Wireless Personal Communications (2019) 108:591–612
https://doi.org/10.1007/s11277-019-06420-z

Medical Image Encryption Based on Hybrid Chaotic DNA Diffusion

Joshua C. Dagadu[1,2] · **Jian-Ping Li**[1] · **Emelia O. Aboagye**[1]

Published online: 25 April 2019

Abstract

We explore the use of two chaotic systems (Bernoulli shift map and Zizag map) coupled with deoxyribonucleic acid coding in an encryption scheme for medical images in this paper. The scheme consists of two main phases: Chaotic key generation and DNA diffusion. Firstly, the message digest algorithm 5 hash function is performed on the plain medical image and the hash value used in combination with the value of an input ASCII string to generate initial conditions and control parameters for two chaotic systems (Bernoulli shift map and Zigzag map). These chaotic systems are subsequently used to produce two separate key matrices. Secondly, a row-by-row diffusion operation between the plain image matrix and the two chaotic key matrices, using the DNA XOR algebraic operation is performed in an alternating pattern to produce the cipher image. The logistic map is used to select the DNA encoding and decoding rules for each row. Experimental results of statistical, differential and key analyses demonstrate that the proposed scheme is robust and provides resistance to various forms of attacks.

Keywords Medical image · Encryption · Chaotic system · DNA computing

1 Introduction

Remote healthcare delivery, facilitated by state-of-the-art technologies such as telemedicine, teleradiology and telesurgery has witnessed concerns raised about the security of medical data, not excepting medical images. Particularly teleradiology has been very successful and popular, and incorporates diverse imaging modalities of ultrasonography, computed tomography, X-ray radiology, magnetic resonance imaging, etc [23]. Medical images form critical components of medical diagnostic procedures as they among other things, offer non-invasive methods of examining anatomical cross sections of internal organs and other features of patients. These images are transmitted over public digital communication networks [19] and are stored in networked storage facilities, sometimes powered by cloud

✉ Joshua C. Dagadu
joscaldag@yahoo.com

[1] School of Computer Science and Engineering, University of Electronic Science and Technology of China, Chengdu 611731, People's Republic of China

[2] University of Education, Winneba, Ghana

computing services to be used for clinical interpretation and diagnosis. However, services such as cloud storage pose critical security challenges to data [38–40]. Medical imaging security schemes are expected to achieve high degrees of resistance against diverse forms of attacks without compromising the diagnostic quality of the images because alterations made to the images during processing might result in irreversible wrong diagnostic consequences. Conventional encryption protocols such as Data Encryption Standard (DES), Advanced Encryption Standard (AES) and Rivest–Shamir–Adleman (RSA) have been used in encrypting medical images; however, these algorithms are not very efficient for images due to certain intrinsic features of images including high redundancy, bulk data capacity and high correlation among adjacent pixels [1, 27]. Consequently, chaos based encryption schemes have been extensively proposed recently [4, 12].

Chaotic systems demonstrate random behaviour and have inherent characteristics such as unpredictability, ergodicity and sensitivity to initial conditions. They are dynamical systems that are unpredictable and resemble noise [29]. These characteristics provide a close relationship between chaotic dynamical systems and cryptosystems. The sensitivity to initial conditions property of chaos systems is used for keys in cryptosystems while the topological transitivity property which ensures the ergodicity of chaos maps, is related to the diffusion property of cryptosystems [20]. The behaviour of a chaos system is predictable if the initial condition and the control parameter are known to attackers. As long as attackers are ignorant about these, the system appears to be random. This random behaviour is employed to provide confusion and diffusion within the cipher image, thereby enabling secure transmissions over unprotected communication channels. Encryption algorithms based solely on chaos, however do not always provide sufficient robustness [22], due to weak diffusion functions, weakness against chosen and known plaintext attacks and poor statistical characteristics of some chaos maps [7, 14, 24]. The security of most chaos-based cryptosystems is not justified [4]; most of them are slow in nature, some have small key spaces, some require considerable iteration steps and others have inappropriate key stream generation defects [4]. This has led to mergers between chaos and other theories such as deoxyribonucleic acid (DNA) computing for designing cryptosystems [26, 28]. Nevertheless, some of these mergers have also been found insecure particularly against chosen-plaintext attacks [16, 18]. Some have been found to be insensitive to changes in plain image or secret key, while others have fixed encoding and decoding rules [15, 17, 37].

The efficiency of both low and high dimensional nonlinear systems play an important role in hardware implementations of encryption algorithms [21]. Despite some associated disadvantages when used in encryption, the low-dimensional nonlinear systems are the more attractive ones that have been widely used in generating pseudorandom key streams in image cryptosystems because the high-dimensional ones require more computational power, time and resources. Their discreteness, simple structure, less arithmetic operations, high output processing and relatively easier implementations in digital systems make the low-dimensional systems more attractive for particularly image cryptosystems. Consequently, approaches that enhance the efficiency of the low-dimensional systems when used in encryption is beneficial.

We examine the bifurcation diagrams of the Bernoulli shift map and the Zigzag map as pseudo-random number generators and deploy them in combination with DNA coding in a novel image encryption scheme that meets state-of-the-art standards. The chaotic systems are used to generate two separate key matrices. The key matrices and the plain image matrix are encoded into DNA sequences using logistic map based selected DNA rules. The DNA XOR algebraic operation is performed between the DNA key sequences and the DNA image sequence in an alternating pattern to achieve a high level of diffusion. The diffused image is then decoded to produce the cipher image. Our system specifically aims at using one round of the diffusion process to achieve robust encryption that meets modern imaging security standards. The rest of the paper is organized as follows: In Sect. 2, we give overviews of the chaos maps and DNA computing. We introduce our proposed scheme in Sect. 3, discuss experimentation and results in Sect. 4 and finally conclude in Sect. 5.

2 Preliminaries

Brief overviews of the chaos maps (Bernoulli shift map, zigzag map, logistic map) and DNA coding are presented in this section. We adopt the analysis reported in [13] for the Bernoulli shift map and the zigzag map.

2.1 Bernoulli Shift Map

A dyadic transformation $dt : [0,1) \to [0,1)^{\infty} \quad v \mapsto \left(v_0, v_2, \ldots\right)$ which is produced by $v_0 = v \quad \forall i \geq 0, \quad v_{i+1} = \left(2v_i\right) \bmod 1.$ gives an example of how simple 1-dimensional maps could result in chaotic behaviours.

The Bernoulli shift map is defined by two linear functions as:

$$v_{i+1} = \begin{cases} \mu v_i - r, & if \quad v_i \geq 0 \\ \mu v_i + r, & if \quad v_i < 0 \end{cases} \tag{1}$$

Equation (1) could be rewritten as

$$v_{i+1} = \mu v_i - r \quad sign(v_i) \tag{2}$$

where v_0 is the initial condition, μ is the control parameter of the stochastic properties of the chaotic system and r is a scale factor which increases or decreases the product μv_i and limits the output values within the range $[-r, r]$.

Figure 1 is the bifurcation diagram for the bernoulli shift map for $r = 1$. It can be seen from the diagram that when $\mu \in [0, 1)$ there is an oscillation between two fixed points. When $\mu = 1$ it is unstable and when $\mu \in (1, 1.4]$, there is a nonuniform distribution in the output values of the system. The distribution improves when μ approaches 1.4 and eventually when $\mu \in [1.4, 2)$, the greatest dispersion in the output values is produced. It is clear from the figure that for $\mu \in [1.4, 2)$, the output values cover the entire range of $[-1, 1]$. For $\mu \geq 2$, the system is unstable and its output tends to infinity for large i values [13].

Obviously, when we take v_0 values within $[0.5, 1)$ and μ values within $(1.5, 2)$ we get a significant chaotic distribution for our encryption scheme.

2.2 Zigzag Map

The zigzag map is mathematically expressed as:

$$x_i = \begin{cases} -\omega\left(x_i + \frac{2}{|\omega|}\right), & for \quad x_i \in \left(-1, -\frac{1}{|\omega|}\right], \\ \omega x_i, & for \quad x_i \in \left(-\frac{1}{|\omega|}, \frac{1}{|\omega|}\right], \\ -\omega\left(x_i - \frac{2}{|\omega|}\right), & for \quad x_i \in \left(\frac{1}{|\omega|}, 1\right] \end{cases} \tag{3}$$

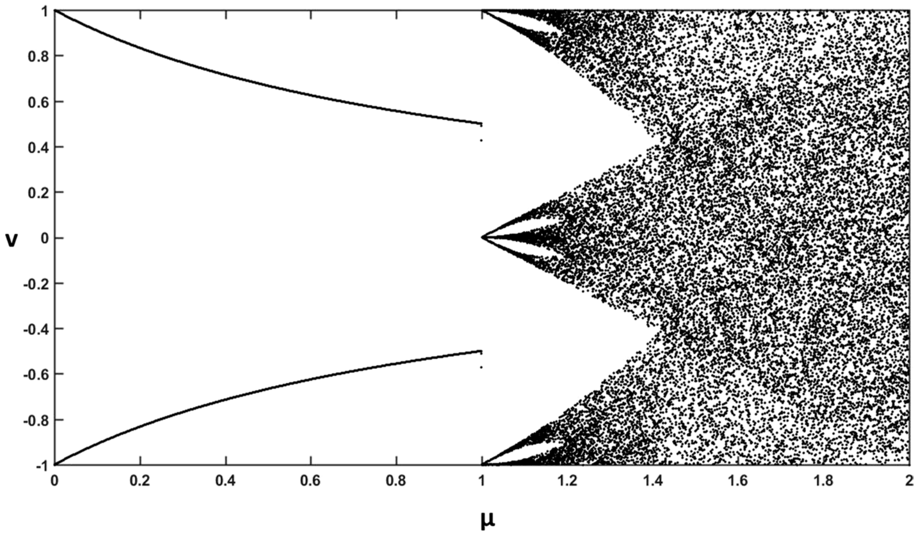


Fig. 1 Bifurcation diagram of the Bernoulli shift map

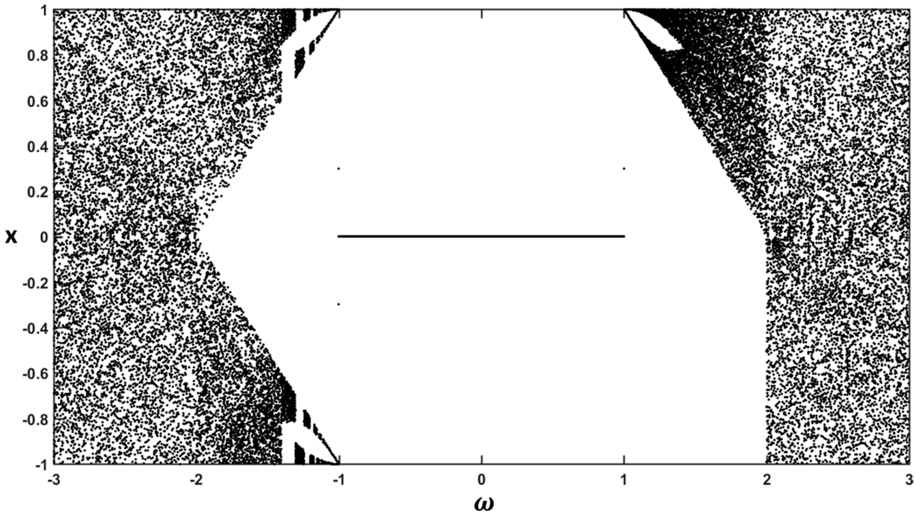


Fig. 2 Bifurcation diagram of the Zigzag map

where x_0 is the initial condition and ω is the control parameter. Figure 2 is the bifurcation diagram for the zigzag map. As shown in the diagram, when $|\omega| < 1$, the system's behaviour is not chaotic but when $\omega \in (2, 1), (1, 2), [3, 2)$ and $(2, 3]$ the system's behaviour is chaotic.

In our proposed system, we take $\omega \in (2, 3]$.

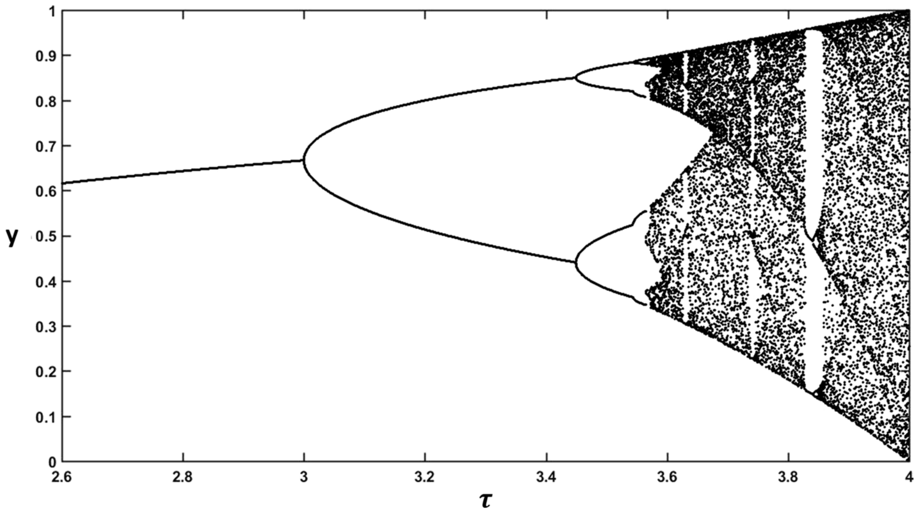


Fig. 3 Bifurcation diagram of the logistic map

2.3 Logistic Map

The logistic map is a polynomial mapping of degree 2. Often, it is cited as a typical example of how very simple non-linear dynamical systems can result in complex chaotic behaviours [6]. It is one of the simple systems that exhibit order to chaos transition and have many features required of a pseudorandom number generator (PRNG) [25]. For the largest value of its control parameter, the logistic map has the ability to generate an infinite chaotic sequence of numbers. When compared to the usual congruential random generators which are periodic, the logistic random number generator is infinite, aperiodic and not correlated [3].

It is mathematically given as:

$$y_{i+1} = \tau y_i \left(1 - y_i\right) \tag{4}$$

where the control parameter $\tau \in (0, 4)$, the initial condition $y_0 \in (0, 1)$ and i is the iteration. The logistic map is in a chaotic condition when the control parameter is [3.57, 4.0]. In our scheme, we use the logistic map to select the DNA encoding and decoding rules due to its high speed. The bifurcation diagram of the logistic map is shown in Fig. 3

2.4 DNA Computing

In recent years, DNA sequence has become extremely useful for basic biological research, and in diverse applied fields such as diagnostic, forensics, biological systematics [10] and information security. The properties of DNA such as huge storage, massive parallelism, big information density and low power consumption [36] have made them attractive candidates for encryption schemes. DNA sequence is made up of four bases: Adenine (A), Thymine (T), Guanine (G) and Cytosine (C). Among these bases, A and T are complementary to each other while G and C are complementary to each other [26]. That is, the purine Adenine always pairs with the pyrimidine Thymine and the purine

Table 1 Watson crick's complementary rule

1	C (00)	G (11)	A (01)	T (10)	5	A (00)	T (11)	C (01)	G (10)
2	C (00)	G (11)	A (10)	T (01)	6	A (00)	T (11)	C (10)	G (01)
3	G (11)	C (00)	A (01)	T (10)	7	A (11)	T (00)	C (01)	G (10)
4	G (11)	C (00)	A (10)	T (01)	8	A (11)	T (00)	C (10)	G (01)

Table 2 DNA encoding and decoding rules

Rules	A	T	C	G
Rule 1	00	11	01	10
Rule 2	00	11	10	01
Rule 3	01	10	00	11
Rule 4	10	01	00	11
Rule 5	01	10	11	00
Rule 6	10	01	11	00
Rule 7	11	00	01	10
Rule 8	11	00	10	01

Table 3 DNA XOR operation

XOR	A	G	C	T
A	A	G	C	T
G	G	A	T	C
C	C	T	A	G
T	T	C	G	A

Guanine always pairs with the pyrimidine Cytosine, according to the rules of base pairing by Watson and Crick [34] as shown in Table 1.

In the binary system, 0 and 1 are complementary, 00 and 11 are complementary while 01 and 10 are also complementary. Mapping the two-bit binary system to the DNA bases, 24 rule sets can be obtained [26]. Among these 24 rules, only 8 satisfy the Watson-Crick base pairing rules. A can only bond with T and C can only bond with G. Based on this, DNA-based computing uses only 8 sets of encoding and decoding rules [28] as shown in Table 2.

Addition, subtraction and XOR algebraic operations can be performed on DNA sequences. These DNA algebraic operations are employed to enhance the diffusion phase in encryption. Table 3 shows the XOR operation which is used in our proposed system.

Using the DNA coding, each 8-bit pixel of a gray scale image can be expressed as a DNA sequence of length 4. Taking a pixel of gray level 25 for instance, its 8-bit binary sequence is (00011001). Using DNA encoding rule 6 from Table 2, (GTAT) is obtained. Decoding (GTAT) with the same rule 6 gives (00011001). Any other rule used to decode (GTAT) will give a different binary value. For instance using rule 8 to decode (GTAT) gives us (01001100) which is 76 in decimal. This obviously changes pixel values to bring about obscurity in the cipher image. Taking two DNA sequences (ATTC) and (GAGT), performing the XOR operation on them results in (GTCG), performing the same XOR operation on (GTCG) and (GAGT) gives back (ATTC) and the same operation on (GTCG)and (ATTC) gives back (GAGT). These reversible operations make it possible to reverse the diffusion operation in encryption.

3 Proposed Scheme

Our proposed scheme uses two chaos maps to generate two different key matrices and DNA algebraic XOR operation for diffusion. The user inputs the plain medical image, a 16-character ASCII string and the initial condition and control parameter of the logistic map. An MD5 hash value of 128 bits is obtained from the plain image matrix and used to generate the initial condition and control parameter of the zigzag map, which is used to produce one of the key matrices. The last two characters of the hash value are used to replace the first two and last two characters of the ASCII string to obtain a new string. This is done to ensure that, slight changes in pixels of the plain image will result in significant changes in the cipher image. The new string is used to generate the initial condition and control parameter of the Bernoulli shift map, which is used to produce the other key matrix.

Following the approach proposed in [32], to select DNA encoding and decoding rules for both plain and key images, the logistic map (Eq. 4) is iterated a number of times corresponding to the number of rows in the image matrix. At every iteration, one DNA coding rule (out of the 8 as in Table 2) which corresponds to the y value at that iteration level is selected. The selected rule is then used to encode all pixels on that row. This continues until all rows in the image are covered. After both key matrices and the plain image matrix are encoded into DNA sequences a diffusion operation using the DNA XOR operation is carried out. The diffusion is done by an alternating application of the two keys on row basis. The diffused image is then decoded (also randomly on row basis just as in the encoding phase) to produce the cipher image. The reverse of the encryption process decrypts the image into its plain form. The block diagram of the proposed scheme is shown in Fig. 4.

3.1 Encryption

3.1.1 Key One Generation

Step 1 Get the matrix of the plain image I and its dimensions M and N

Step 2 Get the number of rows L for the key image

$$L = \frac{1}{2} \times M \tag{5}$$

Step 3 Perform a message digest algorithm 5 function on I to obtain a 128 bit hash value (32 character hexadecimal string)

$$H = h_1, h_2, h_3, \dots, h_{32} \tag{6}$$

Step 4 Convert the hexadecimal characters H into their binary digit representations to obtain the 128-bit stream

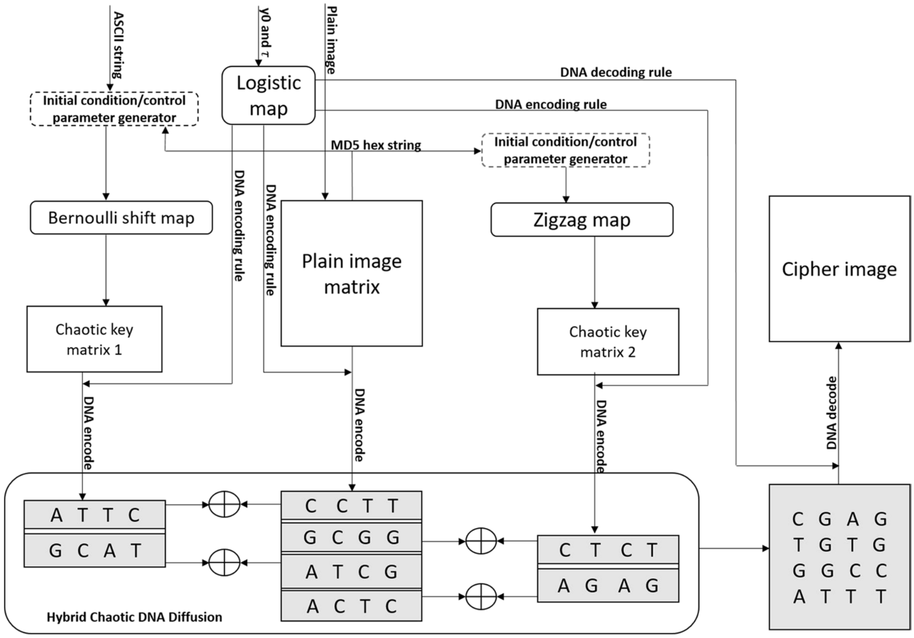


Fig. 4 Block diagram of proposed scheme

$$B = b_1, b_2, b_3, \ldots, b_{128} \tag{7}$$

Step 5 Take the first 96 bits of B and put them into 4 blocks q_1, q_2, q_3, q_4 of 24 bits each and perform the following operations:

$$q_n = \sum_{i=1}^{24} \left(b_i \times 2^i\right) \tag{8}$$

where $n = \{1, 2, 3, 4\}$

$$q_5 = \left(\left((q_1 \oplus q_2) \oplus q_3\right) \oplus q_4\right) \tag{9}$$

Step 6 Using q_5 derive the initial value x_0 of the zigzag map as

$$x_0 = 0.50001 + \mathrm{mod}\left(\left(q_5/2^{32}\right), 1\right) \tag{10}$$

Step 7 Use the last 32 bits of B (i.e. $b_{97}, \ldots, b_{128}$) to obtain the control parameter ω of the zigzag map as

$$q_6 = \sum_{i=1}^{32} \left(b_i \times 2^i\right) \tag{11}$$

$$\omega = 2.009 + \left(\mathrm{mod}\left(q_6, 2\right)\right) \tag{12}$$

Step 8 Iterate Eq. (3) LN times using x_0 and ω to generate the chaos sequence X where L is half the height (i.e. number of rows) and N the width (i.e. number of columns) of the plain image.

Step 9 Convert the chaotic sequence

$$X = \left\{x_1, x_2, x_3, \dots, x_{LN}\right\}$$

into integer sequence to produce the key image

$$K = \left\{k_1, k_2, k_3, \dots, k_{LN}\right\}$$

as

$$k_i = \text{mod}\left(floor\left(x_i \times 10^{14}\right), 256\right) \tag{13}$$

where k_i is a pixel and $k_i \in K$

3.1.2 Key Two Generation

Step 1 Input 16 character ASCII string

$$A = a_1, a_2, a_3, \dots, a_{16} \tag{14}$$

Step 2 Take the last two hexadecimal characters in H as in Sect. 3.1.1 (i.e. $h_{31}, h_{32} \in H$) and use it to substitute the first and last two characters of A

$$A' = h_{31}, h_{32}, a_3, \dots, a_{14}, h_{31}, h_{32} \tag{15}$$

For the purposes of convenience, we rewrite A' as

$$G = g_1, g_2, g_3, \cdots, g_{16} \tag{16}$$

Step 3 Convert the first 4 characters (i.e. $g_1, \dots, g_4$) of G into their hexadecimal form

$$Z = z_1, z_2, \dots, z_8 \tag{17}$$

Step 4 Add the hexadecimal values as

$$\alpha_1 = \left(\sum_{i=1}^{8} \left(z_i\right)_{10}\right) \Big/ 128 \tag{18}$$

Step 5 Convert the 5th to 8th characters (i.e. $g_3, \dots, g_8$) of G into their 8-bit binary values to obtain β_1

$$\beta_1 = d_1, d_2, \dots, d_{32} \tag{19}$$

Step 6 Add the elements in β_1 as

$$\alpha_2 = \left(\sum_{i=1}^{32} \left(d_i \times 2^i\right)\right) \Big/ 2^{32} \tag{20}$$

Step 7 Calculate the initial condition of the Bernoulli shift map as

$$v_0 = \mathrm{mod}\big(\big(\alpha_1 + \alpha_2\big), 1\big) \tag{21}$$

Step 8 Convert the last 8 characters (i.e. $g_9, \ldots, g_{16}$) of G into their binary values to obtain

$$\beta_2 = e_1, e_2, \ldots, e_{64} \tag{22}$$

Step 9 Put β_2 into two blocks of 32 bits each and obtain α_3 and α_4 as follows:

$$\alpha_n = \left(\sum_{i=1}^{32} \left(e_i \times 2^i\right)\right) \Big/ 2^{32} + 1 \tag{23}$$

where $n = \{3, 4\}$

Step 10 Obtain the control parameter of the Bernoulli shift map as

$$\mu = 1.5 + \mathrm{mod}\big(\alpha_3 + \alpha_4, 1\big) \times 0.01 \tag{24}$$

Step 11 Iterate Eq. (1) LN times using v_0 and μ to generate the chaos sequence S

Step 12 Convert sequence $S = \left\{s_1, s_2, s_3, \ldots, s_{LN}\right\}$ into integer sequence to produce the key image

$$P = \left\{p_1, p_2, p_3, \ldots, p_{LN}\right\}$$

as

$$p_i = \mathrm{mod}\big(\mathit{floor}\big(s_i \times 10^{14}\big), 256\big) \tag{25}$$

where p_i is a pixel and $p_i \in P$

3.1.3 Diffusion

Step 1 Read in the plain image I

Step 2 Get the dimensions M and N of I and generate the key matrices K and P as in Sects. 3.1.1 and 3.1.2

Step 3 Using the initial condition y_0 and parameter τ iterate Eq. (4) M times where M is the number of rows of the image

Step 4 For each iteration, preprocess y as

$$y = \mathit{floor}(y \times 7) + 1 \tag{26}$$

Step 5 Choose the DNA encoding rule based on the new value of y and encode the pixels on the row with the selected rule to obtain the DNA sequence of the pixels on the row

Step 6 Repeat step 5 for each member of M (i.e. each row) to get the DNA sequence $I_\delta{}'$ of I

Step 7 Repeat steps 3 to 6 L times each for K (i.e. key matrix one) and P (i.e. key matrix two) to get the DNA sequence K_δ of K and P_δ of P respectively

Step 8 Perform the DNA algebraic XOR operation between the rows in $I_\delta{}'$ and their corresponding rows in K_δ and P_δ in an alternating manner as illustrated in the block diagram (i.e. Fig. 4) to get Q_δ as

$$Q_\delta = I_\delta \oplus \left\{K_\delta \cup P_\delta\right\} \tag{27}$$

Step 9 Repeat steps 4 to 6 to select DNA decoding rules and decode Q_δ to get the cipher image Q.

3.2 Decryption

The reverse operation of the encryption process decrypts the cipher image to its exact original form. With the decryption process, the cipher image, the 16-bit ASCII string, the MD5 hash value of 128 bits represented by 32-hexadecimal string, the initial condition and control parameter of the logistic map are taken as inputs. The two key matrices are generated following the steps in 3.1.1 and 3.1.2. The reverse of steps used during the diffusion process as in 3.1.3 are followed to reverse the diffusion to obtain the deciphered image.

4 Experimentation and Results

4.1 Experimental Setting

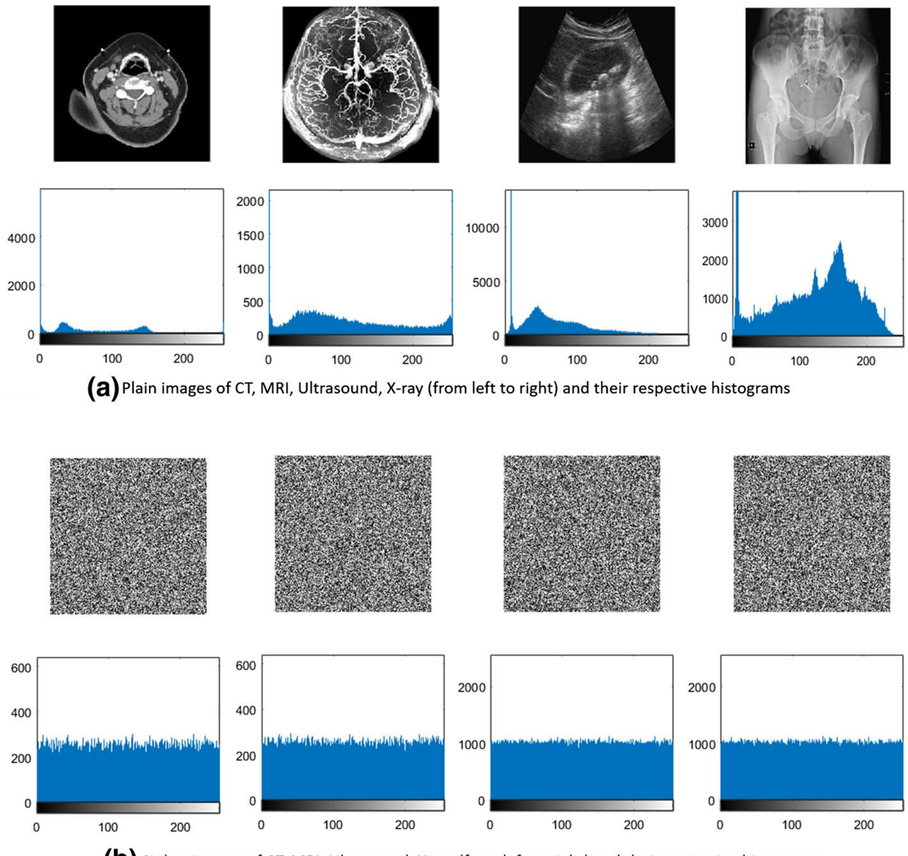
We experiment our proposed scheme on a personal computer with intel core i5, 2.6GHz CPU, 4GB memory, windows 10 and MATLAB 2016b. We use a number of gray scale images (of bit depth 8) of different imaging modalities and sizes in the experiment. Images with dimensions (256 × 256) and (512 × 512) are presented in this paper. An external ASCII string $K = 'zz8dEg5fHYJZYD9Q'$ is used for all the test images and initial condition $y_0 = 0.667$ and control parameter $\tau = 3.999$ are used to control the logistic map. Statistical, differential and key analyses are carried out to assess the security strength of the proposed scheme.

4.2 Statistical Analysis

We carry out statistical analyses to verify the robustness of the proposed scheme. This is done by histogram analysis, correlation analysis and entropy analysis of both plain and cipher images. Shannon [30] indicated the possibility of security breaches on many kinds of encryption schemes through statistical analysis on the correlation of adjacent pixels and their histograms.

4.2.1 Histogram Analysis

An efficient image encryption should produce a uniform histogram distribution of the cipher image in order to make it impossible for attackers to extract any meaningful information from it. This is because the image histogram reveals the pixel value distribution within the image. Results of four of our test images are shown in Fig. 5. It is evident from the figure that the proposed scheme distributes pixels in the cipher image uniformly and as such, is robust against statistical attacks.



(a) Plain images of CT, MRI, Ultrasound, X-ray (from left to right) and their respective histograms

(b) Cipher images of CT, MRI, Ultrasound, X-ray (from left to right) and their respective histograms

Fig. 5 Histograms of plain and cipher medical images; CT and MRI (256 × 256), ultrasound and X-ray (512 × 512)

4.2.2 Correlation Analysis

The correlation coefficients of adjacent pixels of an image give information about the content of the image. In images, the horizontal, vertical and diagonal correlations between adjacent pixels are very high. To resist statistical attacks, cipher images must reduce or totally break these relationships among the adjacent pixels. The correlation coefficients among adjacent pixels is calculated with Eqs. (28), (29), (30) and (31) [9].

$$E(x) = \frac{1}{N}\sum_{i=1}^{N} x_i \tag{28}$$

$$D(x) = \frac{1}{N}\sum_{i=1}^{N} \left(x_i - E(x)\right)^2 \tag{29}$$

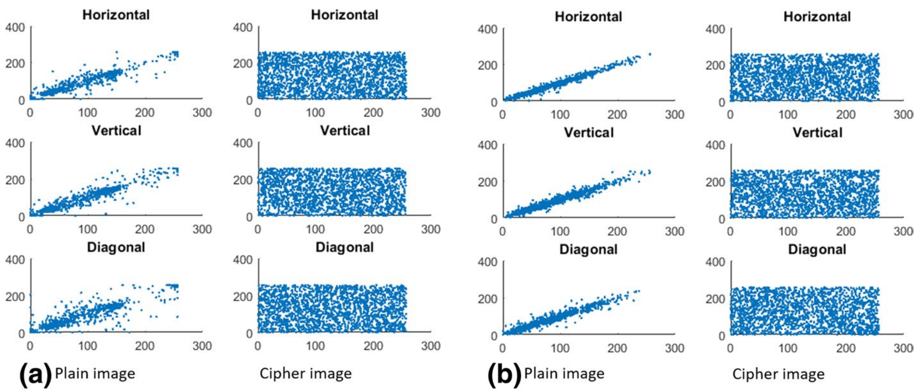


Fig. 6 Correlation analysis of: **a** CT scan (256 × 256) and **b** ultrasound (512 × 512) images

Table 4 Correlation analysis results

Test image	Correlation coefficient					
	Plain			Cipher		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
CT Scan (256 × 256)	0.9753	0.9745	0.9558	– 0.0016	0.0043	– 0.0061
MRI (256 × 256)	0.8929	0.8953	0.8378	– 0.0037	−0.0017	0.0009
Ultrasound (256 × 256)	0.9896	0.9767	0.9689	– 0.0025	−0.0011	– 0.0014
X-Ray (256 × 256)	0.9938	0.9977	0.9908	0.0022	– 0.0034	0.0043
CT scan (512 × 512)	0.9955	0.9949	0.9904	– 0.0035	0.0019	– 0.0031
MRI (512 × 512)	0.9851	0.9856	0.9694	– 0.0009	0.0007	0.0004
Ultrasound (512 × 512)	0.9927	0.9876	0.9812	– 0.0022	0.0028	– 0.0016
X-ray (512 × 512)	0.9798	0.9906	0.9713	0.0011	– 0.0005	0.0002

$$\operatorname{cov}(x,y) = \frac{1}{N}\sum_{i=1}^{N}\left(x_i - E(x)\right)\left(y_i - E(y)\right) \tag{30}$$

$$r_{xy} = \frac{\operatorname{cov}(x,y)}{\sqrt{D(x)\times\sqrt{D(y)}}} \tag{31}$$

where x and y are the gray scale values of two adjacent pixels of the image, $D(x)$ is the variance, $\operatorname{cov}(x,y)$ is the covariance and $E(x)$ is the mean. We randomly selected 2000 pairs of adjacent pixels from both original and encrypted images and calculated their horizontal, vertical and diagonal correlation coefficients. Figure 6 shows the correlation coefficient distributions of plain and cipher CT scan and ultrasound images. It is evident from the figure that the proposed scheme sufficiently breaks the correlation

Table 5 Information entropy and contrast analysis

Test image	Information entropy		Contrast
	Plain image	Cipher image	
CT Scan (256 × 256)	4.0394	7.9972	8.7977
MRI (256 × 256)	6.9381	7.9969	8.8002
Ultrasound (256 × 256)	6.6943	7.9972	8.7902
X-Ray (256 × 256)	5.7693	7.9970	8.8078
CT scan (512 × 512)	7.2220	7.9993	8.8030
MRI (512 × 512)	5.9052	7.9993	8.8281
Ultrasound (512 × 512)	5.8704	7.9993	8.8281
X-Ray (512 × 512)	7.5373	7.9993	8.7940

among adjacent pixels; hence can resist statistical attacks. Table 4 gives the values of the correlation analysis.

4.2.3 Information Entropy

Information entropy is a mathematical property that reflects the randomness and the unpredictability of information [30]. It is given as

$$H(m) = \sum_{i=0}^{2^N-1} p\left(m_i\right) \log \frac{1}{p\left(m_i\right)} \tag{32}$$

where N is the total number of symbols $m_i \in m$; $p\left(m_i\right)$ denotes the probability of occurrence of symbol m_i and *log* represents the base 2 logarithm. It measures the randomness of the encryption. If there are 256 possible outcomes of the 8-bit message m with equal probability, the message origin is said to be random in which case $H(m)$ is equal to 8, the ideal condition. In Table 5, we show the entropy values of plain and cipher images using our scheme. It is clear from the table that our results are very close to the ideal condition. This is evident that there is negligible information leakage during encryption; hence our scheme has strong resistance against entropy attacks.

4.3 Contrast Analysis

The difference of brightness between light and dark parts in an image is referred to as the contrast of the image. It is interpreted visually as the spread of the brightness histogram of the image. The contrast is given as [33]

$$C = \sum_{i,j} |i-j|^2 g(i,j) \tag{33}$$

where $g(i,j)$ is the number of gray-level co-occurrence matrices. In Table 5, we show the results of our contrast analysis on the test images.

Table 6 NPCR and UACI values

Test image	NPCR	UACI
CT Scan (256 × 256)	0.9964	0.3343
MRI (256 × 256)	0.9960	0.3339
Ultrasound (256 × 256)	0.9960	0.3364
X-Ray (256 × 256)	0.9960	0.3351
CT Scan (512 × 512)	0.9961	0.3351
MRI (512 × 512)	0.9962	0.3353
Ultrasound (512 × 512)	0.9960	0.3351
X-Ray (512 × 512)	0.9961	0.3348

4.4 Differential Analysis

Sensitivity of cipher images to slight changes in plain images is one way to measure the resistance of image encryption algorithms to differential cryptanalysis. The two metrics used are the Number of Pixel Change Rate (NPCR) and Unified Average Changing Intensity (UACI) which are defined as

$$NPCR = \frac{1}{W \times H}\left(\sum_{i,j} D(i,j)\right) \times 100\% \tag{34}$$

and

$$UACI = \frac{1}{W \times H}\left(\sum_{i,j}\left|\frac{C_1(i,j) - C_2(i,j)}{255}\right|\right) \times 100\% \tag{35}$$

where C_1 and C_2 are two encrypted images which have one pixel difference in their corresponding plain images. $C_2(i,j)$ are their pixel values and W and H represent their widths and heights. An attacker would inverse a pixel in the plain image and observe the corresponding change in the cipher image. If the changes in the plain image do not lead to non-uniform changes in the cipher image, the differential attack fails [10–12]. In Table 6, we show the NPCR and UACI values of our experiment. It is clear from the table that the proposed scheme is robust against differential attacks.

4.5 Key Analysis

Key space and key sensitivity analyses are used to evaluate the key strengths of encryption algorithms.

4.5.1 Key Space

Our scheme uses an input key of 16 character ASCII string, which is made up of 128 bits and an MD5 hash value of 32 character hexadecimal string made up of 128 bits to generate the initial conditions and control parameters of the Bernoulli shift map and the zigzag map.

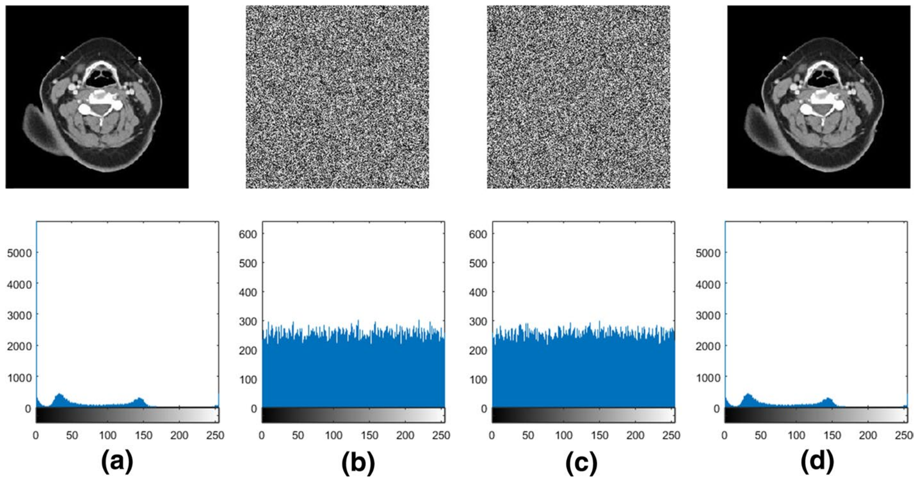


Fig. 7 Key sensitivity test using CT scan: **a** plain image, **b** cipher image, **c** decrypted image with wrong key, **d** decrypted image with correct key

In addition, the system takes in as input, user specified initial condition and control parameter for the logistic map. These make up the set for the key space of our scheme. The computational precision of the 64-bit double precision number is about 10^{-15}, according to the IEEE floating-point standard [35]. For an effective encryption scheme, the key space size should not be smaller than 2^{100} in order to resist brute-force attacks [2]. If a precision of 10^{-16} is assumed, the secret key space for our scheme is more than 2^{256} which is adequate to resist brute-force attacks.

4.5.2 Key Sensitivity

Key sensitivity ensures that partial guesses of the key aimed at decrypting the cipher image is unsuccessful. With the incorrect keys, the guessed key should not provide any pattern of information in the wrongly decrypted image. In other words, if two different keys are used to encrypt the same plain image, the resulting cipher images must be different. Based on this, we made slight changes in the seed key from $K = zz8dEg5fHYJZYD9Q$ to $K = zz8FEg5fHYJZYA9Q$ and in the hash value for decrypting the same cipher image to see the effect. In Fig. 7 we show the resulting images. It is evident from the figure that if the wrong key is applied to decrypt the image, the resulting image still shows no pattern in the original image.

4.6 Computation and Complexity Analysis

In our proposed encryption scheme, the computational cost depends on the diffusion operations needed for encryption. Our scheme uses one round of diffusion to encrypt an image. The time consuming part includes the number of floating-point operations $\Theta\left(2 \times M \times N/2\right)$ used to generate the chaotic sequences in the Bernoulli shift and zigzag maps, and the DNA encoding and decoding operations. With an $M \times N$ image size for gray scale images,

Table 7 Comparative analysis

Method	Metric					
	Correlation coefficient			NPCR	UACI	Entropy
	Horizontal	Vertical	Diagonal			
Proposed	– 0.0016	0.0043	– 0.0061	0.9964	0.3343	7.9972
Wang et al. [31]	0.0038	0.0094	– 0.0189	0.6577	0.1874	7.9932
Dridi et al. [8]	0.0015	0.0026	0.0011	0.9951	0.3342	7.9951
Parvees et al. [23]	0.0067	– 0.0026	0.0032	0.9964	0.3335	7.8917

the complexity for DNA coding is $\Theta(M \times N)$. Furthermore, the XOR operations between encoded image and key matrices on row basis has a complexity of $\Theta(2 \times M \times N)$.

4.7 Comparative Analysis

The performance of encryption algorithms is largely dependent on various factors including memory size, CPU structure, operating system, programming language , programming skills, e.t.c. As such, comparing algorithms using different experimentation environments might not be very accurate. Notwithstanding, we compare our scheme with some algorithms using CT scan image of size 256 × 256. Table 7 gives a summary of our comparison. It is clear from the table that our algorithm meets state-of-the-art standards. This is further evident when compared to results reported in other works including [5, 12, 15]. Besides, the architecture of our scheme makes it possible to implement it using a parallel approach so as to improve performance; which is not possible with most existing methods.

4.8 Application to Colour Medical Images

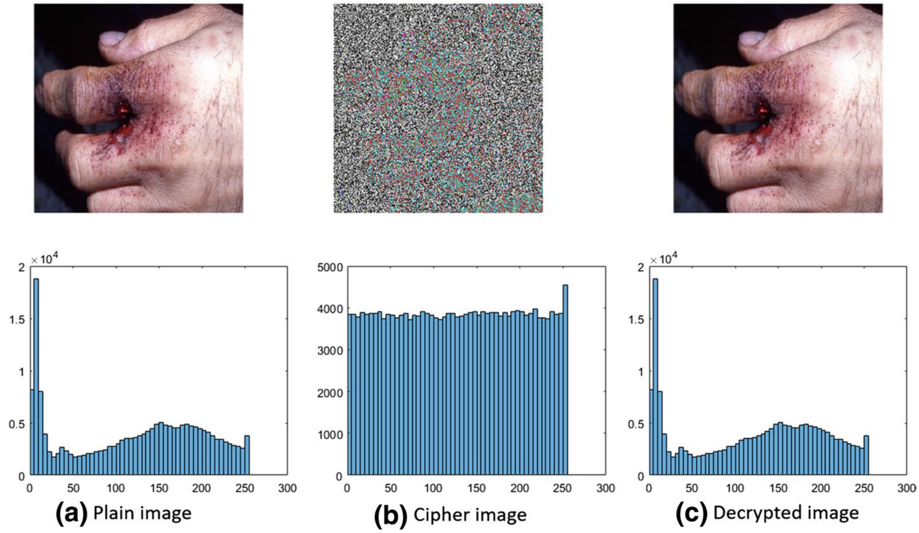
We apply our proposed scheme to encrypt true colour medical images. With the colour images, the red, green and blue (RGB) channels are extracted and encrypted separately as gray images using the same ASCII string (as used for gray scale images) and the MD5 hash value of the colour image (full image) as initial seeds for each channel. The encrypted channels are then recomposed into the encrypted colour image. We herein summarize our experimental results using an image of dimensions 256 × 256.

4.8.1 Histogram Analysis

We analyse the histograms of the full image and the three colour channels. From the graphs in Figs. 8 and 9 it is clear that, our scheme evenly distributes pixels in a true colour image, hence is robust against statistical attacks.

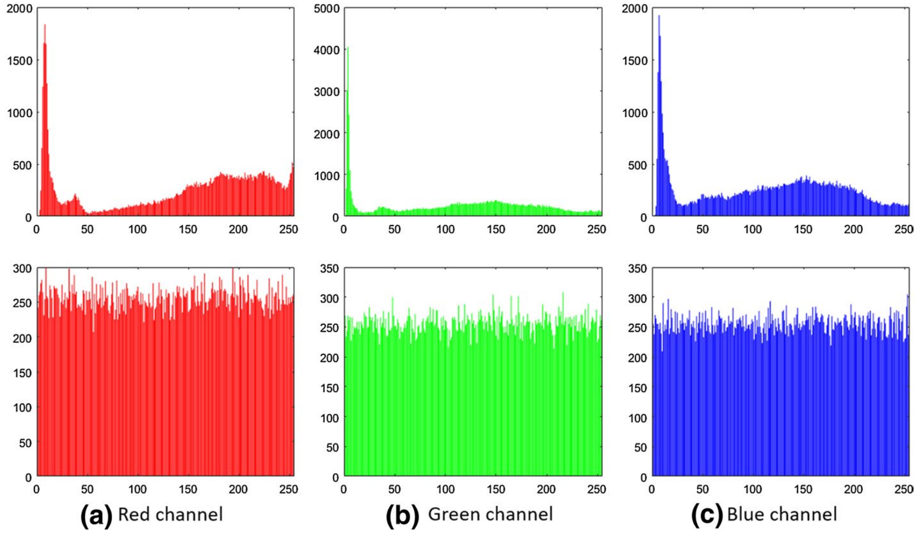
4.8.2 Correlation Analysis

To resist statistical attacks, cipher images must reduce or totally eliminate correlations between the adjacent pixels of the various channels of the true colour image. This eventually results in similar reduction or elimination of correlations in the true colour image. The



(a) Plain image (b) Cipher image (c) Decrypted image

Fig. 8 Histograms of plain, cipher and deciphered true colour images



(a) Red channel (b) Green channel (c) Blue channel

Fig. 9 Histograms of plain and cipher RGB channels

correlation analysis results are given in Table 8. It is clear from the table that, our scheme breaks the correlation between adjacent pixels in colour images as well, thus it can resist statistical attacks.

Table 8 Correlation values of true colour image

Image	Correlation coefficient					
	Plain			Cipher		
	Horizontal	Vertical	Diagonal	Horizontal	Vertical	Diagonal
Red channel	0.9926	0.9926	0.9872	– 0.0027	– 0.0031	0.0010
Green channel	0.9861	0.9878	0.9787	– 0.0037	– 0.0034	0.0051
Blue channel	0.9799	0.9826	0.9701	– 0.0021	0.0005	0.0054

Table 9 Information entropy, NPCR and UACI

Image channel	Information entropy		NPCR	UCAI
	Plain	Cipher		
Red channel	7.5790	7.9976	0.9961	0.3337
Green channel	7.5249	7.9972	0.9961	0.3337
Blue channel	7.7145	7.9968	0.9961	0.3340

4.8.3 Differential Analysis

To measure the resistance of our scheme to differential cryptanalysis when applied to colour images, we made a slight change in the plain colour medical image before extracting the different channels for encryption. We then measured the NPCR and UACI of the RGB channels. The results, as given in Table 9 show that the scheme provides resistance to differential attacks when applied to colour images.

4.8.4 Information Entropy

We test for the randomness and the unpredictability of information of cipher colour images by testing the different colour channels. As seen from Table 9, the entropies of all channels are close to 8, the ideal value. Hence our scheme is resistant to entropy attacks when used for colour images.

5 Conclusion

We have proposed a medical image encryption scheme based on hybrid chaotic DNA diffusion in this paper. The scheme combines multiple chaotic systems, MD5 hash function and DNA XOR algebraic operation. Two chaotic systems are first used to produce two encryption key matrices driven by an external key and a hash value of the plain image. This makes the key sequences partly dependent on the plain image, thus resulting in significant changes in cipher images when there are small changes in the plain image. The key matrices and the image matrix are encoded into DNA sequences followed by a row-by-row DNA diffusion operation in an alternating pattern of key application. The DNA encoding and decoding rules are randomly determined by a chaotic system. Experimental results have demonstrated our scheme's robustness against various forms of attack and is comparable to state-of-the-art medical imaging security standards. Based on the architecture of our scheme, we explore its applicability in a parallel approach in the future to enhance performance.

Acknowledgements This paper was supported by the National Natural Science Foundation of China (Grant No. 61370073), the National High Technology Research and Development Program of China (Grant No. 2007AA01Z423), the project of Science and Technology Department of Sichuan Province.

Compliance with ethical standards

Conflicts of Interest All authors declare that they have no conflict of interest.

References

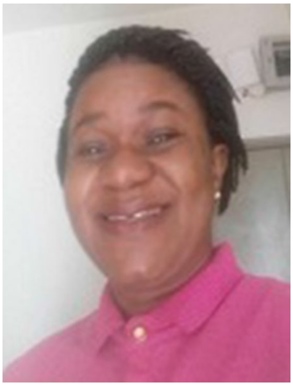
1. Al-Husainy, M. A. F. (2012). A novel encryption method for image security. *International Journal of Security and Its Applications*, *6*(1), 1–8.
2. Alvarez, G., & Li, S. (2006). Some basic cryptographic requirements for chaos-based cryptosystems. *International Journal of Bifurcation and Chaos*, *16*(08), 2129–2151.
3. Andrecut, M. (1998). Logistic map as a random number generator. *International Journal of Modern Physics B*, *12*(09), 921–930.
4. Belazi, A., El-Latif, A. A. A., & Belghith, S. (2016). A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Processing*, *128*, 155–170.
5. Chai, X., Chen, Y., & Broyde, L. (2017). A novel chaos-based image encryption algorithm using DNA sequence operations. *Optics and Lasers in Engineering*, *88*, 197–213.
6. Chakraborty, S., Seal, A., Roy, M., & Mali, K. (2016). A novel lossless image encryption method using dna substitution and chaotic logistic map. *International Journal of Security and Its Applications*, *10*(2), 205–216.
7. Chen, G., Mao, Y., & Chui, C. K. (2004). A symmetric image encryption scheme based on 3d chaotic cat maps. *Chaos, Solitons & Fractals*, *21*(3), 749–761.
8. Dridi, M., Hajjaji, M. A., Bouallegue, B., & Mtibaa, A. (2016). Cryptography of medical images based on a combination between chaotic and neural network. *IET Image Processing*, *10*(11), 830–839.
9. El-Alfy, E. S. M., Thampi, S. M., Takagi, H., Piramuthu, S., & Hanne, T. (2015). *Advances in Intelligent Informatics*. Berlin: Springer.
10. Enayatifar, R., Abdullah, A. H., & Isnin, I. F. (2014). Chaos-based image encryption using a hybrid genetic algorithm and a DNA sequence. *Optics and Lasers in Engineering*, *56*, 83–93.
11. Enayatifar, R., Abdullah, A. H., & Lee, M. (2013). A weighted discrete imperialist competitive algorithm (WDICA) combined with chaotic map for image encryption. *Optics and Lasers in Engineering*, *51*(9), 1066–1077.
12. Enayatifar, R., Sadaei, H. J., Abdullah, A. H., Lee, M., & Isnin, I. F. (2015). A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata. *Optics and Lasers in Engineering*, *71*, 33–41.
13. de la Fraga, L. G., Torres-Pérez, E., Tlelo-Cuautle, E., & Mancillas-López, C. (2017). Hardware implementation of pseudo-random number generators based on chaotic maps. *Nonlinear Dynamics*, *90*(3), 1661–1670.
14. Gao, H., Zhang, Y., Liang, S., & Li, D. (2006). A new chaotic algorithm for image encryption. *Chaos, Solitons & Fractals*, *29*(2), 393–399.
15. Guesmi, R., Farah, M., Kachouri, A., & Samet, M. (2016). A novel chaos-based image encryption using DNA sequence operation and secure hash algorithm SHA-2. *Nonlinear Dynamics*, *83*(3), 1123–1136.
16. Hermassi, H., Belazi, A., Rhouma, R., & Belghith, S. M. (2014). Security analysis of an image encryption algorithm based on a DNA addition combining with chaotic maps. *Multimedia tools and applications*, *72*(3), 2211–2224.
17. Huang, X., & Ye, G. (2014). An image encryption algorithm based on hyper-chaos and DNA sequence. *Multimedia tools and applications*, *72*(1), 57–70.
18. Liu, Y., Tang, J., & Xie, T. (2014). Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map. *Optics & Laser Technology*, *60*, 111–115.
19. Maheshkar, S., et al. (2017). Region-based hybrid medical image watermarking for secure telemedicine applications. *Multimedia Tools and Applications*, *76*(3), 3617–3647.

20. Mao, Y., Chen, G. (2005) Chaos-based image encryption. In *Handbook of Geometric Computing*. Springer, Berlin, Heidelberg
21. Murillo-Escobar, M., Cruz-Hernández, C., Cardoza-Avendaño, L., & Méndez-Ramírez, R. (2017). A novel pseudorandom number generator based on pseudorandomly enhanced logistic map. *Nonlinear Dynamics*, *87*(1), 407–425.
22. Norouzi, B., Mirzakuchaki, S., & Norouzi, P. (2017). Breaking an image encryption technique based on neural chaotic generator. *Optik-International Journal for Light and Electron Optics*, *140*, 946–952.
23. Parvees, M. M., Samath, J. A., & Bose, B. P. (2016). Secured medical images-a chaotic pixel scrambling approach. *Journal of medical systems*, *40*(11), 232.
24. Parvin, Z., Seyedarabi, H., & Shamsi, M. (2016). A new secure and sensitive image encryption scheme based on new substitution with chaotic function. *Multimedia Tools and Applications*, *75*(17), 10631–10648.
25. Phatak, S., & Rao, S. S. (1995). Logistic map: A possible random-number generator. *Physical review E*, *51*(4), 3670.
26. Praveenkumar, P., Devi, N. K., Ravichandran, D., Avila, J., Thenmozhi, K., Rayappan, J. B. B., et al. (2017). Transreceiving of encrypted medical image: A cognitive approach. *Multimedia Tools and Applications*, *77*(7), 8393–8418.
27. Ravichandran, D., Praveenkumar, P., Rayappan, J. B. B., & Amirtharajan, R. (2016). Chaos based crossover and mutation for securing DICOM image. *Computers in Biology and Medicine*, *72*, 170–184.
28. ur Rehman, A., Liao, X., Kulsoom, A., & Abbas, S. A. (2015). Selective encryption for gray images based on chaos and DNA complementary rules. *Multimedia Tools and Applications*, *74*(13), 4655–4677.
29. Sankpal, P.R., & Vijaya, P. (2014). Image encryption using chaotic maps: A survey. In *2014 Fifth International Conference on Signal and Image Processing (ICSIP)* (pp. 102–107). IEEE
30. Shannon, C. E. (1949). Communication theory of secrecy systems. *Bell Labs Technical Journal*, *28*(4), 656–715.
31. Wang, H., Ye, J. M., Liang, H. F., & Miao, Z. H. (2017). A medical image encryption algorithm based on synchronization of time-delay chaotic system. *Advances in Manufacturing*, *5*(2), 158–164.
32. Wang, X., & Liu, C. (2017). A novel and effective image encryption algorithm based on chaos and DNA encoding. *Multimedia Tools and Applications*, *76*(5), 6229–6245.
33. Wang, X. Y., Yang, L., Liu, R., & Kadir, A. (2010). A chaotic image encryption algorithm based on perceptron model. *Nonlinear Dynamics*, *62*(3), 615–621.
34. Watson, J. D., & Crick, F. (1974). Molecular structure of nucleic acids: A structure for deoxyribose nucleic acid. *Nature*, *248*(5451), 765.
35. American National Standards Institute/Institute of Electrical and Electronics Engineers (1985). IEEE standard for binary floating-point arithmetic. In *ANSI/IEEE Std 754–1985* (pp. 754–1985). New York
36. Zhan, K., Wei, D., Shi, J., & Yu, J. (2017). Cross-utilizing hyperchaotic and DNA sequences for image encryption. *Journal of Electronic Imaging*, *26*(1), 013,021–013,021.
37. Zhang, Q., Guo, L., & Wei, X. (2010). Image encryption using DNA addition combining with chaotic maps. *Mathematical and Computer Modelling*, *52*(11), 2028–2035.
38. Zhang, X., Wang, H., & Xu, C. (2019). Identity-based key-exposure resilient cloud storage public auditing scheme from lattices. *Information Sciences*, *472*, 223–234.
39. Zhang, X., & Xu, C. (2018). Trapdoor security lattice-based public-key searchable encryption with a designated cloud server. *Wireless Personal Communications*, *100*(3), 907–921.
40. Zhang, X., Xu, C., Mu, L., & Zhao, J. (2018). Identity-based encryption with keyword search from lattice assumption. *China Communications*, *15*(4), 164–178.

Publisher's Note Springer Nature remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

Joshua C. Dagadu is affiliated to the International Centre for Wavelet Analysis and Its Applications, School of Computer Science and Engineering, University of Electronic Science and Technology of China. His research interests include information security, medical imaging, signal processing, wavelet analysis and cloud computing.

Jian-Ping Li received his Ph.D. in Computer Science from Chongqing University (1998). He is currently a professor in the School of Computer Science and Engineering, University of Electronic Science and Technology of China; Director of International Centre for Wavelet Analysis and Its Applications; Chief Editor of International Computer Conference on Wavelet Active Media Technology and Information Processing. His research interests include wavelet theory and applications, fractals, image processing, pattern recognition, information security, electronic commerce, and optimization techniques of information acquisition and processing.



Emelia O. Aboagye is a Ph.D. candidate in the School of Computer Science and Engineering, University of Electronic Science and Technology of China. Her research interests include machine learning, big data processing, business intelligence and cloud computing.