Multimedia Tools and Applications (2024) 83:30819–30845
https://doi.org/10.1007/s11042-023-16730-x

Image encryption algorithm based on 2D logistic map system in IoHT using 5G network

J. Fotsing[1] · J.-M. Moukam Kakmeni[1] · A. Tiedeu[2] · H. B. Fotsin[3]

Received: 24 February 2022 / Revised: 15 May 2023 / Accepted: 31 August 2023 /
Published online: 13 September 2023

Abstract
In this paper, an image encryption technique is proposed to encrypt the images by using a 2D Logistic map with the SHA-256 sequence generator. The initial conditions and control parameters of the chaotic maps served as the key for the cryptosystem, and were made dependent on the plain image through the SHA-256 protocol. The internal loop of the proposed image encryption method is made of 2D logistic permutation, and 2D logistic diffusion. In order the proposed system performance, widely known and accepted metrics as keyspace, key sensitivity, histogram, correlation and entropy were computed. Experimental results showed that the proposed approach was highly key sensitive and exhibited a good resistance against brute-force and statistical attacks. The cryptosystem presented in this part was designed to ensure the safe exchange of medical images on the 5G telecommunication network using IoHT in the interconnexion of different hospital services.

Keywords Encryption · IoHT · 2D Logistic diffusion · 2D Logistic permutation · Images

1 Introduction

As the internet expands thanks to 4G and 5G networks, the security of data like digital images and videos becomes a real challenge for all internet users. Data exchange between the legitimate doctors or technicians in the environment of network using of Internet of Healthcare Things (IoHT) needs to be protected before transmission by encrypting the latter. In the IoHT context, devices are connected to the internet to be able to communicate medical data of patients effectively and also to have access to remote medical facilities with a focus on improving patients' healthcare. Medical images are a large part of a patient's medical data. It needs security while transmitting. The encryption converts the meaningful

✉ J. Fotsing
fotsing.janvier@ubuea.cm

[1] Department of Physics, Faculty of Science, University of Buea, P.O. Box 63, Buea, Cameroon

[2] Instrumentation, Signal and Image Laboratory, National Advanced School of Engineering of Yaounde, University of Yaounde I, P.O. Box 8390, Yaounde, Cameroon

[3] Department of Physics, Faculty of Science, University of Dschang, P.O. Box 63, Dschang, Cameroon

information into garbage data; so no malicious user can read the data. Moreover, many methods to encrypt the data as RSA, DES and IDEA were proposed by researchers [1–5]. In [5] the well-known solution for securing the data (in any form) is encryption. The traditional encryption techniques such as AES, DES, RSA, etc., exhibit a low level of security and significantly low level of resistance to the attacks. Based on the previous list of works, this problem can be overcomed by chaotic image encryption techniques as they have a high level of randomness in key generation. RSA, DES and IDEA algorithms are most used in data encryption and very few in images encryption based on chaotic system.

Chaos was used in encryption systems because of its characteristics among which are sensitivity to the initial conditions and unpredictability of the chaotic sequences. Many approaches used to design image encryption algorithms are chaos based [6–8]. In [6], the authors presented a new image encryption algorithm based on chaos and deoxyribonucleic acid (DNA) coding. The proposed algorithm uses two keys, an internal key and an external one coming from the image to be encrypted. D. Jiany et al. using multi-chaotic maps, encrypted an image by dividing the process into two main phases: in the first phase pixels are permuted by using an Arnold cat map and in the second phase, the multi-chaotic maps are used to encrypt the permuted pixels [9]. In [1], the authors used image encryption algorithm based on logistic map chaotic function to change the value of the pixel without shuffling the image itself and modified the pixels value by using the rows and columns replacement approach. A. Jolfael and A. Mirghadri have proposed an encryption scheme based on a combination of a chaotic map and stream cipher [10]. Their proposal includes two major parts, chaotic pixel shuffling and W7 secret key stream generator. In [11], the authors used one dimensional chaotic map. It has been shown that the method can be used for binary images encryption with the possibility of using several keys such as the initial state, the external parameters and the number of iterations. It is also shown that the sensitivity to initial state plays an important role in chaotic encryption. In [12], the authors used image encryption based on nonlinear map. In [13], the authors incorporate permutation and substitution methods together, to present a strong image encryption algorithm. An optimized treatment and a cross-sampling disposal have been introduced for enhancing the irregular and pseudorandom characteristics of chaotic sequences. In [14], authors proposed a scheme using two chaotic systems based on the thought of higher secrecy of multi-system. One of the chaotic systems was used to generate a chaotic sequence. Then this chaotic sequence was transformed into a binary stream by a threshold function. The other chaotic system was used to construct a permutation matrix. Firstly, the pixel values of a plain image have been modified randomly using the binary stream as a key stream. Secondly, the modified image was encrypted again by the permutation matrix.

Some weaknesses of the algorithms mentioned above can be stated as follows:

- some methods exclusively depend on the key streams [1, 4, 5];
- the ciphers also have reduced keyspace because of a reduced range of control parameter [8];
- the lack of an exclusive algorithm to be used in an IoHT framework [6].

Medical images convey very vital information concerning the health condition of patients. Usually, hospitals and other health organizations pay special attention to store and transmit medical images. As IoHT technologies are emerging nowadays with 4G and 5G networks, efficient security mechanisms should also be incorporated along them. As we focus on the secure medical images, their importance is not to mention since the confidentiality of patient data is always requested during transmission from one to another

practitioners. Chaos-based cryptography can be applied to transmit medical images effectively [15]. It can simply resist most of the attacks. In this work, the cryptosystem is designed using a single 2D logistic map. The development and test of the cipher which is in charge of protecting patient medical data from hacking is also done in the present study.

To overcome the drawback of the previously listed algorithms, we present here the methodology to achieve a new efficient images cryptosystem. We intend to build a cryptosystem which can effectively ensure security in IoHT environment based on 4G and 5G network. Here, we introduce a 2D map with an infinite number of fixed points, which is particularly new. Besides, the sequences of the said map are used to design a robust encryption scheme for images. Based on literature survey, we can realize that more and more research has been done to develop modern encryption algorithms [16–19]. The algorithm is designed using four main components: Logistic map, SHA-256 model for security, Bit-XOR operation (diffusion), and new n^{th} iteration operation. Some well-known metrics are used to assess the security and speed of our algorithm. The major contributions of the work are listed below.

- the 2D Logistic map is introduced with an infinite number of fixed points exhibiting chaotic dynamics;
- a robust cryptosystem is designed using SHA-256 model to generate the sequences of our proposed algorithm to be used in an IoHT framework of the 5G network;
- the proposed cryptosystem uses new n^{th} iteration operation which help to randomly determine the number of rounds;
- the initial conditions and control parameters of the chaotic systems serve as the key of the cryptosystem, and are made dependent on the plain image through SHA-256 model;
- the proposed cryptosystem robustness is validated using well-known tests;
- the suggested algorithm's dependability, efficacy, and robustness are all proven when compared to previous algorithms;
- Simulation results and security analysis show that it can encrypt different kinds of digital images into unrecognized noise like images with a high level of security.

The rest of the paper is organized as follows. In Section 2, we present the context of our study. In Section 3, our approach is described in detail, from the chaotic system to the algorithm proposed. In Section 4, security analysis of the proposed cryptosystem and evaluation of its performance through various analyses such as statistical analysis, key sensitivity, keyspace analysis, correlation analysis, etc. and comparison of the results to previous works are presented. In Section 5, the comparison of our results with state of the art research is presented. In Section 6, the architecture and the whole flowchart of our secure cryptosystem integrated into the environment of an IoHT is presented. Finally, our conclusions are drawn in Section 7.

2 Related work

Arroyo and al. [20] set forth an extended study of the logistic map as pseudo-random number generator in a cipher. The properties of chaotic systems have been used in very different ways to build new cryptosystems. All of those proposals can be classified into two big families, which are analog chaos-based cryptosystems and digital chaos-based cryptosystems.

Many of them have been widely studied in the last decade. Some examples are Hénon map [21], 2-D sine map [22], CNN system [23], Chen and Lee system [24], jerk system [25], Chua's system [26], and hyperjerk systems [27]. The first type of chaotic cryptosystems is based on the chaotic synchronization technique [28], whereas digital chaotic cryptosystems are based on one or more chaotic maps in such a way that the secret key is either given by the control parameters and the initial conditions or determines those values. The scientific community has extensively discussed Logistic and Sine maps [29, 30]. In [31] new two-dimensional (2D) Tent-cascade-Logistic map (2D-TCLM) is proposed and analysis results demonstrate that it has complex chaotic behaviors.

Researchers always focus on developing effective and exclusive cryptosystem for transmitting medical images [32–34]. In [15] and [34], authors reported an effective cryptosystem aimed at securing the transmission of medical images in an Internet of Healthcare Things (IoHT) environment. Their contributions investigated the dynamics of a 2D trigonometric map designed using some well-known maps: Logistic-sine–cosine maps. In [35], authors suggested an image compression and encryption algorithm based on fractional-order memristive hyperchaotic system and back propagation neural network.

The logistic map is a chaotic map and, having in mind the previous comments, it can be considered for the design of new digital chaotic cryptosytems [20]. The transformation procedure depends on an external parameter called key such that it is only possible to recover the original information if that key is known. As it was required by Kerckhoff [36], the security of a cryptosystem should depend only on its key. It is also necessary that the ciphertext generated by the encryption procedure does not contain enough information to guess either the plaintext or the value of the key, which also forces ciphertexts associated to very similar values of the secret key to be very different from each other. This is the reason why chaotic maps have captured the attention of cryptographers and many chaotic cryptosystems, i.e., cryptosystems based on chaotics maps have been proposed. In [37], authors have used a deterministic system to generate the sequence, rather than a random process, used in the case of truth bit generator. This technique increases complexity of a map and offers many possibilities which can be tested in other systems in the future. It is of interest to develop adaptive chaotic maps with appropriate encryption algorithms, which can be applied to solve cryptographic problems. In the last decade, many researchers have presented several image encryption algorithms based on chaotic systems [38–42]. For instance, chaos-based ciphers are used to protect the transferred information from attacks [43]. In [44], authors have constructed a new encryption scheme using the logistic map.

Different terminologies of the advancement of Internet of Things based technologies in healthcare monitoring systems have listed in the literature: Internet of Healthcare Things (IoHT) [32], Internet of Medical Things (IoMT) [45]. The IoMT comprises different and heterogeneous smart devices, such as wearable, wireless sensors, and medical monitors, which can be applied to the human body, at home or in hospitals to provide better and more efficient remote monitoring. The IoMT presents an application of the Internet of Things (IoT) in the field of medical and healthcare. The IoMT is an architectural infrastructure consisting of user, edge, and cloud layers [46]. In [47], authors propose energy-aware task-offloading approaches which have contributed to reduce the device energy consumption and improve computation resources. In the same work, possibilities of power supply for medical sensors and energy-storage strategies are investigated by the authors. Many IoT network-enabled algorithms were suggested for healthcare applications to protect data and store them cryptographically [48]. In [49], to assure provide and reliable communication in 5G edge computing and Device-to-device (D2D) enabled IoMT systems, authors present an intelligent trust cloud management method. 5G edge computing enabled IoMT system

can be divided into two sub-networks, one is Wireless Body Area Network (WBAN), and the other is 5G cellular network [49]. Table 1 compares the state-of-the-art-related of Internet of Things based technologies in healthcare monitoring systems.

Based on this Table 1, it appears that current research in the IoMT/IoHT fields is quite varied. They are more oriented towards the security of the data transiting in the network infrastructure, computation resource or on the mechanisms for optimizing energy or quality of service.

3 Methodology

3.1 The 1D logistic map

The equation of 1D logistic map is [15]:

$$x_n = rx_n\left(1 - x_n\right) \tag{1}$$

Where $x_n \in [0, 1]$, is the discrete state of the output chaotic sequence, r is the control parameter with values in the range [0, 4]. The chaotic behavior of the Logistic map is observed in the range [3.5, 4].

The bifurcation diagrams and Lyapunov exponents of the seed maps are illustrated in Fig. 1. From the bifurcation graphics, we can observe a limited chaotic range of the different maps and a non-uniform distribution value in the range [0, 1]. Moreover, the values of Lyapunov exponents for each map are not all positive as desired.

3.2 The Henon map

Henon map is a 2D discrete time dynamical system which exhibits chaotic behavior, and is defined by the relation (2) [33]:

$$\begin{cases} x_{n+1}=1-ax_n^2+y_n \\ y_{n+1}=bx_n \end{cases} \tag{2}$$

Where, a and b are the bifurcation parameters, x_0 and y_0 the initial condition. In practice, we use $x_0=y_0=0$. In order to obtain a chaotic behavior of the system, we take $a=1.4$ and $b=0.3$. The bifurcation diagram is obtained by maintaining $b=0.3$ and by varying a from 0 to 1.4. The attractor and bifurcation diagram of Henon map are illustrated on Fig. 2. It is found that the first bifurcation occurs around $a=0.362$, followed by a double bifurcation at $a=0.91$. From $a=0.91$ to $a=1.08$, successive doubling bifurcation occurs periodically [33]. For a higher than 1.1, the periodicity changes to chaotic behavior.

3.3 The 2D logistic map

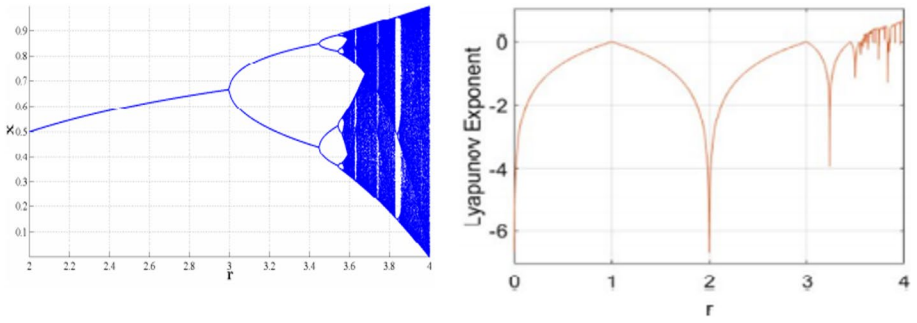
The equation of 2D logistic map is [34]:

$$\begin{cases} x_{n+1}=r(3y_n+1)x_n(1-x_n) \\ y_{n+1}=r(3x_n+1)y_n(1-y_n) \end{cases} \tag{3}$$

where r is the system parameter and (x_n, y_n) is the pair-wise point at the n^{th} iteration.

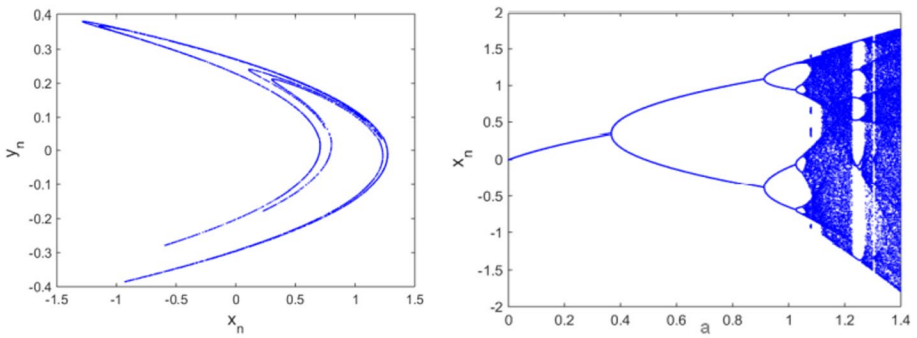
Table 1 Comparison between state-of-the-art surveys on the Internet of Things based technologies in healthcare monitoring systems

Reference	Method	Technology	Application
[32]	A new two-step image encryption algorithm	-	IoHT
[45]	An energy efficient fuzzy data offloading based categorization of medical data	Integration of IoMT and cloud architectures	IoMT
[46]	a data offloading-based heuristic technique	Edge-Based IoT Network	IIoT
[47]	a lightweight secure efficient offloading scheduling (LSEOS) metaheuristic model	Edge-Cloud-Based Networks	IoMT
[48]	Cost-Efficient Service Selection and QoS efficient scheduling of healthcare	healthcare fog servers	IoMT
[49]	an intelligent trust cloud management method	5G edge computing	IoMT
our	Images encryptions algorithm using SHA-256 generator sequence	5G network	IoHT



(a) (b)

Fig. 1 **a** the Bifurcation diagrams and **b** Lyapunov exponent graphics of 1D Logistic map



(a) (b)

Fig. 2 Henon map, **a** attractor for a = 1.4, b = 0.3, **b** bifurcation diagram for b = 0.3

Figure 3 shows the scatter plot of 30, 000 points from the trajectory [50] of the 2D logistic map using the parameter r = 1.19 and the initial value (x_0, y_0) at (0.8909, 0.3342). Therefore, the i^{th} point on the trajectory can be determined by knowing (x_0, y_0, r, i) as Eq. (4) shows.

$$\begin{cases} x_i = L_x^{2D}(x_0, y_0, r, i) \\ y_i = L_y^{2D}(x_0, y_0, r, i) \end{cases} \tag{4}$$

Figure 4 shows the phase portrait [50] of the 2D Logistic map when r = 1.19.

3.4 Complexity

From the Lyapunov Exponent (LE) graphics, we can observe that the values of Lyapunov Exponents for each map are not all positive as desired. This chaotic property of 1D logistic map prove that, this type of system is not suitable to build a secure cryptosystem. The 2D logistic map defined in Eq. (3) has a higher complexity compared to Henon map defined in (2) [51].

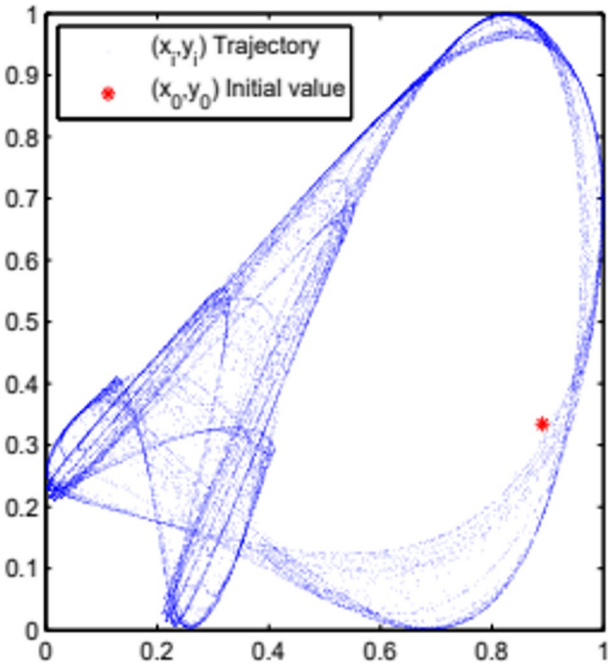


Fig. 3 A trajectory of 2D Logistic map

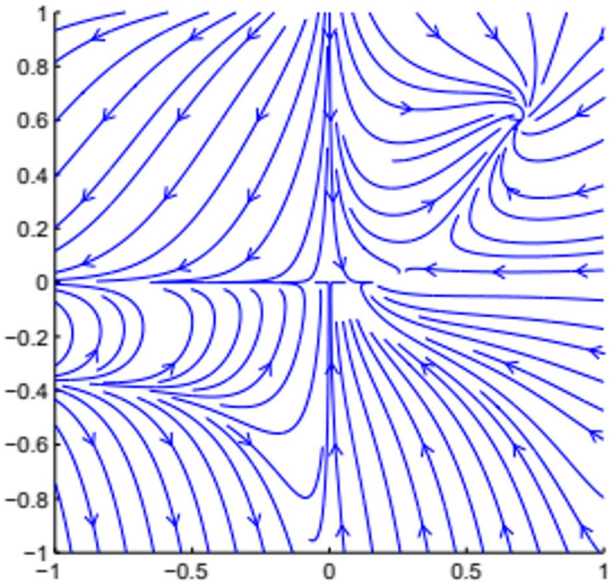


Fig. 4 A phase portrait of 2D Logistic map

Quantitatively, the complexities of 1D and 2D logistic map and Henon map can be measured by several means. The comparison between these chaotic systems using Information Entropy (IE) [50, 52] and LE [53, 54] are shown in Table 2.

Table 2 Chaotic map complexity analysis

Parameters	1D Logistic (r)		Henon (a, b)		2D Logistic (r)			
Measurements/Comments	3.57	4.00	(1.40, 0.3)		1.11		1.19	
	Start of Chaos	End of Chaos	Chaos		Start of Chaos		End of Chaos	
Information Entropy (#Bins 256)	H(x)	H(x)	H(x)	H(y)	H(x)	H(y)	H(x)	H(y)
	4.8115	7.6895	7.8155	7.8155	6.2605	6.5547	7.8944	7.8938
Lyapunov Exponent	λ1	λ1	λ1	λ2	λ1	λ2	λ1	λ2
	0.0012	0.0693	0.4241	-1.6281	0.3646	-0.1166	0.5654	-0.2108
Lyapunov Dimension	-	-	1.2605		4.1287		3.6824	

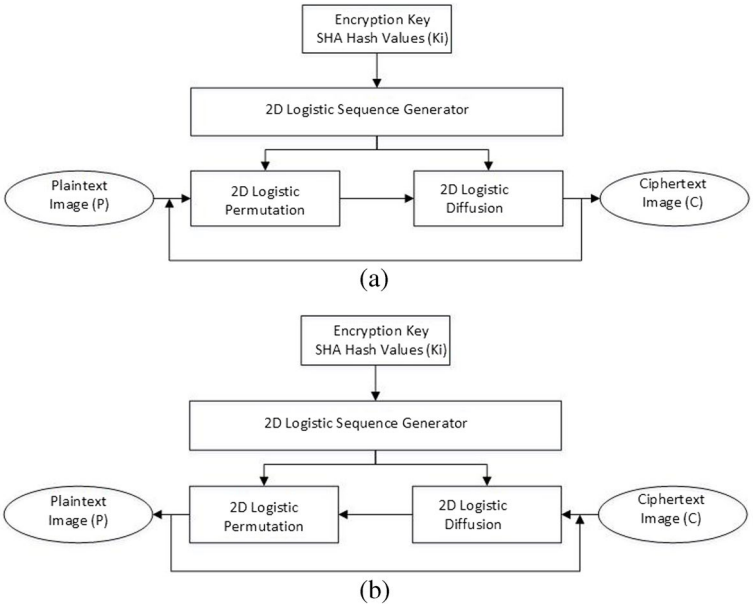


Fig. 5 Flowchart of (**a**) image encryption using the 2D logistic map and (**b**) of image decryption using the 2D Logistic map

On Table 2, we can see that 2D logistic map has higher IE score than 1D logistic map. This observation implies that its trajectory is more random-like. The same table shows that the 2D logistic map has a larger LE than 1D Logistic map, which implies that the 2D Logistic map is more dynamic. The 2D logistic map even has a greater Lyapunov Dimensions (LD) than the Henon map.

3.5 Image encryption using the 2D logistic map

It was shown that, in 2D Logistic map, on the parameter interval $r \in [1.1, 1.19]$, the system is chaotic [50].

Figure 5 shows the flowchart of the proposed image encryption method using the 2D Logistic map.

3.6 Key structure of 2D logistic sequence generator

The SHA 256 has been used to generate the 2D Logistic sequence. In fact, The SHA-256 is a function, which produces for an image a unique 256-hash value [15, 55].

In the proposed algorithm, secret keys, i.e., initial conditions and control parameters of chaotic systems used were obtained from the SHA-256 algorithm to prevent the encryption algorithm from succumbing, to brute force attack. In the process, we first computed the SHA-256 hash value K of the plaintext image and then, divide it into 8-bit blocks, ($i = 1, 2, \ldots, 32$) as indicated in Eq. (5):

$$\left(x_0, y_0, r, T\right) \tag{5}$$

Thus, we define our encryption key K as a 256-bits string compose of four parameters (x_0, y_0, r, T). Those parameters used to encrypt the plaintext image were obtained as follows:

$$x_0' = \frac{3}{4}x_0 + \frac{bin2dec\left(k_1 \oplus k_2 \oplus \cdots \oplus k_8\right)}{2^8 \times 10} \tag{6}$$

$$y_0' = \frac{3}{4}y_0 + \frac{bin2dec\left(k_9 \oplus k_{10} \oplus \cdots \oplus k_{16}\right)}{2^8 \times 10} \tag{7}$$

$$r' = \frac{4}{5}r + \frac{bin2dec\left(k_{17} \oplus k_{18} \oplus \cdots \oplus k_{24}\right)}{2^8 \times 10} \tag{8}$$

$$T' = \frac{4}{5}T + \frac{bin2dec\left(k_{25} \oplus k_{26} \oplus \cdots \oplus k_{32}\right)}{2^8 \times 10} \tag{9}$$

Where bin2dec(.) is the function to convert a binary string to its decimal value, $\oplus$ indicates the bit-wise XOR operation, (x_0, y_0) = (0.8909, 0.3342), r ∈ [1.1, 1.19] and T is the n^{th} point on the trajectory can be determined by knowing (x_0, y_0, r, n) as Eq. (10) shows. This Eq. (10) is the readjustment of Eq. (4), where n is the fixe value determine during the experiment test.

$$\begin{cases} x_n = L_x^{2D}\left(x_0, y_0, r, n\right) \\ y_n = L_y^{2D}\left(x_0, y_0, r, n\right) \end{cases} \tag{10}$$

For each round, the key's parameters $\left(x_0', y_0', r', T'\right)$ are computed respectively by relations (5) to (8). In such of way, we built encryption key to control the pseudo random sequence in 2D logistic map.

3.7 Encryption algorithm

The flowchart of the proposed image encryption method using the 2D logistic map is illustrated in Fig. 5. The internal loop is made of 2D logistic permutation and 2D logistic diffusion. The decryption procedure is just the reverse of the encryption procedure. To make it short, we note the encryption process by C = Enc(P,K) and the decryption process by P = Dec(C,K).

Permutation stage The chaotic sequence was obtained after iterating Eq. (3) N x M times, with [N, M] the size of image P. Then, the algorithm of the permutation process is given following the steps below.

STEP 1: Compute the values of a vector $\left(x_0', y_0', r', T'\right)$ according to Eqs. (6) to (9), where the vector $\left(x_0, y_0, r, T\right)$ is the initial condition obtained based on the 2D Logistic map;

STEP 2: to avoid transient effects, iterate 2D Logistic map for row and column 1000 times, then iterate N times for row and M times for column;
STEP 3: sort the previous values in ascending order;
STEP 4: for each point (x_i, y_j) of a pixel's position, find the previous position of the corresponding point (Xi, Yj) of the pseudo-random number generator sorted value and substitute the following Eq. (11);

$$(x_i, y_j) \leftarrow (X_{i-1}, Y_{j-1}) \tag{11}$$

STEP 5: permute the position of the last pixel of the image with the real one.

Diffusion stage In order to achieve good diffusion properties [52, 55] we apply 2D logistic map diffusion to strengthen the statistical relationship between plaintext image P and cipher image C. The diffusion process steps are detailed as follows:

STEP 1: fix the initial values parameters, x_0, y_0, r using Eq. (3) and T following Eq. (10);
STEP 2: convert the cipher (permuted) image into a column vector;
STEP 3: iterate Eq. (4) N×M times and load the values in a mirror array A of same size with the cipher image;
STEP 4: reshape the values of A as a column vector;
STEP 5: apply the bit-wise XOR operation between the cipher image and the vector A containing the pseudo-random values generated by Logistic map. Then, convert the resultant image into an 8-bit non-signed format to get the encrypted image.

As we said at the beginning of the encryption algorithm, the decryption process is just the reverse of the encryption.

4 Experimental results and security analysis

Our simulation was done in MATLAB R2017a, under the Windows 10 environment with Intel processor ® core TM i5-2450 M CPU @ 2.50 GHz and 4 Go of RAM.

The selected images from the USC-SIPI image database[1] and some medical images are used for testing the performance of the proposed cipher.

4.1 Keyspace analysis

The encryption key of the proposed image encryption algorithm is made of four parts, i.e. x_0, y_0, r and T. Based on the SHA standard, a fraction part for double precision float number is of 64-bit length. As a result, an encryption key used in the proposed method is of $8\times8+8\times8+8\times8+8\times8=256$-bit length. Assume that the computer accuracy is 10^{-15}, and the key space is $10^{15\times8}=10^{120}$. In the literature, a key space of at least 10^{30} is required for the system to be robust [56]. Therefore, the cipher keyspace is comparable to or better

[1] USC-SIPI image database can be publicly accessed via the link http://sipi.usc.edu/database/.

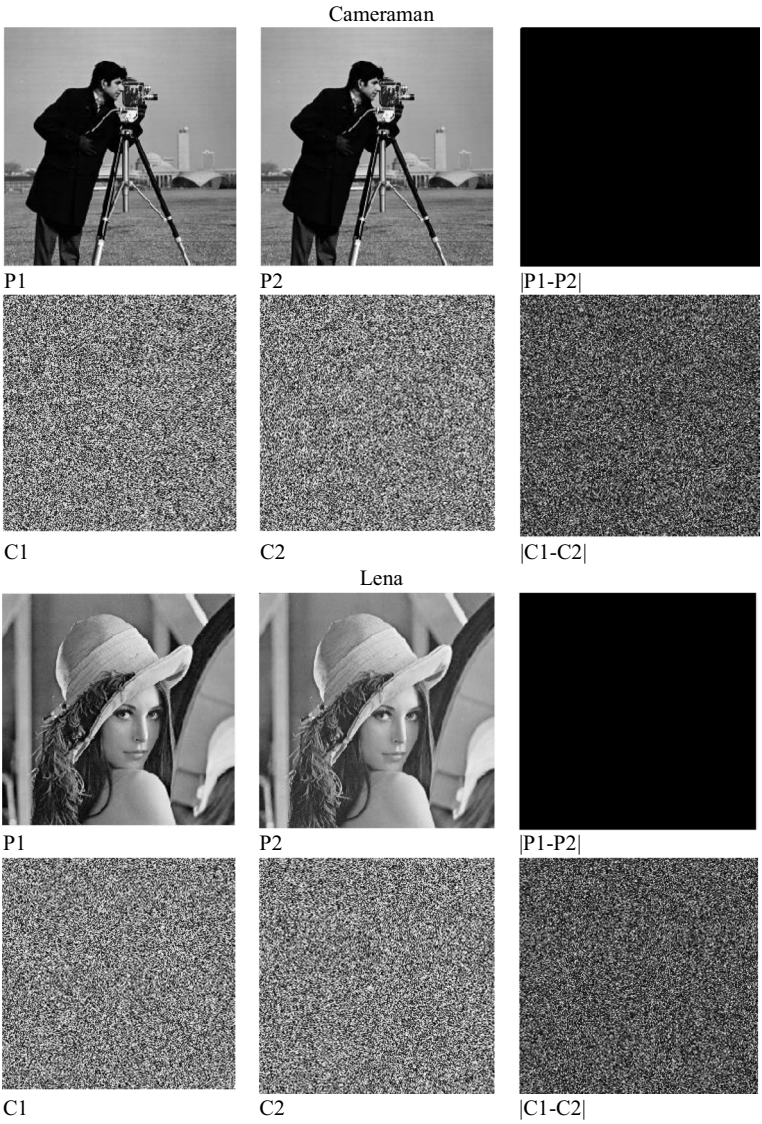


Fig. 6 Sensitivity Tests of Keys of some standard images

than existing prevailing encryption algorithms and standards [15, 50], and thus it has a strong resistance to brute-force attacks [57].

4.2 Keys sensitivity analysis

Two keys are used with infinite change of value in the encryption process to resist any brute force attack ineffective. So, we modify the value of r = 1.1 (Key1 (K1)) to 1.1 + 10–14 (Key2 (K2)) and the results show that the encryption system is very sensitive to the small

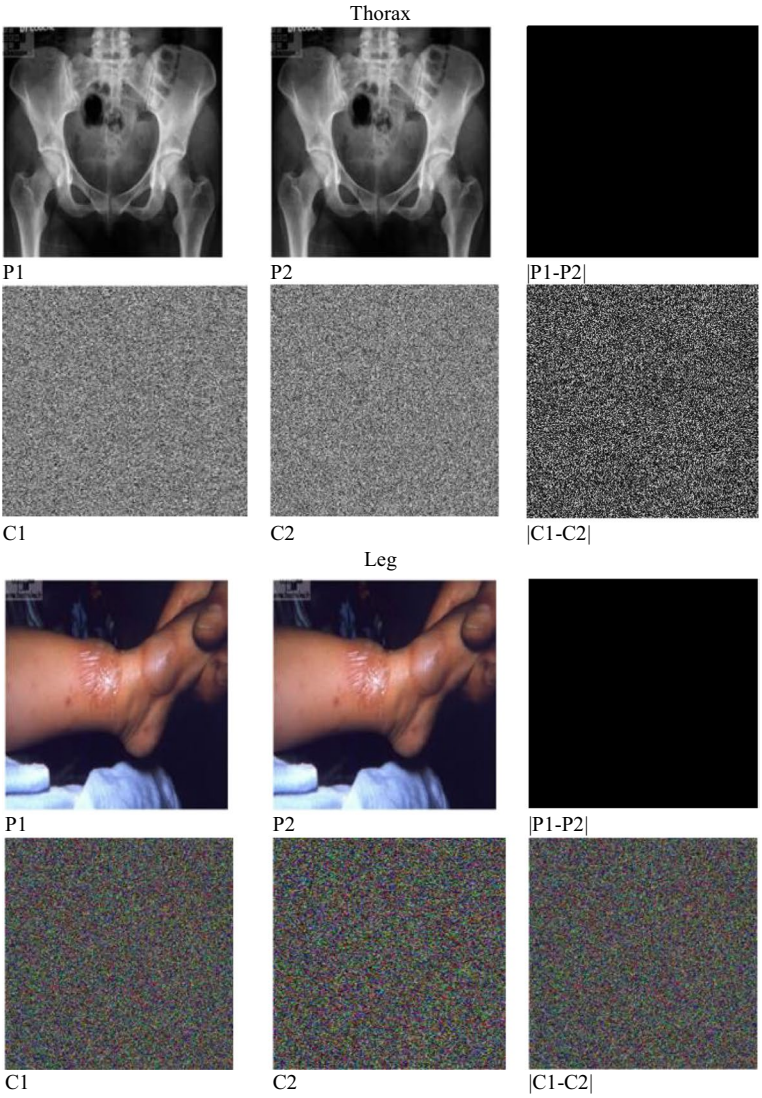


Fig. 7 Sensitivity Tests of Keys of some medical images

changes on the decrypted keys. Figure 6 illustrates the decrypted two tested images for the Cameraman (256×256) and Lena (256×256) by using the correct encryption key (K1) and wrong decryption key (K2).

Since this cryptosystem is dedicated to medical image encryption, the second set is made of 2 other medical images which are Leg (900×900) and Thorax (880×660) (Fig. 7).

The difference of two plaintext images shows that the two images are the same. The difference of two plaintext images shown on Fig. 7 (P1-P2) is entirely black which means that the difference is zero. When a small modification is brought on the original key, the two encrypted images are different. The difference of two encrypted images

shown on Fig. 7 (C1-C2) becomes miserable and different from the plain image. The same observation has been seen by varying the other parameters $\times 0$ and/or y0. The average difference percentage was 99.73%. Base on that, we can conclude that the proposed cryptosystem cannot be broken by hackers and also is very sensitive to any little changes in the security keys.

4.3 Histogram analysis

Figure 8 provides the histogram of the encrypted (H(C)) image and the original (H(P)) of Cameraman and Lena image. Figure 9 provides the histogram of the encrypted (H(C)) image and the original (H(P)) of Leg and Thorax image. It is clear that the two histograms (H(P) and H(C)) are entirely different of each kind of images. Figure 8 shows uniformity distribution of gray scale/color of the histogram of all encrypted images (C). As we can see in Figs.8 and 9, histograms of plain images exhibit clear modes while those of the ciphered images are fat as expected, portraying a uniform grey-level distribution. So, the uniform distribution in the ciphered images histograms illustrates the good quality of our method.

Furthermore, in Figs. 8 and 9, the histogram of the decrypted images is the same as that of the clear images. Therefore, the proposed method succeeds in decrypting the plaintext images without losing any information, when the correct security keys are used.

4.4 Correlation analysis

The encryption quality of the proposal algorithm has been calculated by using the correlation coefficient metric. The following computations were carried out to achieve the correlation values [5]:

$$\begin{aligned} Cor_{xy} &= \frac{E((x - E(x))(y - E(y)))}{\sqrt{D(x)}\sqrt{D(y)}} \\ with \quad E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i \\ and \quad D(x) &= \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)^2 \end{aligned} \tag{12}$$

where x and y symbolized the values of the pixels at the same index of the images I and I', $E(x)$ is the estimation of the mathematical expectation of x, $D(x)$ is the estimation of the variance of x. Figures 10 and 11 group together the correlation coefficients obtained from the plaintext and encoded images. Besides, the distribution of neighbouring pixels is represented in Tables 3 and 4. According to Tables 2 and 3, we can see that the correlation coefficient of the plaintext image is closely to 1 implying that high correlation exists among pixels. For the ciphered image, the correlation coefficient is closely to 0, which implying that no detection correlation exists among pixels. It is evident from Tables 3 and 4 that we achieve minimal correlation values in three directions, including vertical, horizontal, or diagonal. Consequently, the encryption scheme is unbreakable by the attackers regarding the Correlation coefficient.

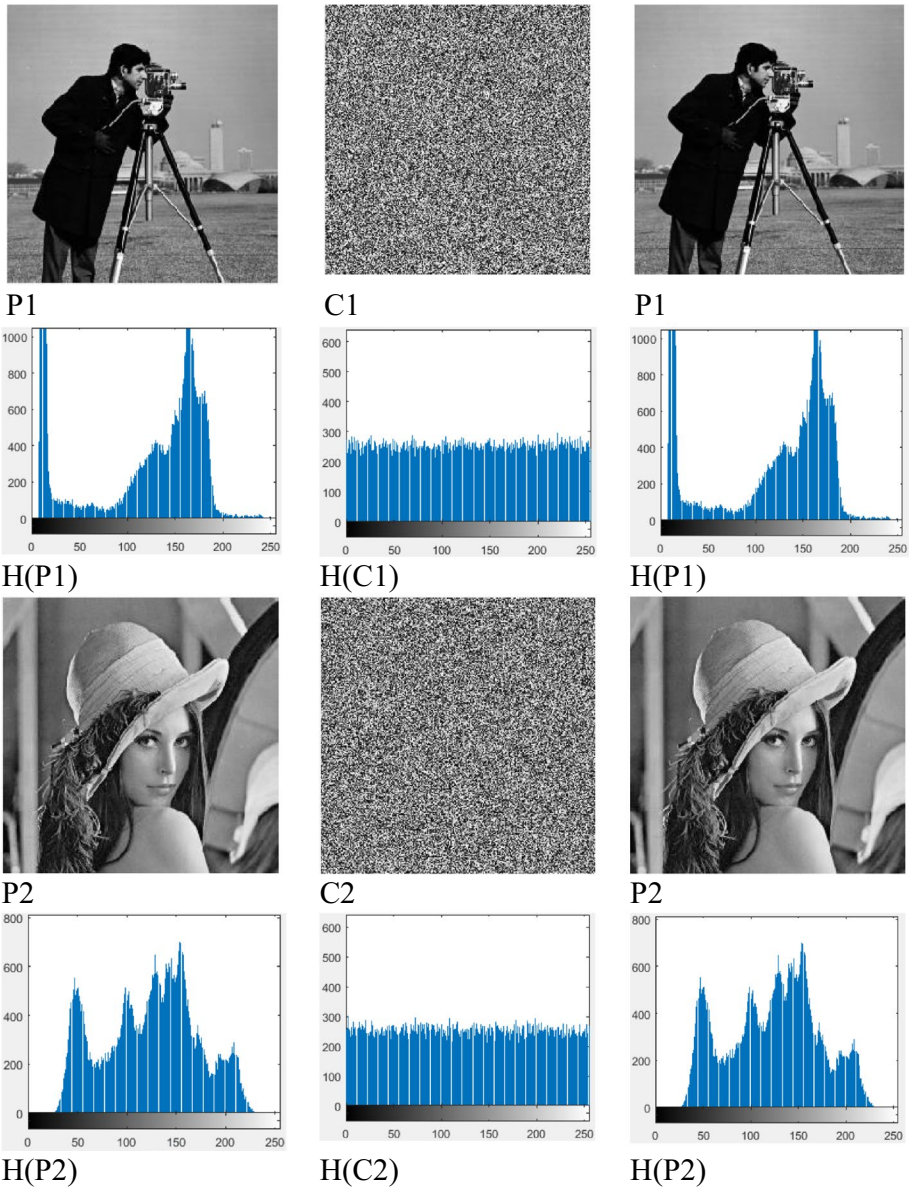


Fig. 8 Histogram analysis of encrypted standard images

4.5 Shannon entropy analysis

Shannon entropy measures the amount of information hidden in an image. It is an evaluation of the randomness for a given image. The well-known formula for calculating information entropy is defined as follows [12, 58, 59]:

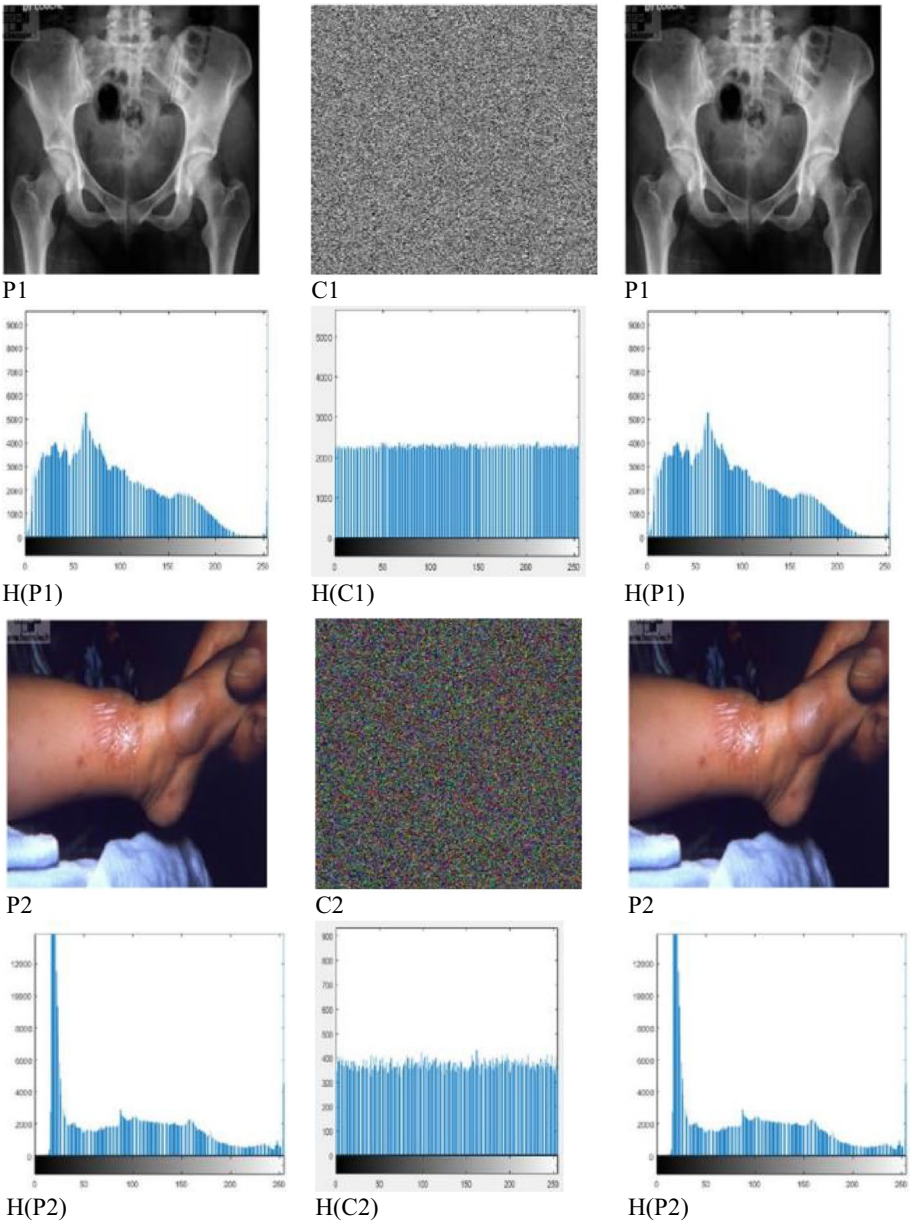


Fig. 9 Histogram analysis of encrypted medical images

$$E(z_i) = -\sum_{i=0}^{255} p(z_i) \log_2 \left(p(z_i)\right) \tag{13}$$

The pixels of an image are randomly distributed if the entropy value is close to 8. Table 5 provides the global and local entropies calculated for the used data set. For the

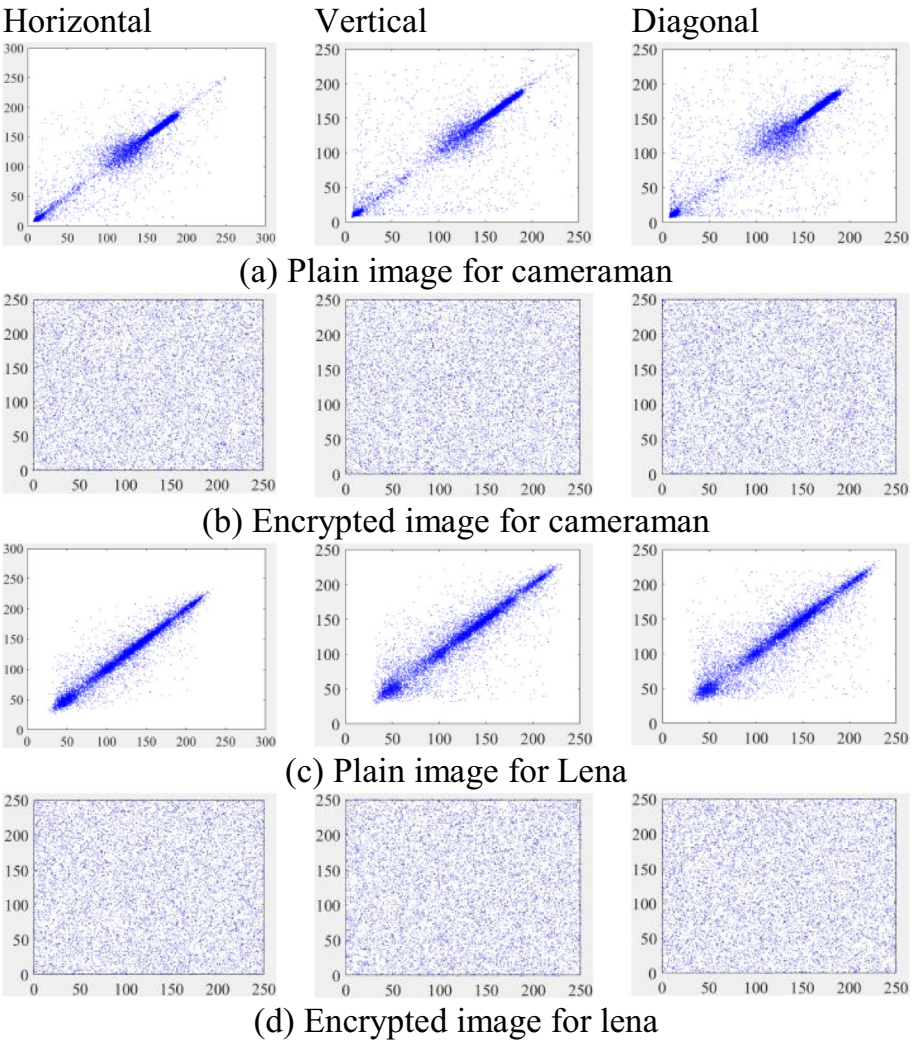


Fig. 10 Correlation coefficients plot for plain respectively encrypted image for (**a**) respectively (**b**) Cameraman and for (**c**) respectively (**d**) Lena (256×0.256)

Cameraman, Lena, Thorax and Leg image, the corresponding entropy are 7.9996, 7.9995, 7.9828 and 7.9886 and $E(z_i)$ is equal to 8, which is the ideal case. This indicates that the cipher images are close to random source and our cryptosystem is secure against entropy attack.

5 Comparison with other cryptosystems

Table 6 shows the performance of the proposed algorithm compared to the mostly cited and good standing ones in the literature. Comparative tests were carried out, and the Lena image of size 512×512 was used as an example. From Table 6, we can observe

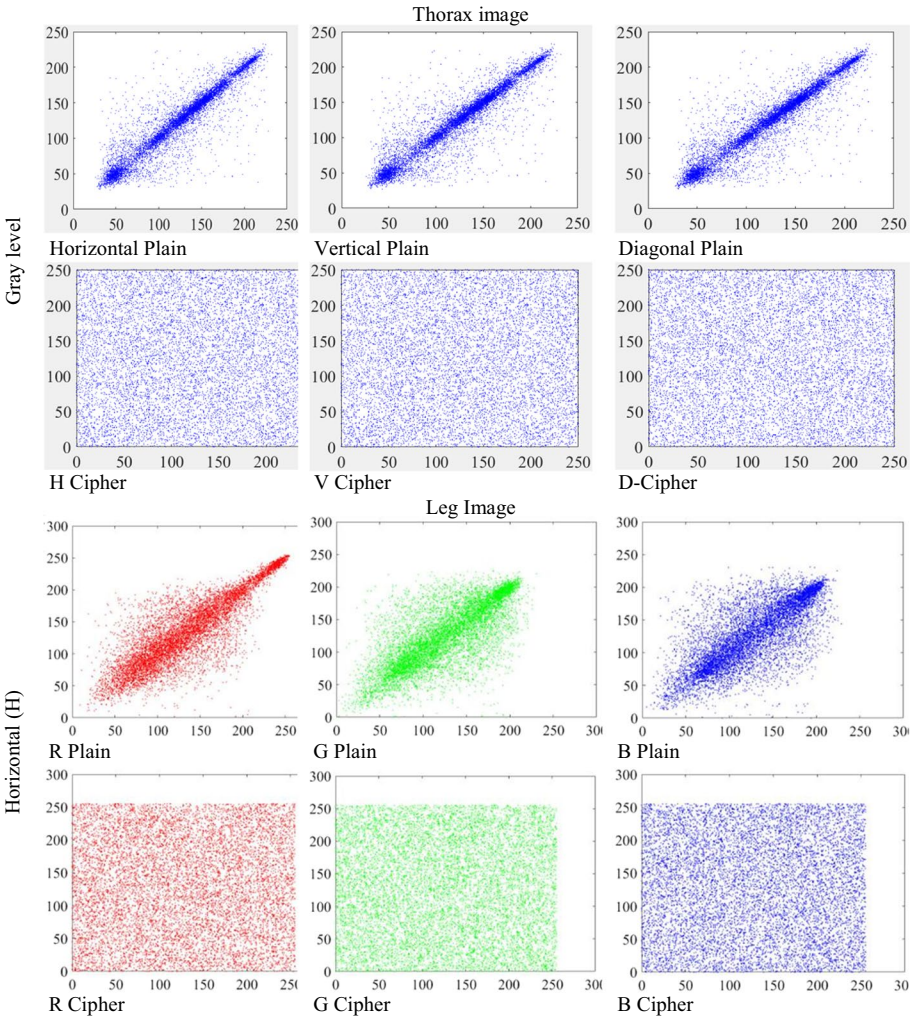


Fig. 11 Correlation coefficients plot for plain respectively encrypted image for Thorax and for Leg set data ((R, G, and B channels)

that the proposed encryption algorithm has the best value of entropy, a large keyspace that gets close to the best performances presented in [59–63], and an average correlation compared to others.

Of those providing such figures using Lena, comparisons are carried out in Fig. 12. The comparison is limited to recent works (3 years or less) and based on the most commonly used image which is Lena. We notice from Table 6 that apart from being the fastest, our scheme exhibits the very large of keyspace, a very good average correlation plus a very good entropy as compared with other works.

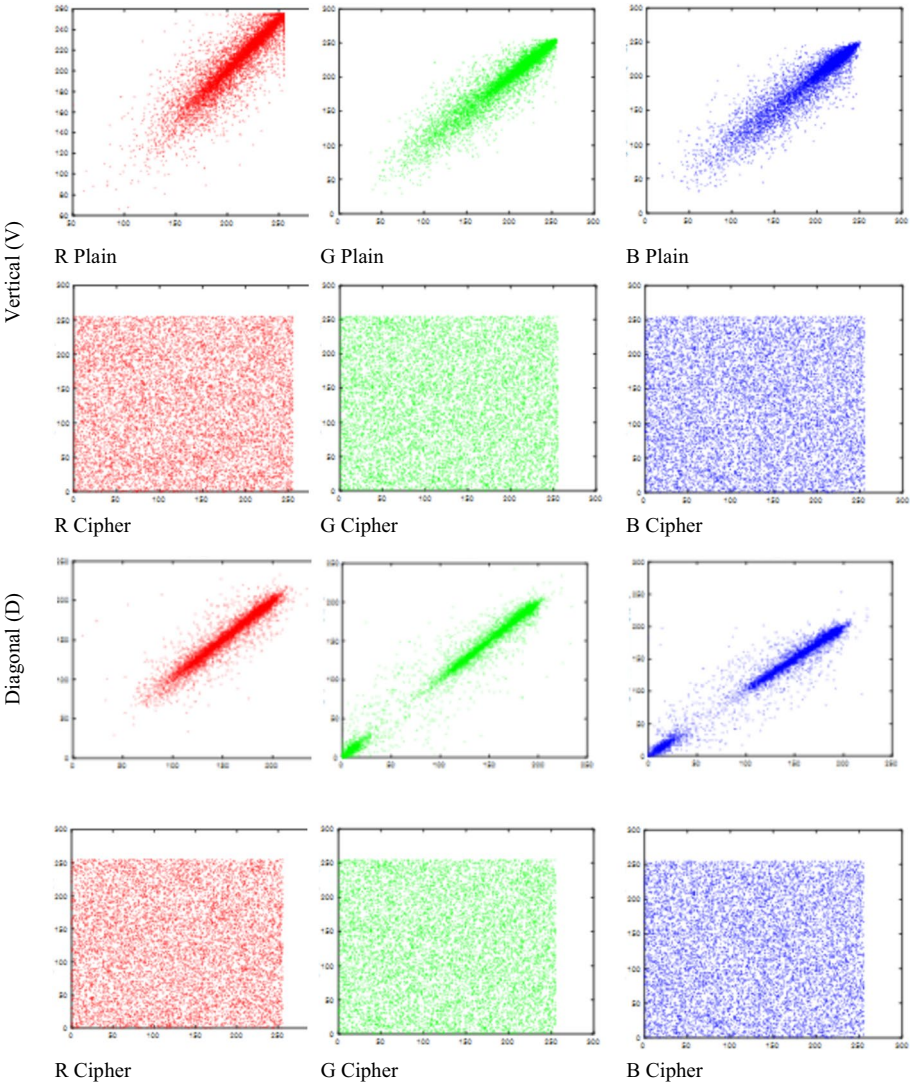


Fig. 11 (continued)

Table 3 Correlation Coefficients of Adjacent Pixels in standard images

	Cameraman				Lena			
	Ours	[15] | [32]	Ours	[15] | [32]		[15] | [32]	Ours	[15] | [32]
	Plaintext image		Cipher image		Plaintext image		Cipher image	
Horizontal	0.9582	0.9900 | -	-0.0021	0.0080 | -	0.9618	- | -	-0.0089	- | -0.0002
Vertical	0.9290	0.9831 | -	0.0006	0.0012 | -	0.9258	- | -	0.0050	- | 0.0015
Diagonal	0.9121	0.9733 | -	0.0159	-0.0020 | -	0.9038	- | -	-0.0010	- | 0.0040

Table 4 Correlation Coefficients of Adjacent Pixels in medical images

	Thorax				Leg			
	Ours	[15]		[15]	Ours	[15]	Ours	[15]
	Plaintext image		Cipher image		Plaintext image		Cipher image	
Horizontal	0.9852	0.9220	0.0053	0.0022	0.9732	0.9986	0.0011	0.0010
Vertical	0.9790	0.9761	0.0102	-0.0014	0.9638	0.9926	0.0058	-0.0020
Diagonal	0.9555	0.9162	0.0012	0.0009	0.9812	0.9912	-0.0152	0.0018

Table 5 Information entropy of different ciphered images

Images	Size	Entropy of image (Ours algorithm)	[13]	[53, 58]
Cameraman	256×256	7.9996	7.9994	-
Lena	256×256	7.9995	7.9993	7.9994
Thorax	880×660	7.9828	7.9994	-
Leg	900×900	7.9886	7.9993	-

Table 6 Comparison of some recent works with the proposed one

	Keyspace	Key sensitivity	Average correlation	Entropy
Proposed algorithm	10^{120}	99.73	0.0053	7.9994
[6]-2021	10^{128}	-	1.583E-03	7.9962
[15]-2021	10^{131}	-	0.004	7.9972
[55]-2021	10^{165}	99.62	0.004	7.9993
[59]-2020	10^{238}	-	0.003	7.9980
[60]-2020	10^{206}	-	0.004	7.9976
[61]-2020	10^{120}	-	0.051	7.9991
[62]-2020	10^{142}	-	0.023	7.9992
[63]-2020	10^{105}	99.04	0.003	7.9975

6 Proposal communication architecture

The healthcare industry is transforming with the growth of the Internet of Things (IoT) and resulting in the development of the IoHT. IoHT for the healthcare industry requires big data, high speed, large bandwidth, and reliable connectivity, which will be fulfilled with 5G technology. Based on the fact that all the environment of 5G network is digital with users equipment in the context IoHT, this research is focused on digital chaotic cryptosystems. Then, information's transmitted on the network can be secured based on encryption methods. Usually, hospitals and other health organizations pay special attention to store and transmit medical images. As IoHT technologies are emerging nowadays, efficient security mechanisms should also be incorporated along with. Thus, the secure healthcare system is designed as per the following architecture (Figs. 13 and 14). The periodical or real-time collection of medical images is stored to health management system. The medical images generated in the health management system are encrypted by our proposal cryptosystem and are transferred using 5G system.

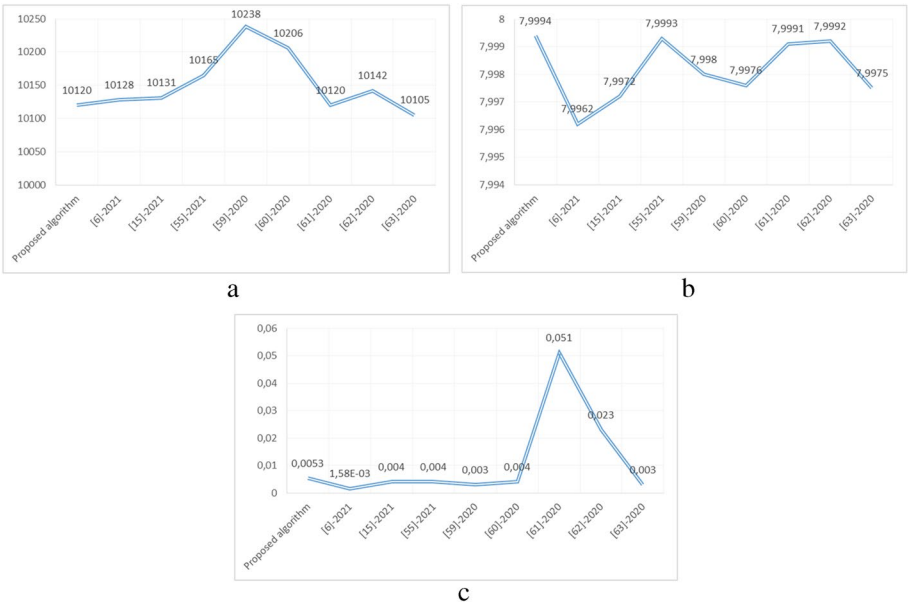


Fig. 12 Plot of some metrics of the proposed scheme compared with recent others: **a** keyspace, **b** entropy and **c** average correlation

Security algorithms implemented inside these health management system include SHA-256 based on 2D Logistic Map in the heterogeneous fog cloud nodes for healthcare applications. These tasks are locally encrypted and decrypted with the proposed secure algorithm. Then, encrypted data are offloaded to edge tasks for execution. After executing tasks, the data are offloaded to cloud computing to complete cloud tasks in the system.

IoHT technology facilitates the medical device to process (collection, analysis and transmission) the healthcare data across the 5G Network. The overall operational functioning of the present architecture is illustrated on Fig. 13.

The basis of IoHT is machine-to-machine (M-M) communication, which is possible by 5G network enabled medical devices. To store and analyze the captured healthcare data, the IoHT devices link to cloud platforms like Amazon Web Services embedded in the environment of 5G Network. Based on the fact that, many of the mobile devices offer Near Field Communication (NFC) radio frequency identification (RFID) tags, which allows collecting and the sharing of the healthcare data over IT systems. The telemedicine is the most common word used in connection with the remote monitoring of patient at home by the use of IoHT. This technology helps the patient from unwanted travelling to the hospital and physician's door for their regular change in condition and the medical questions. It also helps the doctor to get the data of their patients anywhere. However, these ad hoc IoT solutions are unable to interoperate with each other as they are developed using different sensors, data models, communication

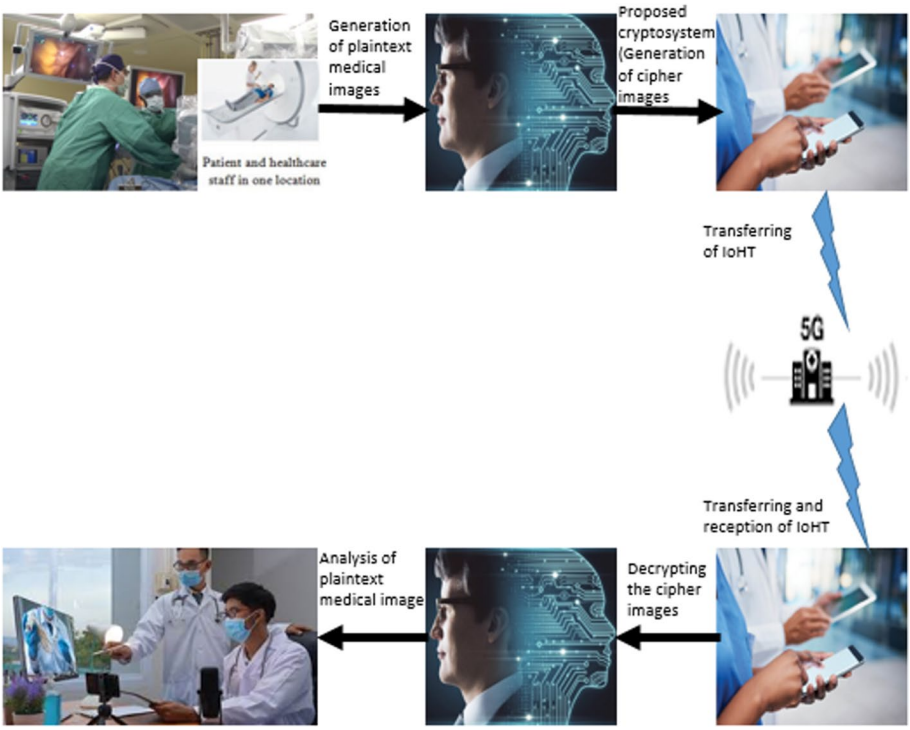


Fig. 13 General Architecture for the proposal secure IoHT

protocols, and applications without any interoperable way to interconnect these heterogeneous systems and exchange data.

7 Conclusion

In this paper, we proposed a cryptosystem to encrypt images and based on a 2D Logistic map combined with a SHA-256 generator sequence. In the proposed algorithm, secret keys based on the initial conditions and control parameters of chaotic systems used were obtained from the SHA-256 algorithm to protect the encryption algorithm from succumbing to brute force attack. The internal loop of the proposed image encryption method is composed of 2D logistic permutation and 2D logistic diffusion. However, we have shown by experimental results that our algorithm is sensitive to initial conditions and strong against the brute force attacks. Moreover, these results can ensure the safe exchange of medical images on the 5G network of different hospital services. The next work will be devoted to the other parts of system (modulation and demodulation techniques being developed for the secure transmission). In order to perform the 5G environment by the best integration of IoHT of the telecommunication devices, the next step of this project will consist of looking how to integrate our algorithm into a FPGA module.

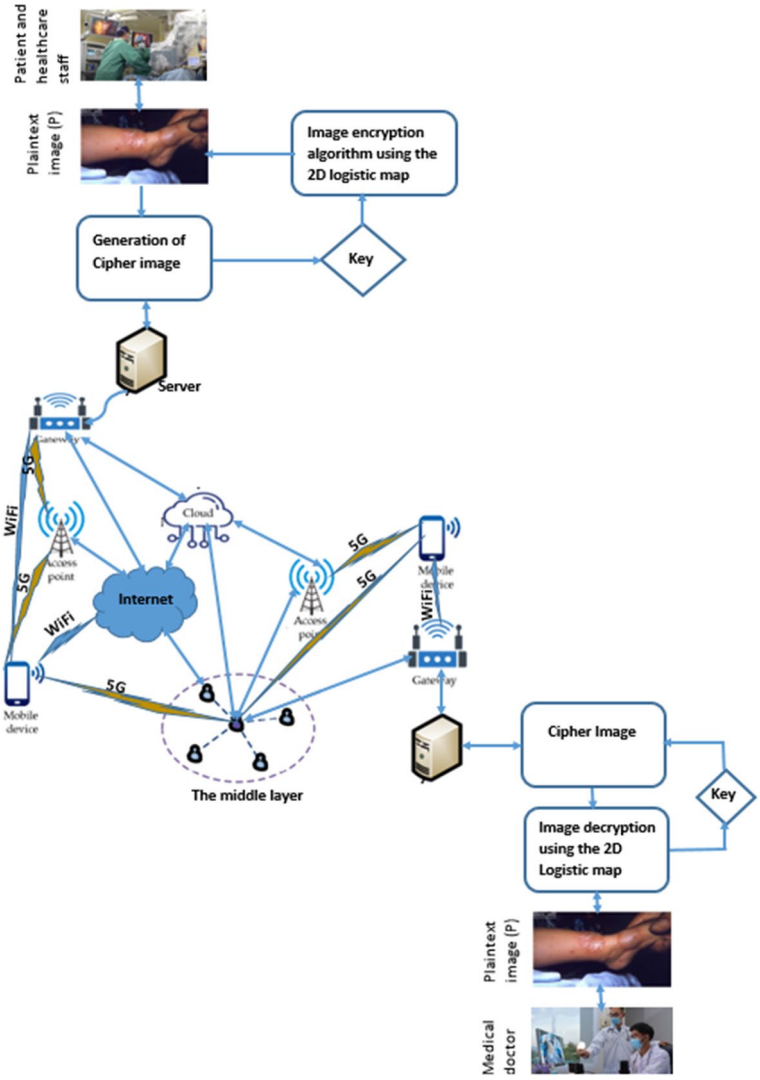


Fig. 14 Detailed IoHT of the whole system

Acknowledgements This work has benefit the support of the manager of "Club des Lecteurs" by offering books and papers need to build up this project.

Data availability The images used to test our cryptosystem are from the internet. Here are the links to get samples of them: colour lena (https://github.com/mikolalysenko/lena), Chest X-ray (https://www.kaggle.com/datasets/nih-chest-xrays/data), brain (https://www.kaggle.com/datasets/navoneel/brain-mri-images-for-brain-tumor-detection?resource=download), cameraman (https://github.com/antimatter15/cameraman), lena (https://www.cosy.sbg.ac.at/~pmeerw/Watermarking/lena.html), pelvis (https://my.clevelandclinic.org/health/diagnostics/23519-pelvis-x-ray).

Declarations

Conflicts of Interest The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

1. Al-Najjar HM, AL-Najjar AM (2011) Image encryption algorithm based on logistic map and pixel mapping table. In Proceeding Computer Science, ImageEA 56–60
2. Kocarev L, Amato P, Ruggiero D, Pedaci I (2004) Discrete Lyapunov exponent for Rijndael block cipher, in Proc. 2004 International Symposium on Nonlinear Theory and its Applications (NOLTA 2004), pp. 609–612
3. Ruggiero D, Pedaci I, Amato P, Kocarev L (2004) Analysis of the chaotic dynamic of Rijndael block cipher, in Proc. RISP Int. Workshop on Nonlinear Circuit and Signal Processing (NCSP'04), pp.77–80
4. Alvarez G, Li S (2006) Some basic cryptographic requirements for chaos-based cryptosystems. Int J Bifurcation Chaos 16(8):2129–2151
5. Ganesh Sekar J, Arun DC (2020) Comparative performance analysis of chaos based image encryption techniques. J Crit Rev 7(9):1138–1143 (**ISSN-2394-5125**)
6. Kengnou Telem AN, Fotsin HB, Kengne J (2021) Image encryption algorithm based on dynamic DNA coding operations and 3D chaotic systems. Multimed Tools Appl. https://doi.org/10.1007/s11042-021-10549-0
7. Gao T, Chen Z (2008) A new image encryption algorithm based on hyper-chaos. Phys Lett A 372:394–400
8. Vaidyanathan S, Akgul A, Kaçar S, Çavuşoğlu U (2018) A new 4-D chaotic hyperjerk system, its synchronization, circuit design and applications in RNG, image encryption and chaos-based steganography. Eur Phys J Plus 133:46
9. Jiany D, Bai S, Dong W (2008) An image encryption algorithm based on Knight's tour and slip encryption filter. In: 2008 International Conference on Computer Science and Software Engineering, Wuhan, pp 251–255. https://doi.org/10.1109/CSSE.2008.1142
10. Jolfaei A, Mirghadri A (2010) An image encryption approach using chaos and stream cipher. J Theor Appl Inf Technol 19(2):117–125
11. Belkhouche F, Qidwai U. (2003) Binary image encoding using 1D chaotic maps. IEEE Proceeding, New Orleans
12. Ying W, DeLing Z, Lei J et al (2004) The spatial-domain encryption of digital images based on high-dimension chaotic system. Proceeding of 2004 IEEE Conference on Cybernetics and Intelligent Systems, Singapore, pp. 1172–1176
13. Xiao H-P, Zhang G-J (2006) An image encryption scheme based on chaotic systems. IEEE Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian
14. Gu G, Han G (2006) An Enhanced Chaos Based Image Encryption Algorithm. IEEE Proceedings of the First International Conference on Innovative Computing, Information and Control (ICICIC'06)
15. Yepdia LMH, Tiedeu A (2021) Secure Transmission of Medical Image for Telemedicine. Springer, Sensing and Imaging. 1–23. https://doi.org/10.1007/s11220-021-00340-8
16 Nkandeu YPK, Mboupda Pone JR, Tiedeu A (2020) Image Encryption Algorithm Based on Synchronized Parallel Diffusion and New Combinations of 1D Discrete Maps. Sens Imaging 21:55. https://doi.org/10.1007/s11220-020-00318-y. (Springer)
17. Nematzadeh H, Enayatifar R, Motameni H, Guimar FG, Coelho VN (2018) Medical image encryption using a hybrid model of modified genetic algorithm and coupled map lattices. Opt Lasers Eng 110:24–32
18. Jizhao L, Yide M, Shouliang L, Jing L, Xinguo Z (2018) A new simple chaotic system and its application in medical image encryption. Multimed Tools Appl 77:22787–22808
19. Kamdjeu Kengne L, Kamdeu Nkandeu YP, Mboupda Pone JR, Tiedeu A, Fotsin HB (2021) Image encryption using a novel quintic jerk circuit with adjustable symmetry. Int J Circuit Theory Appl. 1–32. Wiley. https://doi.org/10.1002/cta.2968
20. Arroyo D, Alvarez G, Fernandez V (2008) On the inadequacy of the logistic map for cryptographic applications, ACTAS DE LA X RECSI, arXiv: 0805.4355 [nlin.CD], pp.1–6, 28
21. Wu X, Hu H, Zhang B (2004) Parameter estimation only from the symbolic sequences generated by chaos system. Chaos Solitons Fractals 22(2):359–366

22. Hua Z, Zhou Y, Pun C-M, Chen CP (2015) 2d sine logistic modulation map for image encryption. Inf Sci 297:80–94
23. Kadir A, Hamdulla A, Guo W-Q (2014) Color image encryption using skew tent map and hyper chaotic system of 6th-order CNN. Optik 125(5):1671–1675
24. Chen H-K, Lee C-I (2004) Anti-control of chaos in rigid body motion. Chaos Solitons Fractals 21(4):957–965
25. Kengne J, Signing VRF, Chedjou JC, Leutcho GD (2017) Nonlinear behavior of a novel chaotic jerk system: antimonotonicity, crises, and multiple coexisting attractors. Int J Dyn Control 6(2):468–485
26. Leutcho GD, Kengne J (2018) A unique chaotic snap system with a smoothly adjustable symmetry and nonlinearity: Chaos, offset-boosting antimonotonicity, and coexisting multiple attractors. Chaos Solit Fractals 113:275–293
27. Maher J, Ayman A (2018) Real-time and encryption efficiency improvements of simultaneous fusion, compression and encryption method based on chaotic generators. Opt Lasers Eng 102(1):59–69
28. Wu G-C, Baleanu D (2014) Chaos synchronization of the discrete fractional logistic map. Signal Process 102:96–99
29. Hua Z, Zhou B, Zhou Y (2019) Sine chaotification model for enhancing chaos and its hardware implementation. IEEE Trans Industr Electron 66(2):1273–1284
30. Hua Z, Wang Y, Zhou Y (2015) Image cipher using a new interactive two-dimensional chaotic map. IEEE International Conference on Systems, Man, and Cybernetics, 978–1–4799–8697–2/15 $31.00 © IEEE. https://doi.org/10.1109/SMC.2015.316
31. Tsafack N, Sankar S, Abd-El-Atty B, Kengne J, Jithin KC, Belazi A, Mehmood I, Bashir AK, Song O-Y, Abd El-Latif AA (2020) A new chaotic map with dynamic analysis and encryption application in Internet of Health Things. IEEE Access. 1–14. https://doi.org/10.1109/ACCESS.2020.3010794
32. Abd El-Latif AA, Abd-El-Atty B, Abou-Nassar EM, Venegas-Andraca SE (2020) Controlled alternate quantum walks based privacy preserving healthcare images in internet of things. Optics Laser Technol 124:105942
33. Abd El-Latif AA, Abd-El-Atty B, Elseuofi S, Khalifa HS, Alghamdi AS, Polat K, Amin M (2020) Secret images transfer in cloud system based on investigating quantum walks in steganography approaches. Physica A Stat Mech Appl 541:123687
34. Yang F, Mou J, Cao Y, Chu R (2020) An image encryption algorithm based on bp neural network and hyperchaotic system. China Commun 17(5):21–28
35. Lin CY, Wu M, Bloom JA, Cox IJ, Miller M (May2001) Rotation, scale, and translation resilient public watermarking for images. IEEE Trans Image Process 10(5):767–782
36. Moysis L, Tutueva A, Volos C, Butusov D, Munoz-Pacheco JM, Nistazakis H (2020) A Two-Parameter Modified Logistic Map and Its Application to Random Bit Generation. Symmetry 12:829. https://doi.org/10.3390/sym12050829
37. Hamza R, Yan Z, Muhammad K, Bellavista P, Titouna F (2019) A privacy-preserving cryptosystem for IoT E healthcare. Inf Sci 527:493–510. https://doi.org/10.1016/j.ins.2019.01.070
38. Kamdeu Nkandeu Y, Tiedeu A, Abanda Y, Mboupda Pone JR (2022) Image encryption using the logistic map coupled to a self-synchronizing streaming. Multimed Tools Appl. Springer. https://doi.org/10.1007/s11042-022-12649-x
39. Pan H, Lei Y, Jian C (2018) Research on digital image encryption algorithm based on double logistic chaotic map. J Image Video Proc 142. https://doi.org/10.1186/s13640-018-0386-3
40. JeatsaKitio G, DjomoFanda A, KemlenackFeulefack IR, Mboupda Pone JR, Kengne R, Tiedeu A (2023) Biomedical Image encryption with a novel memristive Chua oscillator embedded in a microcontroller. Braz J Phys 53:56. https://doi.org/10.1007/s13538-023-01268-y. (Springer)
41. Ramakrishnan B, Kamdeu Nkandeu YP, Natiq H, Mboupda Pone JR, Karthikeyan A, Takougang Kingni S, Tiedeu A (2022) Image encryption with a Josephson junction model embedded in FPGA. Multimed Tools Appl. Springer. https://doi.org/10.1007/s11042-022-12400-6
42. Abanda Y, Tiedeu A, Kom G (2021) Image encryption with fusion of two maps. Security and Communication Networks. 2021, Article ID 6624890. Wiley-Hindawi. https://doi.org/10.1155/2021/6624890
43. Baptista M (1998) Cryptography with chaos. Phys Lett A 240(1–2):50–54
44 Ben Ammar M, Dhaou IB, El Houssaini D, Sahnoun S, Fakhfakh A, Kanoun O (2022) Requirements for EnergyHarvesting-Driven Edge Devices Using Task-Offloading Approaches. Electronics 11:383. https://doi.org/10.3390/electronics11030383
45. Singh BM, Kamali G, Shalli R, Rajnish R (2022) An energy-efficient partial data offloading-based priority rate controller technique in edge-based IoT network to improve QoS. Hindawi Wireless Communications and Mobile Computing, Special issue. Machine Learning Enabled Signal

Processing Techniques for Large Scale 5G and 5G Networks. Volume 2022 | Article ID 4288663. https://doi.org/10.1155/2022/4288663
46. Lakhan A, Sodhro AH, Majumdar A, Khuwuthyakorn P, Thinnukool OA (2022) Lightweight Secure Adaptive Approach for Internet-of-Medical-Things Healthcare Applications in Edge-Cloud-Based Networks. Sensors 22:2379. https://doi.org/10.3390/s22062379,2022
47. Lakhan A, Ali Dootio M, Sodhro AH, Pirbhulal S, Groenli TM, Khokhar MS, Wang L (2021) Cost-efficient service selection and execution and blockchain-enabled serverless network for internet of medical things. Math Biosci Eng 2021(18):7344–7362
48. Yang L, Yu K, Yang SX, Chakraborty C, Lu Y, Guo T (2021) An intelligent trust cloud management method for secure clustering in 5G enabled internet of medical things. IEEE Trans Ind Inform. https://doi.org/10.1109/TII.2021.3128954
49. Wu Y, Yang G, Jin H, Noonan JP (2012) Image encryption using the two-dimensional logistic chaotic map. J Electron Imaging 21(1), id. 013014–013014–15
50. Strogatz S (1994) Nonlinear dynamics and chaos: with applications to physics, biology, chemistry, and engineering. Westview Press
51. Shannon CE (1948) A mathematical theory of communication. Bell Syst Tech J 27:379–423, 623–656
52. Kantz H (1994) A robust method to estimate the maximal lyapunov exponent of a time series. Phys Lett A 185(1):77–87
53. Wolf A, Swift J, Swinney H, Vastano J (1985) Determining lyapunov exponents from a time series. Physica D 16(3):285–317
54. Yepdia LMH, Tiedeu A, Kom G. A Robust and Fast Image Encryption Scheme Based on a Mixing Technique. Hindawi Security and Communication Networks 2021;17. Article ID 6615708. https://doi.org/10.1155/2021/6615708
55. Murillo-escobar MA, Cruz-Hernández C, Abundiz-Pérez F, López-Gutiérrez RM, Acosta Del Campo OR (2015) A RGB image encryption algorithm based on total plain image characteristics and chaos. Signal Processing 109:119–131
56. Belazi A, El-Latif AAA, Belghiht S (2016) A novel image encryption scheme based on substitution-permutation network and chaos. Signal Process 128:155–170
57. Stinson DR (2006) Cryptography: theory and practice. Chapman and Hall CRC
58. Banu S A, Amirtharajan R (2020) A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach. Med Biol Eng Comput 58(7):1445–1458
59. AashiqBanu S, Amirtharajan R (2020) Tri-level scrambling and enhanced diffusion for DICOM image cipher- DNA and chaotic fused approach. Multimed Tools Appl 79(39–40):28807–28824
60. Farah MAB, Guesmi R, Kachouri A, Samet M (2020) A novel chaos based optical image encryption using fractional Fourier transform and DNA sequence operation. Opt Laser Technol 121:105777. https://doi.org/10.1016/j.optlastec.2019.105777
61. Zhou M, Wang C (2020) A novel image encryption scheme based on conservative hyperchaotic system and closed-loop diffusion between blocks. Signal Process 171:107484. https://doi.org/10.1016/j.sigpro.2020.107484
62. Chai X, Fu X, Gan Z, Zhang Y, Lu Y, Chen Y (2020) An efficient chaos-based image compression and encryption scheme using block compressive sensing and elementary cellular automata. Neural Comput Appl 32(9):4961–4988
63. Fu C, Bian O, Jiang H, Ge L, Ma H (2017) A new chaos-based image cipher using hash function. Int J Networked Distrib Comput 5(1):37–44