Secure Image Encryption Model for Cloud-Based Healthcare Storage Using Hyperchaos and DNA Encoding

Arun Amaithi Rajan(✉), Vetriselvi Vetrian, and Aruna Gladys

Department of Computer Science and Engineering, College of Engineering Guindy,
Anna University, Chennai 600025, India
arunamaithirajan@gmail.com, kalvivetri@gmail.com, gladys.vimalan@gmail.com

Abstract. In recent years, security and privacy have drawn a lot of attention due to digital communications and the widespread usage of multimedia transmissions over unsecured channels. In every area of analytics, digital images are essential. Sensitive image information like fingerprints, medical records, or defense satellite images needs to be securely stored and processed in a cloud server. In this article, we come up with a novel image encryption model for medical images utilizing a combination of chaotic maps over the DNA-encoded image with bit plane scrambling. Hyperchaotic maps are used to generate confusion keys and Chaotic maps are used for diffusion keys generation. The robustness and resistance of the system to attacks like differential attacks and statistical attacks are shown and extensively analyzed in terms of the security of the proposed model.

Keywords: Secure Data Storage · Medical Images · Image Encryption · DNA Encoding · Chaotic Maps · Hyperchaos · Bit plane Scrambling

1 Introduction

In the era of digitalization, a huge amount of digital information is transferred everywhere through data networks. Another widely used type of communication is multimedia files. Multimedia files can be images, videos, or audio. According to statistics, 1.72 trillion images are taken every year, it may increase by 10–14% every year just from smartphones. By 2030, the world will have taken 28.6 trillion images, more than doubling the current number [1]. From the statistics, It is vivid that images are playing a major role in digital data analytics.

Typically, digital images are stored in a cloud server, which is prone to cyber-attacks such as statistical attacks, differential attacks, etc., Generally, High-sensitive images like healthcare images are at high risk. This kind of critical data needs to be securely stored and accessed over the cloud [2]. When it comes

Published by Springer Nature Switzerland AG 2023
S. Chandran K R et al. (Eds.): ICCIDS 2023, IFIP AICT 673, pp. 89–103, 2023.
https://doi.org/10.1007/978-3-031-38296-3_8

Fig. 1. Secure Cloud Storage

with cloud security it can be achieved through secure storage and secure access control. Figure 1 depicts the secure cloud storage for any multimedia database in general.

Image encryption is the most effective and secure approach for storing images in a cloud environment. For image encryption, numerous encryption methods are emerging [3]. The chaotic system has emerged as the top option for cryptographic systems because of its super sensitivity to starting values and control parameters, great ergodicity, and greater pseudo-randomness [4]. Large-scale parallel processing of DNA molecules is possible with enormous storage and extremely low power requirements [5]. As a result, a series of image encryption techniques is suggested by fusing chaotic mapping with DNA coding technology [6].

In this article, we introduced a new image encryption technique based on DNA encoding, chaotic maps, and a bit plane scrambling technique. The primary contributions to the proposed work are listed below.

1. A novel image encryption model which combines bit plane scrambling with chaotic maps for secure medical image storage in the cloud is proposed.
2. Utilized 4D hyperchaotic map for confusion. Henon map and Tent map for diffusion.
3. It has been shown through experimental investigation that the suggested model is secure against a variety of attacks.

The rest of the article is structured as follows: Sect. 2 briefs the existing image encryption schemes. Preliminaries have been explained in Sect. 3. Section 4 details the introduced encryption model. Section 5 discusses the security analysis of the suggested encryption model. The conclusion of the paper with future works is summarized in Sect. 6.

2 Literature Review

The Focus of this section is recent works done in image security. There exist different types of image encryption algorithms available in the spatial domain, optical domain, transform domain, and compressive sensing [3]. More intriguing algorithms based on metaheuristics, chaotic maps, DNA encoding, cellular automata, fuzzy, etc. can be found in the spatial domain. One of the key industries that leverage medical image analysis to identify problems is Healthcare.

Priyanka et al. [7] provides a comprehensive analysis of the encryption techniques that can be used for healthcare images along with recommendations for further research.

Nowadays, because of their unique properties, chaotic maps, and systems are used in image encryption techniques. Rakheja et al. [8] utilized a 3D Lorenz chaotic system with QR decomposition in a 2D non-separable linear canonical transform domain for image encryption. They used Lorenz chaotic sequence for the pixel transaction process. Lin et al. [9] suggested a quantum key generator-based image encryption system for medical images employing cutting-edge quantum technology. Hyperchaotic maps have started to be used in encryption models as an alternative to simple chaotic maps. A unique encryption method created by Paul et al. [4] combines pixel-shifting based on the Zaslavskii map with SHA-2 and hyperchaotic maps methods.

DNA encoding provides better diffusion in image encryption schemes. Wan et al. [6] unveiled an image encryption scheme using double chaos with DNA-encoding. They combined a 1D chaotic map with a hyperchaotic Qi System for increased security. Bao et al. [10] employed a compressive sensing technique with Chen chaotic map over the DNA encoded image. Interestingly, a 4D-hyperchaotic map integrated with a DNA-encoding scheme is designed and verified by Aarthi et al. [11] with medical images. DNA-encoding based encryption scheme for multimedia is extended to cloud applications also [12].

Pixel permutations and block permutations are majorly used in image encryption schemes. Bit planes are used for scrambling to diffuse the image matrix. Zhang et al. [13] incorporated both bit-plane decomposition and dynamic DNA encoding for multimedia encryption schemes and proved that the system is secure against noise and crop attacks. Sukumar et al. [14] focused on efficient image steganography technique that exploits Arnold scrambling, laplacian Pyramid, Redundant Integer Wavelet Transform (RIWT), and histogram shifting algorithm in the medical context.

According to the literature review, combining bit-plane scrambling, multiple chaotic maps, and DNA encoding would increase the security of image encryption. In light of these three strategies, we developed a novel image encryption model.

3 Preliminaries

In this section, we have discussed the basic definitions of utilized concepts in an employed encryption model. Bit plane scrambling, DNA encoding, and Chaotic maps are briefed.

3.1 Bit Plane Scrambling

A digital image's bit plane is a collection of bits that correspond to specific bit positions in each of the binary numbers used to represent a pixel. For example, if each pixel is 8-bit, then an image contains 8-bit planes. Figure 2 shows the bit plane scrambling technique which shuffles the bit planes randomly.

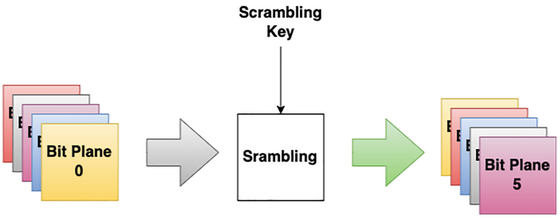


Fig. 2. Bit plane Scrambling

3.2 DNA Encoding

A technique for transforming data into the deoxyribonucleic acid (DNA) sequence of adenine(A), cytosine(C), guanine(G), and thymine(T) is known as DNA encoding [15]. A DNA sequence can be created from binary data. The eight DNA encoding techniques are listed in the following Table 1. We can also perform arithmetic and logical operations on DNA-encoded information.

Table 1. Rules for DNA Encoding

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

3.3 Chaotic Maps

Chaotic Maps are the studies of dynamic systems that exhibit non-linear random behaviors frequently. One-dimensional and high-dimensional systems are two different categories of chaotic systems. Hyperchaotic systems are chaotic systems with more than 4D and 2 positive Lyapunov exponents. Complexity-wise, hyperchaotic maps surpass chaotic ones. The use of 1D chaotic may not always be the most effective method for image encryption. This makes it far more challenging to anticipate the behavior of hyperchaotic maps, even when variables are compromised. Hyperchaotic maps ultimately produce higher degrees of security performance. We elaborated the tent and henon chaotic maps as well as the 4D hyperchaotic map in this subsection.

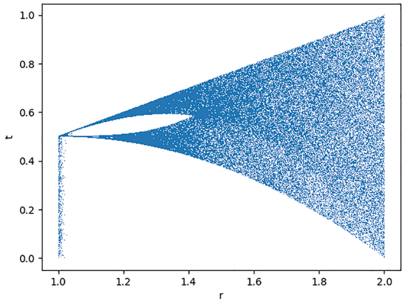


Fig. 3. Tent Map Bifurcation diagram

3.3.1 Tent Map

This map is a piecewise linear, 1D map with chaotic dynamics on the range [0,1] [16]. It is written mathematically as:

$$t_{k+1} = \begin{cases} rt_k, & \text{if } t_k < 0.5. \\ r(1-t_k), & \text{if } t_k \geq 0.5. \end{cases} \tag{1}$$

where t_0 is the initial parameter $t_0 \in [0,1]$ and the control parameter r, $r \in [0,2]$. The bifurcation diagram of the tent map is shown in Fig. 3.

3.3.2 Henon Map

This map is a 2D quadratic map [17] given by the following Eqs. 2 and 3.

$$x_{n+1} = 1 - ax_n^2 + y_n \tag{2}$$

$$y_{n+1} = bx_n \tag{3}$$

Two parameters, a and b, with values of 1.4 and 0.3 for the traditional Henon map, determine the map's behavior. The Henon map is chaotic for these a and b values. The map could be chaotic for different values of a and b. Figure 4 depicts the Henon map's bifurcation diagram.

3.3.3 4D Hyperchaotic Map

The normal three-dimensional Lorenz chaotic equations are extended by one or more state variables to produce hyperchaotic structures. The chaotic behavior is non-periodic because the structure has two or more positive Lyapunov exponents. 4D nonlinear differential Eqs. 4–7 are used to represent the hyperchaotic system [18].

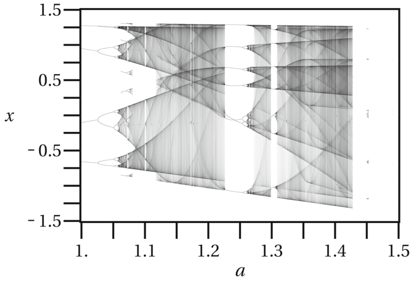


Fig. 4. Henon Map Bifurcation diagram when b=0.3

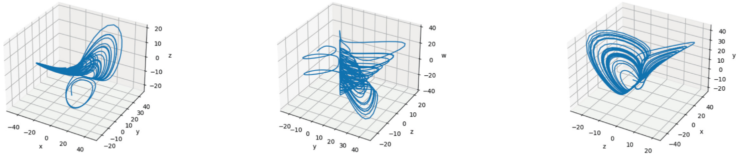
$$x_{n+1} = \alpha(x_n - y_n) - y_n z_n + w_n \tag{4}$$

$$y_{n+1} = -\beta y_n + x_n z_n \tag{5}$$

$$z_{n+1} = -\gamma z_n + \delta x_n + x_n y_n \tag{6}$$

$$w_{n+1} = -\epsilon(x_n + y_n) \tag{7}$$

where the control parameters are α, β, γ, δ, and ϵ. When $\alpha = 0.98$, $\beta = 9$, $\gamma = 50$, $\delta = 0.06$, $\epsilon = 0.9$ and initial values $x_0 = 11.28$, $y_0 =$ -11.21, $z_0 =$ -9, $w_0 = 20.49$, system is chaotic. Figure 5 shows the hyperchaotic map's bifurcation diagram in the 3D planes.



(a) xyz plane

(b) yzw plane

(c) zxy plane

Fig. 5. Hyperchaotic Map Bifurcation diagram

4 Encryption Model

This section explains the proposed encryption model and the steps required in depth. The proposed encryption workflow is depicted in Fig. 6. Keys are generated and shared with users by Key Management Centre (KMC).

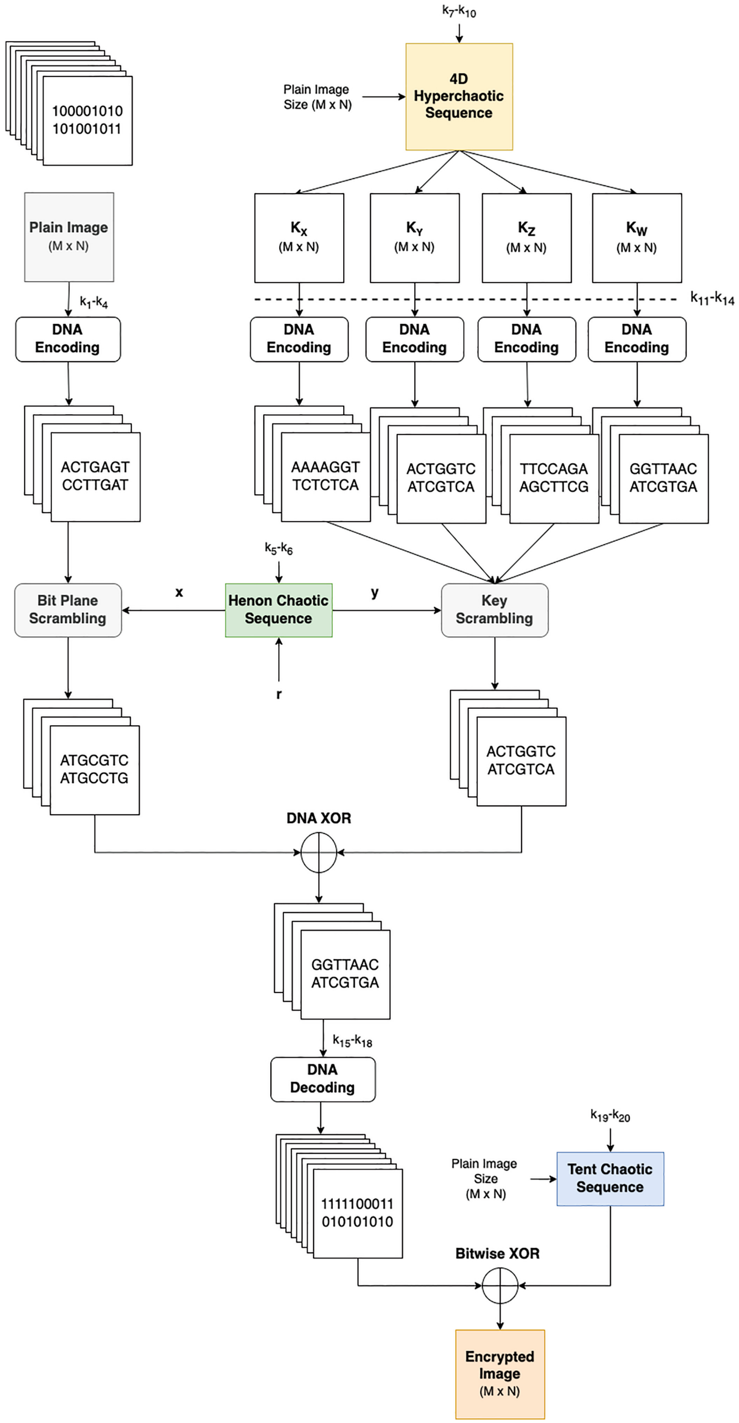


Fig. 6. Proposed Encryption Flow

4.1 Steps Involved in the Encryption Model

Input: Medical Image M_i and $Key = \{k_1, k_2, k_3, k_4, ..., k_{20}\}$ from KMC
Output: Cipher Image C_i
Steps:

Step 1: Read input image $M_i = \{M_{i0}, M_{i1}, M_{i2}, M_{i3}, M_{i4}, M_{i5}, M_{i6}, M_{i7}\}$

Step 2: Convert the 8-bit planes of the image into DNA encoded 4 planes $D_i = \{D_{i0}, D_{i1}, D_{i2}, D_{i3}\}$ using k_1, k_2, k_3, k_4

Step 3: Generate bit plane scrambling key (k_{bps}) and key scrambling key (k_{ks}) from the Henon map by giving initial parameter $x_0 = k_5, y_0 = k_6$ and seed r. There is an assumption that r is being secretly shared between the image sender and the image receiver.

Step 4: Scramble D_i using k_{bps}, Output $BPS_i = \{BPS_{i0}, BPS_{i1}, BPS_{i2}, BPS_{i3}\}$

Step 5: Generate the 4D hyperchaotic sequences K_X, K_Y, K_Z, K_W by feeding the initial parameters $x_0 = k_7, y_0 = k_8, z_0 = k_9, w_0 = k_{10}$ to the chaotic system represented by Eqs. 5–8. Each sequence is exactly the same size as image M_i

Step 6: Convert all 4 keys generated in the previous step K_X, K_Y, K_Z, K_W using $k_{11}, k_{12}, k_{13}, k_{14}$ into 16 DNA encoded keys $\{D_{kx1}, D_{kx2}, D_{kx3}, ..., D_{kz3}, D_{kz4}\}$

Step 7: Utilize k_{ks} as a seed to randomly select 4 keys from the 16 keys $SK_i = \{SK_{i0}, SK_{i1}, SK_{i2}, SK_{i3}\}$

Step 8: $DX_i = DNA\_XOR(BPS_{ik}, SK_{ik})$, k varies from 0 to 3

Step 9: Decode the DNA encoded 4 planes of DX_i into 8-bit planes (INT_i) using $k_{15}, k_{16}, k_{17}, k_{18}$. INT_i is the intermediate image.

Step 10: Generate a chaotic sequence T_i for pixel diffusion using tent key by giving initial parameters $t_0 = k_{19}, \mu = k_{20}$.

Step 11: $C_i = BITWISE\_XOR(INT_i, T_i)$

Decryption is the reverse of the given steps. The original image can be obtained using the following equation.

$$M_i = Decryption(C_i, Key, r) \tag{8}$$

4.2 Key Usage

Table 2. Sub-keys Utilization

Sub-keys	Chaotic Map	Usage
$k_5 - k_6$	Henon 2D Map	Scrambling keys
$k_7 - k_{10}$	Hyperchaotic Map (4D)	Confusion keys
$k_{19} - k_{20}$	Tent 1D Map	Diffusion keys

Encryption and decryption keys are generated and shared by KMC. The master key comprises 20 sub-keys in the encryption model. 8 sub-keys are used for DNA encoding while 4 sub-keys are used for DNA-decoding. The remaining 8 sub-keys are chaotic map initial parameters. Table 2 shows the utilization of the sub-keys in detail.

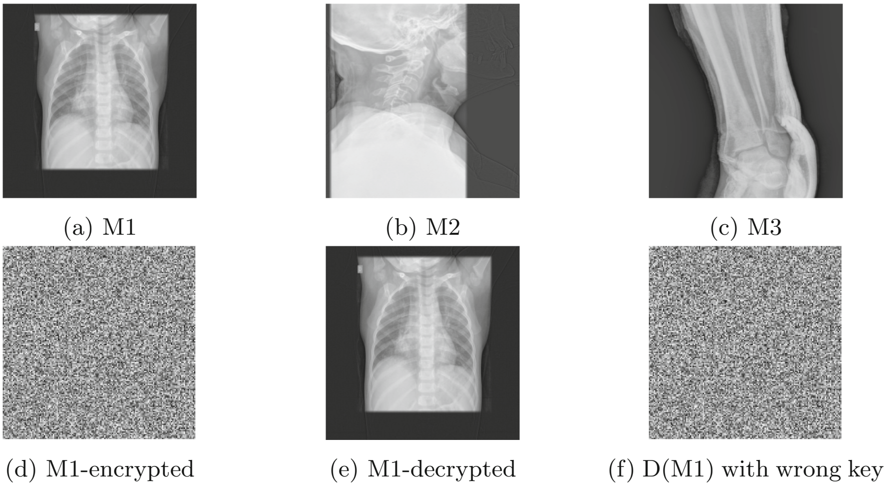
5 Results Discussion

5.1 Experimental Setup

An Intel(R) Core(TM) i7-4790 CPU running at 3.60 GHz, 16 GB of RAM, and Ubuntu 20.04 OS are used in the experiment. Python 3.8.10 is the programming language employed. The suggested encryption model is validated using Kaggle X-Ray Body parts Medical images.

5.2 Security Analysis

The secureness of the put-forward image encryption algorithm is analyzed using multiple metrics. It proves that the introduced scheme withstanding multiple cryptographic attacks such as chosen-plaintext attacks, differential attacks, histogram attacks, statistical attacks, and brute-force attacks. We have taken 3 medical images (M1, M2, M3) throughout the section to show the performance comparison. Figure 7(a)–(c) shows the selected medical images.


(a) M1 (b) M2 (c) M3

(d) M1-encrypted (e) M1-decrypted (f) D(M1) with wrong key

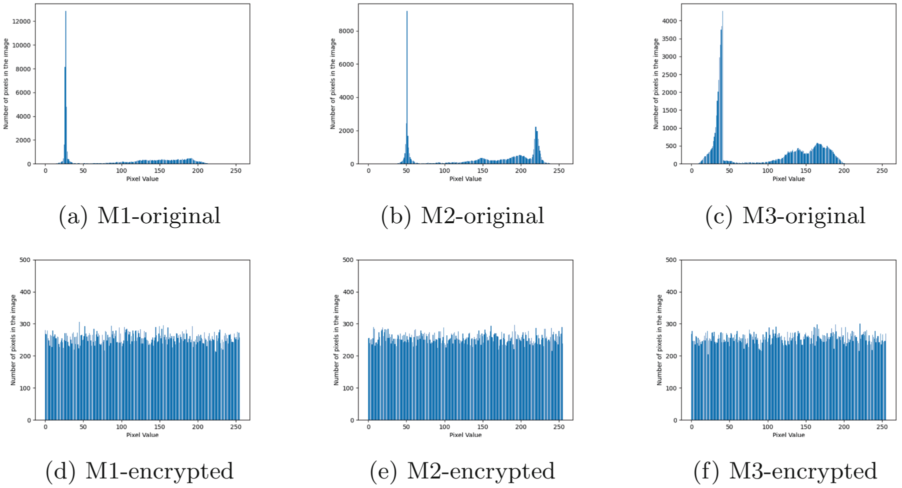
Fig. 7. Medical Images Encryption and Decryption Samples

5.2.1 Key Space Analysis and Key Sensitivity Analysis

The standard encryption model's key space should be adequate in size to fend off exhaustive attacks. There are eight major keys in the suggested algorithm. The size of the key space is $(2^{52} * 8 = 2^{416})$, which is larger than (2^{128}). The outcome shows the resilience of the encryption algorithm against brute-force attacks. The original image cannot be accurately decrypted back, and even a minute modification in the decryption key has a significant impact on the outcome, demonstrating the algorithm's high sensitivity. Figure 7(e) depicts the image that has been correctly decrypted, while Fig. 7(f) depicts the incorrectly decoded image with a slightly altered key.

5.2.2 Histogram Examination

The histogram showed the image's statistical properties. By counting the pixels, it primarily showed how the image's pixel values were distributed. The histogram of an image was flat when the values of each pixel were almost identical. This demonstrated how strong its defenses against statistical attacks were. The plaintext and ciphertext histograms of sample medical images are shown in Fig. 8. It shields the data against attackers using histograms.



(a) M1-original (b) M2-original (c) M3-original

(d) M1-encrypted (e) M2-encrypted (f) M3-encrypted

Fig. 8. Histogram Analysis

5.2.3 Chi-Squared Test

The χ^2 test is used to evaluate the evenness of the histogram. It is calculated using the following Eq. 9.

$$\chi^2 = \Sigma_{i=0}^{255} \frac{(Ob_i - Ex_i)^2}{Ex_i} \tag{9}$$

Here Ob_i is the observed value, Ex_i is the expected value. The critical value for this chi-square test is $\chi^2(255, 0.05) = 293$. Here the null hypothesis is 'Pixels are evenly distributed'. If the χ^2 test value is less than 293, then we can accept the null hypothesis. Table 3 shows the χ^2 test done over the selected images.

Table 3. χ^2 Test

Image	χ^2 Value	Critical Value	Decision (H = 0)
M1	278.93	293	Pass
M2	238.32	293	Pass
M3	251.13	293	Pass

5.2.4 Correlation Analysis

Image correlation is an indicator for evaluating the randomness of an image. The plaintext images adjacent pixels had a strong correlation. Randomness between the pixels could be increased by encrypting the plaintext image. The following Eqs. 10 to 13 help to derive the correlation coefficient of an image. There are 3 correlation coefficients Horizontal, Vertical, and Diagonal in image analysis.

$$E(p) = \frac{1}{n}\Sigma_{i=1}^{n} p_i \tag{10}$$

$$D(p) = \frac{1}{n}\Sigma_{i=1}^{n} (p_i - E(p))^2 \tag{11}$$

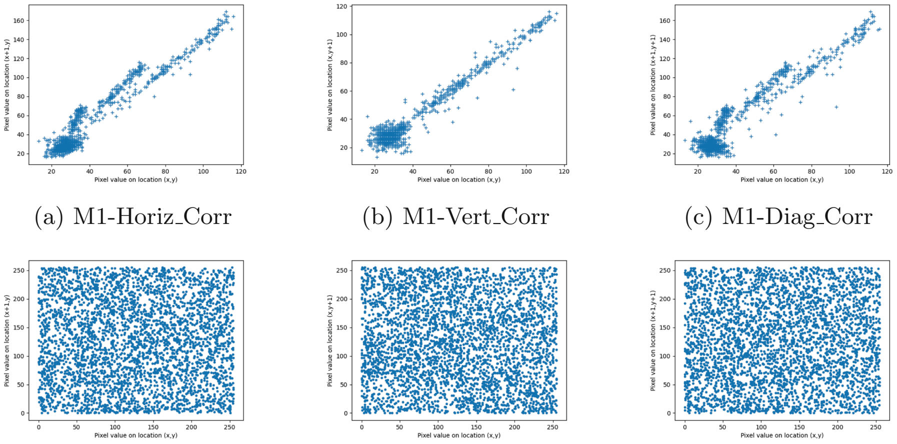
$$cov(p, q) = \frac{1}{n}\Sigma_{i=1}^{n} (p_i - E(p))(q_i - E(q)) \tag{12}$$

$$\rho_{pq} = \frac{cov(p, q)}{D(p)D(q)} \tag{13}$$

Table 4 shows the H, V, and D correlation values of the selected images. Horiz_Corr, Vert_Corr, Diag_Corr represents horizontal, vertical, and diagonal correlation coefficient respectively. Sub figures in Fig. 9 clearly explain the encrypted image M1's randomness in 3 directions.

Table 4. Correlation coefficient and Entropy Analysis

Image	Horiz_Corr		Vert_Corr		Diag_Corr		Entropy	
	Original	Encrypted	Original	Encrypted	Original	Encrypted	Original	Encrypted
M1	0.9169	−0.0046	0.6821	−0.0224	0.9962	−0.0245	5.9096	7.9969
M2	0.9969	0.0003	0.7952	0.0068	0.9933	−0.0280	6.4324	7.9973
M3	0.9983	0.0009	0.9557	−0.0307	0.9878	0.0683	6.4088	7.9972



(a) M1-Horiz_Corr (b) M1-Vert_Corr (c) M1-Diag_Corr

(d) E(M1)-Horiz_Corr (e) E(M1)-Vert_Corr (f) E(M1)-Diag_Corr

Fig. 9. Correlation Analysis of M1

5.2.5 Entropy Analysis

Entropy is a term used to describe how unpredictable visual information is. It is used to assess the uncertainty of the proposed algorithm. It is calculated using the following Eq. 14.

$$Ent = -\Sigma_{i=1}^{255} p_i log(p_i) \tag{14}$$

where Ent stands for Image M's entropy. The probability of event i is indicated by the symbol p_i. IE has a value between 0 and 8. If it's an 8-bit image, it ought to be close to 8. The sample image's entropy values are projected in Table 4.

5.2.6 Differential Attack Analysis

Utilizing a differential attack, it is possible to determine how sensitive the encryption technique is to even the smallest alterations in the plain image. The Unified Average Change in Intensity (UACI) and Number of Pixel Change Rate (NPCR) are the parameters utilized to assess how well the proposed technique thwarts differential attacks. Using the following Eqs. 15 and 16, we can determine NPCR.

$$NPCR = \frac{\Sigma_{l,m} Diff(l,m)}{w \times h} \times 100\% \tag{15}$$

Here,

$$Diff(l,m) = \begin{cases} \text{1, if M(l, m) equals C(l, m).} \\ \text{0, if M(l, m) not equals C(l, m).} \end{cases} \tag{16}$$

The letters w and h stand for the image's width and height, respectively. The value of $Diff(l,m)$ represents the difference between the corresponding pixels of the original image ($M(l,m)$) and the encrypted image ($C(l,m)$). UACI is the average difference in pixel intensity between the test and the encrypted image.

Table 5. Differential Attack Analysis

Image	UACI	NPCR
M1	33.92	99.60
M2	33.23	99.61
M3	33.01	99.63

It is yet another often-employed efficiency indicator for evaluating the capacity to resist a differential attack. The UACI value is determined using Eq. 17.

$$UACI = \frac{\Sigma_{u,v} M(u,v) - C(u,v)}{255 \times w \times h} \times 100 \tag{17}$$

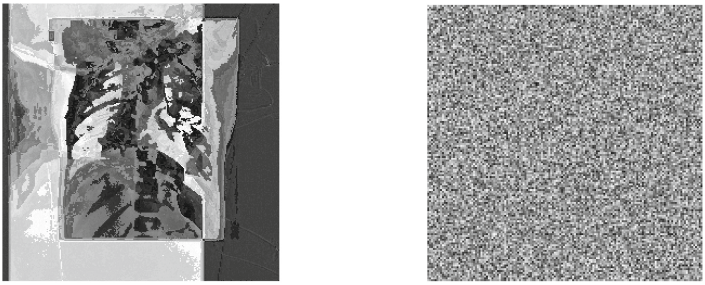
Table 5 lists the UACI and NPCR of the selected medical images in the proposed system.

5.2.7 Chosen Plaintext (CP) Attack Simulation

The suggested approach uses an XOR operation to diffuse the values of the pixels. Equation 18 is utilized to do the CP Attack analysis.

$$M_1(l,m) \oplus M_2(l,m) = Enc_1(l,m) \oplus Enc_2(l,m) \tag{18}$$

where M_1 and M_2 are two test images and the corresponding encrypted images are Enc_1 and Enc_2. If Eq. 18 is satisfied, then the CP attack is possible. The suggested approach is protected from a chosen-plaintext attack, as shown by Fig. 10, which demonstrates that Eq. 18 above is not justified.



(a) $M_1(l,m) \oplus M_2(l,m)$

(b) $Enc_1(l,m) \oplus Enc_2(l,m)$

Fig. 10. CP Attack Simulation

5.2.8 Comparative Analysis

This sub-section compared our proposed encryption model with existing image encryption models. Correlation, entropy, and differential attack metrics are taken for comparison. Table 6 shows the metrics values taken for analysis from existing models and our proposed model. From the analysis, it is vivid that the proposed hyperchaos with the bit-plane scrambling method shows better correlation coefficients.

Table 6. Security Parameters: Comparative Analysis

Reference	Horiz_Corr	Vert_Corr	Diag_Corr	Entropy	UACI	NPCR
[6]	0.0105	0.0020	0.0019	7.9971	33.52	99.61
[11]	0.0032	0.0048	−0.0016	7.9900	40.92	99.61
[19]	0.0007	0.0049	0.0030	7.9970	33.49	99.58
Ours	**−0.0011**	**−0.0154**	**−0.0682**	**7.9971**	**33.39**	**99.61**

6 Conclusion and Future Works

This article presented a novel encryption algorithm for medical images that uses bit-plane scrambling along with chaotic and hyperchaotic maps over DNA-encoded data. The system is strong and resistant to numerous threats, according to the security analysis. In the future, strong hyperchaotic sequences can be used to create keys. To increase the diffusion rate, scrambling can be applied to the row pixels and column pixels of each bit-plane. Fractal structures could potentially be used to increase the key's security.

References

1. Broz, M.: How many photos are there? (2023) 50+ Photos Statistics (2023). https://photutorial.com/photos-statistics/
2. Moosavi, S.R., Izadifar, A.: End-to-end security scheme for E-health systems using DNA-based ECC. In: Chang, S.Y., Bathen, L., Di Troia, F., Austin, T.H., Nelson, A.J. (eds.) SVCC 2021. CCIS, vol. 1536, pp. 77–89. Springer, Cham (2022). https://doi.org/10.1007/978-3-030-96057-5_6
3. Kaur, M., Kumar, V.: A comprehensive review on image encryption techniques. Arch. Comput. Methods Eng. **27**(1), 15–43 (2020). https://doi.org/10.1007/s11831-018-9298-8
4. Paul, L.S.J., Gracias, C., Desai, A., Thanikaiselvan, V., Suba Shanthini, S., Rengarajan, A.: A novel colour image encryption scheme using dynamic DNA coding, chaotic maps, and SHA-2. Multimed. Tools Appl. **81**, 37873–37894 (2022)
5. Namasudra, S.: A secure cryptosystem using DNA cryptography and DNA steganography for the cloud-based IoT infrastructure. Comput. Electr. Eng. **104**, 12 (2022)

6. Wan, Y., Gu, S., Du, B.: A new image encryption algorithm based on composite chaos and hyperchaos combined with DNA coding. Entropy **22**(2), 2 (2020)
7. Priyanka, Singh, A.K.: A survey of image encryption for healthcare applications. Evol. Intel. **16**, 801–818 (2023). https://doi.org/10.1007/s12065-021-00683-x
8. Rakheja, P., Vig, R., Singh, P.: Double image encryption using 3D Lorenz chaotic system, 2D non-separable linear canonical transform and QR decomposition. Opt. Quant. Electron. **52**(2), 2 (2020)
9. Lin, C.H., et al.: Intelligent symmetric cryptography with chaotic map and quantum based key generator for medical images infosecurity. IEEE Access **9**, 118 624–118 639 (2021)
10. Bao, W., Zhu, C.: A secure and robust image encryption algorithm based on compressive sensing and DNA coding (2022)
11. Arthi, G., Thanikaiselvan, V., Amirtharajan, R.: 4D Hyperchaotic map and DNA encoding combined image encryption for secure communication, pp. 15 859–15 878 (2022)
12. Namasudra, S., Chakraborty, R., Majumder, A., Moparthi, N.R.: Securing multimedia by using DNA-based encryption in the cloud computing environment. ACM Trans. Multimed. Comput. Commun. Appl. **16**(3s), 1 (2021)
13. Zhang, J., Huo, D.: Image encryption algorithm based on quantum chaotic map and DNA coding. Multimed. Tools Appl. **78**(11), 15 605–15 621 (2019)
14. Sukumar, A., Subramaniyaswamy, V., Ravi, L., Vijayakumar, V., Indragandhi, V.: Robust image steganography approach based on RIWT-Laplacian pyramid and histogram shifting using deep learning. Multimed. Syst. **27**(4), 651–666 (2021). https://doi.org/10.1007/s00530-020-00665-6
15. Kumar, A.: Data security and privacy using DNA cryptography and AES method in cloud computing. In: Proceedings of the 5th International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud), I-SMAC 2021, pp. 1529–1535 (2021)
16. Li, C., Luo, G., Qin, K., Li, C.: An image encryption scheme based on chaotic tent map. Nonlinear Dyn. **87**(1), 127–133 (2017)
17. Mishra, K., Saharan, R.: A fast image encryption technique using henon chaotic map. In: Pati, B., Panigrahi, C.R., Misra, S., Pujari, A.K., Bakshi, S. (eds.) Progress in Advanced Computing and Intelligent Engineering. AISC, vol. 713, pp. 329–339. Springer, Singapore (2019). https://doi.org/10.1007/978-981-13-1708-8_30
18. Ma, J., Yang, Y.: Hyperchaos numerical simulation and control in a 4D hyperchaotic system. Discrete Dyn. Nat. Soc. **2013**, 1–16 (2013)
19. Brahim, A.H., Pacha, A.A., Said, N.H.: A new image encryption scheme based on a hyperchaotic system & multi specific S-boxes. Inf. Secur. J. **32**, 59–75 (2021)