Medical Image Encryption Scheme Based on Multiple Chaos and DNA Coding

Joshua C. Dagadu[1], Jianping Li[1], Emelia O. Aboagye[1] and Faith K. Deynu[2]
(Corresponding author: Joshua C. Dagadu)

School of Computer Science and Engineering, University of Electronic Science and Technology of China[1]
School of Communication and Information Engineering, University of Electronic Science and Technology of China[2]
No. 2006, Xiyuan Ave. West Hi-Tech, Chengdu 611731, China
(Email: joscaldag@yahoo.com)
(Received Sept. 4, 2017; revised and accepted Nov. 28, 2017)

Abstract

The combination of chaos and deoxyribonucleic acid (DNA) coding for image encryption in recent times has proven to provide robust security for images. In this paper, an encryption scheme based on multiple chaos and DNA coding is proposed for gray scale medical images. The chaotic tent map is used to generate chaotic key stream and the logistic map is used to randomly select DNA encoding and decoding rules. The chaotic key and the plain medical image are first encoded into DNA sequences. A selected DNA algebraic operation (addition/subtraction/XOR) is carried out between the plain image DNA sequence and the key DNA sequence; the outcome is then decoded to obtain the cipher image. The process is carried out both on row and column bases to achieve a robust cipher. The initial experimental results show that the scheme demonstrates strong resistance against diverse forms of attacks.

Keywords: DNA Coding; Encryption; Logistic Map; Medical Image; Tent Map

1 Introduction

The advent of remote healthcare delivery, fueled by modern technologies such as telemedicine, telesurgery and teleradiology exposes medical data, not excepting medical images, to security vulnerabilities; as these images are transmitted over public digital communication networks [21] and are stored in networked storage facilities to be used for clinical interpretation and diagnosis. Schemes used in securing medical images are expected to achieve high degrees of resistance against security attacks without compromising the diagnostic quality of the images after decryption. This is because alterations made to medical images during processing, may result in irreversible wrong diagnostic consequences. Though the conventional encryption schemes such as Rivest-Shamir-Adleman (RSA), data encryption standard (DES) and advanced encryption standard (AES) have been employed in encrypting medical images [20], these schemes have not been found very efficient due to certain intrinsic properties of images including high redundancy, bulk data capacity and high correlation among adjacent pixels [1, 28]. Consequently, chaos based schemes have been extensively proposed in current research [6, 12, 16, 18].

Chaotic systems exhibit random behavior and have inherent features such as ergodicity, unpredictability and sensitivity to initial conditions. A chaotic dynamical system is not predictable and resembles noise [29]. This provides a close relationship between chaotic dynamical systems and cryptosystems. The sensitivity to initial conditions property of chaos is used for keys in cryptosystems while the topological transitivity property which ensures the ergodicity of chaos maps, is linked to the diffusion feature of cryptosystems [22]. This has led to the use of chaos maps in numerous image encryption schemes [4, 6].

However, chaos-based encryption does not always provide a high degree of security [5, 23, 38], due to weak diffusion functions, weakness against chosen and known plaintext attacks and poor statistical properties of some chaos maps [8, 13, 24]. The quest for more robust image cryptosystems has resulted in the combination of chaos maps and other algorithms such as cellular automata [31, 32], DNA coding [15, 19, 35] and other forms of combinations [12, 16, 33] for image encryption schemes.

DNA has been applied to chaotic systems recently due to its properties such as huge storage, massive parallelism and low power consumption [40]. The chaotic tent map was explored for a cryptosystem recently [17]. It is found to have high complexity and the sequences generated have high randomness. Besides, it is highly sensitive to changes in the initial condition. In [17], it was applied directly to the plain image to produce the cipher image. Obviously, with such a scheme, once the initial condition and control parameter are known by an adversary, it is easy to break. In this paper, we combine the chaotic tent map with DNA

coding to encrypt medical images. We first generate the initial condition of the tent map and produce the encryption key using the map. We then apply randomly selected DNA encoding/decoding rules and DNA algebraic operations to produce the cipher image.

The rest of the paper has the following organization: In Section 2, we give overviews of logistic map, tent map and DNA coding. We present our proposed scheme in Section 3, discuss experimentation and results in Section 4 and finally conclude in Section 5.

2 Preliminaries

We give overviews of the chaos maps (logistic map and tent map) and DNA coding in this section.

2.1 Logistic Map

The logistic map is a polynomial mapping of degree 2. It is often cited as a typical example of how very simple nonlinear dynamical systems can result in complex chaotic behaviors [7]. It is one of the simple systems that exhibit order to chaos transition and possesses many properties required of a pseudorandom number generator (PRNG) [25]. The main criterion that distinguishes different PRNGs is usually the quality of randomness. Moreover, the quality of randomness, implementation cost and throughput are essential factors to evaluate the effectiveness of PRNGs in applications [9]. 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:

$$x_{i+1} = u x_i \left(1 - x_i\right), \tag{1}$$

where $u \in (0, 4)$, $x \in (0, 1)$ and i is the iteration. The logistic map is in a chaotic condition when the control parameter is [3.57, 4.0] as shown in Figure 1.

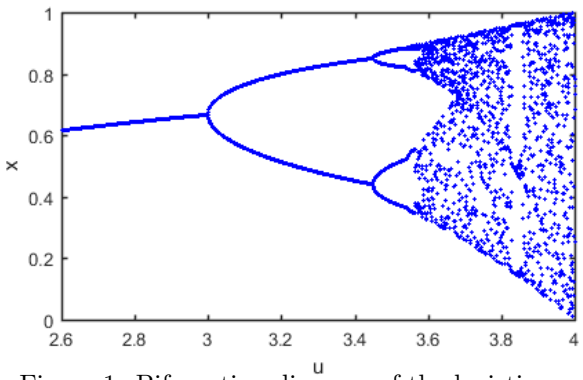


Figure 1: Bifurcation diagram of the logistic map

2.2 Tent Map

The tent map is one of the simplest chaotic maps. It is a one-dimensional and piecewise linear map [14]. The chaotic behaviors of this map were studied in terms of the unchanging density and the power spectrum over its entire chaotic region in [39]. It was realized that as the height of the maximum is reduced, band-splitting change processes that follow in an uninterrupted sequence occur in the chaotic region and accumulate to the transition point into the non-chaotic region. The map is topologically conjugate, thus its behaviors are in this sense, identical under iteration [17]. It is mathematically expressed as:

$$x_{n+1} = f\left(x_n, r\right), \tag{2}$$

$$f\left(x_n, r\right) = \begin{cases} f_L\left(x_n, r\right) = r x_n, & if\ x_n < 0.5 \\ f_R\left(x_n, r\right) = r\left(1 - x_n\right), & otherwise \end{cases} \tag{3}$$

where $x_n \in [0, 1]$ for $n \geq 0$. The map transforms an interval $[0, 1]$ onto itself and has only one control parameter r contained in it; where $r \in [0, 2]$. x_0 is the initial condition of the chaotic map and the set of real values $x_0, x_1, \cdots, x_n, \cdots$ are the orbits of the system [17].

Depending on r, the system exhibits a range of behaviors from predictable to chaotic. When 1000 r values from $r = 0.1$ to $r = 2$ with $x_0 = 0.03$ are plotted, it results in the distribution shown in Figure 2.

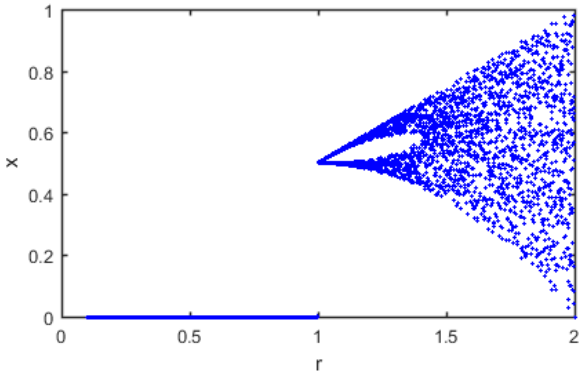


Figure 2: Tent map with r values from 0.1 to 2

When 1000 r values from $r = 1.999999$ to $r = 2$ with $x_0 = 0.03$ are plotted, it results in the distribution shown in Figure 3.

2.3 DNA Coding

DNA sequence has become extremely useful for basic biological research and in diverse applied fields such as diagnostic, forensics and biological systematics [11], not excepting computer science. DNA sequence composes 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 [27]. That is, the purine Adenine always pairs with the pyrimidine Thymine and the purine Guanine always pairs with the pyrimidine Cytosine, according to the

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)

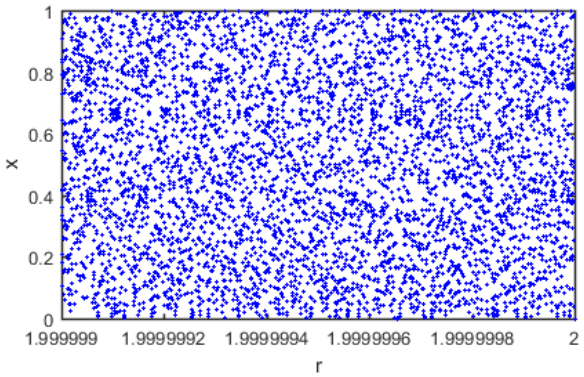


Figure 3: Tent map with r values from 0.999999 to 2

rules of base pairing by Watson and Crick [37] as shown in Table 1.

In the binary system, 0 and 1 are complementary; similarly, 00 and 11 are complementary, 01 and 10 are also complementary. Mapping the two-bit binary system to the DNA bases, 24 rule sets can be obtained [27]. 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 [34] as shown in Table 2.

Table 2: DNA coding 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

Some algebraic operations can be performed on DNA sequences. Tables 3, 4 and 5 show the XOR, addition and subtraction operations respectively. In order to enhance the diffusion phase in encryption, these operations are employed.

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 150 for instance, its 8-bit binary sequence is (10010110). Using DNA encoding rule 4 from Table 2, (ATTA) is obtained. Decoding (ATTA) with the same rule 4 gives (10010110). Any other rule used to decode it would give a different binary value. Taking two DNA sequences (ATTC) and (GAGT), applying one type of addition operation on them would result in (GTAG). Subtracting (GAGT) from (GTAG) would give back (ATTC).

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

Table 4: DNA addition

+	A	G	C	T
A	A	G	C	T
G	G	C	T	A
C	C	T	A	G
T	T	A	G	C

Table 5: DNA subtraction

-	A	G	C	T
A	A	T	C	G
G	G	A	T	C
C	C	G	A	T
T	T	C	G	A

3 The Proposed Scheme

The block diagram of the proposed scheme is given in Figure 4. The user inputs the plain medical image and an initial key string of 16 ASCII characters. This key is preprocessed to generate the initial conditions of the two chaos maps. The logistic map is used to select the DNA encoding and decoding rules while the tent map is used to generate the pseudorandom key stream. Both the image and key stream are encoded into DNA sequences followed by a DNA algebraic operation between them. The resultant sequence is decoded to produce the cipher image. The encryption phase is carried out on both row and column bases as in [36].

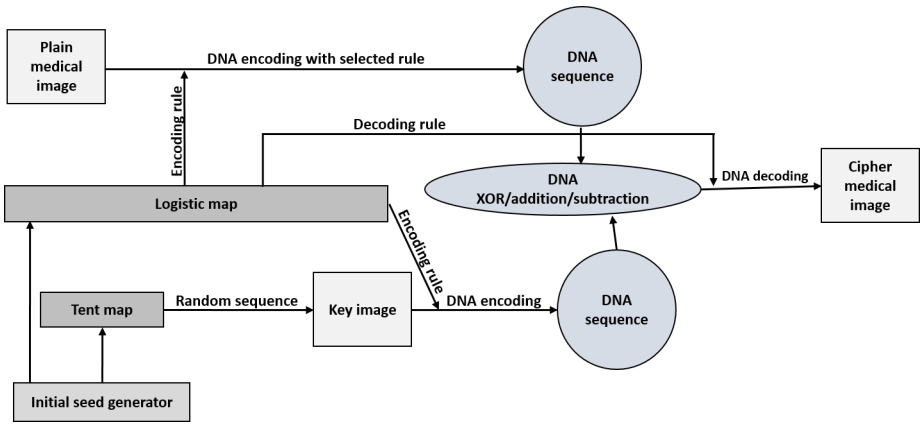


Figure 4: Block diagram of proposed scheme

3.1 Key Generation

Step 1: Enter a key length of 16 ASCII characters made up of 128 bits

$$K = K_1, K_2, K_3, \cdots, K_{16} \tag{4}$$

where $K_i = b_1, b_2, \cdots, b_8$ and $i = 1, 2, \cdots, 16$.

Step 2: Convert the first 8 characters of K into their hexadecimal form

$$\alpha = h_1, h_2, \cdots, h_{16} \tag{5}$$

Step 3: Add the hexadecimal values as

$$x_1 = \left(\sum_{i=1}^{16} (h_i)_{10} \right) \Big/ 256 \tag{6}$$

Step 4: Convert the last 8 characters of K into binary form as

$$\beta = b_1, b_2, \cdots, b_{64} \tag{7}$$

Step 5: Add the binary values β as

$$x_2 = \left(\sum_{i=1}^{64} \left(b_i \times 2^i \right) \right) \Big/ 2^{64} \tag{8}$$

Step 6: Get the initial condition as

$$x_0 = \mathrm{mod}\left((x_1 + x_2), 1 \right) \tag{9}$$

where $x_0 \in [0, 1]$ (suitable for both logistic and tent maps).

Step 7: Choose the control parameter r for the tent map, where $r \in [0, 2]$.

Step 8: Using x_0 and r, iterate Equation (3) (*i.e.* the tent map) MN times to generate the pseudorandom bit sequence X where M and N are the dimensions of the medical image.

Step 9: The chaotic sequence ($X = \{x_1, x_2, x_3, \cdots, x_{MN}\}$). For each $x_i \in X$, convert into integer sequence to generate the key image $Q = \{Q_1, Q_2, Q_3, \cdots, Q_{MN}\}$ as

$$Q_i = \mathrm{mod}\left(floor\left(x_i \times 10^{14} \right), 256 \right) \tag{10}$$

where $Q_i \in Q$.

3.2 Encryption

Step 1: Read in the plain medical image I.

Step 2: Get the dimensions M and N of I and use to generate the key image as described in Section 3.1.

Step 3: Using the initial condition x_0 generated as in Section 3.1 and parameter $u \in [3.57, 4]$, which is user defined, iterate equation 1 (*i.e.* the Logistic map) M times to obtain new values of x.

Step 4: For each iteration, preprocess x as

$$X = floor\left(x \times 7 \right) + 1. \tag{11}$$

Step 5: Select the DNA encoding rule corresponding to X and encode all the pixels on the row with the selected rule to obtain the DNA sequence of the plain medical image.

Step 6: Repeat Steps 3 to 5 for the key image to get the DNA sequence of the key image Q.

Step 7: Select the DNA algebraic operation ($\oplus / + / -$) using

$$Y = floor\left(x \times 3 \right) + 1. \tag{12}$$

Step 8: Perform the selected operation Y between the corresponding rows in the plain image DNA sequence and the key DNA sequence to get I'.

Step 9: Decode I' on row basis using selected decoding rules as in Step 5 to get ϕ'.

Step 10: Repeat Steps 3 to 9 on column basis of ϕ' to produce the cipher medical image ϕ.

The decryption process works similar to the encryption process in the reverse order with the DNA reverse operations, taking in as input, the same initial key string of 16 ASCII characters, the control parameters of the chaos maps and the cipher image.

4 Experimentation and Results

4.1 Experimental Setup

The experiment is carried out on a personal computer with Intel core i5, 2.6GHz CPU, 4GB memory, windows 10 and MATLAB 2016b. A number of gray scale medical images of diverse modalities and sizes are used in the experiment. Four of the images: CT scan and MRI images with dimensions (256×256), and X-ray and Ultrasound images with dimensions (512×512) are presented in this paper. For our experiment, we use an external key $K =' D3A4C1CB687EAF8C'$ to generate the initial condition x_0 of both chaos maps. Control parameters r of 1.999999 for the tent map and u of 3.99999999 for the logistic map are used. Correlation analysis, histogram analysis, key space and information entropy are the evaluation metrics used to assess the security strength of the proposed scheme.

4.2 Histogram Analysis

An efficient image cryptosystem should have a uniform histogram distribution so as to make it impossible for attackers to extract any meaningful information from the encrypted image; since the image histogram reveals the pixel value distribution within the image.

Figures 5, 6, 7 and 8 show the histogram plots for our test images. It is evident from these plots that the proposed scheme uniformly distributes pixel values in the cipher images hence has the capability to resist cipher only attacks.

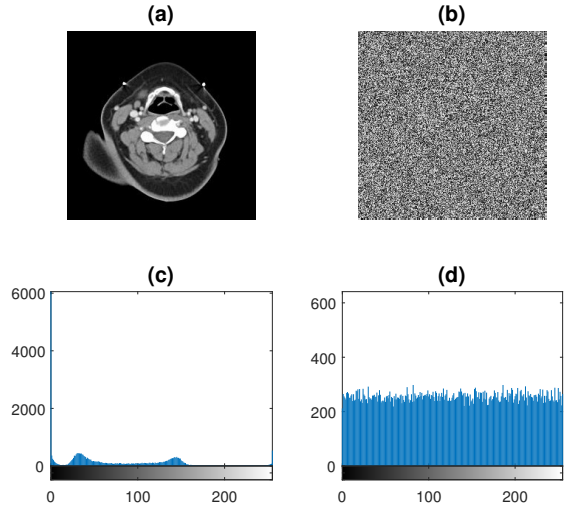


Figure 5: Histograms of plain and encrypted CT scan images. (a) Plain image, (b) Cipher image, (c) Histogram of plain image, (d) Histogram of cipher image.

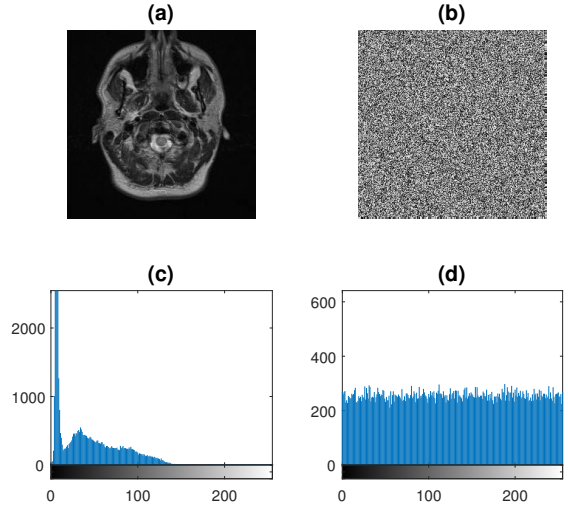


Figure 6: Histograms of plain and encrypted MRI images. (a) Plain image, (b) Cipher image, (c) Histogram of plain image, (d) Histogram of cipher image.

4.3 Correlation Analysis

The correlation coefficients of adjacent pixels of an image provide information about the image. In images, the horizontal, vertical and diagonal correlations between pixels are high. Encryption algorithms must reduce these relationships among the adjacent pixels in the cipher image. The correlation coefficients among adjacent pixels is calculated with following equations:

$$
\begin{aligned}
E(x) &= \frac{1}{N}\sum_{i=1}^{N} x_i \\
D(x) &= \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))^2 \\
\operatorname{cov}(x,y) &= \frac{1}{N}\sum_{i=1}^{N} (x_i - E(x))(y_i - E(y)) \\
r_{xy} &= \frac{\operatorname{cov}(x,y)}{\sqrt{D(x) \times \sqrt{D(y)}}}.
\end{aligned}
$$

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 select 2000 pairs of adjacent pixels from both original and encrypted images and calculate their horizontal, vertical and diagonal correlation coefficients. It is evident from Table 6 and Figure 9 that that the proposed scheme adequately breaks the correlation among adjacent pixels; hence is robust enough against statistical attacks.

4.4 Information Entropy

Information entropy is a mathematical property that reflects the randomness and the unpredictability of infor-

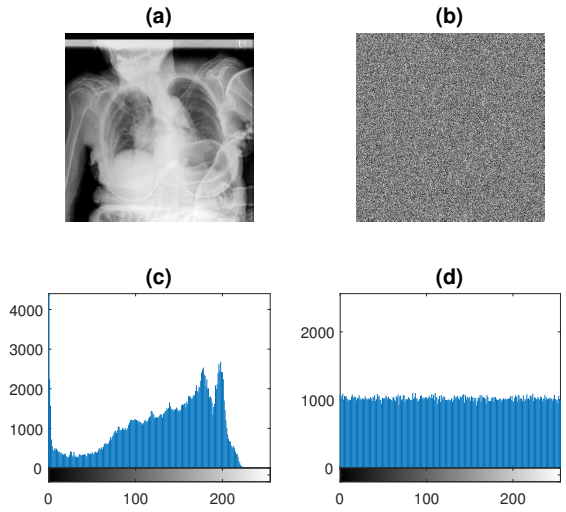


Figure 7: Histograms of plain and encrypted X-ray images. (a) Plain image, (b) Cipher image, (c) Histogram of plain image, (d) Histogram of cipher image.

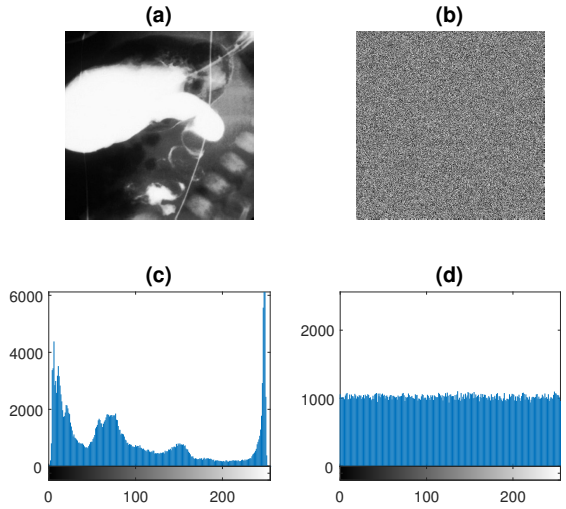


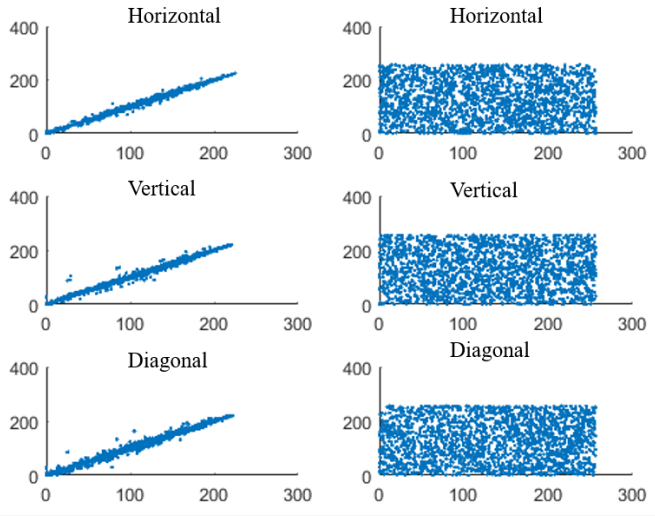
Figure 8: Histograms of plain and encrypted ultrasound images. (a) Plain image, (b) Cipher image, (c) Histogram of plain image, (d) Histogram of cipher image.

Table 6: Correlation coefficients of adjacent pixels

Test image	Format	Correlation Coefficients		
		Horizontal	Vertical	Diagonal
CT (256 × 256)	Original	0.975312	0.974458	0.955728
	Cipher	-0.001043	0.000512	0.003564
MRI (256 × 256)	Original	0.963534	0.965572	0.941237
	Cipher	-0.009193	-0.004846	-0.001906
Ultrasound (512 × 512)	Original	0.998894	0.998637	0.997181
	Cipher	-0.001084	0.000350	0.002023
X-Ray (512 × 512)	Original	0.998516	0.996325	0.994887
	Cipher	-0.001091	0.000924	0.002773

mation [30]. It is given as

$$H(m) = \sum_{i=0}^{2^N-1} p(m_i) \log \frac{1}{p(m_i)} \quad (13)$$



(a) Plain (b) Cipher

Figure 9: Correlation between adjacent pixels of plain and cipher X-ray images

where N is the total number of symbols $m_i \in m$; $p(m_i)$ 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 source is said to be random in which case $H(m)$ is equal to 8; the ideal situation. As seen from Table 7, the entropy values of all test images are very close to the ideal value giving an indication that there is negligible information leakage during encryption hence strong resistance against entropy attacks.

Table 7: Information entropy

Test Image	Information Entropy	
	Original Image	Cipher image
CT (256 × 256)	3.985490	7.997302
MRI (256 × 256)	5.604739	7.997444
Ultrasound (512 × 512)	7.032954	7.999336
X-Ray (512 × 512)	7.332680	7.999365

4.5 Key Space

The control parameters and the initial value used for the logistic map and the tent map to generate the pseudorandom bits form the set for the key space. We generated the initial condition from an external input key of size 128 bits. The computational precision of the 64-bit double precision number is about 10^{-15}, according to the IEEE floating-point standard [26]. 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^{128} which is adequate to resist brute-force attacks.

5 Conclusion

An encryption scheme based on multiple chaos and DNA coding have been proposed for gray scale medical images. The chaotic tent map is used to generate chaotic key stream which is encoded into DNA sequence for pixel value modification. The logistic map is used to randomly select DNA encoding/decoding rules and the DNA algebraic operation. The pixels of an input medical image are encoded into DNA sequence; which is followed by a randomly selected DNA algebraic operation between the plain medical image DNA sequence and the key DNA sequence. The resulting DNA sequence of the algebraic operation is then randomly decoded to obtain the cipher image. The process is carried out both on row and column bases to achieve a robust cipher. The reverse process successfully decrypts the cipher image. Simulation outcomes and performance analyses: histogram analysis, correlation analysis, entropy analysis and key space analysis show that the scheme demonstrates strong resistance against diverse forms of attacks, hence it is reliable for medical image encryption.

Acknowledgments

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.

References

[1] M. A. F. Al-Husainy, "A novel encryption method for image security," *International Journal of Security and Its Applications*, vol. 6, no. 1, 2012.

[2] G. Alvarez and S. Li, "Some basic cryptographic requirements for chaos-based cryptosystems," *International Journal of Bifurcation and Chaos*, vol. 16, no. 08, pp. 2129–2151, 2006.

[3] M. Andrecut, "Logistic map as a random number generator," *International Journal of Modern Physics B*, vol. 12, no. 09, pp. 921–930, 1998.

[4] S. S. Askar, A. A. Karawia, and A. Alshamrani, "Image encryption algorithm based on chaotic economic model," *Mathematical Problems in Engineering*, vol. 2015, 2015.

[5] R. Bechikh, H. Hermassi, A. A. A. El-Latif, R. Rhouma, and S. Belghith, "Breaking an image encryption scheme based on a spatiotemporal chaotic system," *Signal Processing: Image Communication*, vol. 39, pp. 151–158, 2015.

[6] A. Belazi, A. A Abd El-Latif, and Safya Belghith, "A novel image encryption scheme based on substitution-permutation network and chaos," *Signal Processing*, vol. 128, pp. 155–170, 2016.

[7] S. Chakraborty, A. Seal, M. Roy, and K. Mali, "A novel lossless image encryption method using dna substitution and chaotic logistic map," *International Journal of Security and Its Applications*, vol. 10, no. 2, 2016.

[8] G. Chen, Y. Mao, and C. K. Chui, "A symmetric image encryption scheme based on 3d chaotic cat maps," *Chaos, Solitons & Fractals*, vol. 21, no. 3, pp. 749–761, 2004.

[9] S. L. Chen, T. T. Hwang, and W. W. Lin, "Randomness enhancement using digitalized modified logistic map," *IEEE Transactions on Circuits and Systems II: Express Briefs*, vol. 57, no. 12, pp. 996–1000, 2010.

[10] M. El-Sayed, El-Alfy, S. M. Thampi, H. Takagi, S. Piramuthu, and T. Hanne, *Advances in Intelligent Informatics*, 2015. ISBN:3319112171 9783319112176.

[11] R. Enayatifar, A. H. Abdullah, and I. F. Isnin, "Chaos-based image encryption using a hybrid genetic algorithm and a dna sequence," *Optics and Lasers in Engineering*, vol. 56, pp. 83–93, 2014.

[12] R. Enayatifar, H. J. Sadaei, A. H. Abdullah, M. Lee, and I. F. Isnin, "A novel chaotic based image encryption using a hybrid model of deoxyribonucleic acid and cellular automata," *Optics and Lasers in Engineering*, vol. 71, pp. 33–41, 2015.

[13] H. Gao, Y. Zhang, S. Liang, and D. Li, "A new chaotic algorithm for image encryption," *Chaos, Solitons & Fractals*, vol. 29, no. 2, pp. 393–399, 2006.

[14] T. Habutsu, Y. Nishio, Iwao Sasase, and Shinsaku Mori, "A secret key cryptosystem by iterating a chaotic map," in *Eurocrypt*, vol. 91, pp. 127–136, 1991.

[15] T. Hu, Y. Liu, L. H. Gong, and C. J. Ouyang, "An image encryption scheme combining chaos with cycle operation for dna sequences," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 51–66, 2017.

[16] C. Jin and H. Liu, "A color image encryption scheme based on arnold scrambling and quantum chaotic.," *International Journal Network Security*, vol. 19, no. 3, pp. 347–357, 2017.

[17] C. Li, G. Luo, K. Qin, and C. Li, "An image encryption scheme based on chaotic tent map," *Nonlinear Dynamics*, vol. 87, no. 1, pp. 127–133, 2017.

[18] J. Li, Y. Xing, C. Qu, and J. Zhang, "An image encryption method based on tent and lorenz chaotic systems," in *6th IEEE International Conference on Software Engineering and Service Science (ICSESS'15)*, pp. 582–586, 2015.

[19] X. Li, C. Zhou, and N. Xu, "A secure and efficient image encryption algorithm based on dna coding and spatiotemporal chaos," *International Journal Network Security*, vol. 20, no. 1, pp. 110-120, 2018.

[20] G. Lokeshwari, S. Susarla, and S. U. Kumar, "A modified technique for reliable image encryption method using merkle-hellman cryptosystem and rsa algorithm," *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 18, no. 3, pp. 293–300, 2015.

[21] S. Maheshkar *et al.*, "Region-based hybrid medical image watermarking for secure telemedicine applications," *Multimedia Tools and Applications*, vol. 76, no. 3, pp. 36173647, 2017.

[22] Y. Mao and G. Chen, "Chaos-based image encryption," *Handbook of Geometric Computing*, pp. 231–265, 2005.

[23] B. Norouzi, S. Mirzakuchaki, and P. Norouzi, "Breaking an image encryption technique based on neural chaotic generator," *Optik-International Journal for Light and Electron Optics*, vol. 140, pp. 946–952, 2017.

[24] Z. Parvin, H. Seyedarabi, and M. Shamsi, "A new secure and sensitive image encryption scheme based on new substitution with chaotic function," *Multimedia Tools and Applications*, vol. 75, no. 17, pp. 10631–10648, 2016.

[25] S. C. Phatak and S. S. Rao, "Logistic map: A possible random-number generator," *Physical Review E*, vol. 51, no. 4, pp. 3670, 1995.

[26] Floating point Working Group *et al.*, "Ieee standard for binary floating-point arithmetic," *IEEE Std*, pp. 754–1985, 1985.

[27] P. Praveenkumar, N. K. Devi, D. Ravichandran, J. Avila, K. Thenmozhi, J. B. B. Rayappan, and R. Amirtharajan, "Transreceiving of encrypted medical image–a cognitive approach," *Multimedia Tools and Applications*, pp. 1–26, 2017.

[28] D. Ravichandran, P. Praveenkumar, J. B. B. Rayappan, and R. Amirtharajan, "Chaos based crossover and mutation for securing dicom image," *Computers in Biology and Medicine*, vol. 72, pp. 170–184, 2016.

[29] P. R. Sankpal and P. A. Vijaya, "Image encryption using chaotic maps: a survey," in *Fifth International Conference on Signal and Image Processing (ICSIP'14)*, pp. 102–107, 2014.

[30] C. E. Shannon, "Communication theory of secrecy systems," *Bell Labs Technical Journal*, vol. 28, no. 4, pp. 656–715, 1949.

[31] A. Souyah and K. M. Faraoun, "An image encryption scheme combining chaos-memory cellular automata and weighted histogram," *Nonlinear Dynamics*, vol. 86, no. 1, pp. 639–653, 2016.

[32] W. Srichavengsup and W. San-Um, "Data encryption scheme based on rules of cellular automata and chaotic map function for information security," *International Journal Network Security*, vol. 18, no. 6, pp. 1130–1142, 2016.

[33] Z. Tang, X. Zhang, and W. Lan, "Efficient image encryption with block shuffling and chaotic map," *Multimedia Tools and Applications*, vol. 74, no. 15, pp. 5429–5448, 2015.

[34] A. U. Rehman, X. Liao, A. Kulsoom, and S. A. Abbas, "Selective encryption for gray images based on chaos and dna complementary rules," *Multimedia Tools and Applications*, vol. 74, no. 13, pp. 4655–4677, 2015.

[35] X. Y. Wang, Y. Q. Zhang, and Y. Y. Zhao, "A novel image encryption scheme based on 2-d logistic map and dna sequence operations," *Nonlinear Dynamics*, vol. 82, no. 3, pp. 1269–1280, 2015.

[36] X. Wang and C. Liu, "A novel and effective image encryption algorithm based on chaos and dna encoding," *Multimedia Tools and Applications*, vol. 76, no. 5, pp. 6229–6245, 2017.

[37] J. D. Watson and F. H. Crick, "Molecular structure of nucleic acids: A structure for deoxyribose nucleic acid," *Nature*, vol. 248, no. 4356, pp. 765, Apr. 25, 1953.

[38] W. S. Yap, R. C. W. Phan, W. C. Yau, and S. H. Heng, "Cryptanalysis of a new image alternate encryption algorithm based on chaotic map," *Nonlinear Dynamics*, vol. 80, no. 3, pp. 1483–1491, 2015.

[39] T. Yoshida, H. Mori, and H. Shigematsu, "Analytic study of chaos of the tent map: Band structures, power spectra, and critical behaviors," *Journal of statistical physics*, vol. 31, no. 2, pp. 279–308, 1983.

[40] K. Zhan, D. Wei, J. Shi, and J. Yu, "Cross-utilizing hyperchaotic and dna sequences for image encryption," *Journal of Electronic Imaging*, vol. 26, no. 1, pp. 013021–013021, 2017.

Biography

Joshua C. Dagadu is a Ph.D. candidate in 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.

Jianping 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, UESTC; 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.

Faith K. Deynu is a Ph.D. candidate in the School of Communication and Information Engineering, University of Electronic Science and Technology of China. His research interests include signal processing, wireless communication and optical fiber sensing.