



Available online at www.qu.edu.iq/journalcm
JOURNAL OF AL-QADISIYAH FOR COMPUTER SCIENCE AND MATHEMATICS
 ISSN:2521-3504(online) ISSN:2074-0204(print)



A Secure and Efficient Hybrid Scheme for Medical Image Encryption

Husam Khalid Khammas ^{a*}, Maryam Abdulmunem Salman ^b

^aIraqi Ministry of Education, General Directorate of Education in Anbar Governorate, Anbar, Ramadi, Iraq. Email: husam.kh.khammas@gmail.com

^bIraqi Ministry of Education, General Directorate of General, National and Foreign Education, Baghdad, Iraq. Email: mary712712@gmail.com

ARTICLE INFO

Article history:

Received: 14 /03/2026

Revised form: 11 /06/2026

Accepted : 17 /06/2026

Available online: 30 /09/2026

Keywords:

Cryptography,
Image encryption,
Medical image.
Hybrid algorithm

ABSTRACT

In recent years, medical imaging has become essential for diagnosis, especially brain images are sensitive and vital tools used in the medical diagnosis process. These images are produced by advanced imaging technologies such as Magnetic Resonance Imaging (MRI) scans as doctors rely on it to determine disease conditions accurately. Therefore, given the significance of medical imaging in healthcare, protecting this sensitive information from security threats and unauthorized use is essential. This paper suggested a hybrid medical image encryption system using Advanced Encryption Standard (AES), DNA, Hyperchaotic 6D, and Fibonacci, which greatly enhances the level of security and makes decryption difficult. The proposed system was performed using MATLAB, and performance was evaluated using entropy, Mean Square Error (MSE), Peak Signal to Noise Ratio (PSNR), Unified Average Changing Intensity (UACI), Number of Pixel Change Rate (NPCR), the correlation coefficient, and histogram analysis. According to the results, the recommended solution outperforms the conventional approach in terms of efficiency and security. These findings indicate that the suggested scheme effective for protecting sensitive medical image in healthcare applications.

MSC..

<https://doi.org/10.29304/jqcm.2026.18.32738>

1. Introduction

In today's world, security is vital since it keeps people's private and sensitive information safe from dangers. Watermarking, steganography, and encryption are just a few of the many methods used to keep grayscale and color medical images safe [1]. However, these methods are not very efficient, secure, or easy to understand. The researchers aim to establish a balance between security and computing complexity by developing novel and efficient methods for encrypting digital photographs. As a result, Gupta et al. [2] employing DNA for the encryption of medical images. This shows that DNA could be useful for protecting medical data from differential attacks. In contrast, Liu et al. [3] developed a medical image encryption using a 2D logistic Gaussian hyperchaotic map. The results demonstrated a large key space and strong resistance to statistical and differential attacks. Li and Chen [4] suggested a hybrid encryption method based on 6D hyperchaotic system and DNA. The method uses hyperchaotic for pixel permutation, while DNA encoding increase the complexity of encryption process. The results demonstrate that integrating hyperchaotic system with DNA enhances encryption security. On the other hand, Reyad et al. [5] suggested a medical image encryption scheme based on AES with an enhanced key extension method to improve security and key complexity. To make their picture encryption and decryption methodology more secure and

*Corresponding author Husam Khalid Khammas

Email addresses: husam.kh.khammas@gmail.com

Communicated by 'Subject Editor'

resistant to cipher attacks, Dip et al. [6] devised a hybrid method that uses 6D hyperchaotic system and Arnold's Cat Map for the confusion stage, while K-Fibonacci applied in diffusion stage. Senthilkumar et al. [7] introduced hybrid medical image encryption framework combining AES and RSA with adaptive chunk- based approach. The method uses AES for encryption and RSA for secure encryption key, while adaptive chunk enhances the processing efficiency and reduces the encryption time. Kumaran et al. [8] proposed a hybrid medical image encryption based on DNA encoding and elliptic curve cryptography (ECC). the method uses DNA to increase randomness, while ECC provides secure key generation and exchange. Another approach suggested by Alsaraireh et al. [9] presents a lightweight medical image encryption scheme based on AES and image block decomposition. The method enhances security by processing diagonal and non-diagonal blocks separately, combining AES with XOR operation to enhance data integrity and confidentiality.

This paper aims to develop a hybrid encryption system that improve the security and efficiency of medical encryption methods by utilizing AES, Fibonacci sequences, DNA encoding, and hyperchaotic 6D dynamics. Hence, providing a reliable means of safeguarding medical images.

2. Materials and Methods

2.1. AES

AES is one of the most efficient algorithms used for data encryption. It works by employing a symmetric key for both encryption and decryption operations, which means that both the sender and the receiver share the same secret key. AES supports a fixed block size of 128 bits (16 bytes), which employs three operations: transformation, permutation, and substitution procedures. Additionally, it offers three different key lengths: 128, 192, and 256 bits. The algorithm may consist of 10, 12, or 14 rounds, contingent upon the key used [10]. The Fig. 1 shows the structure of the AES algorithm.

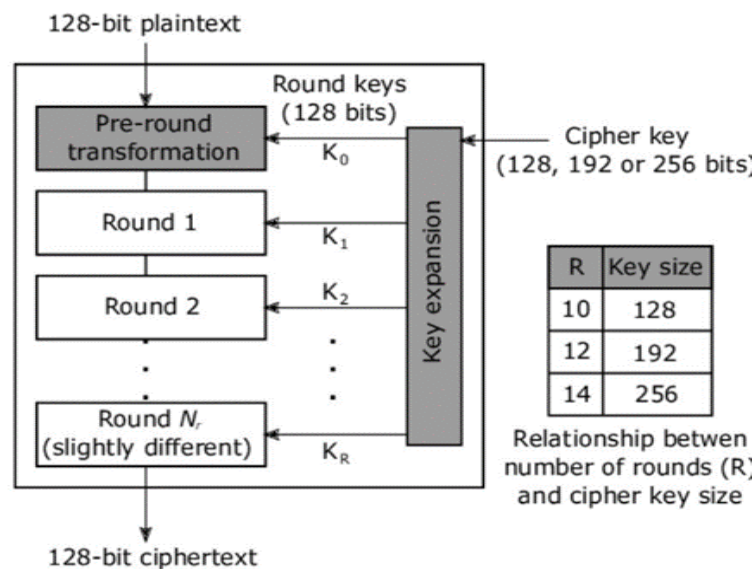


Fig. 1 - AES Structure [11].

The encryption process involves several steps, starting by expanding secret key to generate round keys and initializing the state array with data blocks. In the initial round, the round key adding to the state array in a single operation called Add Round Key, in which each byte of the state is adding with its equivalent byte of the round key. The main round includes four operations: Sub Bytes, Shift Rows, Mix Column, and Add Round Key. Whereas, the final round involves the same operations of the main round without the Mix Column step [12]. Fig. 2 illustrates the AES encryption process. In the Sub Bytes procedure, every byte in a block state is swapped with its corresponding byte from the substitution table (S-box). The Shift Rows procedure involves shifting each row of data to the left side.

Whereas, the Mix Column procedure provides a diffusion process by mixing each column of the state matrix individually. Finally, in the Add Round Key operation, the round key and current state are XORed.

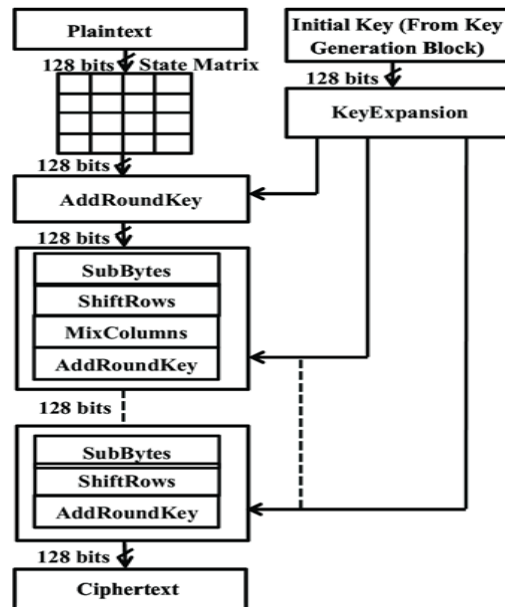


Fig.2 -AES operation [13].

2.2. DNA

The atlas DNA computing is an essential component of human evolution, employing four nucleotide pairs: adenine (A), guanine (G), thymine (T), and cytosine (C) [14]. The DNA sequence offers benefits such as high parallelization, substantial storage capacity, reduced energy consumption, plentiful resources, and a robust economy. Researchers use DNA coding in DNA computing to change image data and build a strong encryption system by combining it with other methods. They don't account for the complex experimental conditions of DNA, such as temperature, the difficulty of extracting DNA sequences, harsh environmental conditions, and the expense of experimental equipment [15]. The following Table 1 illustrates the rules of DNA.

Table 1 -The encoding rules of DNA [16].

Rule	Rule1	Rule2	Rule3	Rule4	Rule5	Rule6	Rule7	Rule8
00	A	A	T	T	C	C	G	G
01	C	G	C	G	A	T	A	T
10	G	C	G	C	T	A	T	A
11	T	T	A	A	G	G	C	C

Table 1 presents 8 of the 24 coding rules that meet the fundamental complementing condition. Since a gray image's pixel values are eight-bit binary numbers that fall between 0 and 255, they can be encoded using four bits of DNA pairs for each pixel value. For example, a pixel with the value 190 is represented in binary as "10111110", and using Rule 2 of DNA from Table 1, the resulting DNA sequence is "CTTC"; the same rule is applied in reverse for decoding [17].

2.3. Hyperchaotic 6D

Hyperchaotic systems are considered mathematical models that show complicated, uncertain dynamics, marked by their sensitivity to initial conditions [18]. They represent a subgroup of chaotic systems characterized by four or more variables, demonstrating increased complexity and unpredictability. There are a lot of positive Lyapunov

exponents in hyperchaotic systems. Two adjacent trajectories in phase space are represented by these exponents, which correspond to the exponential divergence ratio. Mathematical investigations of hyperchaotic systems constitute an important department of nonlinear dynamics and chaos theory [19]. The 6D hyperchaotic system is a six-dimensional dynamical system exhibiting hyperchaotic behavior. Here are the components of the system: six state variables ($X_1, X_2, X_3, X_4, X_5, X_6$), one time variable, and factors h, f, b, d, k , and g . Providing exact parameter values and initial circumstances for state elements allows one to describe the behavior of this hyperchaotic system [20]. Equation (1), defines a 6D hyperchaotic system.

$$\left. \begin{aligned} \dot{x}_1 &= h(x_2 - x_1) + x_4 - x_5 - x_6 \\ \dot{x}_2 &= -fx_1 - x_2 + x_1x_3 \\ \dot{x}_3 &= -bx_3 + x_1x_2 \\ \dot{x}_4 &= dx_4 + -x_2x_3 \\ \dot{x}_5 &= kx_6 + x_3x_2 \\ \dot{x}_6 &= gx_1 \end{aligned} \right\} \quad (1)$$

The hyperchaotic system variables are $X_1, X_2, \dots, X_6$, with $h = 10, f = 28, b = 8/3, d = -1, k = 8$, and $g = 3$ [21].

2.4. Fibonacci

It is a mathematical sequence used in many fields, including engineering, mathematics, and computer science, especially in image encryption and Steganography. The main principle of this method is by creating a series of numbers from the sum of the two preceding numbers [22]. Fibonacci Q matrices, composed of elements of the Fibonacci sequence, exhibit distinctive properties, including convergence to the golden ratio and pseudo-random behavior. These matrices are used due to their superior propagation capabilities, which change pixel values based on initial conditions, enabling the development of robust encryption algorithms capable of withstanding statistical and differential attacks. Incorporating these matrices into the encryption process leads to improves the security of digital images by preventing illegitimate access or alteration of important information [23]. The Fibonacci sequence gradually approaches the golden ratio of $\phi = 1.618$. Equation (2) illustrates the components of the Fibonacci sequence [24].

$$F_n = F(n-1) + F(n-2) \quad (2)$$

Where $n > 1$, and $F_1 = F_2 = 1$. The Q matrix is describing as Equation (3):

$$Q = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \quad (3)$$

In the Fibonacci Q matrix, the nth power can be described as Equation (4):

$$Q^n = \begin{bmatrix} F(n+1) & F(n) \\ F(n) & F(n-1) \end{bmatrix} \quad (4)$$

$F(n)$ denotes the value of the Fibonacci sequence, and the determinants of the Fibonacci Q-matrix are described as Equation (5):

$$\text{Det}(Q^n) = F(n+1) * F(n-1) - F_n^2 = (-1)^n \quad (5)$$

The inverse matrix Q^{-n} is structured as Equation (6):

$$Q^n = \begin{bmatrix} F(n-1) & -F(n) \\ -F(n) & F(n+1) \end{bmatrix} \quad (6)$$

2.5. The Suggested Method

This article suggests a unique encryption algorithm designed specifically for medical images encryption. To render medical images unintelligible to unauthorized individuals, the proposed technique uses Hyperchaotic 6D, Fibonacci sequence, AES, and DNA for encryption. Better protection of sensitive patient information is possible with the proposed algorithm when integrated with the current healthcare infrastructure. An overview of the proposed system for encrypting medical images is shown in Fig. 3.

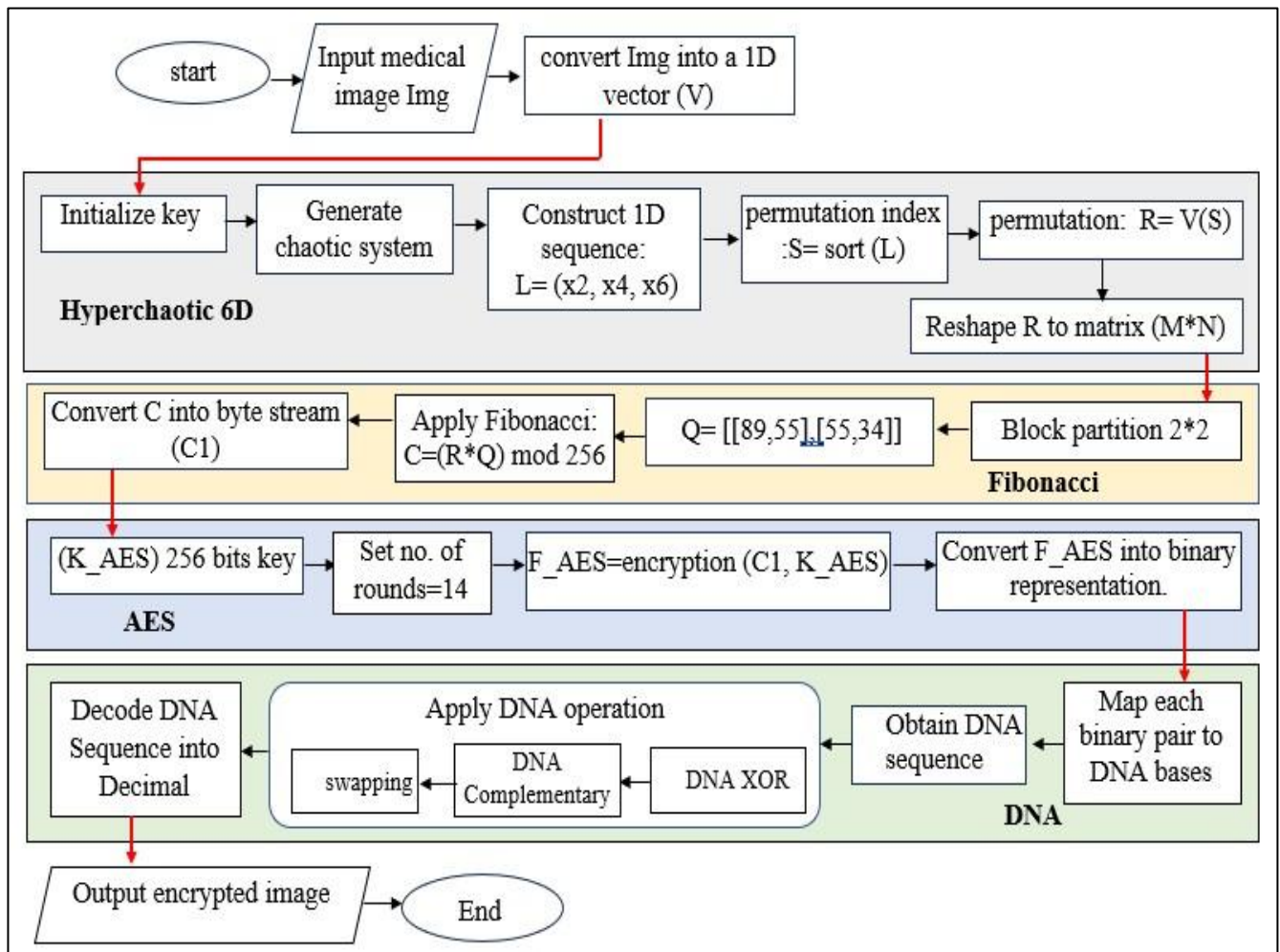


Fig.3 -The Proposed System Flowchart

As illustrated in Fig. 3, the suggested method consists of several interconnected stages, each performing a specific function that contributes to making the encryption process more secure. The following subsections provide a detailed explanation of each stage.

2.5.1 Hyperchaotic permutation and Fibonacci diffusion

The hyperchaotic 6D system is used to generate a pseudo-random sequence that determine a permutation index for pixel rearrangement. This stage transforms the structured spatial data into a shuffled vector, effectively removing

the spatial correlation among pixels without altering the pixel intensity values and improve resistance against statistical attack.

The permuted vector is then reshaped into matrix form and processed using Fibonacci Q-matrix. The diffusion operation is performed through matrix multiplication on 2×2 blocks, thereby enhancing security by ensuring that small variation in the input produce significant changes in the output.

2.5.2 Hybrid AES encryption and DNA encoding

In this stage the diffusion output is converted into a byte stream and encrypted using AES-256 bit. The encryption process operates on 128-bit data block and employs 256-bit secret key and performs 14 rounds of cryptographic transformations to generate cyphertext in byte form, providing high level of security and data confidentiality.

The AES output is then transformed from byte representation into 8-bit binary stream. This binary stream is then segmented into 2-bit groups, where each 2-bit is mapped into DNA nucleotide using DNA encoding rules. This transformation from cryptographic cyphertext into biological representation establish the connection of AES and DNA encoding. Then, DNA operations such as XOR, Complementary Substitution, swapping are applied to increase resistance against cryptanalysis and enhance nonlinearity. Finally, the processed DNA sequence is decoded back into binary representation and reshaped to generate the finally encrypted image.

2.5.3 Pseudocode of the suggested algorithm

Input: Medical image (Img)

Output: Encrypted image (E_img)

Begin;

Step1: Image processing

1. Input medical image (Img)
2. Reshape Img into a vector V

Step2: 6D hyperchaotic system initialization

3. Initialize the chaotic key
4. Generate chaotic system using the 6D hyperchaotic described in Equation (1).
5. Construct 1D sequence using projection:
 $L = (x_1, x_3, x_5)$
6. Generate permutation index by sort L in ascending order:
 $S = \text{sort}(L)$

Step 3: Permutation

7. Obtain permuted value based on S where:
 $R = V(S)$.
8. Reshape R to matrix form ($M \times N$).

Step 4: Fibonacci Diffusion

9. Define Fibonacci Q- matrix:
 $Q = \begin{bmatrix} 89 & 55 \\ 55 & 34 \end{bmatrix}$
10. Divide R into 2×2 non-overlapping blocks (B).
11. Apply Fibonacci Q- matrix on 2×2 blocks:
 For each block B
 $C = (B * Q) \bmod 256$
 end

Step 5: AES Encryption

12. Convert C into byte stream (C1).
13. Generate AES key (K_AES) of size 256 bit.
14. Apply AES encryption rounds (add round key, SubBytes, shift rows, and Mix column) on block C1:
 $F_AES = \text{encryption}(C1, K_AES)$.

Step 6: DNA Encoding

15. Convert F_AES into binary representation.

16. Map each binary pair to DNA bases using DNA rules.
17. Obtain DNA sequence (D).

Step 7: Apply DNA operation:

- DNA XOR.
- DNA Complementary Substitution.
- DNA swapping.

Step 8: DNA Decoding

18. Decode the DNA Sequence into Decimal values.
 19. Construct the final encrypted image (E_img).
- END

3. Results and Discussion

The reliability of the suggested method has been assessed using a range of security metrics, including entropy, MSE, PSNR, UACI, NPCR, and the correlation coefficient. Four (265 * 265) brain tumor photos were used to test efficacy. Every experiment was executed on a laptop computer with a Core i7 processor using MATLAB (R 2022). The following Fig. 4 shows the findings of the suggested method.

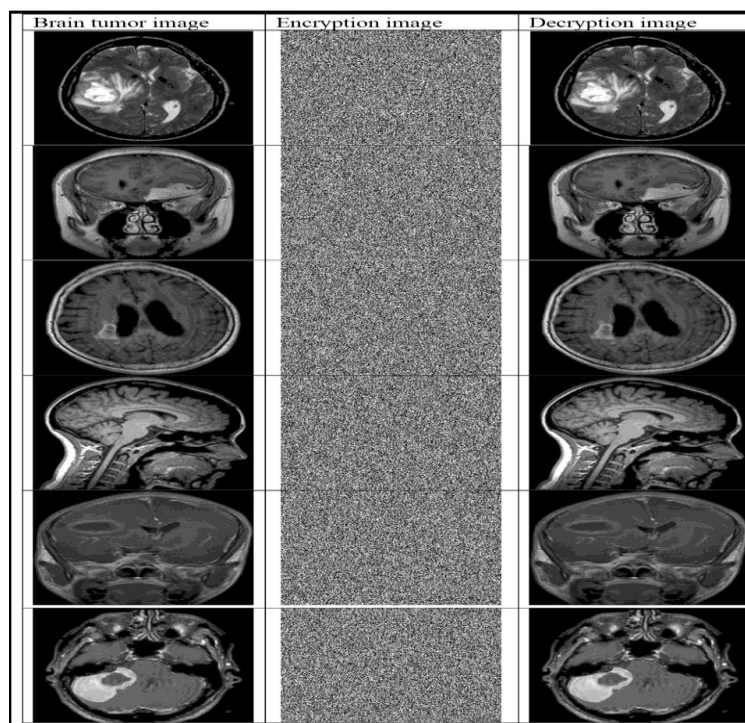


Fig.4 -The Findings of The Suggested Method.

3.1 Entropy

To assess the unpredictability of the encrypted image's pixel values, this statistic is essential. A higher entropy score indicates a more secure, difficult-to-crack encryption method. This statement is especially true as entropy approaches 8 [25]. An equation defining entropy is as follows Equation (7):

$$E(X) = - \sum_{i=0}^{2^n-1} p(x_i) \log_2 p(x_i) \quad (7)$$

The likelihood that pixel (xi) is redundant is denoted by p(xi). Table 2 shows the entropy of brain pictures using the suggested approach.

Table 2 -Entropy results.	
Images	Proposed Algorithm
Img1	7.9964
Img2	7.9832
Img3	7.8450
Img4	7.9143
Img5	7.9902
Img6	7.9762

3.2 MSE

MSE refers to the mean square deviation of pixel values between two pictures [26]. The MSE can be calculated as Equation (8):

$$MSE = \frac{1}{ab} \sum_{m=0}^{a-1} \sum_{n=0}^{b-1} (x(m, n) - y(m, n))^2 \quad (8)$$

Let m and n signify the number of rows columns, respectively. Y denotes the encrypted images, whereas the original is denoted by X. The MSE of the brain images is calculated by using the suggested algorithm, as shown in Table 3.

Table 3 -MSE results.	
Images	Proposed Algorithm
Img1	0.0115
Img2	0.0269
Img3	0.0186
Img4	0.0340
Img5	0.0152
Img6	0.0274

3.3 PSNR

It is a mathematical method used to evaluate the general image quality [28]. Using Equation (9), it is possible to find the PSNR value.

$$PSNR = 10 * \log\left(\frac{R^2}{MSE}\right) \quad (9)$$

For grayscale images, R would be the maximum feasible value (e.g., 255). Table 4 shows the suggested approach and its effect on the PSNR of brain pictures.

Table 4 -PSNR results.

Images	Proposed Algorithm
Img1	34.1642
Img2	38.0528
Img3	36.8942
Img4	37.3283
Img5	36.4821
Img6	37.0039

3.4 Differential Attack Analysis

It is an important security evaluation method in image encryption system. In this type of attack, the attacker aims to decrypt the image without using the encryption key but through determining the relation between the encrypted and original image. The main objective of this attack is how one pixel change in the original image affect their corresponding encryption image. A secure encryption algorithm should be had high resistance even for a tiny change in the original image. to measure the resistance of algorithm against differential attacks two metrics are used: UACI and NPCR. In general, an effective encryption algorithm should have UACI value near 33.46% and NPCR value close to 99.61% [27].

UACI is the average brightness disparity between an encrypted and a plaintext image. An improved encryption method, as shown by a higher UACI value, is more resistant to assaults of many types, including plaintext and cipher-only attacks [28]. Equation (10) can be used to compute the UACI.

$$UACI = \frac{1}{a * b} \left[\sum_{m,n} \frac{|X(m,n) - Y(m,n)|}{\max(Y)} \right] * 100\% \quad (10)$$

Here, X is plaintext, Y is the encrypted version, m is the row count, and n is the column count. The UACI of brain images is calculated using the algorithm suggested in Table 5.

Table 5 -UACI results.

Images	Proposed Algorithm
Img1	33.4688
Img2	33.4160
Img3	33.4525
Img4	33.4903
Img5	33.5029
Img6	33.4752

The NPCR measure can be used to analyze the sensitivity of the plaintext and the encryption scheme to differential assaults [29]. This discrepancy occurs when the encrypted version of the image differs by even a single pixel from the original. Determine the NPCR value by contrasting the encrypted image (Y) with the original image (X). The NPCR calculation can be expressed as Equation (11).

$$NPCR = \left(\frac{\sum_{i,j} D(i,j)}{a * b} \right) * 100\% \quad (11)$$

The equation states that $D(i,j)=0$ when $X(i,j)=Y(i,j)$, and $D(i,j)=1$ when $X(i,j) \neq Y(i,j)$. Here, (a) represents the number of rows, and (b) is the number of columns. Table 6 seen the results of the NPCR on brain images using the suggested method.

Table 6 -NPCR results.

Images	Proposed Algorithm
Img1	99.6241
Img2	99.6586
Img3	99.5370
Img4	99.6802
Img5	99.7204
Img6	99.6975

3.5 Correlation Coefficient

It's an important metric used to determine the degree of correlation between adjacent pixels in an image. In the original image, the correlation values of adjacent pixels are close to one in the horizontal, diagonal, and vertical directions. To ensure the security of the encryption algorithm, the encryption process must reduce this correlation so that the correlation coefficient of adjacent pixels in the encrypted image is close to zero. This indicates the removal of statistical patterns and minimize the predictability of adjacent pixel values. On the other hand, if the correlation is strong, it means the algorithm is vulnerable to statistical attacks, and the original sensitive content can be easily discovered [30]. The correlation coefficient can be calculated using equation (12):

$$Corr(A, B) = \frac{Q((A - Q(A))(B - Q(B)))}{\sqrt{H(A)H(B)}} \quad (12)$$

In this equation, the image pixel values and their decrypted counterparts are represented by sets of numbers A and B, respectively. The sum of all the elements in the sets is represented by the variable (n). Each of the various elements at the index (i) is symbolized by the variables A_i and B_i . Finally, the variables A' and B' are used to denote the means of the respective sets. Table 7 shows the correlation coefficient for brain scans by obtained using the suggested technique.

Table 7 -Correlation Coefficient results.

Images	Horizontal	Vertical	Diagonal
Img1	0.0037	0.0019	0.0015
Img2	0.0031	0.0030	0.0025
Img3	0.0024	0.0017	0.0006
Img4	0.0018	0.0011	0.0043
Img5	0.0050	0.0026	0.0013
Img6	0.0022	0.0038	0.0019

3.6 Histogram Analysis

One excellent way to prove the image encryption is secure is to use histogram analysis. Fig. 5 displays the histograms of the original and ciphertext pictures. The results demonstrate that following picture encryption, the histograms of the encrypted photos become much flatter, in contrast to the skewed histograms of the original images.

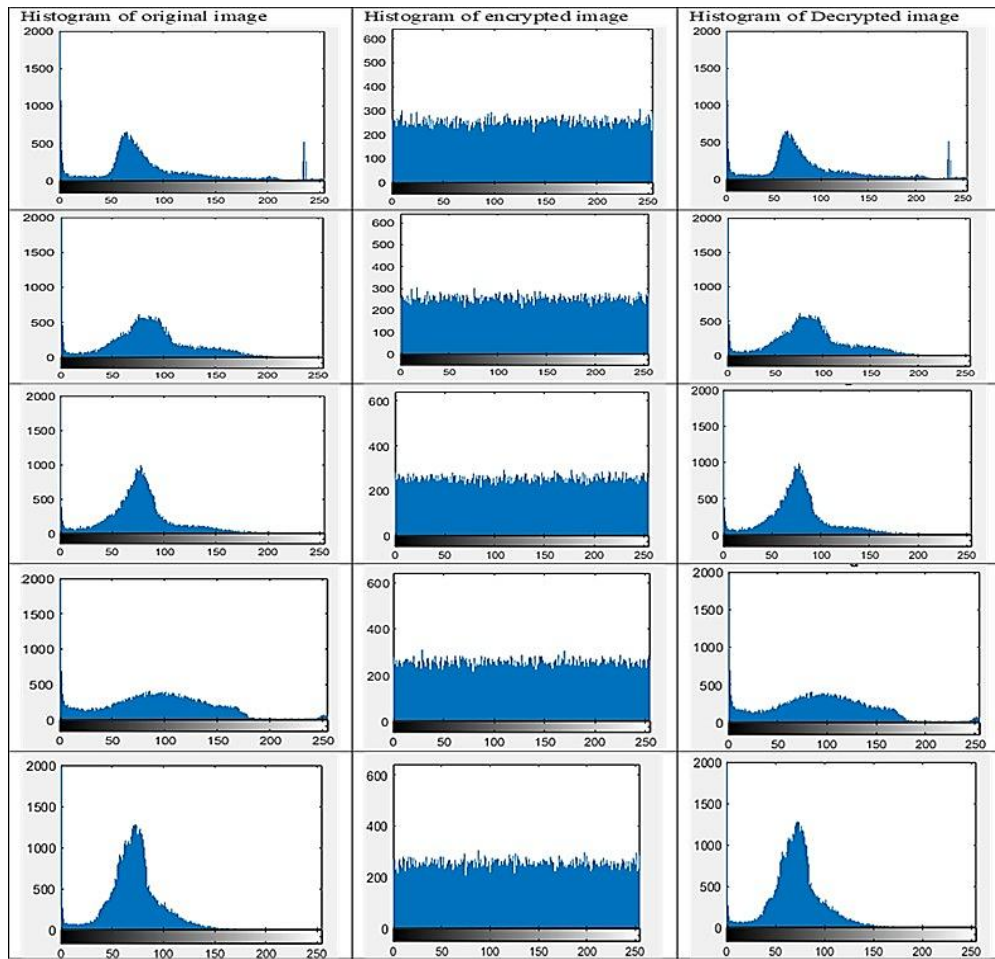


Fig.5 -Histogram of the original, encrypted and decrypted images.

3.7 Key Space

The key space is a critical metric used to evaluate the strength of the suggested encryption algorithm against brute force attacks. The key space is determined by three components: the hyperchaotic 6D, AES, and the DNA encoding rules. While, Fibonacci essential uses a fixed power($n=10$) and therefore Fibonacci does not contribute to the key space.

First, the hyperchaotic 6D system contribute with six independent initial conditions ($x_1, x_2, x_3, x_4, x_5, x_6$). Each initial condition is represented with double-precision floating point, which provides 52 mantissa bits of precision. Yielding 2^{52} possible value for each condition. Therefore, the partial key space contributing by the hyperchaotic 6D is: $KS_{chaotic} = (2^{52})^6 = 2^{312}$.

Second, AES encryption algorithm uses secret key with size 256 bits. Therefore, the partial key space contributing by AES is: $KS_{AES} = 2^{256}$.

Third, DNA encoding select one rule from 8 possible encoding rules. Therefore, the partial key space contributing by DNA is: $KS_{DNA} = 8 = 2^3$.

Therefore, the total key space of the suggested algorithm is: $KS_{Total} = KS_{Chaotic} * KS_{AES} * KS_{DNA} = 2^{312} * 2^{256} * 2^3 = 2^{571}$. Since $2^{571} > 2^{128}$, the key space of the suggested algorithm greatly exceeds the minimum recommended security threshold of 2^{128} , making the suggested algorithm is strong resistance against brute-force attacks.

3.8 Key Sensitivity test

A robust image encryption algorithm should exhibit high sensitivity to every tiny change in the secret key, where even a slight modification in the secret key results in an encrypted image that is entirely different from that produced by the original secret key. To evaluate key sensitivity the original image is first encrypted with the original secret key (K1) to generate the cipher image (C1). Then, a slightly modified key (K2) generated by changing one bit of the original secret key, and the original image encrypted the original again to produce a second cipher image (C2). Fig. 6 show the results of image encryption using original secret key and a modified key. The visual inception of C1 and C2 shows that the two encrypted image are completely different, with no observable similarity and only the original key (K1) can retrieve the original image, while decryption using the modified key (K2) results in a completely distorted image, demonstrating high sensitivity to key change.

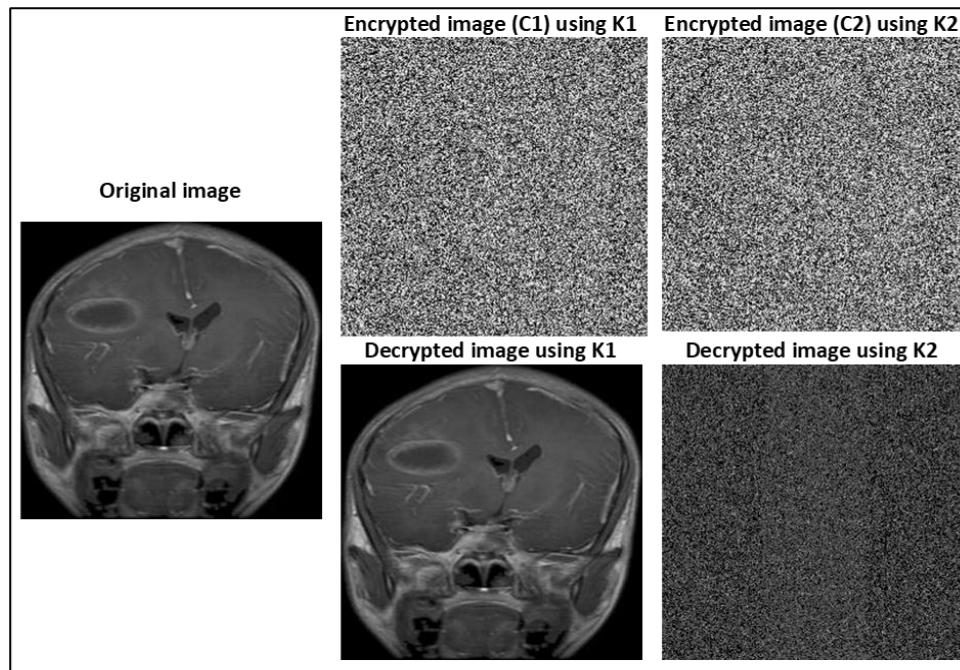


Fig.6 -Key sensitivity test results.

Furthermore, to validate the result, several statistical metrics were computed between the encrypted images, as shown in the following Table 8.

Table 8 -Statistical result of key sensitivity test.

Metric	Proposed Algorithm
NPCR	99.5010 %
UACI	33.2188 %
Correlation	-0.000917

The NPCR value of 99.5010 % indicates that almost all pixels of encrypted image are changed when a slight modified is applied to the key. Also, the UACI value of 33.2188 % confirms a significant average intensity change between the two encrypted images (C1 and C2), which is close to the ideal value 33%. Furthermore, the correlation value of -0.000917 is approximately near to zero, indicating that there is no statistical dependency between the two encrypted images. These results confirms that even a minimal change in the secret key leads to unpredictable change in the encrypted image. Therefore, the suggested algorithm exhibits strong key sensitivity and is highly resistance to related- key attack.

3.9 Comparative Analysis with Previous Works

To evaluate the effectiveness of the suggested method, a comparative analysis was conducted with two existing works as shown in the following Table 9. The suggested method achieved higher UACI (33.4676) and comparable NPCR (99.8196) to the other works, indicating enhanced diffusion and stronger resistance against differential attacks. Entropy value (7.9509) close to eight, reflecting good randomness, while high PSNR (36.6543) and low MSE (0.0223), confirm excellent decrypted image quality. Overall, the suggested method outperforms the compared methods in security and decryption performance.

Table 9 -Comparison of the suggested method with existing methods.

	Entropy	MSE	PSNR	NPCR	UACI	Cross Correlation		
						H	V	D
Suggested Method	7.9509	0.0223	36.6543	99.8196	33.4676	0.00303	0.00235	0.00202
SHA 256 and DNA [32]	7.9993	-	-	99.6174	33.4657	-0.0164	0.0056	0.0289
6D Hyperchaotic and Symmetric matrix [33]	7.9973	-	-	99.5934	33.3054	0.0062	0.0022	0.0036
AES and enhanced CBC mode [9]	7.7348	-	-	99.806	31.1236	-	-	-

4. Conclusion

This study suggested a new hybrid image encryption technique for brain tumor medical imaging. The proposed method hybridizes four techniques: AES, DNA, a hyperchaotic 6D, and the Fibonacci sequence. Security, efficiency, and resistance to various attacks indicate the effectiveness of the suggested method compared to established methods. The findings indicated that the suggested technique worked well in terms of entropy, MSE, PSNR, NPCR, UACI, and the correlation coefficient. The study proved that it was an effective way to protect medical images, especially those of brain tumors against statistical and differential attacks.

5. Recommendations and Future Works

For future work, the suggested technique can be extended to support color and three-dimensional medical image. Another promising, is improve the algorithms to be used in real-world medical applications and integrated with additional security measures, such as image watermarking. Furthermore, combining the suggested method with deep learning techniques for adaptive key generation, that could enhance the overall security of medical data.

Acknowledgements

The authors would like to express their sincere gratitude to everyone who provided support and assistance throughout this study.

References

- [1] S. T. Ahmed, D. A. Hammood, R. F. Chisab, A. Al-Naji, and J. Chahl, "Medical image encryption: A comprehensive review," *Computers*, vol. 12, no. 8, p. 160, 2023. Available from: <https://doi.org/10.3390/computers12080160>
- [2] M. Gupta, S. Bhattacharjee, and B. Chatterjee, "An enhanced security in medical image encryption based on multi-level chaotic DNA diffusion," *J. Image Graph.*, pp. 153–160, 2023. Available from: <https://doi.org/10.18178/joig.11.2.153-160>

- [3] Q. Lai, G. Hu, U. Erkan, and A. Toktas, "High-efficiency medical image encryption method based on 2D Logistic-Gaussian hyperchaotic map," *Appl. Math. Comput.*, vol. 442, no. 127738, p. 127738, 2023. Available from: <https://doi.org/10.1016/j.amc.2022.127738>
- [4] Q. Li and L. Chen, "An image encryption algorithm based on 6-dimensional hyper chaotic system and DNA encoding," *Multimed. Tools Appl.*, vol. 83, no. 2, pp. 5351–5368, 2024. Available from: <https://doi.org/10.1007/s11042-023-15550-3>
- [5] O. Reyad, H. Mansour, E. Zanyaty, and M. Heshmat, "Medical Image Privacy Enhancement Using Key Extension of Advanced Encryption Standard," *Sohag Journal of Sciences*, vol. 9, no. 3, pp. 211–216, Sep. 2024. Available from: <https://doi.org/10.21608/sjs.2024.250176.1154>
- [6] [1]S. Dib, A. Benchiheb, and F. Benmeddour, "A New 6D Hyperchaos-Based Medical Image Encryption Scheme Using k-Fibonacci Numbers," *International Journal of Electrical and Electronic Engineering & Telecommunications*, vol. 13, no. 2, pp. 148–159, Dec. 2023. Available from: <https://doi.org/10.18178/ijeetc.13.2.148-159>
- [7] M. Senthilkumar, S. Kannan, and V. Ravi, "Developing an innovative medical image security framework based on Larger Chunk-adaptive integrated AES and RSA," *Secur. Priv.*, vol. 8, no. 5, 2025. Available from: <https://doi.org/10.1002/spy2.70090>
- [8] V. N. S. Kumaran, T. Manikandan, R. K. Dhanaraj, T. Al-Shehari, N. A. Alsadhan, and S. Selvarajan, "A secure medical image encryption technique based on DNA cryptography with elliptic curves," *Sci. Rep.*, vol. 15, no. 1, p. 20003, 2025. Available from: <https://doi.org/10.1038/s41598-025-03898-5>
- [9] S. Alsaraireh, A. Ahmad, and Y. AbuHour, "New step in lightweight medical image encryption and authenticity," *Mathematics*, vol. 13, no. 11, p. 1799, 2025. Available from: <https://doi.org/10.3390/math13111799>
- [10] M. Naim and A. Ali Pacha, "A new chaotic image encryption algorithm based on a modified version of the AES algorithm," *Multimed. Tools Appl.*, 2024. Available from: <https://doi.org/10.1007/s11042-024-19842-0>
- [11] M. A. G. Dr Asha Ambhaikar, "Aes and rsa-based hybrid algorithms for message encryption & decryption," *INFORMATION TECHNOLOGY IN INDUSTRY*, vol. 9, no. 1, pp. 273–279, 2021. Available from: <http://dx.doi.org/10.17762/itii.v9i1.129>
- [12] N. Chaudhary, T. B. Shahi, and A. Neupane, "Secure image encryption using chaotic, hybrid chaotic and block cipher approach," *J. Imaging*, vol. 8, no. 6, p. 167, 2022. Available from: <http://dx.doi.org/10.3390/jimaging8060167>
- [13] N. Siva Balan and B. S. Murugan, "Low area FPGA implementation of AES architecture with EPRNG for IoT application," *J. Electron. Test.*, vol. 38, no. 2, pp. 181–193, 2022. Available from: <http://dx.doi.org/10.1007/s10836-022-05997-x>
- [14] X. Wang and Y. Su, "Image encryption based on compressed sensing and DNA encoding," *Signal Process. Image Commun.*, vol. 95, no. 116246, p. 116246, 2021. Available from: <http://dx.doi.org/10.1016/j.image.2021.116246>
- [15] A. Mahmoud, M. Elmogay, A. Atwan, and H. Soliman, "A new DNA-based approach for enhancing AES using sequence alignment and dynamic multi modeling techniques," *Mansoura Journal for Computer and Information Sciences*, vol. 16, no. 2, pp. 35–46, 2020. Available from: <http://dx.doi.org/10.21608/mjcis.2020.321074>
- [16] K. Xuejing and G. Zihui, "A new color image encryption scheme based on DNA encoding and spatiotemporal chaotic system," *Signal Process. Image Commun.*, vol. 12, no. 2, pp. 115670, p. 115670, 2020. Available from: <http://dx.doi.org/10.1016/j.image.2019.115670>
- [17] G. Shraida, "Review of DNA-based color image encryption algorithms," *Iraqi Journal of Intelligent Computing and Informatics (IJICI)*, vol. 1, no. 2, pp. 56–65, 2022. Available from: <http://dx.doi.org/10.52940/ijici.v1i2.10>
- [18] S. John and S. Kumar, "6D hyperchaotic encryption model for ensuring security to 3D printed models and medical images," *Journal of Image and Graphics*, vol. 12, no. 2, pp. 117–126, 2024. Available from: <https://doi.org/10.18178/joig.12.2.117-126>
- [19] H. Chen, E. Bai, X. Jiang, and Y. Wu, "A fast image encryption algorithm based on improved 6-D hyper-chaotic system," *IEEE Access*, vol. 10, pp. 116031–116044, 2022. Available from: <http://dx.doi.org/10.1109/access.2022.3218668>
- [20] X. Wang, Q. Ren, and D. Jiang, "An adjustable visual image cryptosystem based on 6D hyperchaotic system and compressive sensing," *Nonlinear Dyn.*, vol. 104, no. 4, pp. 4543–4567, 2021. Available from: <http://dx.doi.org/10.1007/s11071-021-06488-y>
- [21] J. Wang, W. Yu, J. Wang, Y. Zhao, J. Zhang, and D. Jiang, "A new six-dimensional hyperchaotic system and its secure communication circuit implementation," *Int. J. Circuit Theory Appl.*, vol. 47, no. 5, pp. 702–717, 2019. Available from: <http://dx.doi.org/10.1002/cta.2617>
- [22] Z. Liang, Q. Qin, and C. Zhou, "An image encryption algorithm based on Fibonacci Q-matrix and genetic algorithm," *Neural Computing and Applications*, vol. 34, no. 21, pp. 19313–19341, 2022. Available from: <https://doi.org/10.1007/s00521-022-07493-x>
- [23] P. Purwanto et al., "An image encryption based on Fibonacci sequence and fusion of advanced encryption standard-least significant bit method," *TELKOMNIKA*, vol. 22, no. 6, p. 1517, 2024. Available from: <http://dx.doi.org/10.12928/telkomnika.v22i6.26078>
- [24] T. Zhou, J. Shen, X. Li, C. Wang, and H. Tan, "Logarithmic encryption scheme for cyber-physical systems employing Fibonacci Q-matrix," *Future Gener. Comput. Syst.*, vol. 108, pp. 1307–1313, 2020. Available from: <http://dx.doi.org/10.1016/j.future.2018.04.008>
- [25] Z. Man, J. Li, X. Di, and O. Bai, "An image segmentation encryption algorithm based on hybrid chaotic system," *IEEE Access*, vol. 7, pp. 103047–103058, 2019. Available from: <http://dx.doi.org/10.1109/access.2019.2931732>
- [26] M. U. Rehman, A. Shafique, K. H. Khan, and M. M. Hazzazi, "Efficient and secure image encryption using key substitution process with discrete wavelet transform," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 35, no. 7, p. 101613, 2023. Available from: <https://doi.org/10.1016/j.jksuci.2023.101613>
- [27] J. Su, A. Kankani, G. Zajko, A. Elchouemi, and H. Kurniawan, "Review of Image encryption techniques using neural network for optical security in the healthcare sector – PNO System," in *2020 5th International Conference on Innovative Technologies in Intelligent Systems and Industrial Applications (CITISIA)*, 2020. Available from: <https://doi.org/10.1109/CITISIA50690.2020.9371805>
- [28] M. Kumar, A. S. Chivukula, and G. Barua, "Deep learning-based encryption scheme for medical images using DCGAN and virtual planet domain," *Sci. Rep.*, vol. 15, no. 1, p. 1211, 2025. Available from: <https://doi.org/10.1038/s41598-024-84186-6>
- [29] C. L. Chowdhary, P. V. Patel, K. J. Kathrotia, M. Attique, K. P, and M. F. Ijaz, "Analytical study of hybrid techniques for image encryption and decryption," *Sensors (Basel)*, vol. 20, no. 18, p. E5162, 2020. Available from: <http://dx.doi.org/10.3390/s20185162>
- [30] X. Wang and S. Gao, "Image encryption algorithm based on the matrix semi-tensor product with a compound secret key produced by a Boolean network," *Inf. Sci. (Ny)*, vol. 539, pp. 195–214, 2020. Available from: <http://dx.doi.org/10.1016/j.ins.2020.06.030>
- [31] M. Saberikamarposhiti, A. Ghorbani, and M. Yadollahi, "A comprehensive survey on image encryption: Taxonomy, challenges, and future directions," *Chaos Solitons Fractals [Internet]*, vol. 178, 2024. Available from: <https://doi.org/10.1016/j.chaos.2023.114361>
- [32] J. Wu, J. Zhang, D. Liu, and X. Wang, "A multiple-medical-image encryption method based on SHA-256 and DNA encoding," *Entropy (Basel)*, vol. 25, no. 6, p. 898, 2023. Available from: <https://doi.org/10.3390/e25060898>
- [33] A. Panwar, G. Biban, R. Chugh, A. Tassaddiq, and R. Alharbi, "An efficient image encryption model based on 6D hyperchaotic system and symmetric matrix for color and gray images," *Heliyon*, vol. 10, no. 11, p. e31618, 2024. Available from: <https://doi.org/10.1016/j.heliyon.2024.e31618>