




**A DICOM ENCRYPTION ALGORITHM TO INCREASE SECURITY
AND PRIVACY IN HEALTH DATA MANAGEMENT BASED ON
PATIENT BIOMETRICS DATA, ARTIFICIAL INTELLIGENCE,
AND RNA ENCRYPTION ALGORITHM**

Soltani M.  , Shakeri H. * , Houshmand M. 

Abstract In the modern era, unauthorized access to health information systems (HIS) and electronic health records (EHR) must be prevented. In the subject of health data management (HDM), cyber-attacks are one of the important security risks. Medical information, such as EHR is delivered over an open network. Various approaches and technologies are used to ensure the security of medical information. One such technology is encryption, which protects medical images. This paper proposes an efficient hybrid encryption algorithm to secure digital imaging and communications (DICOM) in healthcare. The proposed algorithm uses artificial intelligence and RNA encryption. In the proposed algorithm, before receiving the patient's DICOM image, the patient's biometric information is evaluated using artificial intelligence, and if the received biometric is correct, in the next steps, DICOM is encrypted using an RNA encryption algorithm. The proposed encryption algorithm uses a patient's biometric information such as iris or fingerprint to create keys. According to the results of the proposed algorithm, the maximum entropy is more than 7.9998, NPCR is about 99.899, UACI is about 33.43, key space is more than 10^{89} , and correlation is Nonzero. This means that our algorithm is robust against brute-force attacks.

Key words: HDM, DICOM, Encryption, RNA encryption algorithm, Patient's biometric information, Artificial intelligence.

AMS Mathematics Subject Classification: 68P25.

DOI: 10.32523/2306-6172-2025-13-1-137-153

1 Introduction

Medical information security is one of the most important issues in HDM [1, 2, 3]. Health records such as DICOM images are highly sensitive and generated from various imaging technologies like conventional X-rays, ultrasound imaging, Computed Axial Tomography (CT), digital mammography, Positron Emission Tomography (PET), and Magnetic Resonance Imaging (MRI). To make an accurate diagnosis, DICOM images need to be protected from visual degradation and misdiagnosis [4, 5]. According to Fig. 1, encryption schemes play a key role in HDM security [1, 2, 3, 4, 5]. In this paper, we suggested a new robust hybrid cryptography algorithm based on symmetric keys and algorithms to increase security and prevent unauthorized access to the contents of encrypted DICOMs. Some properties of the proposed algorithm: Using artificial intelligence at the first step of cryptography to verify the validity of

*Corresponding Author.

biometric information, the next step is to use an RNA encryption algorithm and use the patient's biometric information to create its key, and all of the keys are interdependent to patient's biometric information such as fingerprint.

Using XOR to interdependent keys with the patient's biometric information and make the resulting keys unique after the cryptography process and using a digital signature (DSA) for verifying the authenticity of decrypted DICOMs. Using the RNA encryption algorithm and linking the keys of the RNA encryption algorithm to the patient's biometric information will increase the key space and resist brute-force attacks.

2 Literature review

In this section, we will review the preliminaries and related work in the field of image encryption.

2.1 Preliminaries

In this section, the most important concepts used in the proposed algorithm are described.

2.1.1 DICOM

DICOM is the standard for managing and communicating medical imaging information and related data. DICOM is most commonly used to store and transmit medical images such as X-rays, computed tomography (CT), ultrasound, radiotherapy, and magnetic resonance imaging (MRI) [4, 7]. Fig. 2 shows an example of DICOM images and the histogram of each of them.

2.1.2 Biometrics information

Biometrics are physical or behavioral characteristics of a human being that can be used to digitally identify an individual and grant access to systems, devices, or data, and biometric information such as a fingerprint can be considered unique to an individual [20, 21, 22]. Fingerprint has emerged as a successful biometric recognition system and

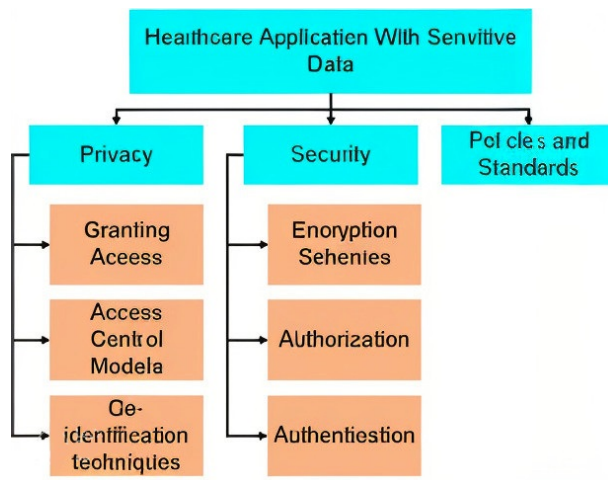


Figure 1: Privacy and security approach categories [2].

found its application in diverse domains [22]. Iris is considered a unique and powerful biometric that can be used as an authentication factor. Protecting the confidentiality of each individual's iris sample is an urgent requirement [23]. Fig. 3 shows an example of a fingerprint image and Fig. 4 shows an example of an iris image.

2.1.3 Using artificial intelligence algorithms to check the validity of biometric information

It is difficult to address cyber security assessment and crime detection in biometric information recognition. To recognize unique and discriminating aspects of biometric data, trained artificial intelligence algorithms like Support Vector Machine (SVM) and Adaptive Neuro-Fuzzy Inference System (ANFIS) have been presented [26]. In addition to the mentioned algorithms, in article number [27], other algorithms have been introduced to verify the accuracy of biometric information.

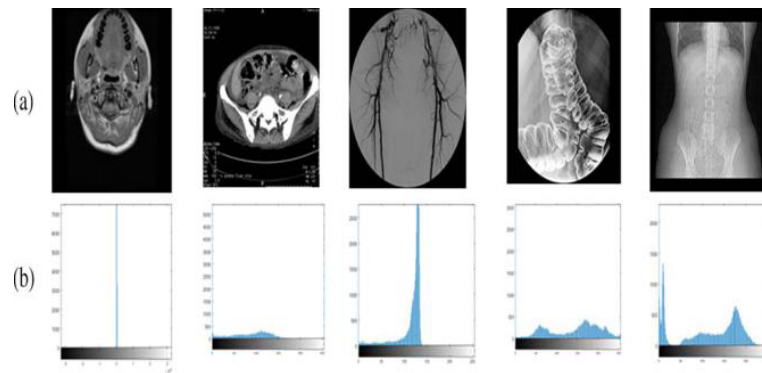


Figure 2: Histogram analysis of DICOM medical images. a: Sample medical images, b: histograms of (a) [20].

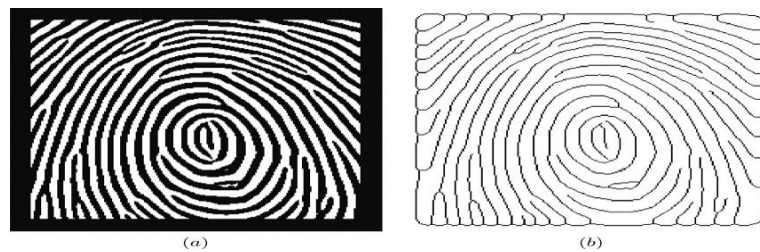


Figure 3: (a) Fingerprint Image and (b) Thinned image [22].

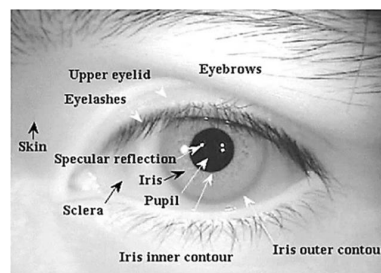


Figure 4: Human eye and iris [24, 25]

2.1.4 DNA encryption algorithm

DNA sequence has become extremely useful for information security and the attributes of DNA such as low power consumption and massive parallelism [7], have made them attractive candidates for cryptography schemes. DNA sequence structures are made up of four bases: Adenine (A), Thymine (T), Guanine (G), and Cytosine (C). Among these bases, A and T are complementary to each other while G and C are complementary to each other. According to Tab. 1, 0 and 1 are complementary in the binary, so 00 and 11 are complementary, and 01 and 10 are also complementary [7, 9]. By using four bases A, C, G, and T to encode 00, 01, 10 and 11, there are 24 kinds of coding schemes. But there are only eight kinds of coding schemes satisfy the Watson-Crick complement rule, which are shown in Tab. 1 [7, 9, 28]. For image encryption each pixel can be expressed as a DNA sequence whose length is 4 (its binary sequence's length is 8). For better understanding, we have given an example for a pixel with grayscale $225 = 11100001_2$. The DNA code for all existing rules in Tab. 2 is as follows: Rule1(TCAG), Rule2(TGAC), Rule3(CTGA), Rule4(GTCA), Rule5(CAGT), Rule6(GACT), Rule7(ACTG) and Rule8 (AGCT) [7, 9, 28]. According to XOR in binary, we can use it for DNA sequences and there exist eight kinds of DNA XOR rules. Each of the rules are defined in Tab. 3 [7, 9, 28].

2.1.5 RNA encryption algorithm

RNA has a single-stranded structure consisting of four nitrogenous bases: adenine (A), guanine (G), uracil (U), and cytosine (C). In RNA, thymine (T) is replaced by uracil

Table 1: The Watson-Crick complementing principle [7, 9, 28]

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

Table 2: Rules for DNA encoding and decoding [7, 9, 28]

Rules	A	T	C	G	Rules	A	T	C	G
Rules1	00	11	01	10	Rules5	01	10	11	00
Rules2	00	11	10	01	Rules6	10	01	11	00
Rules3	01	10	00	11	Rules7	11	00	01	10
Rules4	10	01	00	11	Rules8	11	00	10	01

Table 3: XOR operation in DNA [7, 9, 28]

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

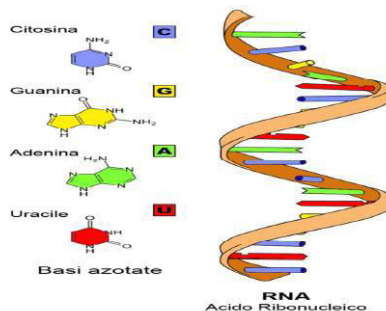


Figure 5: Structure of RNA [30].

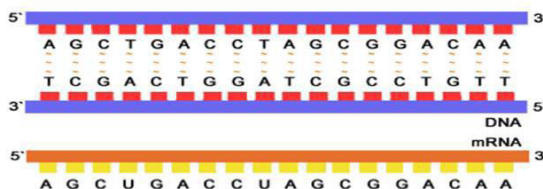


Figure 6: Transcription of DNA to mRNA [30].

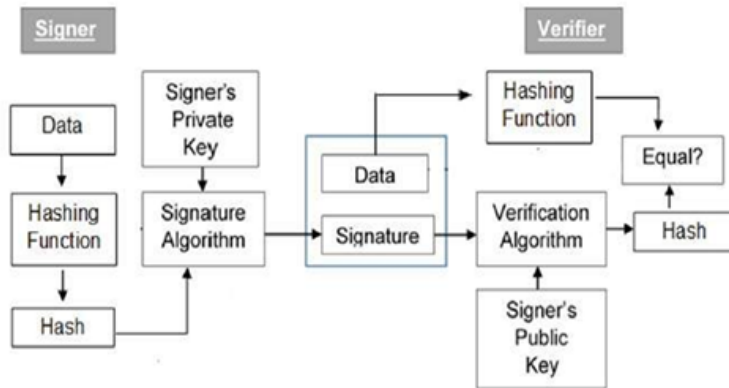


Figure 7: Overview of DSA algorithm [31, 32]

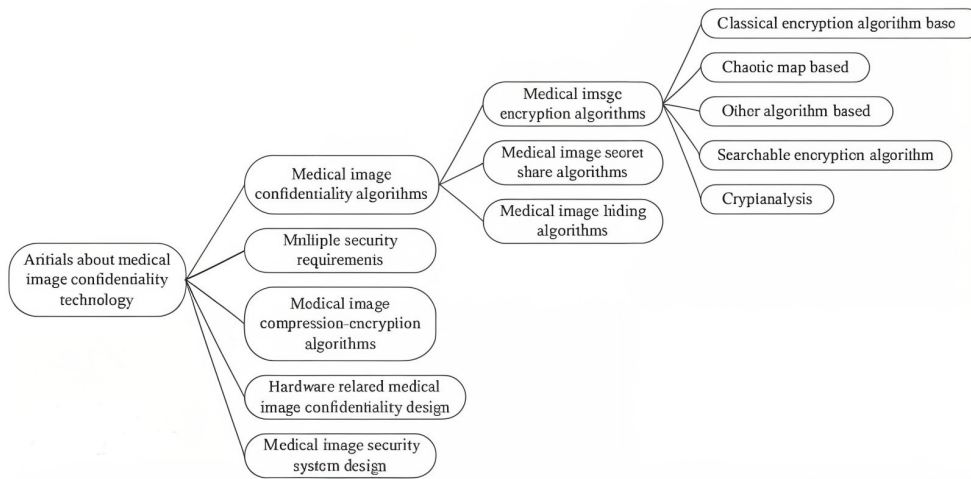


Figure 8: Classification of documents on medical image security techniques [6].

(U), as shown in Fig. 6. RNA undergoes two stages, transcription, and translation, before participating in protein synthesis. First, from the double-stranded DNA structure, coding DNA is used to create an RNA chain. We need to know that there are two types of RNA, mRNA (Messenger Ribonucleic Acid) and tRNA (Transfer Ribonucleic Acid). In this hybrid algorithm, we used mRNA type [7, 9, 28]. In Fig. 5 the structure of RNA is shown.

Fig. 6 demonstrates the fundamental concept of transcription by showing how Uracil replaces thymine in DNA to create mRNA.

2.1.6 DSA

DSA is an asymmetric key and it creates a digital signature [31]. Digital signatures do not directly affect plain text. A digital signature is a signature that is a mathematical method that is used to validate the accuracy and rectitude of a message such as security plain text or DICOM. It provides stronger data security for DICOM and another medical reports. We can use it to prove sender and receiver authentication. In DSA we must use a hash algorithm such as MD5 (Message digest algorithm) or SHA 256 (Secure hash algorithm 256). A hash function can be used by the sender to generate a message digest using private and public keys with encryption and decryption sign it digitally with the user's signature and send it to a receiver. The receiver has to use the sender's public key to decrypt the signature and the signature is valid when hash values are equal [31, 32]. DSA algorithm is displayed in Fig. 7.

2.2 Related work

In the field of encryption of medical images, many research works have been presented, especially in recent years, and various algorithms have been introduced. In reference [6], a comprehensive classification of medical image encryption algorithms is presented, which is shown in Fig. 8.

Dagadu, J.C., J.-P. Li, and E.O. Aboagye. [7], proposed a medical image encryption scheme based on the combination of multiple chaotic systems, MD5 hash functions, DNA, and algebraic XOR operations. This way, a simple image becomes partially dependent on the key sequence.

Chai, Xiuli, et al. [5], proposed a medical image encryption scheme that combines Latin square method and chaotic system. The main techniques used in this study are two-way adaptive diffusion and permutation-based simple images and Latin squares.

Praveenkumar, P., et al. [8], proposed a medical image encryption scheme based on DNA and chaos-based encryption system. In this study, combining Chaos maps and DNA improved the algorithm's robustness to statistical analysis.

Akkasaligar, Prema T. and Sumangala Biradar. [9], They proposed a medical image encryption scheme based on DNA cryptography and dual super-chaotic mapping techniques. In this paper, a permutation of the diffusion process is performed on a small number of selected pixels in a digitized medical image.

Fu et al. [10], Performed pixel shifting and spreading of DICOM images using Chen's 3D chaotic mapping to provide better protection against known chosen plaintext attacks.

Chandrasekaran et al. [4], proposed a DICOM encryption method that combines

number theory and Henon mapping. In this scheme, key matrices are shuffled, chaos is controlled by Henon mapping, and the system is resistant to attacks.

Seyedzadeh et al. [11], proposed a color image encoding high sensitivity, high security, and high-speed technique based on two-dimensional nonlinear chaos mapping. In medical images, multidimensional chaotic cryptography algorithms involving three or four variables are often used to transform image pixels. This increases security at the cost of increasing algorithmic complexity and computational cost.

Dai et al. [12], proposed an algorithm of cryptography medical graphics built on a combination of logistics maps and chebyshev maps. By configuring the logistic map appropriately, this algorithm first encodes the original image using the logistic map and then encodes it again using the chebyshev map. Both the key space and transmission security of this technology are excellent.

In [13] Proposed an image encryption method based on the combination of three one-dimensional chaotic maps. This method is more secure and less computationally expensive than more regular chaotic maps.

Ravichandran et al. [14], In this study logistics, tents and signs a new cryptography algorithm based on chaotic mapping is proposed to improve the security of real-time medical imaging applications. Chaos mapping is shown to improve the security of real-time medical imaging applications.

Boussif et al. [15], proposed an image encryption algorithm based on a matrix product and a separate add-on, which realizes the secure transmission of smartphone-encoded medical images. The operation of the cryptography technology is simple and the above system is very secure.

Wen et al. [16], applied DNA sequencing, and the chaotic system was used to encode sub-images. Chaos-based encryption method is ideal for encrypting medical images on mobile devices because it is considered secure and fast due to the limited processing power of smart devices.

Muthu, Joan S and Murali, P [17], proposed a DICOM encoding algorithm. To achieve high efficiency, the proposed system is designed to operate at the bit plane level. To create an effective encryption system, the number of bit planes is based on the characteristics of the stored bits, rather than the traditional method of assigning bits to each pixel.

Mortajez, S. et al. [18], proposed a DICOM encryption method. In this article, a chaotic system-based encryption method using a dynamic secret key was developed to encrypt medical images.

Ravichandran, D. et al. [19], proposed a DICOM cryptography algorithm. In order to protect digital medical images, this article analyzes an encryption method based on integer wavelet transform mixed with chaos and deoxyribonucleic acid.

3 Proposed scheme

In this section, we describe the proposed algorithm for DICOM encryption and explain its steps and details. The proposed scheme is defined based on the following.

Proposed scheme is defined based on the following.

3.1 Encryption algorithm

The block diagram of the proposed algorithm is shown in Fig. 9 and pseudo-code in Fig. 10. To increase security and prevent unauthorized access to the encrypted DICOM, our proposed hybrid algorithm uses patient's biometric information to makes the keys unique for each of the patients and create a digital signature using biometrics information.

The proposed scheme is determined based on the following steps:

1. Getting valid patient's biometric information using artificial intelligence algorithms.
2. Encrypting the hash results of the valid patient's biometric information using the private key and then creating a digital signature.
3. In this step, RNA keys are converted to the hash result, and then a digital signature from step 2 is converted to the hash result, and then hash results will be XOR to each other to make keys for RNA encryption algorithm and, after that DICOM will be encrypted using RNA encryption algorithm.

3.2 Decryption algorithm

Based on the digital signature structure, the User can find the hash result of the patient's biometric information by using a public key and then the reverse operation of the encryption process in step 3 decrypts the cipher image to its exact original form.

4 Experimentation results and security analysis

In this section, based on the most important encryption parameters, the proposed algorithm is evaluated in different DICOM images. In this evaluation, issues such as key space have also been evaluated.

4.1 Introducing the most important parameters in image encryption algorithms

The parameters defined in this section are the most important in image encryption algorithms. Parameters are calculated based on their mathematical formulas.

4.1.1 MSE and PSNR

The mean-square error (MSE) and the peak signal-to-noise ratio (PSNR) are employed to assess the picture compression quality. MSE represents the cumulative squared error between the encrypted image and the main image. In other words, MSE calculates approximately the average of squared errors between the original medical image in digital format I_o and the ciphered medical digitalized image I_e . MSE is defined in Eq. (1), whereas peak error is measured by PSNR or in other words, It is used to determine whether the transmission of noise alters how valuable the digitalized medical image is Eq. (2) defines the PSNR [9].

$$MSE = \frac{1}{S} \sum_S [I_o(m, n) - I_e(m, n)]^2 \quad (1)$$

$$PSNR = 10 \log_{10}(L - 1)^2 / MSE. \quad (2)$$

Here, L is the total number of intensity levels that can exist in a picture with a minimum intensity level of 0.

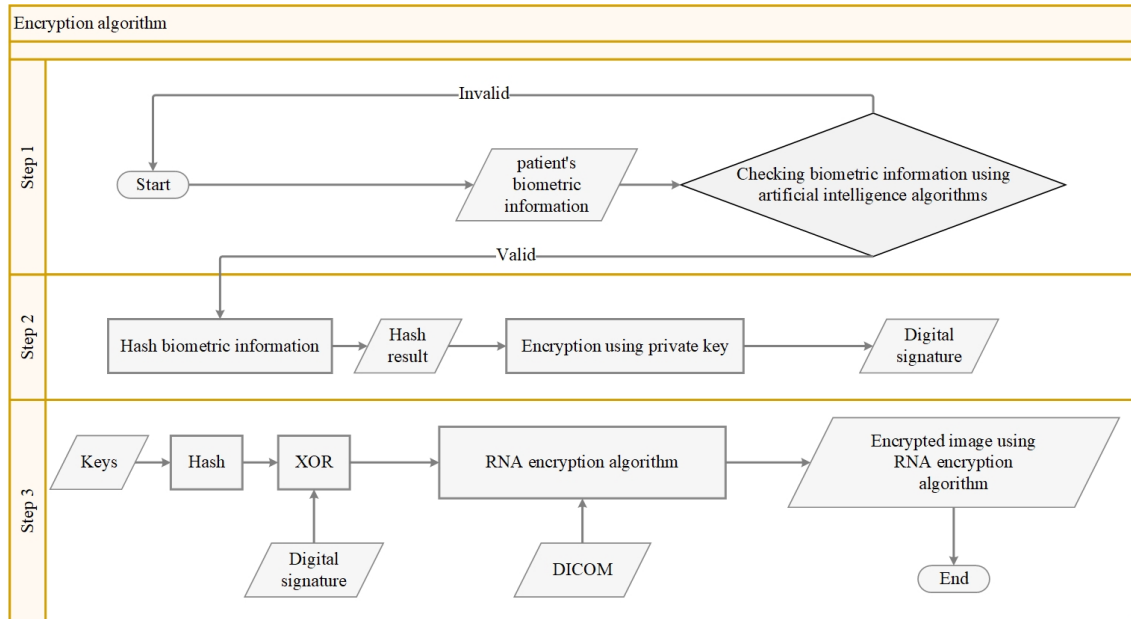


Figure 9: Block diagram of the proposed hybrid encryption algorithm.

```

1. START
2. PROGRAM DICOM_Encryption
3. Create variable patient_biometric_information
4. READ INPUT into patient_biometric_information
5. Checking patient_biometric_information using artificial intelligence, If the biometric information is valid, go to the next step.
6. Create variable Hash_result_of_the_patient_biometric_information
7. FUNCTION Patient_Biometric_Information_Hash
8. Pass IN: patient_biometric_information
9. Pass Out: Hash_result_of_the_Patient_Biometric_Information
10. END FUNCTION
11. CALL: Patient_Biometric_Information_Hash
12. Create variable Private_Key
13. Create variable Digital_Signature
14. READ INPUT into Private_Key
15. FUNCTION Digital_Signature
16. Pass IN: Private_Key
17. Pass IN: Hash_result_of_the_Patient_Biometric_Information
18. Pass Out: Digital_Signature
19. END FUNCTION
20. CALL: Digital_Signature
21. Create variable: Hash_result_of_the_Digital_Signature
22. READ INPUT into Digital_Signature
23. FUNCTION DigitalSignature_Hash
24. Pass IN: Digital_Signature
25. Pass Out: Hash_result_of_the_Digital_Signature
26. END FUNCTION
27. Create variable RNA_Key
28. Create variable Hash_result_of_the_RNA_Key
29. READ INPUT into RNA_Key
30. FUNCTION RNA_Key_Hash
31. Pass IN: RNA_Key
32. Pass Out: Hash_result_of_the_RNA_Key
33. END FUNCTION
34. Call: RNA_Key_Hash
35. Call: DigitalSignature_Hash
36. Create variable XOR_Result1
37. FUNCTION XOR
38. Pass IN: Hash_result_of_the_RNA_Key
39. Pass IN: Hash_result_of_the_Digital_Signature
40. Pass Out: XOR_Result1
41. END FUNCTION
42. Call: XOR
43. Create variable Encrypted_Image_Using_RNA_Algorithm
44. FUNCTION RNA_Encryption
45. Pass IN: XOR_Result1
46. Pass IN: DICOM
47. Pass Out: Encrypted_Image_Using_RNA_Algorithm
48. END FUNCTION
49. END

```

Figure 10: Pseudo-code for encryption algorithm.

4.1.2 NPCR and UACI

NPCR stands for the change rate of how many pixels in the cipher image change when just one pixel in the plain image changes. The average intensity of differences between the plain picture and the ciphered image is measured by the unified average changing intensity (UACI). NPCR and UACI are defined in Eq. (3) and Eq. (4) [9, 33]:

$$NPCR = \left(\frac{1}{WH} \sum_{i,j} D(i,j) \right) \cdot 100\% \quad (3)$$

$$UACI = \left(\frac{1}{WH} \frac{1}{255} \sum_{i,j} |C_1(i,j) - C_2(i,j)| \right) \cdot 100\%. \quad (4)$$

Here $D(i,j)$ is defined in Eq. (5):

$$D(i,j) = \begin{cases} 0 & \text{if } C_1(i,j) = C_2(i,j) \\ 1 & \text{if } C_1(i,j) \neq C_2(i,j) \end{cases} \quad (5)$$

4.1.3 Entropy

The quality of the encryption algorithm is measured by entropy value. The probability distribution of the image's gray levels is measured by the entropy. A uniform distribution of gray levels is indicated by a greater score for entropy. The distribution of the gray levels is uniform. This indicates that the simple medical image's pixels are scrambled so that intruders are unable to guess a small portion of it. Hence, Better confusion features are indicated by a higher entropy score. In other words, entropy is the average amount of information from the data [9, 33]. It is an important feature of randomness. Entropy is defined in Eq. (6):

$$H(U) = \sum_{i=0}^{255} p(u_i) \log_2 p(u_i) \quad (6)$$

According to Eq. (6), $p(u_i)$ shows the eventuality of distribution of gray level of the encrypted digitized image.

4.1.4 Histogram

The graphical distribution of pixels is what makes up a histogram analysis. The sample DICOM or plain image is distributed in Fig. 11a, and the pixels are distributed unevenly in the original DICOM or plain image as shown in Fig. 11b. In the cipher image as in Fig. 11c, the pixels are distributed uniformly as shown in Fig. 11d.

4.1.5 Horizontal, vertical, and diagonal correlation

4.1.6 Key space analysis

For an effective encryption algorithm, the key space must be large enough to withstand brute-force attacks. It is generally accepted that a key space of size smaller than (2^{128}) is not secure enough [36, 38].

4.2 Simulations and security analysis

According to the proposed scheme, for the simulations discussed in this section, DICOMs are randomly chosen for the tests. Some popular security analyses such as histogram, entropy, NPCR, UACI, MSE, and PSNR are also used to evaluate the security of the proposed algorithm, and this analysis is shown in Tab. 4.

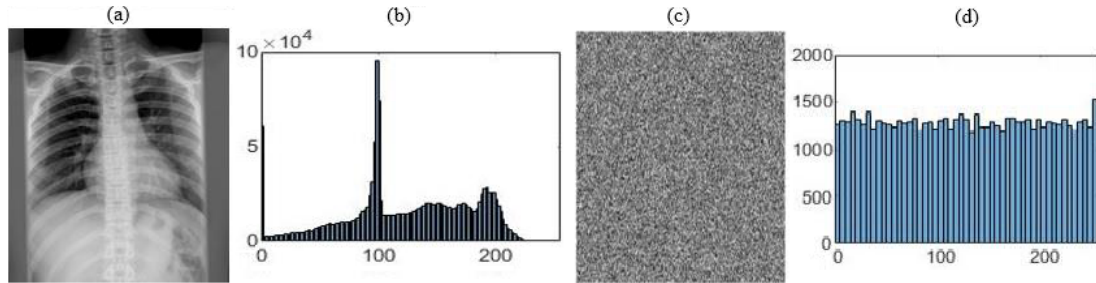


Figure 11: a: sample DICOM or plain image [39, 40], b: histogram of the plain image, c: cipher image, d: histogram of the cipher image.

Table 4: Entropy, Elapsed time, MSE, PSNR, UACI, and NPCR of encrypted DICOMs

DICOM samples	Encrypted images	Elapsed time (S)	Entropy (bits/pixel)	MSE	PSNR	UACI (%)	NPCR (%)
D1	ED1	63.903	7.998326374	116.41	27.5050786	0.33	0.995412
D2	ED2	57.117	7.997775945	57	30.6058256	0.329236	0.993411
D3	ED3	57.045	7.998042883	112.49	27.6537821	0.32784	0.995769

4.2.1 Experimental setting

We experiment our proposed scheme on a personal computer with an Intel Core i7, 2.1 GHz CPU, 8GB memory, Windows 10 and MATLAB 2016b. We use several grayscale DICOM images (of bit depth 8) of different imaging modalities and sizes in the experiment. Images with dimensions (256×256) and (512×512) are presented.

4.2.2 Data availability statement

For DICOM we have used [39, 40] and the biometric data that support the findings of this study are available in references [41, 42]. The differential and statistical analysis of the proposed algorithm are available within the study.

4.2.3 Sensitivity of the Plain Image

In this section, some security analyses such as Entropy, NPCR, UACI, MSE, PSNR, and Elapsed time are analyzed for each of the plan images. For evaluation, sample DICOM images and their encryption are shown in Figs. 12 and 13.



Figure 12: Sample DICOMs [39, 40].

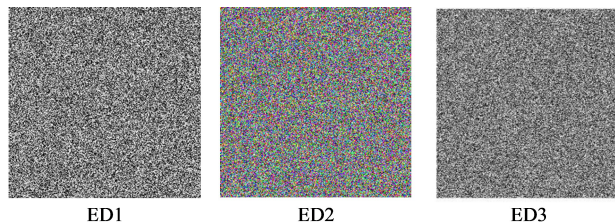


Figure 13: Encrypted DICOMs.

4.2.4 Histogram analysis

The ideally encrypted image should have a flat histogram [43] and based on histogram characteristics, this section presents the quantitative analysis of the deviation in histogram between the plain image and the encrypted image. The histogram evaluation of encrypted images is shown in Fig. 14.

4.2.5 Correlation analysis

For a plain image, a high correlation normally exists among most pairs of adjacent pixels because of pixel conjunction, and a strong encryption algorithm will lead to a decrease in the correlation coefficients [34, 35, 43]. This section presents a quantitative analysis of the correlation between plain and encrypted images. Correlation analysis of encrypted images is shown in Fig. 15.

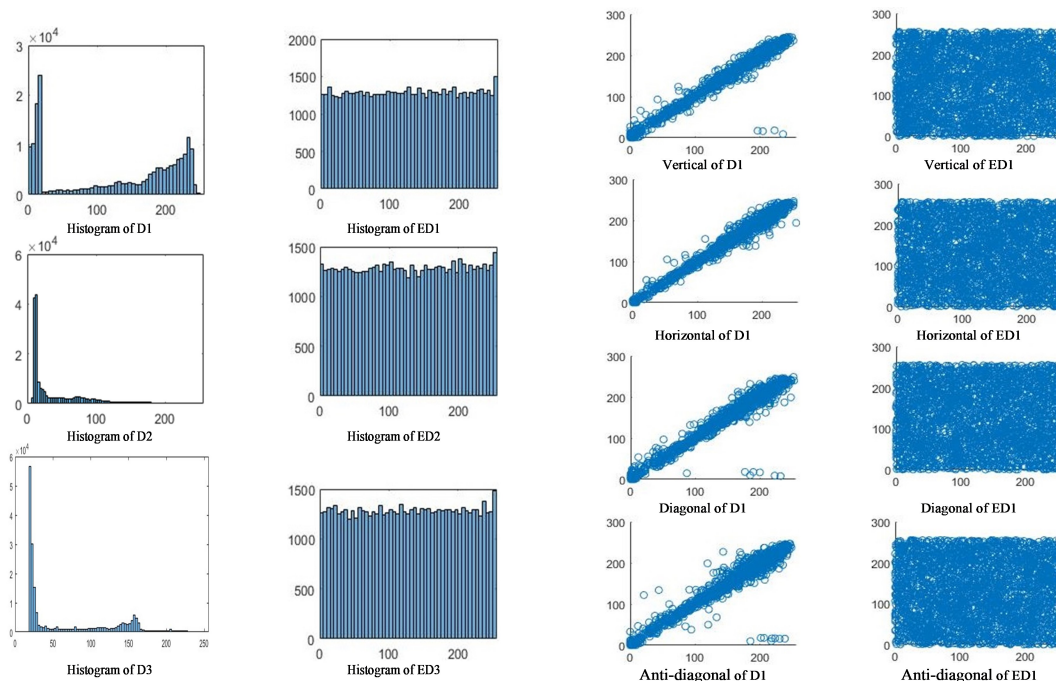


Figure 14: Histogram of D1, Histogram of D2, Histogram of D3, Histogram of ED1, Histogram of ED2, Histogram of ED3.

Figure 15: Correlation analysis of D1 and ED1.

4.2.6 Key sensitivity analysis

For an effective cryptography scheme and to resist brute-force attacks, key space should not be smaller than (2^{128}) [36, 38]. The block diagram of the proposed scheme shows that, key space of each of the cryptography algorithms (RNA and RSA) is more than 2^{128} which means that the proposed algorithm is secure from brute force attacks.

4.3 Comparative analysis of proposed algorithm

The proposed encryption algorithm is compared with some algorithms discussed in the literature survey and their methods. The comparative analysis is shown in Tab. 5. According to Table 5, using artificial intelligence algorithms and patient's biometric information to make the key of the RNA encryption algorithm has increased the security and key space of our proposed algorithm.

4.4 Performance analysis of proposed algorithm

Based on some parameters including entropy, NPCR, UACI, and histogram, the performance analysis of the proposed algorithm is shown in Tab. 6. Improving the parameters shown in Table 6, as well as using the artificial intelligence algorithms and patient's biometric information to generate keys makes the proposed algorithm resistant to brute force attacks.

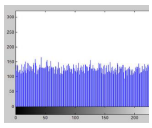
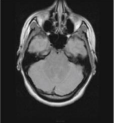
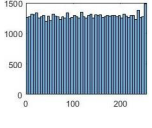
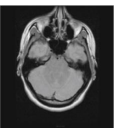
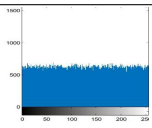

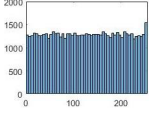

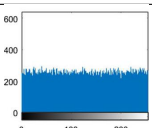
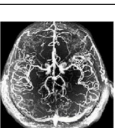
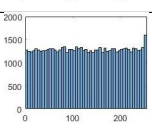

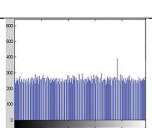

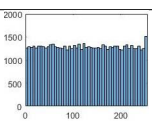

5 Conclusion and future work

HISs need to design and implement privacy and security as key considerations [3, 45, 46, 47, 48]. In this manuscript, we have proposed a novel medical image encryption algorithm based on a hybrid model of RNA computing, artificial intelligence, and Digital Signature. In the proposed algorithm we use digital signature and patient's biometric information to increase security from cyber-attacks and identity confirmation. According to the proposed algorithm, each of the keys is interdependent together and patient's biometric information. The proposed DICOM encryption algorithm has a high sensitivity to the plain image. Simulation results and performance analyses show that the proposed encryption algorithm has a high security level and robustness which means that our algorithm is robust against brute force attacks. In the future, we will decide to design the encryption algorithm in such a way that it has more key space, as well as more security in the cloud space and in HDM.

Table 5: Comparison of algorithms

Reference	Dual hyper chaos map	Piecewise linear chaotic map	1D logistic map	2D logistic map	Latin square	Hash function	Digital signature	Zigzag map	RNA	RSA	Artificial intelligence	Biometric information
44			✓		✓	✓						
43		✓	✓						✓			
7				✓		✓		✓	✓			
9	✓								✓			
Our manuscript						✓	✓		✓	✓	✓	✓

Table 6: Comparison results of algorithms and Comparative analysis

Histogram	NPCR (%)	UACI (%)	Entropy (bits/pixel)	Plain image	Reference
	99.80	33.49	7.9953		[43]
	99.61	36.26	7.9971		Proposed algorithm
	99.61	33.41	7.9971		[44]
	99.61	35.22	7.9980		Proposed algorithm
	99.60	33.69	7.9969		[7]
	99.42	35.48	7.9976		Proposed algorithm
	99.8	33.29	7.89		[9]
	99.57	29.38	7.9970		Proposed algorithm

References

- [1] Mann K., Bansal A., *HIS integration systems using modality worklist and DICOM*, Procedia Computer Science, 37 (2014), 16-23.
- [2] Puppala M., He T., Yu X., Chen S., Ogunti R., Wong S., *Data security and privacy management in healthcare applications and clinical data warehouse environment*, IEEE-EMBS International Conference On Biomedical And Health Informatics (BHI), 2016, 5-8.
- [3] Shojaei P., Vlahu-Gjorgievska E., Chow Y., *Security and privacy of technologies in health information systems: A systematic literature review*, Computers, 13.41 (2024), 2-25.
- [4] Chandrasekaran J., Thiruvengadam S., *A hybrid chaotic and number theoretic approach for securing DICOM images*, Security And Communication Networks, 2017 (2017), 6729896.
- [5] Chai, X., Chen, Y., Broyde, L., *A novel chaos-based image encryption algorithm using DNA sequence operations*, Optics And Lasers In Engineering, 88 (2017), 197-213.
- [6] Zhang, B., Rahmatullah, B., Wang, S., Zaidan, A., Zaidan, B., Liu, P., *A review of research on medical image confidentiality related technology coherent taxonomy, motivations, open challenges and recommendations*, Multimedia Tools And Applications, 82 (2023), 21867-21906.
- [7] Dagadu, J., Li, J., Aboagye, E., *Medical image encryption based on hybrid chaotic DNA diffusion*, Wireless Personal Communications, 108 (2019), 591-612.
- [8] Praveenkumar P., Amirtharajan R., Thenmozhi K., Rayappan J., *Medical data sheet in safe havens: A tri-layer cryptic solution*, Computers In Biology And Medicine, 62 (2015), 264-276.
- [9] Akkasaligar P., Biradar S., *Selective medical image encryption using DNA cryptography*, Information Security Journal: A Global Perspective, 29 (2020), 91-101.
- [10] Fu C., Zhang G., Bian O., Lei W., Ma H., *A novel medical image protection scheme using a 3-dimensional chaotic system*, PloS One, 9.12 (2014), e115773.
- [11] Seyedzadeh S., Mirzakuchaki S., *A fast color image encryption algorithm based on coupled two-dimensional piecewise chaotic map*, Signal Processing, 92 (2012), 1202-1215.
- [12] Dai Y., Wang X., *Medical image encryption based on a composition of logistic maps and chebyshev maps*, 2012 IEEE International Conference On Information And Automation, 2012, 210-214.
- [13] Zhou Y., Bao L., Chen C., *A new 1D chaotic system for image encryption*, Signal Processing, 97 (2014), 172-182.
- [14] Ravichandran D., Praveenkumar P., Rayappan J., Amirtharajan R., *Chaos based crossover and mutation for securing DICOM image*, Computers In Biology And Medicine, 72 (2016), 170-184.
- [15] Boussif M., Aloui N., Cherif A., *Smartphone application for medical images secured exchange based on encryption using the matrix product and the exclusive addition*, IET Image Processing, 11 (2017), 1020-1026.
- [16] Wen W., Wei K., Zhang Y., Fang Y., Li M., *Colour light field image encryption based on DNA sequences and chaotic systems*, Nonlinear Dynamics, 99 (2020), 1587-1600.
- [17] Muthu J., Murali P., *A novel DICOM image encryption with JSMP map*, Optik, 251 (2022), 168416.
- [18] Mortajez S., Tahmasbi M., Zarei J., Jamshidnezhad A., *A novel chaotic encryption scheme based on efficient secret keys and confusion technique for confidential of DICOM images*, Informatics In Medicine Unlocked, 20 (2020), 100396-100404.
- [19] Ravichandran D., Banu S.A., Murthy B., Balasubramanian V., Fathima S., Amirtharajan R., *An efficient medical image encryption using hybrid DNA computing and chaos in transform domain*, Medical Biological Engineering Computing, 59 (2021), 589-605.
- [20] Yang W., Wang S., Hu J., Zheng G., Valli C., *Security and accuracy of fingerprint-based biometrics: A review*, Symmetry, 11 (2019), 141-160.
- [21] Banu S.A., Amirtharajan R., *A robust medical image encryption in dual domain: chaos-DNA-IWT combined approach*, Medical Biological Engineering Computing, 58 (2020), 1445-1458.

- [22] Trivedi A., Thounaojam D., Pal S., *Non-invertible cancellable fingerprint template for fingerprint biometric*, Computers and Security, 90 (2020), 101690.
- [23] Wickramaarachchi W., Zhao D., Zhou J., Xiang J., *An effective iris biometric privacy protection scheme with renewability*, Journal Of Information Security And Applications, 80 (2024), 103684.
- [24] Polash P., Monwar M., *Human iris recognition for biometric identification*, 10th International Conference On Computer And Information Technology, 2007, 1-5.
- [25] Jan F., Alrashed S., Min-Allah N., *Iris segmentation for non-ideal Iris biometric systems*, Multimedia Tools And Applications, 83 (2024), 15223-15251.
- [26] Abdullahi, S., Khunpanuk, C., Bature, Z., Chiroma, H., Pakkaranang, N., Abubakar, A., Ibrahim, A., *Biometric information recognition using artificial intelligence algorithms: A performance comparison*, IEEE Access, 10 (2022), 49167-49183.
- [27] Iyer A., Karthikeyan J., Khan R., Binu P., *An analysis of artificial intelligence in biometrics-the next level of security*, J. Crit. Rev., 7 (2020), 571-576.
- [28] Zefreh E., *An image encryption scheme based on a hybrid model of DNA computing, chaotic systems and hash functions*, Multimedia Tools And Applications, 79 (2020), 24993-25022.
- [29] Devi R., Aravind A., Vishal J., Amritha D., Thenmozhi K., Rayappan J., Rengarajan A., Padmapriya P., *Image encryption through RNA approach assisted with neural key sequences*, Multimedia Tools And Applications, 79 (2020), 12093-12124.
- [30] Nafea S., Ibrahim M., *Cryptographic Algorithm based on DNA and RNA Properties*, International Journal Of Advanced Research In Computer Engineering and Technology, 7 (2018), 804-811.
- [31] Karim R., Rumi L., Ashiqul Islam M., Kobita A., Tabassum T., Sagar Hossen M., *Digital signature authentication for a bank using asymmetric key cryptography algorithm and token based encryption*, Evolutionary Computing And Mobile Sustainable Networks: Proceedings Of ICECMSN, 2020, 853-859.
- [32] Yang T., Zhang Y., Xiao S., Zhao Y., *Digital signature based on ISRSAC*, China Communications, 18 (2021), 161-168.
- [33] Khanzadi H., Eshghi M., Borujeni S., *Image encryption using random bit sequence based on chaotic maps*, Arabian Journal For Science And Engineering, 39 (2014), 1039-1047.
- [34] Hou W., Li S., He J., Ma Y., *A novel image-encryption scheme based on a non-linear cross-coupled hyperchaotic system with the dynamic correlation of plaintext pixels*, Entropy, 22 (2020), 779-800.
- [35] Radwan A., Abd-El-Hafiz S., AbdelHaleem S., *Image encryption in the fractional-order domain*, International Conference On Engineering And Technology, 2012, 1-6.
- [36] François M., Grosjes T., Barchiesi D., Erra R., *Image encryption algorithm based on a chaotic iterative process*, Applied Mathematics, 3 (2012), 1910-1920.
- [37] Li Z., Peng C., Tan W., Li L., *An effective chaos-based image encryption scheme using imitating jigsaw method*, Complexity, 2021 (2021), 8824915.
- [38] Wang X., Guan N., Zhao H., Wang S., Zhang Y., *A new image encryption scheme based on coupling map lattices with mixed multi-chaos*, Scientific Reports, 10 (2020), 9784.
- [39] Rosset, *The world famous medical imaging viewer*, Available at <https://www.osirixviewer.com/>, version 2022.5.
- [40] NCI Cancer imaging archive, Available at <https://www.cancerimagingarchive.net/2022>, version 2022.
- [41] Newhauser W., Jones T., Swerdloff S., Newhauser W., Cilia M., Carver R., Halloran A., Zhang R., *Anonymization of DICOM electronic medical records for radiation therapy*, Computers In Biology And Medicine, 53 (2014), 134-140.
- [42] Gauriau R., Bridge C., Chen L., Kitamura F., Tenenholtz N., Kirsch J., Andriole K., Michalski M., Bizzo B., *Using DICOM metadata for radiological image series categorization: a feasibility study on large clinical brain MRI datasets*, Journal Of Digital Imaging, 33 (2020), 747-762.

- [43] Praveenkumar P., Kerthana Devi N., Ravichandran D., Avila J., Thenmozhi K., Rayappan J., Amirtharajan R., *Transreceiving of encrypted medical image – a cognitive approach*, Multimedia Tools And Applications, 77 (2018), 8393-8418.
- [44] Chai X., Zhang J., Gan Z., Zhang Y., *Medical image encryption algorithm based on Latin square and memristive chaotic system*, Multimedia Tools And Applications, 78 (2019), 35419-35453.
- [45] Soltani M., Bardsiri A., *Designing A Novel Hybrid Algorithm for QR-Code Images Encryption and Steganography*, J. Comput., 13 (2018), 1075-1088.
- [46] Soltani M., *A new secure cryptography algorithm based on symmetric key encryption*, J. Basic Appl. Scient. Res, 3 (2013), 465-472.
- [47] Soltani M., *A New Robust Cryptography Algorithm Based on Symmetric Key to Prevent Unauthorized Access to Contents of Encrypted Files*, International Journal of Computer Science Issues, 10 (2013), 444-452.
- [48] Soltani M., *A New Secure Image Encryption Algorithm using Logical and Visual Cryptography Algorithms and based on Symmetric Key Encryption*, Journal Of Basic And Applied Scientific Research, 3 (2013), 1193-1201.

Mohammad Soltani,
Department of Computer Engineering,
Mashhad Branch,
Islamic Azad University,
Mashhad, Iran,
Email: mohammad.soltani@mshdiau.ac.ir,

Hassan Shakeri* ,
Department of Computer Engineering,
Mashhad Branch,
Islamic Azad University,
Mashhad, Iran,
Corresponding author's email:
hassan_shakeri@outlook.com,

Mahboobeh Houshmand
Department of Computer Engineering,
Mashhad Branch,
Islamic Azad University,
Mashhad, Iran
Email: houshmand@mshdiau.ac.ir.

Received 28.07.2024 , Accepted 25.01.2025, Available online 31.03.2025.