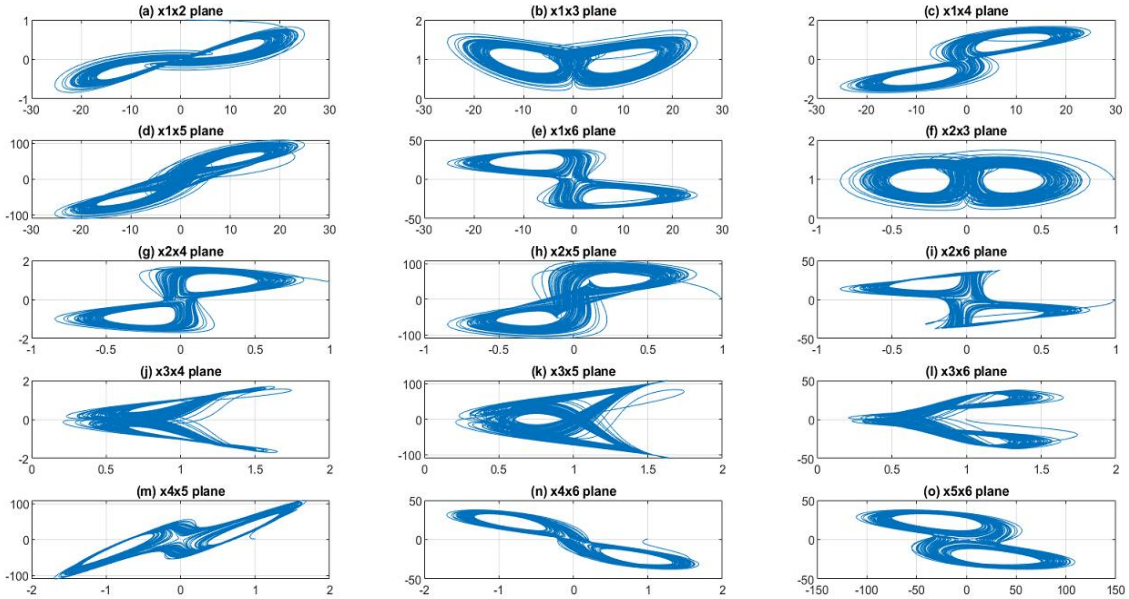


Fig. 1. Phase portrait of system (1).

B. The k-Fibonacci Matrix

For any real positive number k, the k-Fibonacci sequence is defined by [39]:

$$\mathbf{F}_{k,n+1} = kF_{k,n} + F_{k,n-1}, n \geq 1 \quad (2)$$

where $\mathbf{F}_{k,0} = 0$ and $\mathbf{F}_{k,1} = 1$ for k=1, the classical numerical Fibonacci sequence.

In order to study the recurrence sequences, we define the generator matrix by:

$$\mathbf{F} = \begin{bmatrix} 0 & 1 \\ 1 & k \end{bmatrix} \quad (3)$$

with $\det(\mathbf{F}) = -1$. For $n \geq 1$ and any real positive number k, the nth power of the k-Fibonacci matrix can be defined by:

$$\mathbf{F}^n = \begin{bmatrix} F_{k,n-1} & F_{k,n} \\ F_{k,n} & F_{k,n+1} \end{bmatrix} \tag{4}$$

where $F_{k,n}$ is the k-Fibonacci number, and the determinant of $\mathbf{F}$ is equal to $(-1)^n$. Hence, the inverse matrix $\mathbf{F}^{-n}$ has the following form:

$$\mathbf{F}^{-n} = \begin{bmatrix} F_{k,n+1} & -F_{k,n} \\ -F_{k,n} & F_{k,n-1} \end{bmatrix} \tag{5}$$

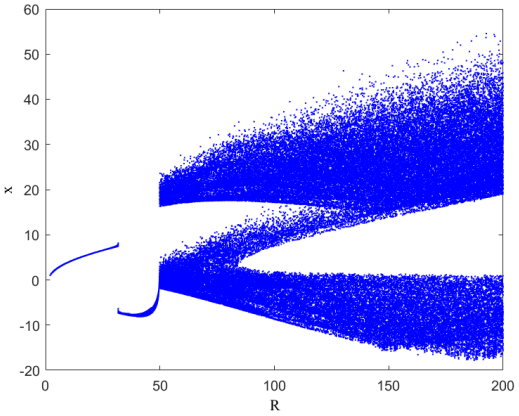


Fig. 2. Bifurcation diagram of system (1) versus parameter R.

C. The Cat Map System

The Arnold Cat Map (ACM) is a discrete system that allows efficient rearrangement of pixel positions in the original image. One can represent it by:

$$\begin{bmatrix} x_1 \\ y_1 \end{bmatrix} = \begin{bmatrix} 1 & p \\ q & pq+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \bmod N \tag{6}$$

where (x, y) are the coordinates of the plain image pixel and (x', y') correspond to the modified pixel. The ACM control parameters are the positive numbers p and q, which will be used as the confusion key parameters along with the iteration number n, i.e.,

$$\begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} pq+1 & -p \\ -q & 1 \end{bmatrix} \begin{bmatrix} x_1 \\ y_1 \end{bmatrix} \bmod N \tag{7}$$

III. Proposed Cryptosystem

In this section, we will describe in detail the main steps of the proposed algorithm. The plain image is first encrypted in an unreadable form; then it will be recovered after passing the decryption step.

Chaos-based image encryption solutions typically employ two phases of application: confusion and diffusion. It is known that normal images have high correlations between adjacent pixels, which must be broken even before applying the encryption method. The literature uses a number of strategies to ensure this process. In this work, we suggest using ACM.

A. Encryption

In the proposed algorithm, the plain image is strongly confused when using ACM within the 6D hyperchaotic system where initial conditions are calculated using the plain image. The k-Fibonacci generating matrix is used to ensure the diffusion process, which is essential for improving security.

In the following, we will present the steps of the encryption process:

1) Consider an original image of size $M \times N$.
2) Select p, q and n, and use (6) to obtain the scrambled image (IA).
3) Convert the IA image to a vector Vect.
4) Compute the first values of $x_1, x_2, \ldots, x_6$ using:

$$\begin{cases} x_1 = \dfrac{\sum_{i=1}^{MN} \text{Vect}(i) + MN}{2^{23} + MN} \\ x_i = \text{mod}(x_{i-1} 10^6, 1), \ i = 2, 3, \cdots, 6 \end{cases} \tag{8}$$

5) Choose $N_0 = 2.955MN$ and solve system (1) by setting the number of iterations equal to $N_0 + MN/3$. Then create a sequence $\mathbf{S}_l$ of size $M \times N$.
6) Order in the increasing direction $\mathbf{S}_l$ and load their positions in the vector $\mathbf{S}_p$.
7) Generate the sequence $\mathbf{R}$ as follows:

$$R_i = \text{Vect}(S_{p_i}), \quad i = 1 : M \times N \tag{9}$$

8) Reshape $\mathbf{R}$ into the matrix $\mathbf{R}_s$ and partition it into sub-blocks 2×2. Then, multiply each block with $\mathbf{F}^9$ by taking k=27, and then derive the cipher image $\mathbf{C}$ by:

$$\mathbf{C} = \mathbf{R}_s \mathbf{F}^9 \bmod 256 \tag{10}$$

9) Taking $\mathbf{IA} = \mathbf{C}$, repeat Step 3 to Step 8 two times to obtain the encrypted image $\mathbf{C}$.

B. Decryption

The decryption process involves recovering the plain image by following these steps:

1) Divide the encrypted image $\mathbf{C}$ into blocks 2×2. Then use the following equation for each block:

$$\mathbf{Db} = \mathbf{C}\mathbf{F}^{-9} \bmod 256 \tag{11}$$

2) Convert the scrambled image $\mathbf{Db}$ into a vector $\mathbf{Z}$.
3) Reposition each pixel to its original location by applying the following equation:

$$\mathbf{ER}(S_i) = Z_i, \quad i = 1 : M \times N \tag{12}$$

4) Reshape the $\mathbf{ER}$ vector into a matrix $\mathbf{D}$.
5) Taking $\mathbf{C} = \mathbf{D}$, repeat Steps 1 to Step 4 two times.
6) Derive the decrypted image using (7).

IV. Simulation Results

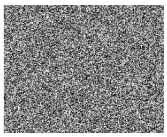
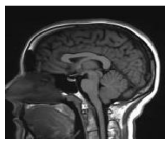
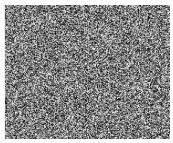
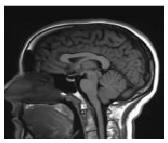
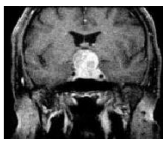
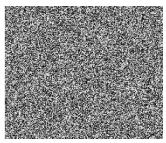
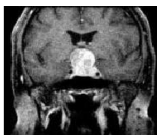
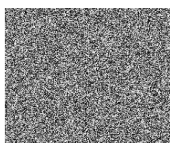
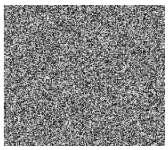
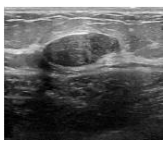
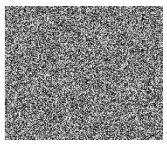
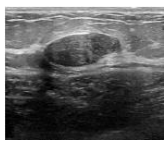
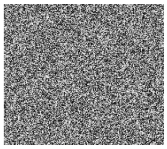
The proposed cryptographic method was evaluated using a variety of standard reference images of different sizes and modalities, namely: X-ray, ultrasound, medical imaging and computed tomography images extracted from open databases [40, 41].

All simulations were executed using MATLAB MATLAB (R2013a) with a laptop computer with a Core

i5-2430M 2.4 GHz processor and 4 GB of RAM. Moreover, a comparison was made with existing algorithms to prove its efficiency.

Accordingly, we performed several tests on the selected images to analyze the performance of the proposed cryptosystem. The input images, their encrypted images as well and their associated decrypted images are presented in Table I. As we can see, all the encrypted images are so noisy that it is impossible to obtain even the slightest information. Moreover, decrypted images are indistinguishable from their original copies. This confirms that our algorithm is effective.

TABLE I: PLAIN, ENCRYPTED AND DECRYPTED IMAGES

Image name	Plain image	Encrypted image	Decrypted image
Img1			
Img2			
Img3			
Img4			
Img5			
Img6			
Img7			

In the following, we give a mathematical example to describe the key generation and encryption processes:

1) We take the image of the Baby whose size is $N\times M$ = 230×230= 52900 ;
2) We select the ACM parameters: p = 5, q=4 and n=20 and use (6) to obtain the scrambled image (IA).
3) We convert IA to a vector Vect.
4) We compute the first values of x_1, x_2, …, x_6 using (8), and consequently we obtain: x_1=0.4684, x_2=0.9633, x_3=0.9347, x_4=0.3689, x_5=0.2540, x_6=0.0264.
5) We choose N_0=2.955$M\times N$=1.5632e+05, and solve system (1) with a number of iterations equal to $N_0+M\times N/3$=1.7395e+05. Then, we create a $\mathbf{S}_l$ sequence of size $M\times N$.
6) We order $\mathbf{S}_l$ in the increasing direction and load their positions in the vector $\mathbf{S}_p$.
7) Then, we generate the sequence **R** containing the values of $\mathbf{S}_l$ in the corresponding position of $\mathbf{S}_p$.
8) Reshape **R** into the matrix $\mathbf{R}_s$ and partition it into sub-blocks of size 2×2. Then, multiply each block with $\mathbf{F}^9$ by taking k=27, and obtain the cipher image **C** by using (10).
9) Finally, taking **IA**=**C**, we repeat Step 3 to Step 8 two times to obtain the encrypted image **C** illustrated in Table I.

A. Histogram Analysis

As is well known, the histogram of an image indicates the number of pixels in each gray level. One can validate an algorithm if the histogram of the encrypted image is uniformly distributed, which makes it difficult to guess any image information.

As can be seen from Fig. 3 (next page), the cipher images are very noisy, and their histograms are uniform. This indicates that they are random and difficult to decrypt and the proposed method can strongly resist histogram attacks.

To determine whether a histogram is uniform, we calculate the Chi-square function as follows:

$$\chi^2 = \sum_{i=1}^{256} \frac{(O_i + \mathrm{EV})^2}{\mathrm{EV}} \tag{13}$$

where O_i represents the repetition rate of the gray value i and EV is the expected frequency of each gray value and equals $O/256$. In general, we consider a significant level of 0.05 where $\chi^2(255.05)$=293.2478. Usually, if the value of χ^2 is less than 293, the histogram of the encrypted image is considered to be uniform as introduced in [16] by Liu *et al*.

The results of the Chi-square test for the proposed algorithm are summarized in Table II. We note that all values are less than 293, which indicates that the histograms of the encrypted images are uniform. This confirms the robustness of the proposed scheme.

TABLE II: CHI SQUARE AND ENTROPY VALUES OF ENCRYPTED IMAGES

Test image	Chi square	Entropy
Img1	282.89	7.9962
Img2	243.01	7.9999
Img3	280.96	7.9926
Img4	244.31	7.9988
Img5	242.34	7.9999
Img6	267.62	7.9999
Img7	257.37	7.9997
Average	**259.79**	**7.9981**

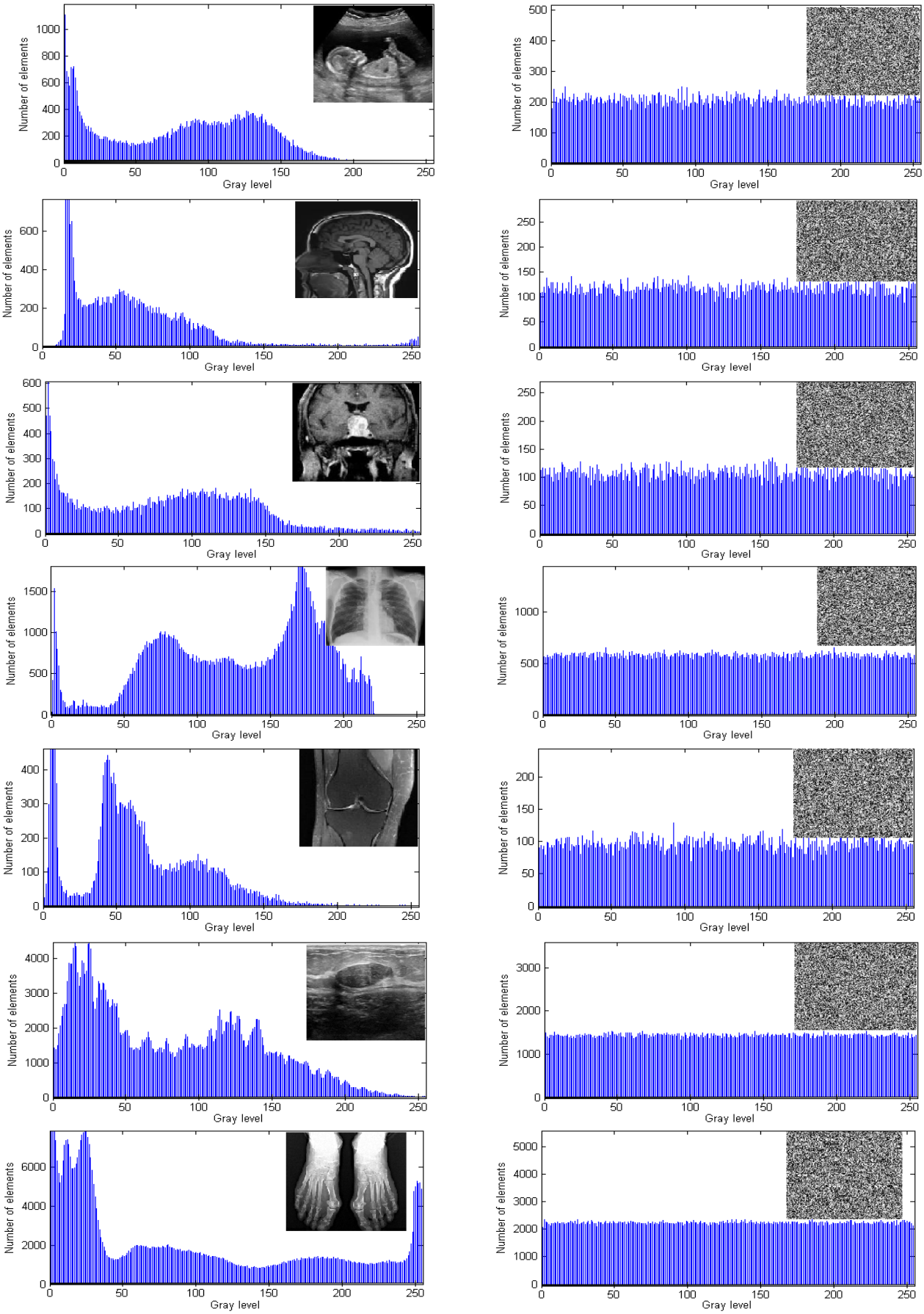


Fig. 3. Histogram of plain images at the left and encrypted images at the right.

B. Information Entropy Analysis

For the encrypted image, the pixel values should be randomly distributed so that they have no relationship to the original image. The tool that allows measuring randomness is entropy, which is calculated as follows:

$$H(x) = -\sum_{i=1}^{N} P(x_i)\log_2 P(x_i) \quad (14)$$

where $P(x)$ is the probability of appearance of x. A higher entropy value translates into a more random image. This entropy reaches a maximum value of 8 for grayscale images.

It is quite clear from Table II that the entropy analysis provided values very close to 8, which indicates that our algorithm succeeded in generating encrypted images very random and therefore very difficult to decipher.

C. Correlation Analysis

The correlation between adjacent pixels is a very important parameter for image encryption. In fact, it is known that the adjacent pixels of a plain image are strongly linked in any direction; while for the encrypted image, they are weakly linked to resist statistical attacks.

In this work, we considered 2000 pairs of adjacent pixels from the original image and the encrypted image in order to analyze the pixel dependence. The authors in [28] used (15) to determine the correlation coefficient:

$$\begin{cases} r_{ab} = \dfrac{\mathrm{cov}(a,b)}{\sqrt{D(a)D(b)}} \\ D(a) = \dfrac{1}{M}\sum_{i=1}^{M}(a - E(a_i))^2 \\ E(a) = \dfrac{1}{M}\sum_{i=1}^{M} a_i \\ \mathrm{cov}(a,b) = \dfrac{1}{M}\sum_{i=1}^{M}(a_i - E(a))(b_i - E(b)) \end{cases} \quad (15)$$

where a and b are the values of two adjacent pixels, $E(a)$ and $E(b)$ represent their respective mean, and M is the number of adjacent pixels of the image.

The correlation coefficient ranges from −1 to 1. If it is equal to 1, it reflects the strong dependence of the original image with the encrypted one as well as the exact similarity between the two images. If it is zero, the two images are no longer correlated. In the case where the pixels are strongly independent, the value of the correlation coefficient should be very close to 0.

TABLE III: THE CORRELATION COEFFICIENT VALUES OF TESTED IMAGES

Test image	Correlation Coefficient					
	Plain Image			Encrypted image		
	horizontal	vertical	diagonal	horizontal	vertical	diagonal
Img1	0.9859	0.9228	0.9302	0.02048	−0.00362	−0.00444
Img2	0.9001	0.9263	0.8317	−0.01301	−0.007209	0.003386
Img3	0.9402	0.9615	0.8939	−0.01307	−0.00103	−0.01635
Img4	0.9962	0.9972	0.9939	0.0044	−0.0083	−0.0042
Img5	0.7958	0.9799	0.8376	−0.00707	0.01072	0.01203
Img6	0.9982	0.9902	0.9878	-0.00465	0.00165	0.02779
Img7	0.9947	0.9975	0.9938	−0.00151	0.01786	0.00164
Average	**0.9444**	**0.9679**	**0.9241**	**-0.00206**	**0.00144**	**0.00284**

The results obtained are shown in Table III. Obviously, the two adjacent pixels of the plain image are strongly correlated in the three directions. However, the correlation is very weak for the two adjacent pixels of the encrypted image. Hence, we can conclude that our algorithm has excellent confusion and diffusion properties, and therefore can resist any attack that attempts to decrypt the encrypted image.

In addition to the calculated values, the correlation can be illustrated by a graphical representation that is a useful tool for visual inspection of the dependence related to image pixels and the efficiency of the encryption algorithm. The graph of an original image should show a concentration of points on the 45-degree line. This is because the adjacent pixels are highly linked. These points should be scattered for an encrypted image to justify the power of the algorithm to break any link between adjacent pixels.

Fig. 4 consists of the graphical representation of the correlation for the chest X-ray image in the horizontal, vertical and diagonal directions. Accordingly, graphs of the plain image (Fig. 4 (a) to (c)) show a concentration of points on the first diagonal. Whereas, the graphs for the encrypted images (Fig. 4 (d) to (f)) are scattered in all directions. This clearly indicates the efficiency of our algorithm in breaking the strong dependency between adjacent pixels.

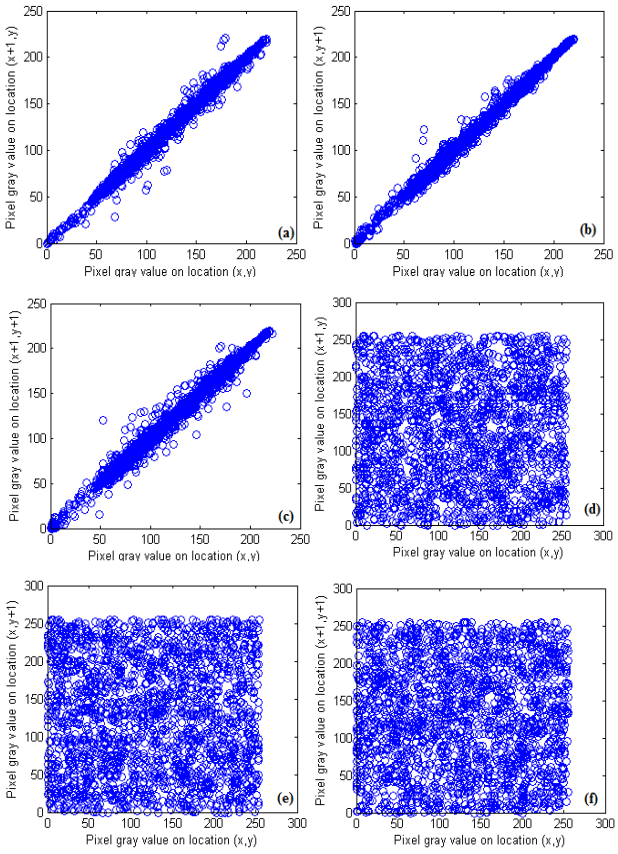


Fig. 4. Correlation distribution of the plain image in horizontal, vertical and diagonal direction in (a)–(c) and distribution of the encrypted image in horizontal, vertical and diagonal direction in (d)–(f).

D. Differential Attack Analysis

1) NPCR and UACI tests

In order to assess the robustness of an image encryption algorithm, the number of pixel rate of change (NPCR) and unified average change of intensity (UACI) values are used. In this analysis, we determine the relationship between two encrypted images, after modifying a pixel of the plain image for one of them. The NPCR represents a measure of the minimum number of modified pixels, while the UACI consists of the average difference between the two encrypted images. These two quantities are defined as follows [28]:

$$\mathrm{NPCR} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} D(i,j)}{MN} \times 100 \tag{16}$$

$$\mathrm{UACI} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} \left|E_2(i,j) - E_1(i,j)\right|}{255MN} \times 100$$
$$\text{subject to } D(i,j) = \begin{cases} 0 & \text{if} \quad E_2(i,j) = E_1(i,j) \\ 1 & \text{if} \quad E_2(i,j) \neq E_1(i,j) \end{cases} \tag{17}$$

where E_1 and E_2 are the encrypted images.

As tabulated in Table IV, the values of NPCR and UACI for the proposed algorithm are close to the ideal values equal to 99.6094% and 33.4635%, respectively. This clearly indicates that the algorithm strongly resists differential attacks.

TABLE IV: NPCR AND UACI VALUES

Test image	NPCR (%)	UACI (%)
Img1	99.5898	33.4647
Img2	99.6003	33.4771
Img3	99.6262	33.4873
Img4	99.6229	33.4141
Img5	99.5794	33.438
Img6	99.5983	33.4378
Img7	99.6123	33.4708
Average	**99.6042**	**33.4557**

2) MSE, PSNR and SSIM

Three other criteria have been used to evaluate the performance of the proposed image encryption algorithm, i.e., the Mean Square Error (MSE), the Peak Signal-to-Noise Ratio (PSNR) and the Structural Similarity (SSIM) values. These metrics are defined as follows [42]:

$$\mathrm{PSNR} = 20 \times \log_{10} \frac{\mathrm{MAX}}{\sqrt{\mathrm{MSE}}} \tag{18}$$

$$\mathrm{MSE} = \frac{\sum_{i=1}^{M}\sum_{j=1}^{N} \left[I(i,j) - K(i,j)\right]^2}{MN} \tag{19}$$

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \tag{20}$$

where MAX is the maximum supported pixel value, $I(i, j)$ denotes the original image pixel value at location (i, j), and $K(i, j)$ denotes the received image pixel value at location (i, j).

To have a good image encryption algorithm, especially for medical images, the decrypted image should be the same as the original. The values of the MSE, PSNR, and SSIM are gathered in Table V. It is clearly observed that MSE is very high, PSNR is less than 10 dB and the SSIM is very close to 0 for all the encrypted images. This means that the original and encrypted images are significantly different from each other. In contrast, the MSE is null, the SSIM is practically equal to 1, and the PSNR is infinite for the decrypted images. This indicates that the decrypted images have been well reconstructed.

In addition, we calculated the average values for all criteria. The results showed that the proposed image encryption algorithm has high values of entropy, NPCR, UACI, and Chi-Square, and has low values of PSNR, SSIM and correlation coefficient. These results confirm that the proposed method is highly secure and powerful in protecting medical images. Accordingly, the proposed method achieved the main goals of image encryption, namely illegibility and indeterminacy.

TABLE V: THE MSE, SSIM AND PSNR VALUES FOR THE ENCRYPTED/DECRYPTED IMAGES

Test image	Encrypted images			Decrypted images		
	MSE	PSNR	SSIM	MSE	PSNR	SSIM
Img1	1.168e+04	7.49	0.01	0	∞	1
Img2	1.259e+04	7.16	0.01	0	∞	1
Img3	1.202e+04	7.37	0.01	0	∞	1
Img4	8.446e+03	8.90	0.04	0	∞	1
Img5	1.189e+04	7.41	0.01	0	∞	1
Img6	1.092e+04	7.78	0.03	0	∞	1
Img7	1.398e+04	6.71	0.05	0	∞	1
Average	**1.165e+04**	**7.55**	**0.02**	**0**	∞	**1**

E. Encryption Quality Analysis

1) Maximum deviation

The maximum deviation is a metric used to evaluate the encryption quality. A high maximum deviation indicates that the original and encrypted images are significantly different from each other, which makes it more difficult to decrypt. The maximum deviation is determined using the following formula:

$$D = \frac{M_0 + M_{255}}{2} + \sum_{i=1}^{254} M_i \tag{21}$$

where M_i is the difference in the histogram between the original and the encrypted images at index i. The high value of the maximum deviation reflects the large difference between the two images.

Table VI shows the values of the maximum deviation for different images. Obviously, these values are very

high, which indicates the difference between encrypted and original images. This proves the robustness of the proposed algorithm in terms of security.

TABLE VI: DEVIATION ANALYSIS

Test image	Maximum deviation	Histogram deviation
Img1	3076	0.06154
Img2	344.5	0.07661
Img3	1491	0.08362
Img4	1129.5	0.03689
Img5	137.5	0.08154
Img6	1598.5	0.02577
Img7	22599	0.02064
Average	**4339.5**	**0.05523**

2) Deviation from the uniform histogram

In order to confirm that the obtained histogram is uniform, one often measures the deviation from the uniform histogram using the following formulas:

$$H_{C_i} = \begin{cases} \dfrac{MN}{256} & , \quad 0 \le C_i \le 255 \\ 0 & , \quad \text{elsewhere} \end{cases} \tag{22}$$

$$D_H = \frac{\sum_{C_i=0}^{255} \left| H_{C_i} - H_C \right|}{MN} \tag{23}$$

where H_C refers to the histogram of the encrypted image. It is worth noting that the lower the deviation from the uniform histogram value, the closer the histogram of the encrypted image is to a uniform histogram. This means that decrypting the encrypted image is more difficult. The results in Table VII show that the proposed image encryption method has a low deviation from uniform histogram value. This proves that the method is effective in protecting the confidentiality of images.

TABLE VII: NIST STATISTICAL TEST FOR X-RAY CHEST IMAGE

Test	*p*-value	Results
Frequency	1	Random
Block-frequency	1	Random
Runs	0.82107	Random
Longest run	0.9998	Random
Discrete Fourier Transform Test	0.10000	Random
Approximate Entropy	0.966376	Random
Rank	0.1487	Random
Non-overlapping template	0.7432	Random
Serial *p*-value 1	0.3935	Random
Serial *p*-value 2	0.0811	Random

F. NIST Statistical Tests

Achieving high randomness in an encrypted image is crucial for its security. The NIST statistical test suite provides a set of tests to evaluate the randomness of the generated sequence. In this experiment, the *p*-values of the encrypted "X-Ray Chest" image were calculated for various NIST tests and the results are gathered in Table II. All *p*-values exceeded the significance level of 0.01, indicating the randomness of the encrypted sequence. This confirms the effectiveness of the proposed algorithm in generating random sequences.

G. Key Sensitivity Analysis

Key sensitivity analysis is an important part of assessing the security of a chaos-based cryptosystem. It ensures that the images are secure, even if the attacker has some knowledge of the encryption algorithm. A cryptosystem is considered highly sensitive if a slight modification of the key results in a very different encrypted image. Accordingly, decrypting the encrypted image becomes a very difficult task if the encryption key is missing. To discuss key sensitivity, we have to consider two cases:

i) A slight difference in the decryption key would never allow the correct decryption of the encrypted image.
ii) Using slightly different keys to encrypt the same image leads to totally different encryption images.

For the first case, a second key is generated from the first, chosen as x_1=0.2131, with a slight modification of order 10^{-11}. Next, we encrypt the same MRI image using both keys and decrypt the encrypted images using the two keys. As can be seen in Fig. 5, the decrypted image using a slightly different key from the original is completely unreadable. This demonstrates the sensitivity of the keys used.

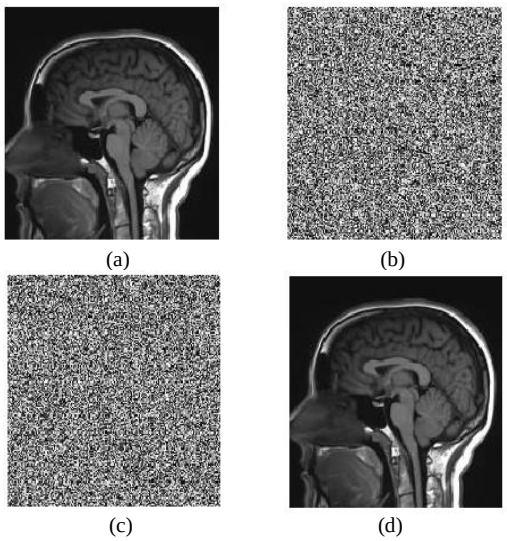


Fig. 5. Key sensitivity: (a) The plain image; (b) The encrypted image of (a) using the first key, x_1; (c) The decrypted image of (b) using the second key, $x_1 + 10^{-11}$; (d) The decrypted image of (b) using the first key.

The sensitivity analysis of the second key was conducted using an encrypted ultrasound image with a calculated key of x_1=0.4684. In addition, the plain Baby image was encrypted using three slightly different test keys, namely *p*, *q* and *n* parameters from the Cat map step. Fig. 6 shows the corresponding encryption images as well as the differential ones. Table VIII shows the correlation coefficients and the difference between encrypted images. Clearly, the obtained values confirm the robustness of the proposed algorithm and its resistance against differential attacks. Indeed, we notice that a slight modification in the encryption keys leads to incorrect encryption results.

TABLE VIII: DIFFERENCES AND CORRELATION BETWEEN THE CIPHER IMAGES PRODUCED BY SLIGHTLY DIFFERENT KEYS

Fig. 6	Keys				Differential figures	Difference %	Correlation coefficient
	x_1	*p*	*q*	*n*			
(b)	0.4684	5	4	20			
(c)	0.4681	5	4	20	(d)	99.5992	−0.0074
(e)	0.4684	7	4	20	(f)	99.5293	0.0055
(g)	0.4684	5	11	20	(h)	99.5898	−0.0066
(i)	0.4684	5	4	17	(j)	99.6352	0.0072

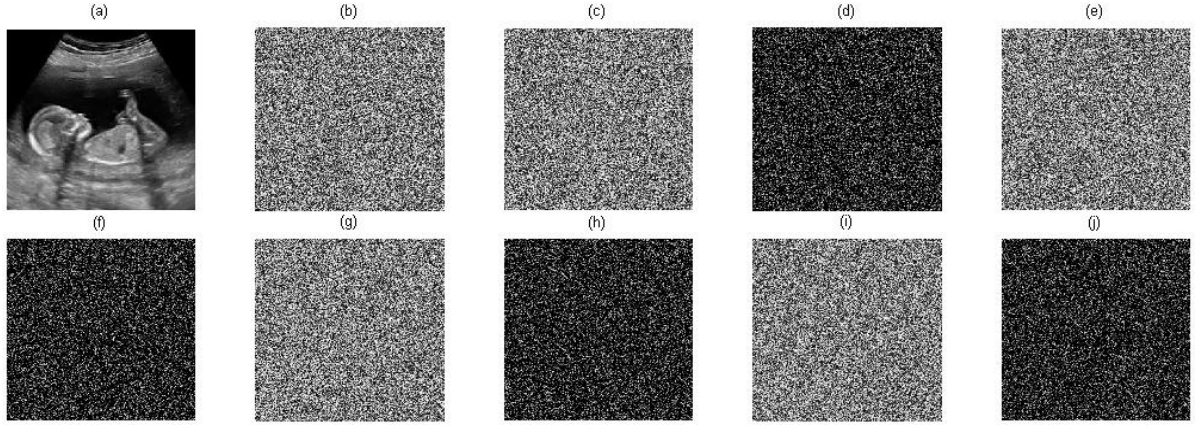


Fig. 6. Key sensitivity in the second case: (a) The plain image; (b) The ciphered image using key (1): (c) The ciphered image using key (2), (d) The differential image between (b) and (c), (e) The ciphered image using key (3), (f) The differential image between (b) and (e), (g) The ciphered image using key (4), (h) The differential image between (b) and (g), (i) The ciphered image using key (5), (j) The differential image between (b) and (i).

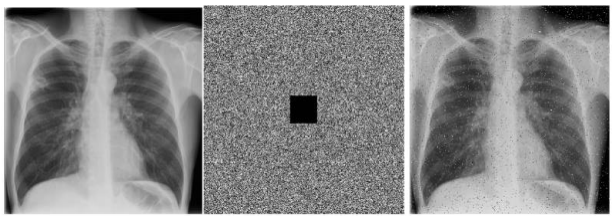


Fig. 7. Data loss analysis: (a) Original X-Ray image; (b) Cipher image with 50×50 data cut; (c) Decrypted image of (b).

H. Data Loss and Noise Attack Analysis

During transmission, the image is vulnerable to data loss. A strong image cryptosystem must bear this loss. Crop attack and noise attack analysis are performed to find out how robust the algorithm is against data loss when sending the image over the public channel. Fig. 7 shows an example of a loss attack simulation. The X-ray test image is first encrypted using the proposed algorithm. Next, a 50×50 data slice of the encrypted image is performed. According to the result obtained, the decrypted image contains most of the original information. Even after cropping, the intended receiver will be able to restore the plain image to some extent, thus proving its robustness against this type of cropping.

Moreover, the ability to defend against noise attacks is measured by adding different types of noise. In this test, salt and pepper noise is added in the cipher ultrasound image with a density of 1% and 2%. Gaussian noise affects the encrypted image with intensities of 0.0001 and 0.0002 as shown in Fig. 8. Therefore, we concluded that the proposed algorithm has good strength to defend against noise attacks. It is also demonstrated that the proposed method is still able to restore the original images when the encrypted images are exposed to different forms of noise attacks.

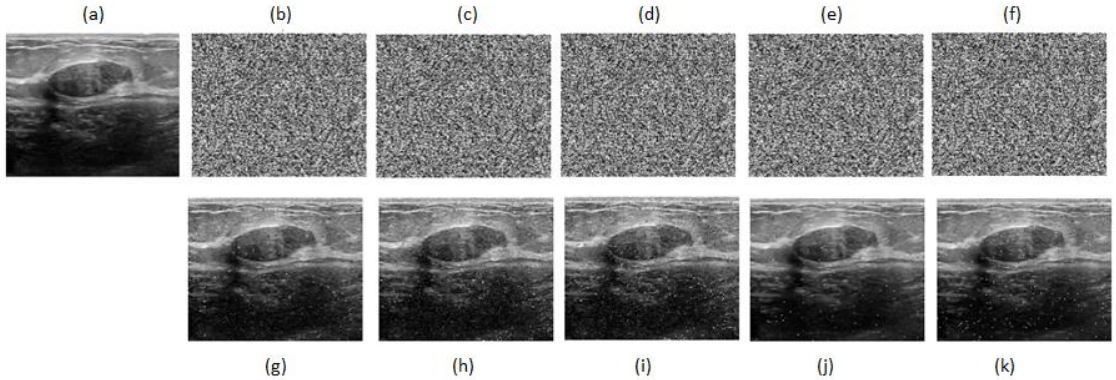


Fig. 8. Noise attack analysis: (a) Original Ultrasound image; (b)-(c) Cipher images added with 1% “salt & pepper” and 2% “salt & pepper” noise ; (d)-(f) Cipher images under Gaussian noise with the degree of Mean=0, Variance=0.0001, 0.0002 and 0.0003 ; (g)-(k) Decrypted images.

I. Time Complexity Analysis

An encryption algorithm is judged to be effective if it has a high level of security and fast encryption speed. Table IX depicts the time required to encrypt each image. We note that the proposed scheme has very low computational complexity, even for large images.

TABLE IX: TIME TAKEN FOR ENCRYPTION/DECRYPTION

Test image	Size	Encryption time (s)	Decryption time (s)
Img5	158×158	0.388103	0.255463
Img3	166×166	0.382716	0.358559
Img2	174×174	0.417648	0.315836
Img1	230×230	0.629005	0.461424
Img4	384×384	1.666685	1.293313
Img6	606×606	3.869101	3.208262
Img7	756×756	5.870159	4.986675
Average		**1.8891**	**1.5542**

TABLE X: COMPARISONS IN TERMS OF DIFFERENT PARAMETERS

Test image		Adjacent pixel correlation			NPCR(%)	UACI(%)	Entropy
		Horizontal	Vertical	Diagonal			
	Ref [28]	0.0082	0.0058	0.0041	99.5943	33.3964	7.9874
	Ref [29]	0.0092	0.0062	0.0092	99.5712	33.3847	7.9862
	Ref [30]	−0.0186	0.0030	0.0042	99.6014	33.4112	7.9932
	Ref [31]	0.0072	0.0048	0.0041	99.5955	33.421	7.9955
	Ref [32]	−0.0025	−9.4017e-04	−0.0033	99.6002	33.4203	7.9974
	proposed	**0.0044**	**-0.0083**	**-0.0042**	**99.6229**	**33.4141**	**7.9988**
	Ref [28]	0.0034	0.0046	0.0060	99.9874	33.3994	7.9797
	Ref [29]	0.0050	0.0049	0.0046	99.5817	33.3913	7.9847
	Ref [30]	−0.0057	−0.0063	0.0055	99.6014	33.4089	7.9931
	Ref [31]	0.0044	0.0059	0.0076	99.5984	33.4215	7.9901
	Ref [32]	−0.0017	−0.0013	−0.0013	99.5573	33.3654	7.9976
	proposed	**0.0235**	**−0.0017**	**−0.0386**	**99.6003**	**33.4771**	**7.9999**

J. Comparison and Discussions

To highlight the efficiency and robustness of the proposed encryption method, we compared it with other algorithms reported in the literature. The comparison is carried out using two different images, and the results obtained are given in Table X. It can be seen that all algorithms can generate good-quality encrypted images. However, the obtained values for the proposed algorithm are much better than the others. In particular, the very low value of the correlation coefficient as well as that of entropy which is very close to 8 shows that the proposed algorithm is more efficient and offers superior security. Therefore, this comparison chart demonstrates that the proposed cryptosystem represents a promising new approach to image encryption.

V. CONCLUSION

Medical images are often sensitive and confidential, and it is important to protect them from unauthorized access. In this context, we proposed a new chaos-based cryptosystem using a 6D hyperchaotic system with *k*-Fibonacci numbers. We used the plain image to generate the key, which helps to prevent well-known and chosen plaintext attacks. Alternative keys taken from Arnold's map were used to improve the security performance of the proposed algorithm. The diffusion step is performed using a *k*-Fibonacci matrix.

We conducted several simulations to demonstrate the robustness and efficiency of our algorithm. Accordingly, we have obtained excellent results confirming the effectiveness of this cryptosystem for medical image security. It is also demonstrated that the proposed algorithm is highly secure against various external attacks, including brute-force attacks, differential attacks, and statistical attacks. Additionally, our cryptosystem is versatile and can be used to encrypt a wide variety of medical images. A comparison with some modern encryption algorithms showed that the proposed cryptosystem has superior performance.

We believe that this study has the potential to maintain the safety of medical images as we are confident that the proposed cryptosystem will be used to protect sensitive patient data and ensure the accuracy of medical diagnoses and treatments. From the perspective of this work, we plan to implement the proposed algorithm for 3D color images and videos as well as in real-world medical applications.

CONFLICT OF INTEREST

The authors declare no conflict of interest.

AUTHOR CONTRIBUTIONS

Samira DIB conducted the research focusing on the analysis of the results and wrote the article; Fadila BENMEDDOUR supervised the work with a focus on Chaos Encryption; Asma BENCHIHEB emphasized the security of medical images; all authors approved the final version.

REFERENCES

[1] Y. Dai, H. Wang, Z. Zhou, and Z. Jin, "Research on medical image encryption in telemedicine systems," *Technology and Health Care*, vol. 24, no. 2, pp. 435–442, 2016.

[2] V. Pavithra and J. Chandrasekaran, "Developing security solutions for telemedicine applications: medical image encryption and watermarking," in *Research Anthology on Telemedicine Efficacy, Adoption, and Impact on Healthcare Delivery*, pp. 612–631, 2021, https://doi.org/10.4018/978-1-7998-8052-3.ch032.

[3] S. Agarwal, "Secure image transmission using fractal and 2D-chaotic map," *J. of Imag.*, vol. 4, no. 1, 17, 2018.

[4] J. Ahmad, F. Masood, S. A. Shah, S. S. Jamal, and I. Hussain, "A novel secure occupancy monitoring scheme based on multi-chaos mapping," *Symmetry*, vol. 12, no. 3, #350, 2020.

[5] 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, pp. 45-51, 2015, https://doi.org/10.1016/j.image.2015.03.003.

[6] Y. Ma, C. Li, and B. Ou, "Cryptanalysis of an image block encryption algorithm based on chaotic maps," *J. Inf. Secur. Appl*, vol. 54, #102566, 2020.

[7] N. Sasikaladevi, K. Geetha, K. Sriharshini, and M. D. Aruna, "H3-hybrid multilayered hyper chaotic hyper elliptic curve based image encryption system," *Optics & Laser Technology*, vol. 127, #106173, 2020.

[8] M. Khan, F. Masood, and A. Alghafis, "Secure image encryption scheme based on fractals key with Fibonacci series and discrete dynamical system," *Neur. Comp. and Appl.*, vol. 32, no. 15, pp. 11837–11857, 2020.

[9] K. M. Hosny, S.T. Kamal, M. M. Darwish, and G. A. Papakostas, "New image encryption algorithm using hyperchaotic system and Fibonacci Q-matrix," *Electronics*, vol. 10, #1066, 2021.

[10] X. Wang, Y. Wang, X. Zhu, and C. Luo, "A novel chaotic algorithm for image encryption utilizing one-time pad based on pixel level and DNA level," *Opt, Lasers Eng.*, vol. 125, #105851, 2020.

[11] Y. Xian, X. Wang, and X. Yan, "Image encryption based on chaotic sub-block scrambling and chaotic digit selection

diffusion," *Opt, Lasers Eng.*, vol. 134, #106202, 2020.
[12] J.S. Khan and J. Ahmad, "Chaos based efficient selective image encryption," *Multidimens. Syst. Signal Processing*, vol. 30, pp. 943–961, 2019, https://doi.org/10.1007/s11045-018-0589-x.
[13] X. Chai, X. Fu, Z. Gan, Y. Lu, and Y. Chen, "A color image cryptosystem based on dynamic DNA encryption and chaos," *Signal Process*, vol. 155, pp. 44–62, 2019, https://doi.org/10.1016/j.sigpro.2018.09.029.
[14] C. Pak and L. Huang, "A new color image encryption using combination of the 1D chaotic map," *Signal Process*., vol. 138, pp. 129–137, 2017, https://doi.org/10.1016/j.sigpro.2017.03.011.
[15] G. Mathur, "A survey on medical image encryption," *Intern. J. of Sci Research in Sci & Tech.*, vol. 3, no. 5, pp. 1-8, 2019.
[16] H. Liu, A. Kadir, and J. Liu, "Color pathological image encryption algorithm using arithmetic over Galois field and coupled hyper chaotic system," *Opt, Lasers Eng.*, vol. 122, pp. 123–133, 2019, https://doi.org/10.1016/j.optlaseng.2019.05.027.
[17] S. Liu, L. Liu, and M. Pang, "Encryption method and security analysis of medical images based on stream cipher enhanced logical mapping," *Technology and Health Care*, vol. 29, pp. 185–193, 2021, https://doi.org/10.3233/THC-218019.
[18] D. S. Laiphrakpam and M. S. Khumanthem, "Medical image encryption based on improved ElGamal encryption technique," *Optik*, vol. 147, pp. 88–102, 2017, 1016/J.IJLEO.2017.08.028.
[19] Z. Hua, S. Yi, and Y. Zhou, "Medical image encryption using high speed scrambling and pixel adaptive diffusion," *Signal Process*., vol. 144, pp. 134-144, Mar. 2018.
[20] X. Chen and C.-J. Hu, "Adaptive medical image encryption algorithm based on multiple chaotic mapping," *Saudi J. of Bio. Sci*, vol. 24, no. 8, pp. 1821–1827, 2017.
[21] 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, no. 12, pp. 1–25, 2014.
[22] E. A. Adedokun, J. B. Akan, H. Bello-Salau *et al.*, "A secure chaotic framework for medical image encryption using a 3D logistic map," *Applications of Modelling and Simulation*, vol. 4, pp. 141-148, 2020.
[23] J. B. Akan, E. A. Adedokun, G. Onuh *et al.*, "Medical image encryption scheme based on hybrid chaotic permutation," *International Journal of Scientific Research in Computer Science and Engineering*, vol. 8, no. 4, pp. 97-104, 2020.
[24] J. Liu, S. Tang, J. Lian, Y. Ma, and X. Zhang, "A novel fourth order chaotic system and its algorithm for medical image encryption," *Multidimensional Syst. Signal Process*., vol. 30, no. 4, pp. 1637-1657, 2019.
[25] L. D. Singh and K. M. Singh, "Image encryption using elliptic curve cryptography," *Procedia Comput. Sci.*, vol. 54, pp. 472-481, 2015, https://doi.org/10.1016/j.procs.2015.06.054.
[26] T. S. Ali and R. Ali, "A novel medical image signcryption scheme using TLTS and Henon chaotic map," *IEEE Access*, vol. 8, pp. 71974-71992, 2020.
[27] A. Banu S and R. Amirtharajan, "A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach," *Med. Biol. Eng. Comput.*, vol. 58, no. 7, pp.1445-1458, 2020.
[28] S. Kumar, B. Panna, and R.K. Jha, "Medical image encryption using fractional discrete cosine transform with chaotic function," *Medical, & Biological Eng. & Computing*, vol. 57, no. 11, pp. 2517–2533, 2019.
[29] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "DNA chaos blend to secure medical privacy," *IEEE Trans. on NanoBioscience*, vol. 16, no. 8, pp. 850–858, 2017.
[30] J. C. Dagadu, J. P. Li, and E. O. Aboagye, "Medical image encryption based on hybrid chaotic DNA diffusion," *Wireless Pers. Commun.*, vol. 108, pp. 591–612, 2019, https://doi.org/10.1007/s11277-019-06420-z.
[31] A. Belazi, M. Talha, S. Kharbech, and W. Xiang, "Novel medical image encryption scheme based on chaos and DNA encoding," *IEEE Access*, vol. 7, pp. 36667–36681, 2019.
[32] P. Sarosh, S. A. Parah, and G. M. Bhat, "An efficient image encryption scheme for healthcare applications," *Multimed. Tools Appl.*, vol. 81, pp. 7253–7270, 2022, https://doi.org/10.1007/s11042-021-11812-0.
[33] S. T. Kamal, K. M. Hosny, T. M. Elgindy *et al.*, "A new image encryption algorithm for grey and color medical images," *IEEE Access*, vol. 9, pp. 37855-37865, 2021.
[34] F. Masood, M. Driss, W. Boulila *et al.*, "A lightweight chaos-based medical image encryption scheme using random shuffling and XOR operations," *Wireless Pers. Commun.*, vol. 127, pp. 1405-1432, 2021, https://doi.org/10.1007/s11277-021-08584-z.
[35] Q. Lai, G. Hu, U. Erkan, and A. Toktas, "High-efficiency medical image encryption method based on 2D logistic-Gaussian hyperchaotic map," *Appl. Math. & Comput.*, vol. 442, #127738, 2023, https://doi.org/10.1016/j.amc.2022.127738.
[36] X. Wang and Y. Wang, "Multiple medical image encryption algorithm based on scrambling of region of interest and diffusion of odd-even interleaved points," *Expert Sys. Appli.*, vol. 213, Part A, #118924, 2023, https://doi.org/10.1016/j.eswa.2022.118924.
[37] M. S. Bouridah, T. Bouden, and M. E. Yalçin, "A delayed outputs fractional-order hyperchaotic systems synchronization for images encryption," *Multimed. Tools Appl.*, vol. 80, pp. 14723-14752, 2021, https://doi.org/10.1007/s11042-020-10425-3.
[38] M. Kopp and A. Kopp, "A new 6D chaotic generator: Computer modelling and circuit design," *Int. J. Eng. Technol. Innov.*, vol. 12, no. 4, pp. 288–307, 2022.
[39] 42A. Borges, P. Catarino1, A. P. Aires *et al.*, "Two-by-two matrices involving k–Fibonacci and k-Lucas sequences," *Appl. Math. Sci.*, vol. 8, no. 34, pp. 1659 – 1666, 2014.
[40] W. Al-Dhabyani, M. Gomaa, H. Khaled, and A. Fahmy, "Dataset of breast ultrasound images", *J. Data in Brief*, vol. 28, #104863, 2020, https://doi.org/10.1016/j.dib.2019.104863.
[41] T. Preston-Werner and C. Wanstrath. COVID-19 image data collection. [Online]. Available: https://github.com/ieee8023/covid-chestxray-dataset/tree/master/images.com. [Accessed: Feb-2023].
[42] W. Zhou, A. C. Bovik, H. R. Sheikh, and E. P. Simoncelli, "Image quality assessment: from error visibility to structural similarity," in *IEEE Trans. on Image Proc.*, vol. 13, no. 4, pp. 600-612, 2004.

Samira Dib received the Ph.D. degree in Electronics – Signal Processing and Communication- from the University of Batna (Algeria) in 2014. She got her Engineer and Magister degrees in electrical engineering from the University of Constantine in Algeria, in 1991 and 1995 respectively. Since 1997, she has been an associate professor at the Electronic Department of Jijel University in Algeria. She is a member of the Nondestructive Tests Laboratory (LEND) at the same University. She is a reviewer of some reputed journals and international conferences. Her main research interests concern radar detection, Nondestructive testing, signal processing, and medical data security. She authored and co-authored many papers in International conferences and journals.

Fadila Benmeddour received the engineer diploma in electronic engineering in 1995 and the Magister degree in communication in 2003, from Constantine University, Algeria. Since 2004, she has been working as a teaching assistant in the Department of Electronics at M'sila University, Algeria. She received the Ph.D. degree in micro-systems and instrumentation engineering in 2012 from Constantine University and an HDR degree in 2019 from M'sila University. Her research interests include microstrip antennas and computational electromagnetic.

Benchiheb Asma received her engineer diploma in 1991, the magister diploma in 1996, and a Ph.D. degree in electronics in 2018 all from the Department of Electronics, University of Constantine 3, Algeria. She is working as an Associate Professor in the Faculty of Medicine, University of Constantine3, Algeria. Her research interests include microelectronics structures, nanotechnologies, photovoltaics, and Securing medical data.