I. J. Computer Network and Information Security, **2022, 2, 67-76**
Published Online April 2022 in MECS (http://www.mecs-press.org/)
DOI: 10.5815/ijcnis.2022.02.06

Robust 4-D Hyperchaotic DNA Framework for Medical Image Encryption

Shaymaa Fahmee Alqazzaz
Faculty of Science, Al-Azhar University, Cairo, Egypt
E-mail: shaemaaabdalrhman.stuw.1871@azhar.edu.eg

Gaber A. Elsharawy
Faculty of Science, Al-Azhar University, Cairo, Egypt
E-mail: gaberelsharawy274.el@azhar.edu.eg

Heba F. Eid
Faculty of Science, Al-Azhar University, Cairo, Egypt
E-mail: heba.fathy@azhar.edu.eg, eid.heba@gmail.com

Received: 26 July 2021; Revised: 17 September 2021; Accepted: 03 November 2021; Published: 08 April 2022

Abstract: With the integration of cloud computing approaches in the healthcare systems, medical images are now processed and stored remotely on third-party servers. For such digital medical image data, privacy, protection, and security must be maintained by using image encryption methods. The aim of this paper is to design and apply a robust medical encryption framework to enhance the protection of medical image transformation and the patient information confidentiality. The proposed Framework encrypt the digital medical images using DNA computation and hyperchaotic RKF-45 random sequence approach. For which, the DNA computation is enhanced by applying hyperchaoticRKF-45 random key to the different Framework phases. The simulation results on different medical images were measured with various security analyses to prove the proposed framework randomness and coherent. Simulation results showed the ability of the hyperchaotic DNA encryption framework to withstand multiple electronic attacks with high performance compared to its counterparts of encryption algorithms. Finally, simulation and comparative studies have shown that, the proposed cryptography framework reported UACI and NPCR values 33.327 and 99.603 respectively, which are near to the theoretical optimal value.

Index Terms: Image Encryption, Medical Image, DNA Computing, Hyperchaotic System.

1. Introduction

In the contemporary internet world, e-Health services plays a vital role [1, 2]. With the assistance of cloud computing and telecommunication model, the medical data are transmitted and stored from one location to another via different network media [3]. The e-Health services necessitate the medical image enabled health information exchange to provide doctors for faster access, interpretation and clinical diagnosis. Therefore, providing patient's medical image confidentiality is an essential security aspect of eHealth services.

For medical diagnosis purpose, the sent medical image should be received in perfect condition without any loss [4-6]. Cryptography is a science of applying logic and complex mathematics to design strong encryption methods to secure data and to retrieve the original data back by applying decryption [7-10].

Chaos-based ciphers can be used to employ secured and robust cryptosystem, due to the sensitivity to the deterministic pseudorandom behavior and initial conditions [11-13]. Hence, ciphers Chaos-based have been adapted for medical applications security [14-16]. However, most of the chaos encryption systems have showed severe security weaknesses that leave them open to classical attacks [17-19].

Due to the DNA molecule special characteristics, large information density and vast parallelism; DNA coding is applied to cryptography for improving the security and efficiency of encryption schemes [20-24].

Inspired by the DNA computing and chaos advantages, in this paper, a secure robust image encryption framework is proposed. The proposed cryptography Framework aims to enhance the confidentiality of patient information by protection of the digital medical images transformation. The proposed cryptography Framework encrypt the digital medical images using DNA computation and 4D chaotic system by utilizing hyperchaotic RKF-45 random key to the different Framework phases. Experimental and simulation results reveal that the proposed medical image cryptography framework exhibited high confidentiality and security in e-health care systems.

The rest of the manuscript is organized as follows: Section 2 presents the existing work related to image encryption. In section 3 and 4, a brief description of DNA Computing and Runge-Kutta-Fehlberg Method (RKF45) is presented. In section 5, the proposed medical image encryption HC RK45-DNA Framework is elaborated. In section 6 and 7, the simulation and security analysis of the proposed HC RK45-DNA encryption framework on different medical images is investigated and discussed. Finally, in section 8 the main findings of this work are discussed.

2. Related Work

Hu et al. [25] introduced a DNA-based image cryptography, for which, they overcome the DNA complementary operation limitations by including the DNA operation into the diffusion process. In [24] Shyam et al. presented a novel image DNA computing encryption scheme, where they utilized the DNA sequences to encode the information and the XOR operation to encrypted the image.

Meanwhile, Chen et al, [26] proposed an encryption approach that classified an excellent performance due the features of 3D chaos maps such as periodicity. Li [27] has studied the performance of the Hierarchical Chaotic Image Encryption (HCIE) algorithm. HCIE is a two-stage permutation-based image encryption technique. The first stage permutes the image by dividing it into different blocks. While, the second stage permutes each image block pixel values. The author has remarked that the HCIS algorithm is less secure compared to the non- hierarchical structures permutation algorithms.

Zhao et al. [28] have introduced an image encryption chaos based system. The proposed system adapts the Arnold chaotic maps, where it is based on the permutation and substitution stages. For which, the pseudo random vectors for permutation are generated using Arnold map. Authors reported that the algorithm is secure in nature and has shown effective results. In [29] the authors introduced an image encryption model by generating a DNA masks using 2D logistic map; which was then used to produce the DNA matrix.

3. DNA Computing

DNA computing was proposed by L. Adleman [30] to solve the complex computational problem. In his research, Adleman discovered that DNA contains high computational and storage capability. He used DNA computation to solve the directed Hamiltonian route problem including seven vertices. For which, the molecules assumed as vertices and are encoded in a molecule sequence, then applied computations by chemical operations in lab.

DNA is a storing information particle in the living organisms .The DNA sequence contains four various bases; Adenine (A), Thymine (T), Cytosine (C) and Guanine (G) [31-33]. Therefore, in DNA computing; data is interpreted by four genetic character P= (A, T, C, G) as an alternative of the binary character P= (0, 1).By using DNA four genetic bases to encode 11, 10, 01 and 00, there are 24 coding schematics. However, only eight coding schematics content the Watson–Crick complement rules, given in Table 1. [31]. Moreover, in DNA computing [34, 35], the subtraction and addition executions are performed based on the classical rules of binary subtraction and addition rules.

Table 1. DNA Encoding and Decoding Rules

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

4. Runge-Kutta-Fehlberg Method (RKF45)

Runge-Kutta method is emerged for the numerical solving of initial value problems (IVP) with oscillating solution. It can be adapted to developed accurate high order numerical solution by finding the value of the functions' self without needing to calculate its derivatives [36]. To ensure the accuracy of the IVP solution, the problem need to be solved using two step sizes h=2 and h; then comparing the solutions at the mesh points correlating to the greater step size. However, this method necessitates a large computation for the smaller step size and have to be replicated if the agreement is insufficient. To try to resolve the above problem, the Runge-Kutta-Fehlberg (RKF45) method is developed [37]. RKF45 regulates if the proper step size (h) is being used. For which, two distinct approximations of the solution at each step are developed and compared. If the solutions are close in agreement to a certain accuracy, the approximation solution is accepted, otherwise the step size is minimized. While, the step size is maximized, if the two answers agree to a more significant than required. Each step requires the computation of the following:

$$\mathrm{k1} = \mathrm{hf}(t_k,\ t_y) \tag{1}$$

$$k2 = hf\left(t_k + \frac{1}{4}h, y_k + \frac{1}{4}k1\right) \quad (2)$$

$$k3 = hf\left(t_k + \frac{3}{8}h, y_k + \frac{3}{32}k1 + \frac{9}{32}k2\right) \quad (3)$$

$$k4 = hf\left(t_k + \frac{12}{13}h, y_k + \frac{1932}{2197}k1 - \frac{7200}{2197}k2 + \frac{7296}{2197}k3\right) \quad (4)$$

$$k5 = hf\left(t_k + h, y_k + \frac{439}{216}k1 - 8\,k2 + \frac{3680}{513}k3 - \frac{843}{4104}k2\right) \quad (5)$$

$$k6 = hf\left(t_k + \frac{1}{2}h, y_k - \frac{8}{27}k1 + 2\,k2 - \frac{3544}{2565}k3 + \frac{1859}{4104}k4 - \frac{11}{40}k5\right) \quad (6)$$

Then, the IVP approximation solution is determined using the following equation:

$$y_{k+1} = y_k + \frac{16}{135}k1 + \frac{6656}{12825}k3 + \frac{28561}{56430}k4 - \frac{9}{50}k5 + \frac{2}{55}k6 \quad (7)$$

5. The Proposed Medical Image Encryption Framework

The proposed framework hybrid the hyperchaotic RKF-45 random sequence and DNA computation for medical image encryption. The proposed schematic framework is shown in Fig.1.

A 4D hyperchaotic system is adapted to generate a random sequence. The obtained hyperchaotic sequence key is incorporated to the different Framework phases. The dynamics of the adapted 4D Hyperchaotic system has been presented by the following non-linear equations [38]:

$$\begin{cases} \dot{x_1} = a(x_2 - x_1) + \lambda_1 x_4 \\ \dot{x2} = cx_1 - x_1x_3 + \lambda_2 x_4 \\ \dot{x3} = -bx_3 + x_1x_2 + \lambda_3 x_4 \\ x4 = -dx_1 \end{cases} \quad (8)$$

The 4D Hyperchaotic system contains two non-linear product terms. For which, a, b , c , d , ג1 ,ג2 and ג3 are the system's control parameters. For parameter values, a = 35, b = 3, c = 35, d = 5, ג1 = 1, ג2 = 0.2, ג3 = 0.3, the 4D Hyperchaotic system's Lyapunov exponent is 0.5, 0.2117, 0, -38.7068; for which the system presents a super hyperchaotic behavior.

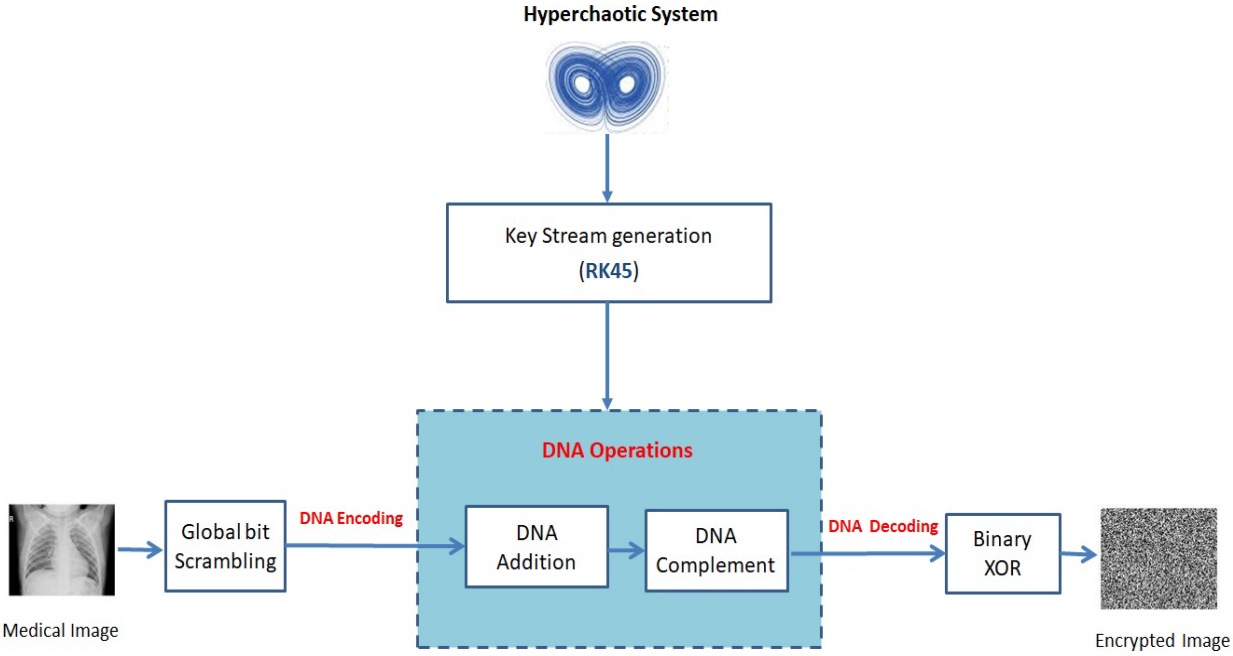

Fig.1. Hyperchaotic RKF45-DNA Encryption Framework.

5.1. Hyperchaotic RKF-45 Random Sequence Generation Algorithm

The Hyperchaotic RKF-45 random sequence key generation methodology is as follows:

Step 1: Iterate the 4D-hyperchaotic system equation 8 with (h, x_n) for N iteration to eliminate the harmful transitional procedure effect and to increase the security.

Step 2: For (n * m) times iterate equation 8; using the RKF45 equation 7 to calculate the values of x1, x2, x3 andx4.

Step 3: Each x_i value generate two different key elements c_i^1 and c_i^2 where i = 1, 2, 3;,4 using the following equation:

$$c_i^1 = floor(((|x_i| - floor(|x_i|)) * 10^{15})/10^8) \; mod \; 256 \tag{9}$$

$$c_i^2 = floor(((|x_i| - floor(|x_i|)) * 10^{15}) mod 10^8)) \; mod \; 256 \tag{10}$$

Step 4: Concatenate c_i^1 andc_i^2 elements to obtain the random sequence key k.

5.2. Medical Image Encryption Algorithm

The proposed image encryption framework for medical images is given in detail as follows:

Step 1: Import the DICOM image P and get (m* n) the size of P.

Step 2: Generate the Hyperchaotic RKF-45 random sequence k, as discussed above.

Step 3: Perform image bit scrambling, where, the intensity values of P are represented by the binary values (b) that correspond to them. Then, divide image P intensity values into 8 bit planes.

Step 4: Fetch and sort different values of the hyperchaotic RKF45 sequence key k is, to obtain the index sequence k^t. Then, based on the index sequence moves b to b_k^t.

Step 5: Choose randomly a DNA encoding rule to encode b_k^t into a DNA sequence d1.

Step 6: apply DNA addition operation to d1 elements to obtain d2.

Step 7: Fetch a sequence k_{mn} from k, and transform it to a binary sequence k_b.

Step 8: Encode k_b with the same encoding rule (from step 5) to obtain d3.

Step 9: Based on the DNA XOR operation, perform: $\mathrm{b2} = k_b \; \mathrm{XOR} \; \mathrm{d3}$. Then, convert the binary sequence b2 to a cipher image Pc.

6. Simulation and Security Analysis

With the aim of investigating the efficiency and capabilities of the proposed HC RK45-DNA encryption framework; Matlab R2015b was used for the implementation purposes. All of the study experiments were carried out on Intel(R), Core i7-4910 MQ CPU 2.90GHz and 16GB RAM.

The proposed encryption framework was applied on six medical images. The initial parameters of the proposed HC RK45-DNA frame work are set as following "x1(0), x2(0), x3(0), x4(0) = 0.12, 0.23, 0.34, 0.45". All the medical images and their counterparts' encrypted/decrypted images are depict in Fig.2. Fig.2 demonstrates that; no effective information can be obtained from the encrypted images and are in a random noise style.

6.1. Key sensitivity analysis

Key sensitivity is a crucial part to assess the strength of the encryption method. Whereby, a little change on the encryption/decryption key value leads to a completely different encrypted/decrypted image. To experiment the proposed HCRK45-DNA key sensitivity, the value of the initial parameterx_0 is changed from 0.12 to 0.12e-10; from the original encryption key. The related decrypted images after the key alteration are shown in Fig.3. Fig.3 demonstrates that, applying decryption with a slightly differing key will not give the original image; which proves that the proposed HC RK45-DNA has adequate capability of resisting exhaustive attack.

6.2. Histogram Analysis

The histogram of the image illustrates the image pixel value distribution. The encrypted medical images histograms are shown in Fig.4. From Fig.4 it's clear that; the encrypted medical images histograms are very stale and smooth. This uniform encrypted image distribution will not provide any meaningful information to an attacker; therefor, the proposed HC RK45-DNA resists statistical attacks effectively.

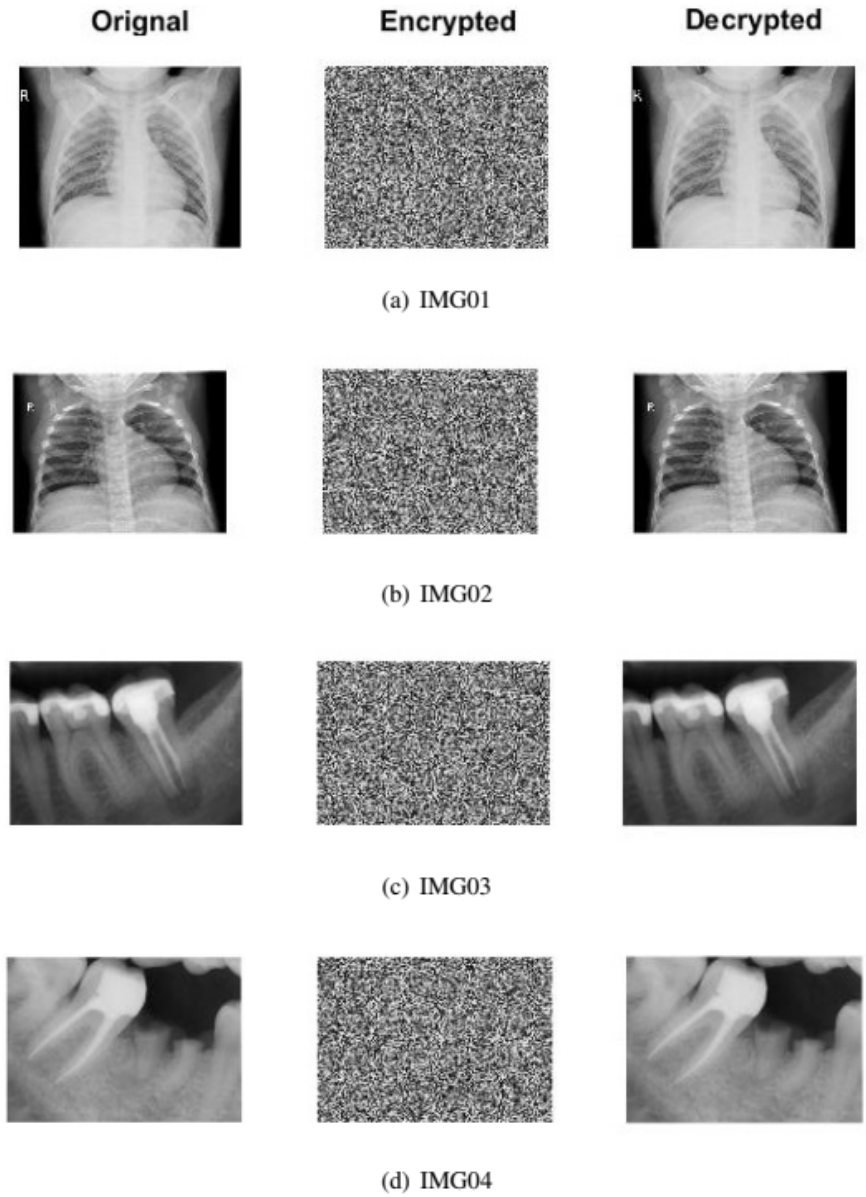

Fig.2. Medical original and encrypted test images

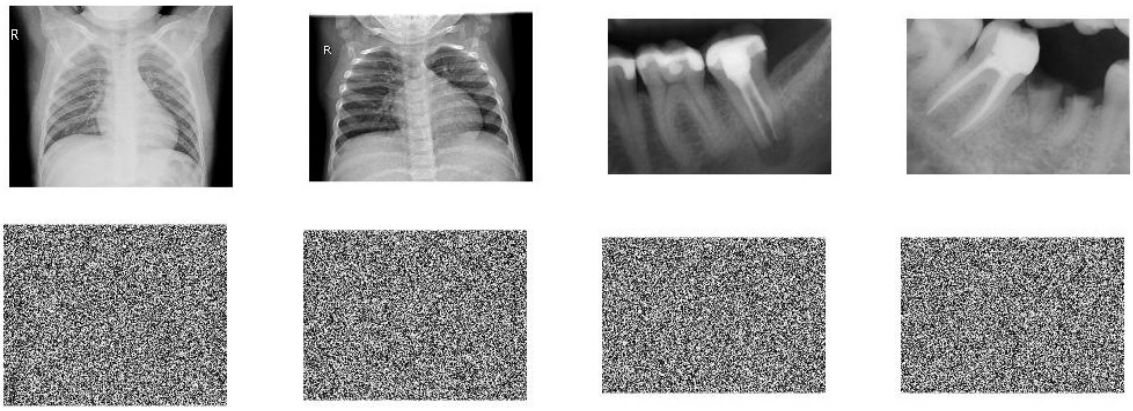

Fig.3. Decrypted medical images with correct key x0 = 0.12 and incorrect key x0 = 0.12e - 10

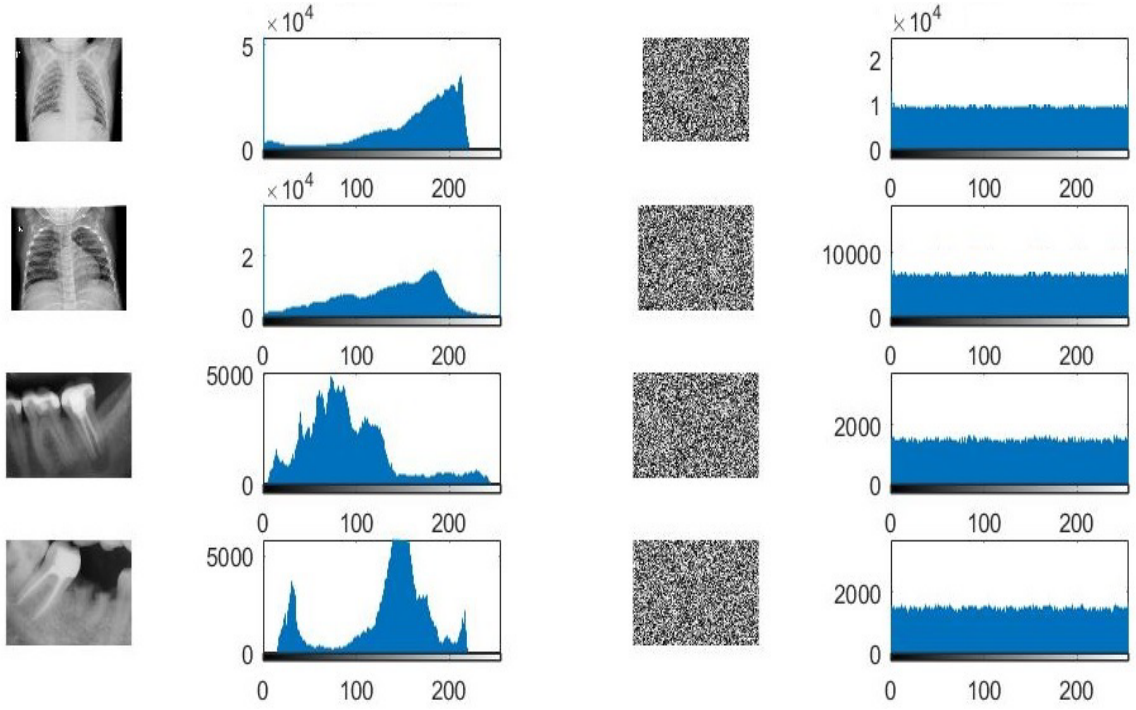

Fig.4. Histograms of the medical images and their corresponding encrypted images

6.3. Correlation Coefficient Analysis

Correlation coefficient is a crucial metric to assess the correlation between the image adjacent pixels. To verify the proposed HC RK45-DNA encryption security, the correlation coefficient is analyzed in the vertical, horizontal and diagonal direction. The formula of the correlation coefficient is given by:

$$\lambda_{xy} = \frac{COV(x,y)}{\sqrt{D(x)\sqrt{D(y)}}} \tag{11}$$

$$\mathrm{D(x)} = \frac{1}{W\times H}\sum_{P=1}^{H}\ \sum_{q=1}^{W}\ [x(p,q) - E(x)]^2 \tag{12}$$

$$\mathrm{Cov(x,y)} = \frac{1}{W\times H}\sum_{P=1}^{H}\ \sum_{q=1}^{W}[x(p,q) - E(x)][y(p,q)E(y)] \tag{13}$$

$$\mathrm{E(X)} = \frac{1}{W\times H}\sum_{P=1}^{H}\ \sum_{q=1}^{W} x(p,q) \tag{14}$$

The correlation coefficient values of the original medical images and the encrypted images that correspond to them are reported in Table 2. From Table 2., the horizontal, vertical, and diagonal correlation coefficient values are close to ”0” for encrypted images. Thereby indicates that; the randomness of the encrypted image pixels reached maximum. Fig.5 shows the adjacent pixels correlation in original and encrypted image.

Table 2. The Correlation Coefficient of Original Test and Encrypted Images

Medical Image	Vertical correlation λ_v		Horizontal correlation λ_h		Diagonal correlation λ_d	
	Original Image	Encrypted Image	Original Image	Encrypted Image	Original Image	Encrypted Image
IMG01	0.9970	0.00021	0.99729	-0.00087	0.9960	-0.00021
IMG02	0.9962	-0.00109	0.9977	-0.00082	0.9963	0.00089
IMG03	0.9989	0.00048	0.9985	-0.00163	0.9984	-0.00051
IMG04	0.9983	0.00015	0.9973	0.00037	0.9982	0.00014

Fig.5 reveals that; the high correlation existence in the original image is scattered in its resulting encrypted images; which verifies the good encryption security the proposed HCRK45-DNA algorithm provides.

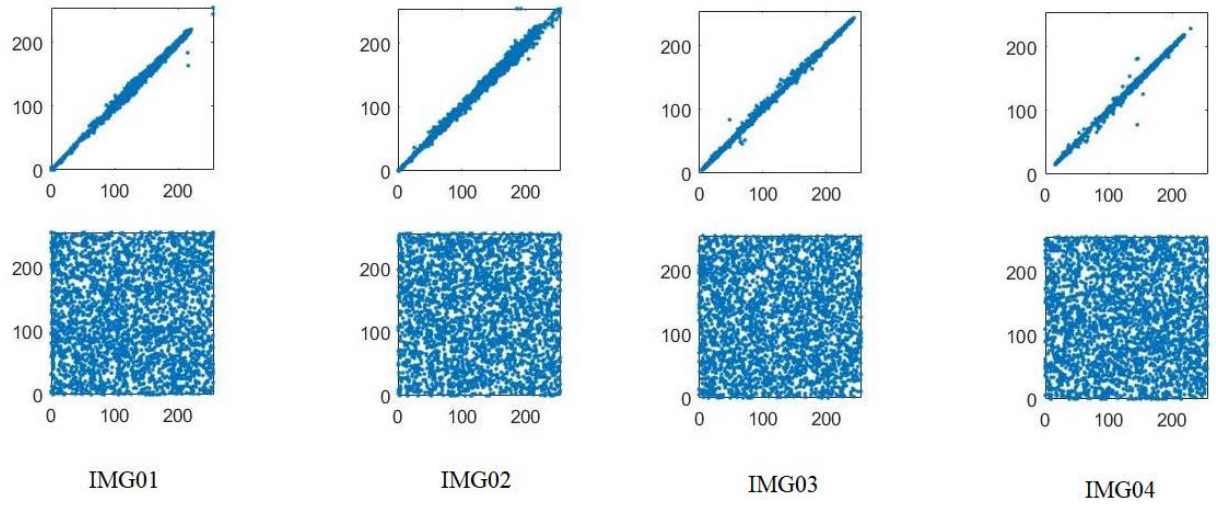

Fig.5. Horizontal adjacent pixel distribution of the original images and the encrypted images.

6.4. Information Entropy Analysis

The entropy of the image measures the amount of information redundancy in an event. Bigger information entropy indicates more randomness and higher security the encryption algorithm provides. Since each byte has 8 bits, the maximum information amount present in a byte of an image should be 8. The information entropy of an image is defined as:

$$H(Q_i) = -\sum_{i=0}^{255} p(Q_i)\, log_2\ \ p(Q_i) \tag{15}$$

Where p $(Q)_i$ is the occurring probability of symbol Q_i. The information entropy values of the medical original and encrypted images are given in Table 3. As shown in Table 3, the encrypted images entropy values are near to the ideal value "8". Hence, the encrypted image pixels are independent of each other statistically, which indicates the difficulty to decrypt the HC RK45-DNA encrypted images.

Table 3. The Information Entropy Values of the Test Medical Images

Medical Image	Original Image Entropy	Encrypted Image Entropy
IMG01	6.94104236604948	7.99649256554477
IMG02	5.29059671063522	7.98910516850633
IMG03	6.39696019981591	7.99873639562868
IMG04	6.08646923173147	7.9989390680445

6.5. Differential Attack Analysis

To assess the ability of the proposed HC RK45-DNA system to resist differential attack; the unified average changing intensity (UACI) and the number of pixel change rate (NPCR) are measured. If a small variation in the original medical image can effectuate to a great variation in the encrypted image, then the algorithm can subsequently be able to effectively defend against differential attacks. The UACI and NPCR are calculated by the following equations:

$$\text{NPCR} = \frac{1}{w \times H} \sum_{i=1}^{w} \sum_{j=1}^{H} D_{ij} \times 100 \tag{16}$$

Where:

$$D_{ij} = \begin{cases} 0, & Q1(i;\ j) = Q2(i,j) \\ 1, & Q1(i;\ j) \neq Q2(i,j) \end{cases} \tag{17}$$

$$\text{UACI} = \frac{1}{w \times H} \sum_{i=1}^{w} \sum_{j=1}^{H} D_{ij} \frac{(Q1(i,j) - Q2(i\ j))}{255} \times 100 \tag{18}$$

Theoretically the optimal values of UACI and NPCR and 33.4635 and 99.6094, respectively. A pixel is selected randomly from the original medical image and is changed for 10 times; the average values of UACI and NPCR are calculated.

The calculated UACI and NPCR results are summarized in Tables 4. As reported in Tables 4 the NPCR values are nearing to 99.6 which illustrate that, at most all the pixels between encrypted images Q_1 and Q_2 have been changed

entirely. Furthermore, the reported UACI values are nearing to the theoretical optimal value. Therefore, the results indicate that the proposed HC RK45-DNA satisfy the expected secure performance against differential attacks.

Tables 4. The UACI and NPCR Values of the Medical Test Images

Medical Image	NPCR	UACI
IMG01	99.105679	32.762518
IMG02	99.565625	33.327747
IMG03	99.603908	33.014542
IMG04	99.603908	33.012166

7. Discussion

In this study, a 4D hyperchaotic framework based on RKF45 and DNA to be utilized in the e-healthcare systems is presented. The 4D hyperchaotic system has ten terms, two of which are nonlinear. The maximum Lyapunov exponent of the 4D hyperchaotic system is 0.5. The bigger the Lyapunov exponent is, the faster the trajectories separate the chaotic region is. Thus, the dynamic behavior of the system is better than one-dimensional chaotic system. For solving the 4D hyperchaotic system and generating a random sequence key, RKF-45 algorithm has been chosen. Which leads to enhance the uncertainty and randomness in the hyperchaotic system. Hence, to adequate capability of resisting exhaustive attack by increasing the cryptography key sensitivity. Moreover, the framework is conceptually based on the DNA biological operation with conjunction with XOR and computational operations, which increases the complexity of the framework. Therefore, as shown by the experimental studies the proposed 4D hyperchaotic RK45-DNA framework effectively satisfy the secure performance against resists statistical attacks and differential attacks.

8. Conclusion

In order to improve the security of e-health care systems, medical image encryption is the best method to conserve the patient’s information confidentiality. This study aims to propose a robust and efficient medical image encryption framework based on 4-D hyperchaotic RKF45-DNA. The proposed framework chaotic sequences are produced by the RKF45 method. Then, the sequence are integrated to 4-D hyperchaotic to generate the random key sequence. Moreover, DNA addition and subtraction operations were adopted to increase the proposed framework cipher unpredictability and efficiency. For the proposed encryption framework the DICOM image is used as the input image. The security analysis, including key sensitive, correlation, histogram and information entropy, verify that the proposed encryption framework has good complexity and security in medical image. The key space is sufficiently large to withstand the brute-force attack. Moreover, NPCR and UACI analysis are conducted, results show that the proposed HC-RK45-DNA framework is robust against differential attacks. In future work, the proposed framework will be improved by studding different 4-D Hyperchaotic system. In addition, an enhanced version of the proposed framework will be studied by proposing and examining higher Hyperchaotic system dimensions.

References

[1] Thinzar Saw, Phyu Hnin Myint, "Feature Selection to Classify Healthcare Data using Wrapper Method with PSO Search", International Journal of Information Technology and Computer Science, Vol.11, No.9, pp.31-37, 2019.

[2] Senny Hapiffah, Ardiles Sinaga, "Analysis of Blokchain Technology Recommendations to be Applied to Medical Record Data Storage Applications in Indonesia", International Journal of Information Engineering and Electronic Business, Vol.12, No.6, pp. 13-27, 2020.

[3] S. C. S. Rabi Prasad Padhy, Manas Ranjan Patra, Cloud computing: Security issues and research challenges, International Journal of Computer Science and Information Technology Security, 2 (1) (2011) 136–148.

[4] X. Deng, Z. Chen, F. Zeng, Y. Zhang, Y. Mao, Authentication and recovery of medical diagnostic image using dual reversible digital watermarking, J Nanosci Nanotechnol 13 (3) (2013) 2099–2107.

[5] S. Das, M. K. Kundu, Effective management of medical information through a novel blind watermarking technique, J Med Syst 36 (5) (2012) 3339–3351.

[6] Z. Subedar, A. Araballi, Hybrid cryptography: Performance analysis of various cryptographic combinations for secure communication, International Journal of Mathematical Sciences and Computing 6 (4) (2020) 35–41.

[7] Sunil Kumar, Sandeep Kumar, Gaurav Mittal, Dharminder Dharminder, Shiv Narain," Non-singular Transformation Based Encryption Scheme ", International Journal of Mathematical Sciences and Computing, Vol.7, No.3, pp. 32-40, 2021.

[8] B. Delman, Genetic algorithms in cryptography, m. s. thesis (2004).

[9] Zuhi Subedar, Ashwini Araballi. " Hybrid Cryptography: Performance Analysis of Various Cryptographic Combinations for Secure Communication ", International Journal of Mathematical Sciences and Computing, Vol.6, No.4, pp.35-41, 2020.

[10] S. Jamuna, P. Dinesha, K. Shashikala, K. Kishore Kumar, Design and implementation of reliable encryption algorithms through soft error mitigation, International Journal of Computer Network and Information Security 12 (4) (2020) 41–50.
[11] S. G. Lian, A bloc cipher based on chaotic neural networks, Neuro computing 72 (4) (2009) 1296–1301.
[12] C. Fu, W.-H. Meng, Y.-F. Z. al., An efficient and secure medical image protection scheme based on chaotic maps, Computers in Biology and Medicine 43 (8) (2013) 1000–1010.
[13] C.-F. Lin, C.-H. Chung, J.-H. Lin, A chaos-based visual encryption mechanism for clinical eeg signals, Medical and Biological Engineering and Computing 47 (7) (2009) 757–762.
[14] N. Zhou, A. Zhang, F. Zheng, L. Gong, Novel image compression encryption hybrid algorithm based on key controlled measurement matrix in compressive sensing, Optics Laser Technology 62 (2014) 152–160.
[15] C. Fu, G.-Y. Zhang, O. Bian, W.-M. Lei, M. Hong-feng, A novel medical image protection scheme using a 3-dimensional chaotic system, PLoS ONE 9 (2015) 12.
[16] L. B. Zhang, Z. L. Zhu, B. Q. Yang, W. Y. Liu, H. F. Zhu, M. Y. Zou, Cryptanalysis and improvement of an efficient and secure medical image protection scheme, Mathematical Problems in Engineering 11 (2015).
[17] E. Solak, C. Cokal, Algebraic break of image ciphers based on discretized chaotic map lattices, Inf. Sci 181 (1) (2011) 227–233.
[18] D. Arroyo, G. Alvarez, J. M. Amig´o, S. Li, Cryptanalysis of a family of self-synchronizing chaotic stream ciphers, Commun. Nonlinear Sci Numer. Simul 16 (2) (2011) 805–813.
[19] X. Wang, L. Liu, Cryptanalysis of a parallel sub-image encryption method with high-dimensional chaos, Nonlinear Dyn. 73 (1) (2013) 795– 800.
[20] B. Wang, Q. Zhang, X. Wei, Tabu variable neighborhood search for designing dna barcodes, IEEE Trans. NanoBiosci 19 (2020) 127–131.
[21] X. Li, B. Wang, H. Lv, Q. Yin, Q. Zhang, X. Wei, Constraining dna sequences with a triplet-bases unpaired, IEEE Trans. NanoBiosci 19(2020) 299–307.
[22] G. Xiao, L. Mingxin, L. Qin, X. Lai, New field of cryptography: Dna cryptography, Chin. Sci Bull 51 (12) (2006) 1413–1420.
[23] Y. Zhang, L. H. B. Fu, Research on dna cryptography, Applied cryptography and network security, InTech Press, Rijeka, Croatia (2012) 357–376.
[24] M. Shyam, N. Kiran, V. A. Maheswaran, novel encryption scheme based on dna computing, HIPC 2007 (2007).
[25] T. Hu, C.-J. Ouyang, Y. Liu, L.-H. Gong, An image encryption scheme combining chaos with cycle operation for dna sequences, Nonlinear Dyn 87 (2016) 51–66.
[26] G. Chen, Y. Mao, C. K. Chui, A symmetric image encryption scheme based on 3d chaotic cat maps, Chaos, Solitons Fractals 21 (3) (2004) 749–761.
[27] Li, C. “Cracking a hierarchical chaotic image encryption algorithm based on permutation”, Signal Processing, 118, 203-210 2016.
[28] Zhao, J., Guo, W. and Ye, R.: A chaos-based image encryption scheme using permutation substitution architecture. Int. J. Comput Trends Technol, 15(4), 174-185 2014
[29] H. Liu, B. Zhao, L. Huang, Aremote-sensing image encryption scheme using dna bases probability and two-dimensional logistic map, IEEE Access 7 (2019) 65450–65459.
[30] Adleman LM. “Molecular computation of solutions to combinatorial problems”. Science, JSTOR ,1994;266:1021–4
[31] J. D. Watson, F. H. Crick, Molecular structure of nucleic acids: a structure for deoxyribose nucleic acid, Nature 171 (4356) (1953) 737–738.
[32] K. Li, S. Zou, J. Xv, Fast parallel molecular algorithms for DNA based computation: Solving the elliptic curve discrete logarithm problem over gf(2 n), Journal of Biomedicine and Biotechnology, Hindawi. 2008 (2008) 1–10.
[33] S. Roweis, E. Winfreel, R. Burgoyne, A sticker based model for DNA computation, Journal of Computational Biology 5 (4) (1998) 615–629.
[34] E. B. Baum, DNA sequences useful for computation, in: Proceedings of DNA-based Computers II, Princeton. In AMS DIMACS Series, Vol. 44, 1999, pp. 235–241.
[35] O. D. King, P. Gaborit, Binary templates for comma-free dna codes, Discrete Applied Mathematics 155 (6-7) (2007) 831–839.
[36] L. Zheng, X. Zhang, Chapter 8 - numerical methods, in: Modeling and Analysis of Modern Fluid Problems, Mathematics in Science and Engineering, Academic Press, 2017, pp. 361–455.
[37] C. F. Mayo, Implementation of the runge-kutta-fehlberg method for solution of ordinary differential equations on a parallel processor, M.S. in Applied Mathematics (1987).
[38] L. Chunlai, Y. Simin, A new hyperchaotic system and its adaptive tracking control, Acta Phys. Sin. 61 (4) (2012) 22–28.

Authors’ Profiles

Shaima Fahmee Al-Qazzaz, graduated in 2017 from Mosul University, Faculty of Computer Science and Mathematics, she is currently a master student at Department of Mathematics, Faculty of Science, Al-Azhar University, Cairo, Egypt.

Gaber A Elsharawy, Professor of computer science at Faculty of science, Al Azhar university. Ph.D. in Computer and Systems Engineering, Faculty of Engineering, Al Azhar University. M.Sc.in computer system U.S. Air Force University, Air Force Institute of Technology (AFIT), Dayton, Ohio, USA. Author of many publications in the fields of Database management systems, artificial intelligent, modeling & simulation, and programming languages.

Heba F. Eid is an Associate Professor at Faculty of Science, Al-Azhar University, Egypt. She received her Ph.D. degree in Network Intrusion Detection and M.S. degree in Distributed database systems, both from Faculty of Science, Al-Azhar University, Egypt. Her research interests include multi-disciplinary environment involving computational intelligence, pattern recognition, computer vision, bio-inspired computing and cyber security. Dr. Heba has served as a reviewer for various international journals and a program committee member of several international conferences.

How to cite this paper: Shaymaa Fahmee Alqazzaz, Gaber A. Elsharawy, Heba F. Eid, "Robust 4-D Hyperchaotic DNA Framework for Medical Image Encryption", International Journal of Computer Network and Information Security(IJCNIS), Vol.14, No.2, pp.67-76, 2022. DOI: 10.5815/ijcnis.2022.02.06