Medical Image Encryption Algorithm based on Dynamic DNA Sequencing and 2D-3D Chaotic Equations

Anwesha Kar and Dilip Kumar Gayen

1 Department of Computer Science & Engineering, College of Engineering & Management, Kolaghat, KTPP Township, West Bengal, 721171, India
e-mail: dilipgayen@yahoo.com

Abstract. Digital images are now widely used in modern clinic diagnosis. The diagnostic images with confidential information related to patients’ privacy are stored and transmitted via public networks. Secured schemes to guarantee confidentiality of patients’ privacy are becoming more and more vital. Medical images are considered as one of the most important and sensitive data in information systems. Sending medical images over the network requires a strong encryption algorithm such that it is resistant against cryptographic attacks. Among the three security objectives for the security of information systems namely confidentiality, integrity and availability, confidentiality is the most important aspect that need to be taken much care for the secure storage and transmission of medical images. This paper proposes an adaptive medical image encryption algorithm based on Dynamic DNA Sequencing and 2D-3D Chaotic Equations that encrypts any medical image with same uniformity and efficiency.

1. Introduction

In this era of Digitalisation, we exchange a lot of personal information through the Internet. A medical image contains sensitive data [1]. To transfer any medical image securely, it must be encrypted and stored which requires developing a strong, secure and efficient encryption algorithm is necessary [2]. The three main features of any security service is confidentiality, integrity and availability. Confidentiality being the most essential criteria for exchanging medical images has to be given utmost priority. Generally medical image encryption algorithm is chaoses based or are based on information entropy [3]. DNA Sequencing has also been gaining popularity. The paper combines the image encryption, chaotic system along with DNA Sequencing to improve the security. This way, it can increase the security of key space and image in a much more efficient way.

2. Chaotic Systems

With the ever increasing demand of requirement of more and more reliable, trustable and strong security for images/videos with confidential information, chaos-based systems have an important method in process of image encryption because of their excellent random properties and encryption performance. Chaos theory is used in various fields of physics, engineering, biology and economy in recent years. Wang et al. have used an extension of fractal Fourier transformation and a digital holographic scheme to propose a cryptographic algorithm [4]. Due to the parameters used in this scheme and security enhancement of the encryption process is very high. A type of complex nonlinear system, chaotic systems have initial value sensitivity, pseudo randomness and non-periodicity, which are consistent with the requirements for cryptography. That can be used to generate random keys, which will have equal encryption effect for all samples. This is not capable of being broken. Thus,
chaotic encryption method is being used in the field of information security, more precisely in the field of image encryption. We introduce a chaotic map, the intertwining logistic map or 3D chaotic equations, which is defined as follows:

\[
\begin{align*}
  x_{n+1} &= [\mu \times k_1 \times y_n \times (1 - x_n) + z] \mod 1 \\
  y_{n+1} &= [(\mu \times k_2 \times y_n + z \times 1) / (1 + (x_n + 1)^2)] \mod 1 \\
  z_{n+1} &= [\mu \times (x_{n+1} + y_{n+1} + k_3) \times \sin (z_n)] \mod 1
\end{align*}
\]

where \( \mu, k_i \) are the system parameters. The 2D Chaotic Equations are defined as:

\[
\begin{align*}
  x_{n+1} &= 1 - ax_n^2 + y_n \\
  y_{n+1} &= bx_n
\end{align*}
\]

where \( a, b \) are constants.

3. DNA Sequence and Dynamic DNA Sequencing

DNA is a carrier of the biological genetic information that is stored in the body. It has a high degree of parallelism, massive storage capacity, and least energy consumption with a unique molecular structure producing a unique molecular recognition mechanism, which determines its excellent information storage and information processing ability enhancing its potential and suitability in the field of information security, information hiding, and authentication, paving a new way for the development of modern cryptography through DNA Sequencing. DNA consists of a linear string of nucleotides, or bases, for simplicity referred to by the first letters of their chemical names-A(Adenosine), T(Thymine), C(Cytosine) and G(Guanine). The process of deducing the order of nucleotides in DNA is called DNA sequencing. A RGB image encryption algorithm based on DNA encoding and chaotic map by Liu et al. proposed [5, 6]. Chai et al proposed an image encryption algorithm based on chaos combined with DNA operations [7]. A type of digital image encryption technology based on hyperchaos mapping and DNA sequence library arithmetic to realize a scrambling position transformation of image pixels and the spread of the pixel values was proposed by Niu et al. [8]. Most algorithms only chose fixed DNA encoding rules to encode with only a maximum of eight experiments can break it. In this paper, the DNA encoding rules are dynamically selected according to the random keys generated through chaotic sequences.

Algorithm:

1. Read the Medical Image
2. Convert Image to Gray scale
3. Form Image Matrix \( I(n \times n) \)
4. Generate the initial values of \( x, y \) and \( z \) for 3D chaotic equation.
   4.1 Take random 72 characters.
   4.2 Convert it into binary sequence (288 bits).
   4.3 Divide into three group (each group=96 bits)
   4.4 Repeat for group 1 to 3
      4.4.1 Generate four blocks - q1, q2, q3, q4 (each block =24 bits)
      4.4.2 Convert blocks to decimal.
      4.4.3 Perform the bitwise XOR operation("X"):
         \( q^5 = (((q1 \times q2) \times q3) \times q4) \)
      4.4.4 \( X(group) = 0.5000 + \mod((q5/2^{12}),1) \)
   4.5 \( X(group\{1 to 3\}) = x, y, z \) respectively.
5. Generate \( n \times n \) set of values for \( x_{n+1}, y_{n+1}, z_{n+1} \) as \( x, y, z \) respectively based on 3D chaotic equations:

\[
x_{n+1} = [\mu \times k_1 \times y_n \times (1 - x_n) + z] \mod 1
\]
\[ y_{n+1} = \left( \mu \times k_2 \times y_n + z \times 1 \right)\left(1 + (x_n + 1)^2\right) \mod 1 \]

\[ z_{n+1} = \left[ \mu \times (x_{n+1} + y_{n+1} + k_3) \times \sin(z_n) \right] \mod 1 \]

k1, k2, k3 values are constant

6. Mix columns of I
7. Mix rows of I
8. Generate X : n*n set of randomized values in range of 1 to 4 for DNA operations based on equation 1 of 2D chaotic equation:

\[ x_{n+1} = 1 - a \times x_n^2 + y_n \] ------ Equation (1) a, x_n, y_n are constants.

9. Generate Y : n*n set of randomized values in range of 1 to 8 for Rule Conversions based on equation 2 of 2D chaotic equation:

\[ y_{n+1} = b \times x_n \] ------ Equation (2) b and x_n are constants

10. Repeat for n*n elements
    10.1. Take each value of I and convert it to DNA sequence based on corresponding rule of Y. Store in P
    10.2. Take each value of Z and convert it to DNA sequence based on corresponding rule of Y. Store in B
    10.2.1. Perform DNA operations (add, sub, xor, nor) based on corresponding value from X
    10.2.2. Store the binary value after reversing rule conversion based on Y

10.2.2. Store resultant in decimal in matrix J
11. Repeat step 4, 5 for random key generation matrix.
12. Perform XOR with J and randomized matrix
13. Display the encrypted image matrix.

4. Results and Discussions
The simulation is done with the help of Matlab using different input images. We have taken different types of input images such as X-Ray of Human Teeth, CT scan for Lung Cancer, Radiology of Human Hand, Brain Imaging of Multiple Sclerosis, X-Ray detecting Pulmonary Fibrosis and Ultrasoundography Of Renal Cyst for our algorithm. In this paper we describe only one input image as shown in the Figure 1. After applying different operations as describe in the algorithm on input image, the results of different stages are shown in Figure 2 to Figure 10.

Figure 1. X-Ray of Human Teeth
Figure 2. The input image is read, converted it to gray scale and then resized to desired size (nXn).

Showing the pixel values of the input image based on 3D chaotic equations whose initial values are taken from 2D equations. The 2D equations are in turn generated from an arbitrary set of 72 character set.

Figure 3. Showing the pixel values and image of the input image after exchanging columns of Figure 2 based on corresponding one to one indexing of sorted random values of x and y from 3D equations.
Figure 4. Histogram of the image after exchanging columns.

Figure 5. Showing the pixel values and image of the input image after exchanging rows of Figure 3 based on corresponding one to one indexing of sorted random values of x and y from 3D equations.
Figure 6. Histogram of the image after exchanging rows.

Figure 7. Generate X: 256x256 set of randomized values in range of 1 to 4 for DNA operations based on equation 1 of 2D chaotic equation.

Generate Y: 256X256 set of randomized values in range of 1 to 8 for Rule Conversions based on equation 2 of 2D chaotic equations. Resultant pixel values after perform DNA operations(ADD, SUB,
XOR and XNOR) based on corresponding value from X and storing the binary value after reversing rule conversion based on Y.

**Figure 8.** Histogram of resultant image after perform DNA operations(ADD, SUB, XOR and XNOR) based on corresponding value from X and storing the binary value after reversing rule conversion based on Y.

**Figure 9.** Encrypted image after performing the operations.
From the above results, clearly we can see that despite the original images being very tilted with non-uniform histograms, the encrypted image histograms become very flat and uniform after encryption. We see a uniformly-distributed histogram for the encrypted image. This can be witnessed from the final encrypted medical images and their histograms.

5. Conclusions

A novel medical image encryption algorithm based on dynamic DNA sequencing and chaotic systems is proposed in this paper. A detailed process of the novel encryption algorithm is given. Based on the experimental results of our algorithm, we conclude that the proposed chaos and dynamic DNA sequencing based image encryption technique is perfectly suitable for the practical image encryption. The pseudo number sequences generated from the two-dimensional and three-dimensional logistic map equations for image encryption are very much random and complicated. The comparison of original medical image with the encrypted image and the histogram comparison between the same clearly reflect the efficiency of the algorithm. All the encrypted medical images have the same histogram uniformity which makes it efficient.

References

[1] Nyeem H, Boles W and Boyd C 2013 A Review of Medical Image Watermarking Requirements for Teleradiology Journal of Digital Imaging 26 326–343.

[2] Akkasaligar P T and Biradar S 2016 Secure medical image encryption based on intensity level using Chao's theory and DNA cryptography IEEE International Conference on Computational Intelligence and Computing Research (ICCIC), Chennai 1-6.

[3] Belazi A, Talha M, Kharbech S and Xiang W 2019 Novel Medical Image Encryption Scheme Based on Chaos and DNA Encoding IEEE Access 7 36667-36681.
[4] Wang X Y, Zhang Y Q and Zhao Y Y 2015 A novel image encryption scheme based on 2-D logistic map and DNA sequence operations Nonlinear Dynamics 82 1269–1280.

[5] Liu L, Zhang Q and Wei X 2012 A RGB image encryption algorithm based on DNA encoding and chaos map Computers & Electrical Engineering 38 1240–1248.

[6] Liu Y, Tang J and Xie T 2014 Cryptanalyzing a RGB image encryption algorithm based on DNA encoding and chaos map Optics and Laser Technology 60 111–115.

[7] Chai X, Chen Y and Brody L 2017 A novel chaos-based image encryption algorithm using DNA sequence operations Optics Lasers in Engineering 88 197–213.

[8] Niu Y, Zhang X and Han F 2017 Image encryption algorithm based on hyperchaotic maps and nucleotide sequences database Computational Intelligence and Neuroscience 2017 1–9.