Frontiers of Information Technology & Electronic Engineering
www.jzus.zju.edu.cn; engineering.cae.cn; www.springerlink.com
ISSN 2095-9184 (print); ISSN 2095-9230 (online)
E-mail: jzus@zju.edu.cn

Bio-inspired cryptosystem on the reciprocal domain: DNA strands mutate to secure health data*

S. AASHIQ BANU, Rengarajan AMIRTHARAJAN‡

School of Electrical & Electronics Engineering, SASTRA Deemed University, Thanjavur 613401, India

E-mail: aashiqbanu@sastra.ac.in; amir@ece.sastra.edu

Received Feb. 13, 2020; Revision accepted May 24, 2020; Crosschecked June 16, 2021

Abstract: Healthcare and telemedicine industries are relying on technology that is connected to the Internet. Digital health data are more prone to cyber attacks because of the treasure trove of personal data they possess. This necessitates protection of digital medical images and their secure transmission. In this paper, an encryption technique based on DNA mutated with Lorenz and Lü chaotic attractors is employed to generate high pseudo-random key streams. The proposed chaos-DNA cryptic system operates on the integer wavelet transform (IWT) domain and a bio-inspired crossover, mutation unit for enhancing the confusion and diffusion phase in an approximation coefficient. Finally, an XOR operation is performed with a quantised chaotic set from the developed combined attractors. The algorithm attains an average entropy of 7.9973, near-zero correlation with an NPCR of 99.642%, a UACI of 33.438%, and a keyspace of 10^{203}. Further, the experimental analyses and NIST statistical test suite have been designed such that the proposed medical image encryption technique has the potency to withstand any statistical, differential, and brute force attacks.

Key words: Medical image encryption; DNA; Chaotic attractors; Crossover; Mutation; e-Healthcare
https://doi.org/10.1631/FITEE.2000071 **CLC number:** TP309.7

1 Introduction

Over the past few years, the healthcare sector has embraced a digital transformation by improving quick access for faster diagnoses and transfer of medical records around the world. The amounts of data and applications are increasing and are transferred to the public cloud by decentralised Internet networks. Significant challenges are faced in telemedicine and e-healthcare because of the many different threats such as malicious attacks and data breaches. Security of digital information is critical in such sectors as a patient's medical images. These are sensitive with privacy concerns and hinge on legal compliance and secure approval of electronic health records (EHRs). Cyber criminals may be able to view medical images illegally and acquire medical services easily. They may steal protected health information (PHI) and exchange sensitive information on the dark web or modify data, all of which can produce severe threats to the health and safety of patients.

According to IBM's annual report 2019, the highest cost of data breach in the healthcare sector was near to $6.5 million. The cybercriminals can steal healthcare cards and seek insurance for treatment fraudulently (https://portswigger.net/daily-swig/the-latest-healthcare-data-breaches). This leads to an urgent need to develop a robust and dynamic method to maintain digital medical information securely. Digital medical image encryption has a crucial role in protecting the secrecy of data content. For example, medical imaging technology can be used to generate digital images of a person's internal organs. These can be in Digital Imaging and COmmunications in Medicine (DICOM) standards and stored in Picture

‡ Corresponding author

* Project supported by DST FIST Funding, New Delhi, India (No. SR/FST/ET-II/2018/221)

ORCID: S. AASHIQ BANU, https://orcid.org/0000-0002-7708-0307; Rengarajan AMIRTHARAJAN, https://orcid.org/0000-0003-1574-3045

Archiving and Communication Systems (PACS) servers for transmission. These are likely to be vulnerable to illegal access.

The standard security techniques used in medical schemes are the Advanced Encryption Standard (AES), Triple Data Encryption Standard (3DES), and International Data Encryption Algorithm (IDEA). These conventional methods, for the basic modes of DICOM images, are insufficiently efficient and take up a lot of computational time to protect files. The inherent characteristics of the digital medical image are (1) large capacity of pixels, (2) enormous data size, (3) huge correlation between pixels, (4) massive repetition, and (5) low resolution. To address security issues, many researchers have proposed encryption techniques based on traditional algorithms. The interesting link between chaos and cryptography has been of fascination to researchers, stimulating them to generate different encryption designs based on chaotic maps.

The attractive features of chaotic maps are robust ergodicity, high randomness, and immense sensitivity to initial states, leading them to be satisfactory for image encryption (Fridrich, 1998; Mohamed Parvees et al., 2017; Dhall et al., 2018; Ghebleh and Kanso, 2019; Luo J et al., 2019; Wang et al., 2019; Yosefnezhad Irani et al., 2019; Aashiq Banu and Amirtharajan, 2020). Fridrich (1998) first proposed an image encryption method using two-dimensional (2D) chaotic maps by two major modules, confusion and diffusion. To curtail the redundancies implied by Fridrich's structure, Diaconu (2016) suggested image encryption based on chaos by a circular inter-intra pixel permutation and achieved an entropy of 7.9976. A bitwise XOR and a modulo arithmetic technique were employed for high-speed scrambling and a pixel adaptive diffusion for medical image encryption by Hua et al. (2018). Later, there was cryptanalysis due to weak randomness of the cipher image by Chen et al. (2020). The encryption technique was improved by non-linear operation on the permuted image and is able to withstand the chosen plain text attack.

The existing techniques based on chaotic maps do have many drawbacks like chaos degradation, non-complex behaviour, small keyspace, and being discontinuous. By report, it appears that several image encryption techniques using chaotic maps are vulnerable to cryptanalysis. To overcome such problems, Ed N. Lorenz has described deterministic, non-periodic, and chaotic attractors based upon three-dimensional (3D) differential equations, which tend to be stronger, unpredictable and have larger keyspace (Al-Hazaimeh et al., 2017). The significant advantages of combining chaotic attractors and maps are that they enlarge the keyspace, offer a uniform key distribution, an intensified chaotic range, and high randomness. Ravichandran et al. (2016) proposed a medical image encryption technique by two methods: a crossover unit using the combined logistic-tent map for permutation, followed by a mutation unit with the combined logistic-sine map for encryption. Another study is for a colour medical image by adopting high-speed permutation and diffusion using the Chen-based hyperchaotic system (Moafimadani et al., 2019).

However, a chaos-based encryption algorithm cannot ensure the security of an encrypted image. To overcome the weaknesses of the chaotic system, several algorithms have been recommended based on merging DNA cryptography with a chaotic scheme because of its excellent storage and data processing capacity. Aqeel-ur-Rehman et al. (2018) suggested a DNA-based chaos system for image encryption by employing a substitution method in a 2-bit level inter-intra process. To increase the security, SHA 256 hash was chosen, producing an entropy of 7.997. To secure medical images, Ravichandran et al. (2017) proposed a DNA blended with combined chaotic maps to perform encryption for colour DICOM images. The permutation data were encoded by a DNA addition rule from a DNA decoder, and then diffusion was performed. Zhang et al. (2018) proposed a system based on a Feistel network and DNA encoding by hyperchaotic systems. For the substitution, a Hill encryption matrix was constructed, and the keyspace was 10^{100}. Likewise, DNA and chaos based medical image encryption was proposed with two rounds of encryption with combined logistic-Chebyshev and sine-Chebyshev. Each round performs six operations, thus providing redundancy to the cryptosystem (Belazi et al., 2019). By DNA addition, pixel- and base-level rearrangement by 2D logistic map image encryption was achieved by Liu H et al. (2019b).

Liu ZT et al. (2019) suggested a colour image encryption based on DNA and four-dimensional (4D) memristive hyperchaos. The chaotic matrices were

created from 4D hyperchaos using the original image and encoded based on the DNA rule on three planes. By analysing the unified average change in intensity (UACI) values, it failed to attain the theoretical values. Rehman et al. (2019) suggested a colour image encryption by the DNA scheme, chaos, and SHA 512. The image was encoded in a DNA-based rule and separated into least significant bit (LSB) and most significant bit (MSB), in which only MSB was substituted by addition and XOR. MSB and LSB were cross-substituted by a random concatenation and achieved a larger keyspace of 10^{254} (Rehman et al., 2019). An enhanced pseudorandom logistic map and a DNA encoding technique were implemented by a random pixel permutation function by Dagadu et al. (2019a). A medical image encryption was proposed based on Bernoulli shift and the zigzag map, which were coupled with DNA encoding and achieved an entropy of 7.9972 (Dagadu et al., 2019b). For fast and secure encryption, Stalin et al. (2019) suggested a method based on a non-linear 4D logistic map and a DNA sequence with a keyspace of 10^{60}.

Image encryption can be implemented in two realms, i.e., the spatial domain and the transform domain. The spatial domain performs with the image plane alone, whereas the transform domain performs with the rate of pixel transformation. Presently, various image encryption algorithms based on DNA-chaos have been executed in the spatial domain. Applying image encryption techniques in the transform domain produces more security and resistance. By analysing standard wavelets in the transfer domain, integer wavelet transform (IWT) has the benefits of multi-resolution characteristics by generating integer coefficients and lossless decryption (Daubechies and Sweldens, 1998). Moreover, IWT seems to be faster and more effective. The image will be decomposed in IWT, where it is separated into approximation and detailed coefficients. The maximum amount of significant bits of data is in the low-low sub-band, i.e., for the approximate coefficient, and this is sufficient for performing the encryption technique as stated in Arumugham et al. (2018) with a keyspace of 10^{140}.

To improve the security level, Belazi et al. (2017) proposed an image encryption system by operating the lifting wavelet transform (LWT) method in the frequency domain. The keyspace of hybrid S-box is constructed by a Chebyshev map in this technique. Bolourian Haghighi et al. (2019) performed an image tamper detection by LWT and DNA genetic algorithm. Luo Y et al. (2015) suggested a lightweight algorithm on IWT and achieved near-zero correlation and final diffusion in the spatial domain. Guan et al. (2019) proposed a new technique based on DNA encoding and a hyperchaos map in the frequency domain by diffusing and confusing the original image.

From a literature survey, we see that many DNA-based image encryptions have been executed in the spatial domain. Performing DNA algorithms in the IWT domain has not yet been examined for medical image encryption. The IWT domain has a strong resistance to intrusion and produces integer coefficients in order. The major highlights of the proposed digital medical image encryption algorithm are as follows:

1. A bio-inspired cryptosystem based on DNA strands with a crossover and mutation process on the transform domain is proposed.

2. Combined chaotic attractors are implemented in this method to generate high randomness of chaotic key sequences.

3. The performance of security is estimated by histogram, entropy, chi-square test, correlation coefficients, keyspace, key sensitivity, brute force attacks, encryption quality analysis, and the National Institute of Standards and Technology (NIST) test suite.

4. Results are significantly enhanced with high robustness, when compared with existing DNA encryption methods.

5. The developed algorithm can be applied for medical image security applications that are resistant to cyber attacks.

2 Methodology

2.1 DNA

An essential genetic data carrier in biology is DNA, which represents an essential part of the metabolism of genetic organisms (Mahdi et al., 2019). DNA determines large-scale parallelism and small power consumption, and has a peculiar molecular structure. DNA contains four nucleic acid bases, i.e., A-Adenine, T-Thymine, C-Cytosine, and G-Guanine. It is a complementary base pairing because each base can bond only with a specific base partner. A bonds with T and C bonds with G, known as base-pairs

following the Watson-Crick principle. As a DNA sequence in the binary system, 0 and 1 are a complement to each other, likewise 00 and 11, 01 and 10.

For example, a grayscale image of eight bits can be encoded by four DNA base sequences. A pixel value 10010011 is encoded as CGAT by rule 1 as in Table 1. DNA addition and subtraction sequences are implemented in various algorithms. Likewise, DNA XOR and DNA XNOR sequences can be performed according to the conventional binary form (Table 2).

Table 1 Eight rules of DNA mapping sequence

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

Table 2 XNOR and XOR operations for the DNA sequence

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

2.2 Integer wavelet transform

Sweldens and Daubechies started the research on IWT in 1995 (Daubechies and Sweldens, 1998). It appears to be more durable and dynamic than the conventional wavelet transforms and possess the idea of a lifting scheme. IWT maps an integer data set with another integer data set. The other wavelets such as discrete wavelet transform (DWT), fast Fourier transform (FFT), and discrete cosine transform (DCT) generate floating-point values to an integer by a truncation process, resulting in loss of data (Aashiq Banu and Amirtharajan, 2020).

In several applications like multimedia files, the input data comprise integer units. The lifting scheme can be altered quickly to a transform domain, which maps integers to integers and is also reversible. The lifting scheme based decomposition consists of three phases, splitting, predicting, and updating, whereas the reconstruction phases are updating, predicting, and merging (Fig. 1). IWT based on the detachment of frequency sub-bands is presented in Fig. 2.

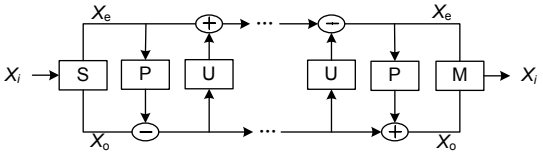


Fig. 1 Lifting scheme of decomposition and reconstruction (S: splitting; P: predicting; U: updating; M: merging)

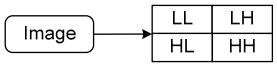


Fig. 2 Integer wavelet transform stages

2.2.1 Splitting

The original plain image X_i is split into an odd X_o sequence and an even X_e sequence. Let the sequences be $\dot{S}$ for the splitting of odd and even:

$$\dot{S} = (X_o, X_e).$$

2.2.2 Predicting

The data sequences are approximated. The difference between the approximation and the real data substitutes the odd elements of the data sequences, in which even components are left unaltered and taken as the input for the next stage in the transform. The odd value is predicted from the even value, represented as follows:

$$\text{High} = X_o - P\{X_e\}.$$

2.2.3 Updating

The attained higher standards are utilised to update the lower coefficients:

$$\text{Low}=P\{X_e\}+\text{High}/2.$$

Subsequent to operating all the three steps of the lifting scheme, the plain image is again split into low- and high-frequency segments by a decomposition method, as given below:

$$\text{LH} = \text{Low}_{\text{odd}} - \text{Low}_{\text{even}},$$
$$\text{LL} = \text{Low}_{\text{even}} + \text{LH}/2,$$
$$\text{HL} = \text{High}_{\text{odd}} - \text{High}_{\text{even}},$$
$$\text{HH} = \text{High}_{\text{even}} + \text{HL}/2.$$

The preceding sequence of equations can be repeated m times to produce m-level decomposition. The significant advantages of IWT are that it requires less memory space, is simple for constructing non-linear wavelet transforms, and has time-frequency localisation capacity and no quantisation errors, unlike other traditional wavelet transforms.

2.3 Lorenz attractor

Ed N. Lorenz first analysed the chaotic Lorenz attractor in 1963. It is an example of a strange attractor, and it was procured from a simplified pattern of convection in the Earth's atmosphere. Strange attractors have a unique characteristic in that they never block on themselves, and the chaotic behaviour is non-periodic (Farah et al., 2020). The method is commonly represented as 3D non-linear differential equations. Generally, the set of constants used for Lorenz attractors are α=10, β=28, γ=8/3 (Aashiq Banu and Amirtharajan, 2020).

$$X_1=\frac{\mathrm{d}x}{\mathrm{d}t}=\alpha(y_i-x_i), \tag{1}$$

$$Y_1=\frac{\mathrm{d}y}{\mathrm{d}t}=x_i(\beta-z_i)-y_i, \tag{2}$$

$$Z_1=\frac{\mathrm{d}z}{\mathrm{d}t}=x_iy_i-\gamma z_i. \tag{3}$$

The sequences do not form limit cycles or reach a steady state. Preferably, it is a pattern of deterministic chaos, and is also sensitive to the initial conditions. The x-y-z planes are given in Fig. 3.

The 3D Lorenz attractor is combined as [X; Y; Z], named the combined Lorenz attractor (CLA). Initialise the Lorenz attractor Lz(α, β, γ, x, y, z) as per Eqs. (1)–(3):

for l=1:n

$X(l_i)=x(l_i)-\mathrm{floor}(x(l_i))$,

$Y(l_i)=y(l_i)-\mathrm{floor}(y(l_i))$,

$Z(l_i)=z(l_i)-\mathrm{floor}(z(l_i))$,

end

$\mathrm{CLA}=[X;Y;Z]'$,

$S_z=(\mathrm{CLA},256)$.

$$K_\mathrm{L}=\mathrm{floor}(\mathrm{mod}(S_z\cdot10^{14},256)), \tag{4}$$

where K_L is the CLA which produces the pseudo-random key sequence. Fig. 4 shows the chaotic range achieved for the CLA attractor for 1000 iterations. It indicates that the CLA has raised irregular distribution and improved chaotic series more than individual maps.

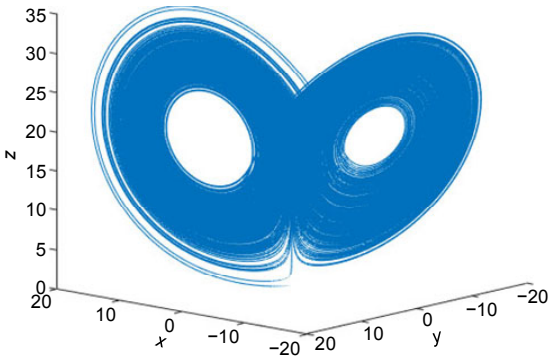


Fig. 3 Illustration of the complex performance of the Lorentz attractor (x-y-z planes)

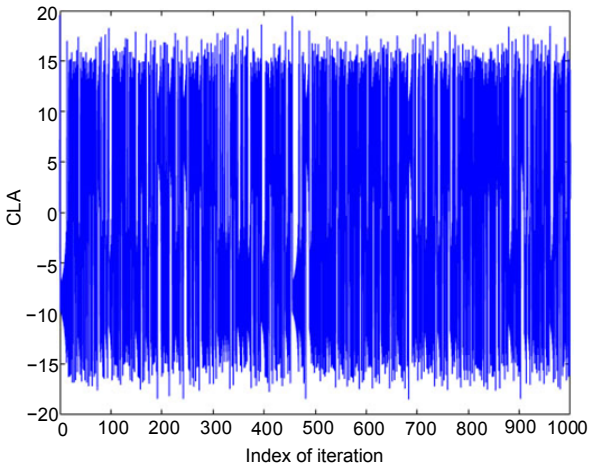


Fig. 4 Chaotic range of the combined Lorenz attractor (CLA) with 1000 iterations

2.4 Lü attractor

The Lü attractor is also a strange attractor. The system is represented with 3D non-linear differential equations, where a=36, b=3, c=20:

$$X_2=\frac{\mathrm{d}x}{\mathrm{d}t}=-y_i-z_i, \tag{5}$$

$$Y_2=\frac{\mathrm{d}y}{\mathrm{d}t}=x_i+ay_i, \tag{6}$$

$$Z_2=\frac{\mathrm{d}z}{\mathrm{d}t}=b+z_i(x_i-c). \tag{7}$$

These generate a chaotic behaviour that leads to trajectories of chaotic illustrations (Fig. 5).

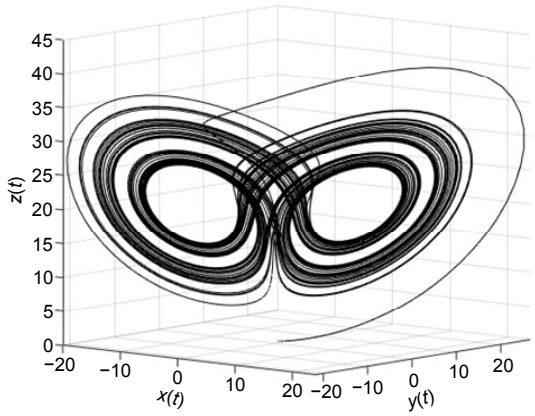


Fig. 5 Illustration of the complex behaviour of the Lü attractor

The 3D Lü attractor is combined as [X; Y; Z], called the combined Lü attractor (CLuA). Initialise the Lü attractor Lü(a, b, c, x, y, z) as per Eqs. (5)–(7):

$$\begin{aligned}&\text{for } l=1{:}n\\&X(l_i)=x(l_i)-\text{floor}(x(l_i)),\\&Y(l_i)=y(l_i)-\text{floor}(y(l_i)),\\&Z(l_i)=z(l_i)-\text{floor}(z(l_i)),\\&\text{end}\\&\text{CLuA}=[X;Y;Z]',\\&S_z=(\text{CLuA},256).\end{aligned}$$

$$K_{\mathrm{R}}=\text{floor}(\text{mod}(S_z\cdot 10^{14},256)), \tag{8}$$

where K_{R} is the pseudo-random key sequence by CLuA. Fig. 6 exhibits the bifurcation diagram of CLuA for 1000 iterations.

3 System design

The proposed technique has a novel cryptic design based on an IWT and DNA mutated chaos attractor for encrypting digital medical images. It comprises two stochastic genetic operations, namely crossover and mutation of DNA sequences, as intra-inter bit-level execution in approximate coefficients. This is sufficient for executing an encryption algorithm. Pseudo-random sequences are generated from two chaotic attractors, CLA and CLuA. Further, it is decoded based on a DNA rule, and an inverse integer wavelet transform (IIWT) is executed. To enhance certainty, it is XOR-ed by a quantized chaotic sequence from CLuA to obtain the encrypted image. The complete architecture of the proposed algorithm steps is given in Section 3.3, and an illustration is shown in Fig. 7.

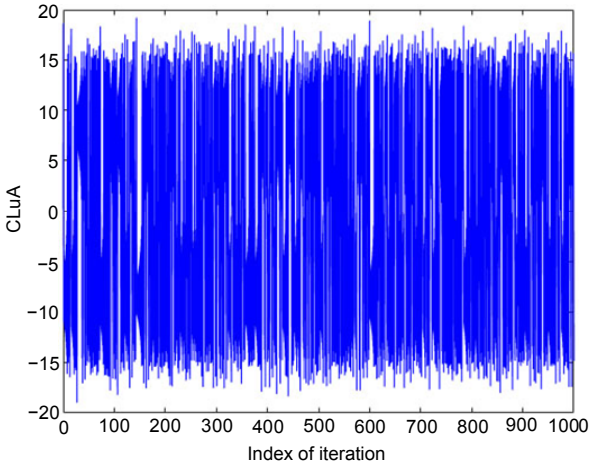


Fig. 6 Chaotic range of the combined Lü attractor (CLuA) with 1000 iterations

The most crucial part of security based upon the chaos theory is choosing the initial value. The proposed encryption method is directly proportionate to the strength of the key. To improve the security of the secret key, a pseudo-random number generator sequence is taken from the developed chaos attractors to produce a large keyspace. The user predefines the initial value and parameter value of CLA→K_{L} and CLuA→K_{R}. These are all defined parameters as specified in Section 4.4.

3.1 Quantization process

In the quantization process, CLA and CLuA generate chaotic sequences that are mapped to their equivalent states as per the sorted sequence. Let the chaotic sequence produced from CLA be S_1={S_{11}, S_{12}, …, S_{1n}} with the initial value K_1. The S_1 sequence is in ascending order to obtain the sorted sequence S_1' accompanied by the weights assigned to the element based on the position to perform the quantization.

Example 1 Let the chaotic series produced by the combined 3D Lorenz attractor (CLA) be S_1→X={0.231, 0.874, 0.214, 0.754, 0.467}, Y={0.124, 0.532, 0.287, 0.484, 0.327}, and Z={0.976, 0.426, 0.1897, 0.3824, 0.1027}. Sort the sequence in ascending order

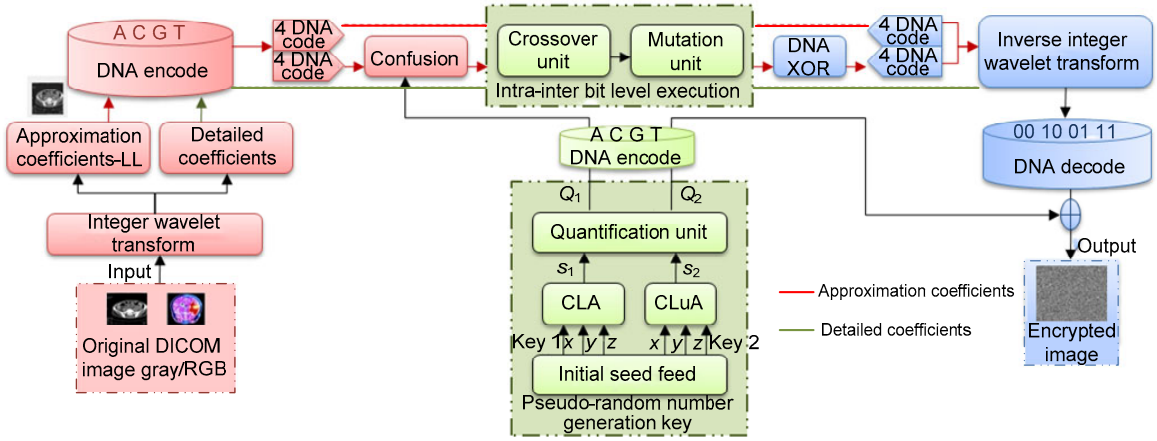


Fig. 7 Overall architecture of the proposed method (References to color refer to the online version of this figure)

$S_1' \rightarrow \{0.231, 0.124, 0.976, 0.874, 0.532, 0.426, 0.214, 0.287, 0.1897, 0.754\}$. The corresponding quantized key sequence is $Q_1 \rightarrow \{4, 1, 10, 9, 7, 6, 3, 5, 2, 8\}$. The same process is performed for the 3D Lü attractor→CLuA, and the quantized key sequence is Q_2.

3.2 Intra-inter bit-level execution

3.2.1 Crossover unit

In biological terms, crossover implies the transfer of genetic material within chromosomes to produce the recombinant chromosomes (Ravichandran et al., 2016; Premkumar and Anand, 2019). The stated technique has been derived from the crossover rules for encrypting the digital medical image. The words chromosomes, genetic material, and recombinant chromosomes are reformed with an original image, image pixels, and a permuted image in image encryption.

The crossover rules are useful in combining two parents' chromosomes to generate offspring; i.e., the image pixels are blended in terms of DNA rules to produce an image crossover. Fig. 8 exhibits the operation of the two image pixels that are encoded in the DNA rule 1 sequence and the inter-bit level execution with the DNA XNOR and DNA XOR processes. Following the crossover process, the position of the pixel is placed to the next location sequentially, and the last pixel code will be located first.

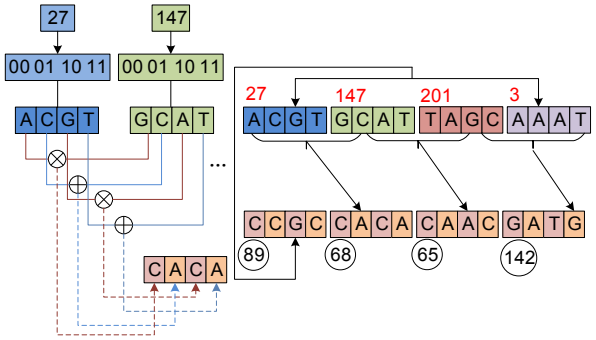


Fig. 8 Crossover process

3.2.2 Mutation unit

A mutation is a change of the nucleotide sequence of the DNA, which reconstructs the amino acid sequences and has the potential to alter the character of the gene. It is also defined as a random change to an individual parent's chromosomes to produce offspring (Liu JZ et al., 2019; Premkumar and Anand, 2019). In the proposed technique, mutation leads to an immediate and permanent change transpiring in the pixel level of an image based upon the DNA sequences. Fig. 9 shows the intra-bit execution in which each pixel of the image is encoded by a DNA rule 1 sequence. For the first-third code DNA XNOR is performed; for the second-fourth DNA XOR is performed. The last two codes are taken to their positions, and the pixels are concatenated simultaneously for every individual pixel.

3.3 Overall encryption algorithm

The proposed encryption method is described as follows:

Step 1: Take the original digital medical image Img of size $M_1 \times N_1$.

Step 2: Apply IWT on Img where the approximation and detailed sub-band frequencies are obtained as LL, LH, HL, and HH.

Step 3: In the approximation coefficients, low-low (LL) sub-band, which is of 16 bits, is encoded by DNA rule 1, which generates eight DNA codes. The eight DNA codes are divided into four DNA codes in each of P_1 and P_2.

Step 4: With the initial values, iteration is performed on CLA and CLuA to generate pseudo-random chaotic sequences S_1 and S_2, respectively, as per the example mentioned in Section 3.1.

Step 5: Apply the quantization method to quantize sequences S_1 and S_2 to the key streams Q_1 and Q_2 as per the example mentioned in Section 3.1.

Step 6: The pixel P_2 of four DNA codes is performed as confusion with the chaotic sequence CLA→conf_P_2.

Step 7: The conf_P_2 has performed a crossover unit operation as presented in Fig. 8.

Step 8: Perform the mutation, and the locations of the pixel elements are arranged as shown in Fig. 9.

Step 9: After the intra-inter bit-level execution is performed, the values generated are DNA XOR-ed with the random chaotic sequence produced by Q_2.

Step 10: The pixel P_1 and final processed P_2 are concatenated and combined with other sub-bands by performing inverse integer wavelet decomposition and decoded by DNA rule 1.

Step 11: To increase the resistance, the final processed sub-bands are XOR-ed with the keystream Q_2 to produce the encrypted image.

Decryption is performed as the reverse of encryption. Fig. 10 shows the outcomes of encryption and decryption.

4 Simulation results and discussion

For the experimental study, we have taken grayscale and RGB DICOM images (CT and MRI) of dimension 256×256. The proposed algorithm is executed using MATLAB 2018 with the key sets K_L and K_R on a PC with Intel Xeon CPU E3-1220 v6 at 3 GHz CPU, 32 GB memory with Windows 10. To verify the performance of the suggested algorithm, several analyses are carried out such as statistical, differential, keyspace, sensitivity of key, cropping attack, complexity analysis, and the NIST suite test.

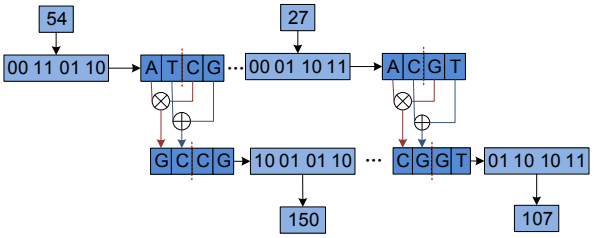


Fig. 9 Mutation process

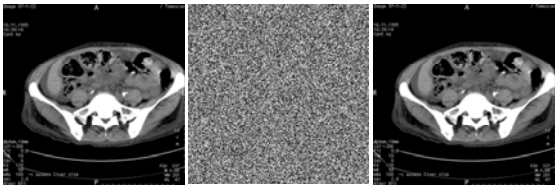


Fig. 10 Overall outcome of the proposed encryption and decryption: (a) original image; (b) encrypted image; (c) decrypted image

4.1 Statistical analysis

To withstand statistical analysis attack, Shannon recommended that confusion and diffusion must be performed in a cryptosystem. In the proposed method, combined chaotic attractors are used for permutation and substitution. This analysis has been done to validate the robustness by evaluating the histogram, chi-square test, entropy, and correlation coefficient of the encrypted image.

4.1.1 Histogram analysis

This is a graphical illustration of an image pixel outlining how the number of pixels is distributed at each grayscale level. A flat and evenly dispersed histogram will verify a good level of randomness. From the procured histograms, it is observed that the encrypted image histogram is uniformly distributed (Figs. 11f–11h and 12c); it is also dissimilar from the original image (Figs. 11b–11d and 12b). This analysis proves that the proposed method produces a histogram with good quality.

4.1.2 Chi-square test

The evenness of the histogram is evaluated with the chi-square (χ^2) test:

$$\chi^2=\sum_{l=1}^{256}\frac{(\text{observed}_l-\text{expected})^2}{\text{expected}}. \tag{9}$$

Here l is the intensity level, and the required value is 256 for 256×256. The outcome of the χ^2 test for several encrypted images is shown in Table 3, from which it is evident that the suggested algorithm obtains the null hypothesis, and the ρ-values are larger than 0.05 for the encrypted images. Therefore, it is notable that the redundancy of the original image is entirely obscured, which rebuffs the statistical attack.

The values of the correlation between a pixel and its adjacent pixel are evaluated from Eq. (10):

$$\mathrm{Corr}_{xy} = \frac{F_i[(x - F_i(x))(y - F_i(y))]}{\sigma_x \sigma_y}, \tag{10}$$

where σ_x and σ_y are standard deviations and $F_i(\cdot)$ is the expected value of i. The correlation coefficients of the test images in horizontal, diagonal, and vertical directions are given in Table 4. The near-zero values confirm that the proposed method strongly shatters the correlation between neighbouring pixels.

Table 3 Chi-square test analysis

Parameter	DICOM_R	DICOM_G	DICOM_B	DICOM-1	DICOM-2	DICOM-3	DICOM-4	DICOM-5
χ^2 value	234.5546	242.3203	261.7421	253.4453	236.8281	229.2814	237.5469	259.2891
ρ-value	0.1756	0.3461	0.5963	0.4842	0.2132	0.1511	0.2231	0.5863
Decision (H=0)	Pass	Pass	Pass	Pass	Pass	Pass	Pass	Pass

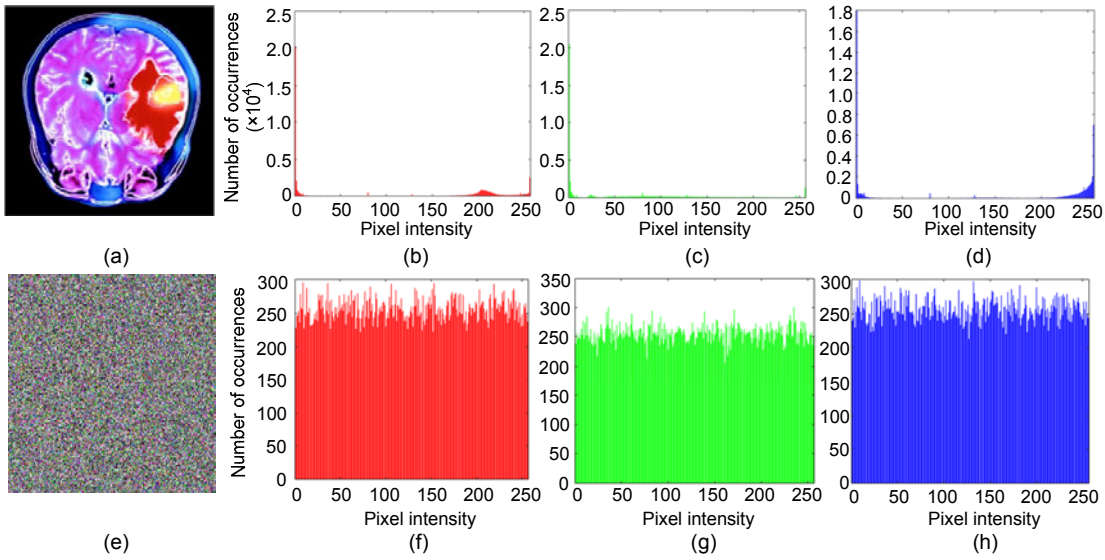


Fig. 11 Histogram analysis of the colour DICOM image: (a) original image; (b) red plane of the original image; (c) green plane of the original image; (d) blue plane of the original image; (e) encrypted image of the original image; (f) encrypted image of the red plane; (g) encrypted image of the green plane; (h) encrypted image of the blue plane (References to colour refer to the online version of this figure)

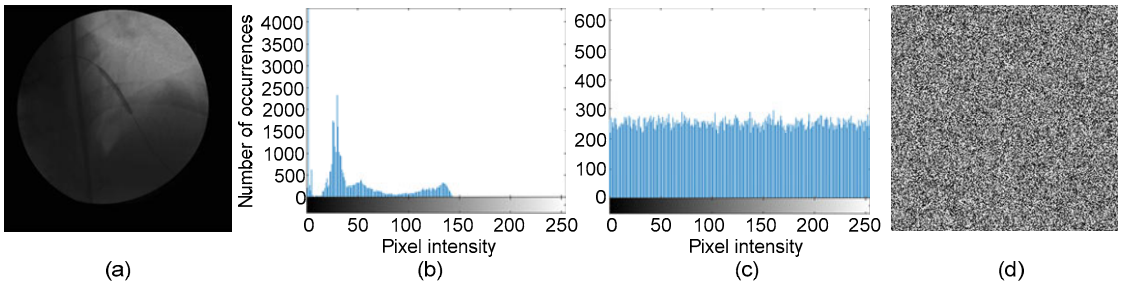


Fig. 12 Analysis of the gray DICOM image: (a) original image; (b) histogram of (a); (c) histogram of the encrypted image; (d) encrypted image

4.1.3 Correlation coefficient

In general, for an informative image, the correlation between adjacent pixels will be high in any direction. The correlation coefficient must be very low or near-zero for the cipher image to resist statistical attacks. The graphical illustration is performed by plotting the pixel values between the adjacent pixels, i.e., horizontal, vertical, and diagonal directions. The correlation coefficient analysis of the original and cipher images is described along the horizontal, vertical, and diagonal directions (Figs. 13 and 14).

4.1.4 Information entropy

A vital metric to estimate the randomness of the information is entropy:

$$I(n)=-\sum_{i=1}^{L}P(n_i)\log_2 P(n_i), \tag{11}$$

Table 4 Correlation analyses of the colour and gray DICOM images

Image/Plane	Type	Correlation coefficient		
		Horizontal	Vertical	Diagonal
Colour DICOM_R	Original	0.9526	0.9620	0.9209
	Encrypted	**0.0043**	**0.0033**	**0.0027**
Colour DICOM_G	Original	0.9139	0.9314	0.8535
	Encrypted	**0.0011**	**0.0047**	**0.0011**
Colour DICOM_B	Original	0.9649	0.9727	0.9402
	Encrypted	**0.0023**	**0.0037**	**0.0019**
DICOM-1	Original	0.9749	0.9766	0.9576
	Encrypted	**−0.0013**	**−0.0033**	**0.0065**
DICOM-2	Original	0.9587	0.9449	0.9196
	Encrypted	**0.0063**	**0.0047**	**−0.0012**
DICOM-3	Original	0.9635	0.9798	0.9503
	Encrypted	**−0.0032**	**−0.0019**	**0.0016**
DICOM-4	Original	0.9809	0.9760	0.9603
	Encrypted	**−0.0006**	**−0.0001**	**0.0015**
DICOM-5	Original	0.9898	0.9875	0.9801
	Encrypted	**0.0009**	**0.0055**	**−0.0015**

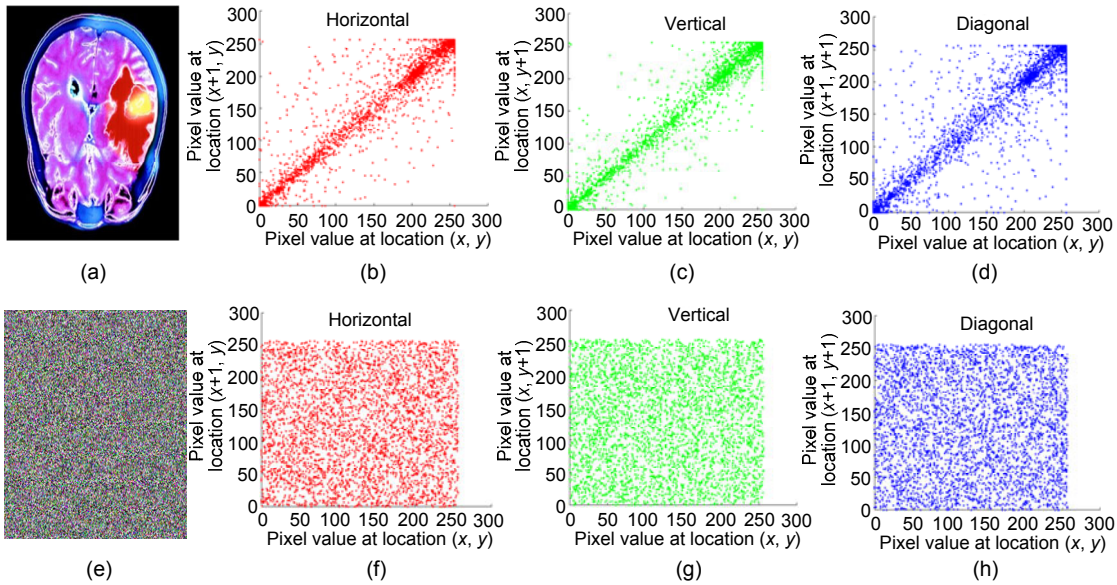


Fig. 13 Correlation coefficient analysis of the colour DICOM image: (a) original image; (b) horizontal direction for red plane correlation of (a); (c) vertical direction for green plane correlation of (a); (d) diagonal direction for blue plane correlation of (a); (e) encrypted image of (a); (f) horizontal direction for red plane correlation of (e); (g) vertical direction for green plane correlation of (e); (h) diagonal direction for blue plane correlation of (e) (References to colour refer to the online version of this figure)

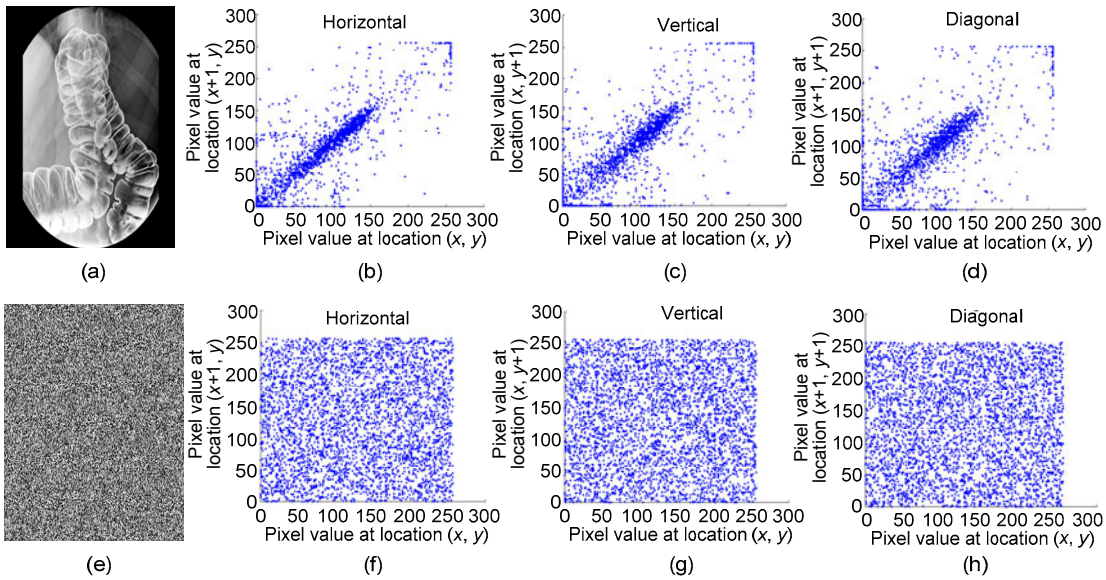


Fig. 14 Correlation coefficient analysis of the gray DICOM image: (a) original image; (b) horizontal direction correlation of (a); (c) vertical direction correlation of (a); (d) diagonal direction correlation of (a); (e) encrypted image of (a); (f) horizontal direction correlation of (e); (g) vertical direction correlation of (e); (h) diagonal direction correlation of (e)

where $P(n_i)$ is the possibility of the occurrence of n_i. For an arbitrary image with $2L$ symbols, the range of the information entropy is $[0, L]$, whereas the entropy must be nearer to L. The entropy of the proposed encrypted images is nearer to the hypothetical value (≈8). Table 5 indicates that the proposed technique is highly random.

Table 5 Information entropy analysis

Image	Information entropy	
	Original	Encrypted
Colour DICOM_R	5.8124	7.9972
Colour DICOM_G	6.1789	7.9974
Colour DICOM_B	5.5982	7.9973
DICOM-1	4.2948	7.9975
DICOM-2	4.4251	7.9971
DICOM-3	5.0322	7.9972
DICOM-4	6.3200	7.9976
DICOM-5	6.5136	7.9973

4.2 Differential analysis

The most significant parameters to estimate the resistance of the proposed algorithm to differential attacks are the number of pixel change rate (NPCR) and unified average change in intensity (UACI). This can be ascertained from two encrypted images C_1 and C_2; the plain image is the encrypted image C_1, and C_2 is the change of any pixel in the plain image. NPCR estimates the smallest number of pixels modified; UACI estimates the average variation within C_1 and C_2 of the two encrypted images of size $M_1 \times N_1$:

$$\mathrm{NPCR} = \frac{1}{M_1 N_1} \sum_{i,j} B(i,j) \times 100\%, \tag{12}$$

$$\mathrm{UACI} = \frac{1}{M_1 N_1} \sum_{i,j} \frac{|C_1(i,j) - C_2(i,j)|}{255} \times 100\%, \tag{13}$$

where $B(i, j)$ is a bipolar array of the same sizes C_1 and C_2, and

$$B(i,j) = \begin{cases} 0, & C_1(i,j) = C_2(i,j), \\ 1, & C_1(i,j) \neq C_2(i,j). \end{cases} \tag{14}$$

The NPCR and UACI analyses are performed for colour and gray DICOM images where the mean values are approximately an NPCR of 99.642% and a UACI of 33.438% (Tables 6 and 7). The values are near to the optimal value, and this determines the ability to defy differential attacks.

4.3 Keyspace analysis

A perfect encryption algorithm must have a large enough keyspace to withstand a brute force attack. The proposed algorithm has a 3D chaotic Lorenz attractor and a 3D chaotic Lü attractor to perform the

whole algorithm. The initial key sets of CLA→K_L={x, y, z, a, b, c} and CLuA→K_R={x, y, z, a, b, c} of 17 decimal points are set as the precision. Therefore, the total keyspace for the proposed algorithm is 10^{203}, which is larger than 2^{128}. This confirms that the keyspace of the suggested method is sufficiently large to oppose brute force attacks to a greater extent than the existing techniques.

4.4 Key sensitivity analysis

The keys are significant developmental factors for a cryptosystem. In this subsection we evaluate the strength of the proposed algorithm by the sensitivity of the keys. To check the efficiency of the encryption technique, if any one of the key set is altered, it will result in undesired output. Figs. 15b–15d show the analysis of the key sensitivity of the proposed DNA chaos cryptic system. Fig. 15b is the encrypted image of the original DICOM using the original key set K_L→{a=10; b=28; c=8/3; X=6.255 410 907 1, Y=−6.875 612 455 1, Z=2.875 124 778 7} and K_R→{a=36; b=3; c=20; X= 0.000 005, Y=5, Z=25}, and the decrypted image is as given in Fig. 15e. For comparison, a similar analysis has been performed with two different sets of keys as given below:

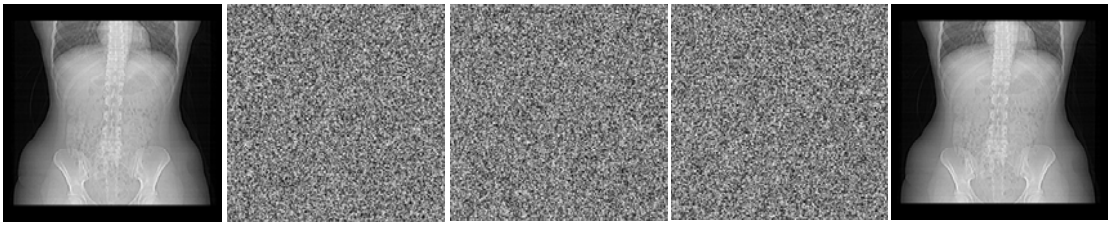
1. K_L→{a=10; b=28; c=8/3; X=6.255 418 907 1, Y=−6.875 612 455 1, Z=2.875 124 778 7} and K_R→{a=36; b=3; c=20; X=0.000 105, Y=5, Z=25}.

Table 6 NPCR analysis

DICOM image	Decision		
	NPCR*0.05=99.5693%	NPCR*0.01=99.5527%	NPCR*0.001=99.5341%
Colour DICOM_R	Pass	Pass	Pass
Colour DICOM_G	Pass	Pass	Pass
Colour DICOM_B	Pass	Pass	Pass
DICOM-1	Pass	Pass	Pass
DICOM-2	Pass	Pass	Pass
DICOM-3	Pass	Pass	Pass
DICOM-4	Pass	Pass	Pass
DICOM-5	Pass	Pass	Pass

Table 7 UCAI analysis

DICOM image	Decision		
	UACI*−0.05=33.2824% UACI*+0.05=33.6447%	UACI*−0.01=33.2255% UACI*+0.01=33.7016%	UACI*−0.001=33.1594% UACI*+0.001=33.7677%
Colour DICOM_R	Pass	Pass	Pass
Colour DICOM_G	Pass	Pass	Pass
Colour DICOM_B	Pass	Pass	Pass
DICOM-1	Pass	Pass	Pass
DICOM-2	Pass	Pass	Pass
DICOM-3	Pass	Pass	Pass
DICOM-4	Pass	Pass	Pass
DICOM-5	Pass	Pass	Pass



(a) (b) (c) (d) (e)

Fig. 15 Key sensitivity analysis: (a) original DICOM image; (b) correct key set of an encrypted image; (c) decrypted image with altered key set 1; (d) decrypted image with altered key set 2; (e) correct key set: producing the decrypted image

2. $K_L \rightarrow \{a=10;\ b=28;\ c=8/3;\ X=6.255\ 410\ 907\ 1,\ Y=-6.875\ 612\ 455\ 1,\ Z=2.875\ 124\ 778\ 7\}$ and $K_R \rightarrow \{a=36;\ b=3;\ c=20;\ X=0.000\ 005,\ Y=0.5,\ Z=15\}$.

Figs. 15c and 15d are obtained by decrypting the encrypted image with the key sets $\{K_{L1}, K_{R1}\}$ and $\{K_{L2}, K_{R2}\}$. By analysis, it is proved that the keys are highly sensitive to small changes in the proposed algorithm technique.

An example of key sensitivity of CLA is shown in Figs. 16a and 16b to represent the changes that arise while the keys are altered with the original key set and key set 2 for various numbers of iterations.

4.5 Cropping attack analysis

For real-time applications, cyber attackers might purposely crop a portion of the encrypted image while it is transmitted over public channels. To test the resistant capacity of the proposed algorithm against cropping, a few parts of the encrypted image are cropped and implemented in the proposed decryption algorithm. Figs. 17a–17d show the cropping of the encrypted image and its equivalent decrypted images. It is notable that the proposed algorithm can retrieve a significant image even after cropping.

4.6 Encryption quality analysis

The quality of the encryption technique determines the robustness of an algorithm. By visual inspection, one can easily understand the potency of an algorithm but cannot obtain the cryptic outlets (Belazi et al., 2016).

4.6.1 Maximum deviation

To estimate the quality of the proposed algorithm, the deviation between the original and the encrypted images of pixel values has to be measured by a mathematical equation. If the variation is higher, then the algorithm is more secure.

$$D_{\max} = \frac{D_0 + D_{N-1}}{2} + \sum_{i=1}^{N-2} D_i, \tag{15}$$

where N is the entire number of pixel values ($N=2^p$ and p is the pixel depth) and D_i ($i=1, 2, \ldots, N-2$) is the difference between the original image and the i^{th} encrypted image histogram. Table 8 shows the outcomes of the maximum deviation. A higher $D_{\max}$ indicates that the encrypted image has deviated more from the original image.

4.6.2 Deviation from the uniform histogram

For a perfect encryption algorithm, the distribution of pixels in a histogram must be equal for an encrypted image. The histogram for an ideal encrypted image of size $M \times N$ can be calculated by

$$H_{c_i} = \begin{cases} MN/256, & 0 \le c_i \le 255, \\ 0, & \text{otherwise}, \end{cases} \tag{16}$$

$$D_H = \frac{1}{MN} \sum_{c_i=0}^{255} \left| H_{c_i} - H_c \right|, \tag{17}$$

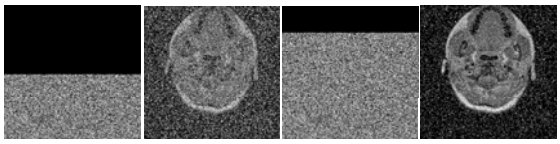


Fig. 17 Analysis of cropping attack: (a) image with 128×256 cropped; (b) decipher of (a); (c) image with 50×256 cropped; (d) decipher of (c)

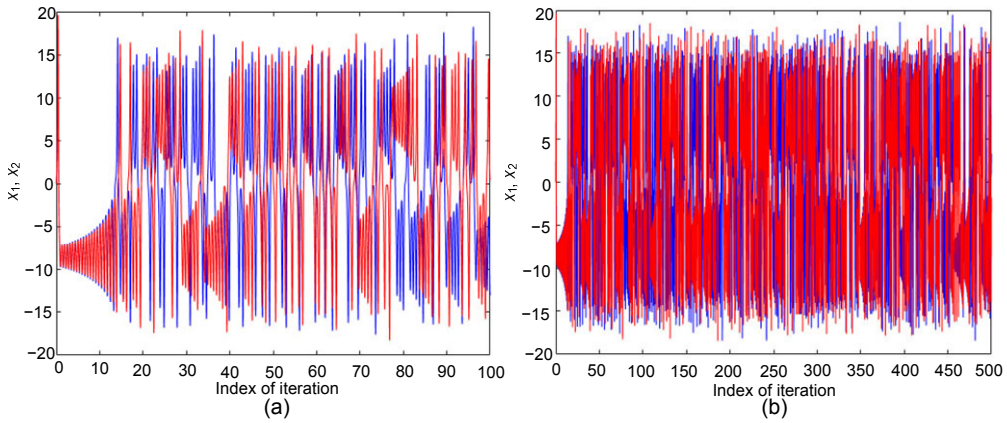


Fig. 16 Illustration of key sensitivity with the original key set (x_1, red line) and key set 2 (x_2, blue line) for the combined Lorenz attractor for 100 (a) and 500 (b) iterations (References to colour refer to the online version of this figure)

where H_c is the histogram of the cipher image. The D_H value must be small for the ideal case. Table 8 indicates that the histogram of the encrypted image procured from the proposed technique is less varied from the ideal histogram.

4.7 NIST test suite analysis

For analysis, the randomness of the proposed encryption algorithm and the developed CLA and CLuA keys is tested by the NIST test suite (Devi et al., 2019). To execute the NIST test, the proposed encrypted DICOM images, CLA and CLuA, are converted into binary, in which 10 bits are examined from the 10 000 bits. From Table 9, the proportion value is not less than 0.8, which confirms that the proposed encryption algorithm and the combined chaotic attractors produce high randomness.

4.8 Performance comparison

The proposed crypt DNA attractor on the IWT algorithm is compared with state-of-the-art techniques. The performance analysis is done by analysing entropy, NPCR, UACI, keyspace, and NIST test suite. The proposed algorithm attains an entropy of 7.9973 in the transform domain and a keyspace greater than 2^{128}, which is better than earlier work.

In Table 10, the ✓ symbol represents that the analysis has been performed and × denotes that the particular analysis has not been executed in the literature. The proposed algorithm is evaluated through the NIST test suite, which proves that the keys and encrypted image produce good random values.

By the estimated outcomes, it is proven that the proposed digital medical image encryption algorithm on the reciprocal domain can resist statistical attacks and differential attacks, and perform well on the NIST test.

Table 8 Encryption quality analysis

Image	Deviation from ideality	Maximum deviation
Colour DICOM_R	0.0501	59 427
Colour DICOM_G	0.0453	40 654
Colour DICOM_B	0.0497	67 310
DICOM-1	0.0528	67 260
DICOM-2	0.0443	56 774
DICOM-3	0.0482	53 886
DICOM-4	0.0462	55 318
DICOM-5	0.0499	46 222

5 Conclusions

A bio-inspired medical image encryption method is proposed which employs DNA blended with combined chaotic attractors. To intensify the substitution and permutation phase, a crossover and mutation process is performed. Analyses have been carried out to verify its security and complexity. It is validated that the proposed method yields security for transmitting digital medical images across the public communication network and is beneficial for real-time medical applications. In the future, the proposed digital image encryption scheme will be implemented on programmable ASIC (FPGA) to achieve a high level of parallelism and reconfigurability.

Table 9 NIST test suite results

Test	*P* value			Proportion			Conclusion
	DICOM-1	CLA	CLuA	DICOM-1	CLA	CLuA	
Frequency	0.3505	0.5341	0.9114	1.0	1.0	1.0	Random
Block frequency	0.5341	0.5341	0.7399	0.9	1.0	1.0	Random
Cumulative sum I	0.5341	0.3504	0.9114	1.0	1.0	1.0	Random
Cumulative sum II	0.0668	0.7399	0.7399	1.0	1.0	1.0	Random
Runs	0.5341	0.7391	0.9114	1.0	0.9	1.0	Random
FFT	0.7399	0.3504	0.7399	1.0	1.0	1.0	Random
Nonoverlapping template	0.5341	0.1222	0.3504	1.0	1.0	1.0	Random
Overlapping template	0.1223	0.9114	0.2133	1.0	1.0	1.0	Random
Approximate entropy	0.5341	0.9914	0.7399	1.0	1.0	1.0	Random
Serial I	0.5341	0.5341	0.3504	1.0	1.0	1.0	Random
Serial II	0.5341	0.0179	0.5341	1.0	1.0	1.0	Random
Linear complexity	0.3505	0.3505	0.7399	1.0	1.0	0.9	Random

Table 10 Performance comparison

Reference	Domain	Entropy	NPCR (%)	UACI (%)	Keyspace	NIST test
Chen et al., 2020	Spatial	7.9971	99.62	33.44	2^{256}	×
Ravichandran et al., 2016	Spatial	7.9992	99.99	33.37	10^{168}	×
Ravichandran et al., 2017	Spatial	7.9972	99.59	33.43	10^{168}	×
Belazi et al., 2019	Spatial	7.9991	99.61	33.47	$>2^{716}$	×
Liu H et al., 2019b	Spatial	7.9984	99.61	33.45	$>2^{128}$	×
Liu H et al., 2019a	Spatial	7.9993	99.59	49.70	10^{112}	×
Rehman et al., 2019	Spatial	7.9993	99.61	33.46	10^{254}	×
Dagadu et al., 2019a	Spatial	7.9994	99.59	33.41	$>2^{128}$	×
Farah et al., 2020	Spatial	7.9990	99.56	33.41	$>2^{128}$	×
Chai et al., 2019	Spatial	7.9993	99.58	33.46	10^{98}	×
Liu JZ et al., 2019	Spatial	7.9991	99.61	33.42	10^{74}	×
Dagadu et al., 2019b	Spatial	7.9972	99.64	33.43	10^{74}	×
Dzwonkowski and Rykaczewski, 2019	Spatial	7.9969	NA	NA	2^{256}	×
Kumar et al., 2019	Spatial	4.7453	99.60	33.46	10^{60}	×
Suri and Vijay, 2020	Spatial	7.9519	99.45	31.35	$>2^{128}$	×
Praveenkumar et al., 2015	Spatial	7.9972	99.59	33.47	2^{269}	×
Belazi et al., 2017	Transform	7.9025	99.64	33.43	2^{208}	×
Arumugham et al., 2018	Transform	7.9916	NA	NA	2^{168}	×
Bolourian Haghighi et al., 2019	Transform	7.9970	99.61	33.46	$>2^{128}$	×
Luo Y et al., 2015	Transform	7.9820	99.47	33.37	10^{78}	×
Guan et al., 2019	Transform	7.9923	99.63	33.61	10^{58}	×
Aashiq Banu and Amirtharajan, 2020	Spatial-transform	7.9980	99.68	33.47	10^{238}	×
This paper	**Transform**	**7.9973**	**99.64**	**33.44**	$\mathbf{10^{203}}$	✓

✓ represents that the analysis has been performed and × denotes that the particular analysis has not been executed in the literature

Contributors

Rengarajan AMIRTHARAJAN designed the research. S. AASHIQ BANU processed the data and drafted the manuscript. Rengarajan AMIRTHARAJAN helped organize the manuscript. S. AASHIQ BANU and Rengarajan AMIRTHARAJAN revised and finalized the paper.

Compliance with ethics guidelines

S. AASHIQ BANU and Rengarajan AMIRTHARAJAN declare that they have no conflict of interest.

References

Aashiq Banu S, Amirtharajan R, 2020. A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach. *Med Biol Eng Comput*, 58:1445-1458. https://doi.org/10.1007/s11517-020-02178-w

Al-Hazaimeh OM, Al-Jamal MF, Alhindawi N, et al., 2017. Image encryption algorithm based on Lorenz chaotic map with dynamic secret keys. *Neur Comput Appl*, 31(7): 2395-2405. https://doi.org/10.1007/s00521-017-3195-1

Aqeel-ur-Rehman, Liao XF, Hahsmi MA, et al., 2018. An efficient mixed inter-intra pixels substitution at 2bits-level for image encryption technique using DNA and chaos. *Optik*, 153:117-134. https://doi.org/10.1016/j.ijleo.2017.09.099

Arumugham S, Rajagopalan S, Rayappan JBB, et al., 2018. Networked medical data sharing on secure medium—a web publishing mode for DICOM viewer with three layer authentication. *J Biomed Inform*, 86:90-105. https://doi.org/10.1016/j.jbi.2018.08.010

Belazi A, El-latif AAA, Belghith S, 2016. A novel image encryption scheme based on substitution-permutation network and chaos. *Signal Process*, 128:155-170. https://doi.org/10.1016/j.sigpro.2016.03.021

Belazi A, El-Latif AAA, Diaconu AV, et al., 2017. Chaos-based partial image encryption scheme based on linear fractional and lifting wavelet transforms. *Opt Laser Eng*, 88:37-50. https://doi.org/10.1016/j.optlaseng.2016.07.010

Belazi A, Talha M, Kharbech S, et al., 2019. Novel medical image encryption scheme based on chaos and DNA encoding. *IEEE Access*, 7:36667-36681. https://doi.org/10.1109/ACCESS.2019.2906292

Bolourian Haghighi B, Taherinia AH, Mohajerzadeh AH, 2019. TRLG: fragile blind quad watermarking for image tamper detection and recovery by providing compact digests with optimized quality using LWT and GA. *Inform Sci*, 486: 204-230. https://doi.org/10.1016/j.ins.2019.02.055

Chai XL, Gan ZH, Yuan K, et al., 2019. A novel image encryption scheme based on DNA sequence operations and chaotic systems. *Neur Comput Appl*, 31(1):219-237.

https://doi.org/10.1007/s00521-017-2993-9

Chen YC, Tang CM, Ye RS, 2020. Cryptanalysis and improvement of medical image encryption using high-speed scrambling and pixel adaptive diffusion. *Signal Process*, 167:107286. https://doi.org/10.1016/j.sigpro.2019.107286

Dagadu JC, Li JP, Addo PC, 2019a. An image cryptosystem based on pseudorandomly enhanced chaotic DNA and random permutation. *Multim Tools Appl*, 78(17): 24979-25000. https://doi.org/10.1007/s11042-019-7693-2

Dagadu JC, Li JP, Aboagye EO, 2019b. Medical image encryption based on hybrid chaotic DNA diffusion. *Wirel Pers Commun*, 108(1):591-612. https://doi.org/10.1007/s11277-019-06420-z

Daubechies I, Sweldens W, 1998. Factoring wavelet transforms into lifting steps. *J Four Anal Appl*, 4(3):247-269. https://doi.org/10.1007/BF02476026

Devi RS, Thenmozhi K, Rayappan JBB, et al., 2019. Entropy influenced RNA diffused quantum chaos to conserve medical data privacy. *Int J Theor Phys*, 58(6):1937-1956. https://doi.org/10.1007/s10773-019-04088-6

Dhall S, Pal SK, Sharma K, 2018. Cryptanalysis of image encryption scheme based on a new 1D chaotic system. *Signal Process*, 146:22-32. https://doi.org/10.1016/j.sigpro.2017.12.021

Diaconu AV, 2016. Circular inter–intra pixels bit-level permutation and chaos-based image encryption. *Inform Sci*, 355-356:314-327. https://doi.org/10.1016/j.ins.2015.10.027

Dzwonkowski M, Rykaczewski R, 2019. Secure quaternion Feistel cipher for DICOM images. *IEEE Trans Image Process*, 28(1):371-380. https://doi.org/10.1109/TIP.2018.2868388

Farah MAB, Guesmi R, Kachouri A, et al., 2020. A novel chaos based optical image encryption using fractional fourier transform and DNA sequence operation. *Opt Laser Technol*, 121:105777. https://doi.org/10.1016/j.optlastec.2019.105777

Fridrich J, 1998. Symmetric ciphers based on two-dimensional chaotic maps. *Int J Bifurc Chaos*, 8(6):1259-1284. https://doi.org/10.1142/S021812749800098X

Ghebleh M, Kanso A, 2019. A novel efficient image encryption scheme based on chained skew tent maps. *Neur Comput Appl*, 31(7):2415-2430. https://doi.org/10.1007/s00521-017-3199-x

Guan MM, Yang XL, Hu WS, 2019. Chaotic image encryption algorithm using frequency-domain DNA encoding. *IET Image Process*, 13(9):1535-1539. https://doi.org/10.1049/iet-ipr.2019.0051

Hua ZY, Yi S, Zhou YC, 2018. Medical image encryption using high-speed scrambling and pixel adaptive diffusion. *Signal Process*, 144:134-144. https://doi.org/10.1016/j.sigpro.2017.10.004

Kumar S, Panna B, Jha RK, 2019. Medical image encryption using fractional discrete cosine transform with chaotic function. *Med Biol Eng Comput*, 57(11):2517-2533. https://doi.org/10.1007/s11517-019-02037-3

Liu H, Zhao B, Huang LQ, 2019a. A novel quantum image encryption algorithm based on crossover operation and mutation operation. *Multim Tools Appl*, 78(14):20465-20483. https://doi.org/10.1007/s11042-019-7186-3

Liu H, Zhao B, Huang LQ, 2019b. A remote-sensing image encryption scheme using DNA bases probability and two-dimensional logistic map. *IEEE Access*, 7:65450-65459. https://doi.org/10.1109/ACCESS.2019.2917498

Liu JZ, Tang SS, Lian J, et al., 2019. A novel fourth order chaotic system and its algorithm for medical image encryption. *Multidim Syst Sign Process*, 30(4):1637-1657. https://doi.org/10.1007/s11045-018-0622-0

Liu ZT, Wu CX, Wang J, et al., 2019. A color image encryption using dynamic DNA and 4-D memristive hyper-chaos. *IEEE Access*, 7:78367-78378. https://doi.org/10.1109/ACCESS.2019.2922376

Luo J, Qu SC, Xiong ZL, et al., 2019. Observer-based finite-time modified projective synchronization of multiple uncertain chaotic systems and applications to secure communication using DNA encoding. *IEEE Access*, 7:65527-65543. https://doi.org/10.1109/ACCESS.2019.2917706

Luo Y, Du M, Liu J, 2015. A symmetrical image encryption scheme in wavelet and time domain. *Commun Nonl Sci Numer Simul*, 20(2):447-460. https://doi.org/10.1016/j.cnsns.2014.05.022

Mahdi MSR, Al Aziz MM, Alhadidi D, et al., 2019. Secure similar patients query on encrypted genomic data. *IEEE J Biomed Health Inform*, 23(6):2611-2618. https://doi.org/10.1109/JBHI.2018.2881086

Moafimadani SS, Chen YC, Tang CM, 2019. A new algorithm for medical color images encryption using chaotic systems. *Entropy*, 21(6):577. https://doi.org/10.3390/e21060577

Mohamed Parvees MY, Abdul Samath J, Parameswaran Bose B, 2017. Medical images are safe—an enhanced chaotic scrambling approach. *J Med Syst*, 41(10):167. https://doi.org/10.1007/s10916-017-0809-1

Praveenkumar P, Amirtharajan R, Thenmozhi K, et al., 2015. Medical data sheet in safe havens—a tri-layer cryptic solution. *Comput Biol Med*, 62:264-276. https://doi.org/10.1016/J.COMPBIOMED.2015.04.031

Premkumar R, Anand S, 2019. Secured and compound 3-D chaos image encryption using hybrid mutation and crossover operator. *Multim Tools Appl*, 78(8):9577-9593. https://doi.org/10.1007/s11042-018-6534-z

Ravichandran D, Praveenkumar P, Balaguru Rayappan JB, et al., 2016. Chaos based crossover and mutation for securing DICOM image. *Comput Biol Med*, 72:170-184. https://doi.org/10.1016/j.compbiomed.2016.03.020

Ravichandran D, Praveenkumar P, Rayappan JBB, et al., 2017. DNA chaos blend to secure medical privacy. *IEEE Trans NanoBiosci*, 16(8):850-858. https://doi.org/10.1109/TNB.2017.2780881

Rehman AU, Wang HW, Shahid MMA, et al., 2019. A

selective cross-substitution technique for encrypting color images using chaos, DNA rules and SHA-512. *IEEE Access*, 7:162786-162802. https://doi.org/10.1109/ACCESS.2019.2951749

Stalin S, Maheshwary P, Shukla PK, et al., 2019. Fast and secure medical image encryption based on non linear 4D logistic map and DNA sequences (NL4DLM_DNA). *J Med Syst*, 43(8):267. https://doi.org/10.1007/s10916-019-1389-z

Suri S, Vijay R, 2020. A Pareto-optimal evolutionary approach of image encryption using coupled map lattice and DNA. *Neur Comput Appl*, 32:11859-11873. https://doi.org/10.1007/s00521-019-04668-x

Wang XY, Zhang JJ, Cao GH, 2019. An image encryption algorithm based on zigzag transform and LL compound chaotic system. *Opt Laser Technol*, 119:105581. https://doi.org/10.1016/j.optlastec.2019.105581

Yosefnezhad Irani B, Ayubi P, Amani Jabalkandi F, et al., 2019. Digital image scrambling based on a new one-dimensional coupled sine map. *Nonl Dynam*, 97(4): 2693-2721. https://doi.org/10.1007/s11071-019-05157-5

Zhang XC, Zhou Z, Niu Y, 2018. An image encryption method based on the feistel network and dynamic DNA encoding. *IEEE Photon J*, 10(4):3901014. https://doi.org/10.1109/JPHOT.2018.2859257