(IJRST) 2024, Vol. No. 14, Issue No. 3, Jul-Sep **e-ISSN: 2249-0604, p-ISSN: 2454-180X**

Encryption of Medical Image Based on Cascaded Design of AES Block Algorithm and Chaotic Map

***Gaidaa S. Mahdi, ** Marwa Fadhel Jassim, *** Mustafa Q. Ali**

* University of Technology-Iraq
Chemical Engineering Department
Baghdad, Iraq
** University of Technology-Iraq
Control and Systems Engineering Department
Baghdad, Iraq
*** University of Baghdad
College of Islamic Sciences
Baghdad, Iraq

DOI:10.37648/ijrst.v14i03.001

[1]*Received: 26 April 2024; Accepted: 1 August 2024; Published: 12 August 2024*

ABSTRACT

Security concerns in the transfer of medical images have drawn a lot of attention to the topic of medical picture encryption as of late. Furthermore, recent events have brought attention to the fact that medical photographs are constantly being produced and circulated online, necessitating safeguards against their inappropriate use. To improve the design of the AES algorithm standard for medical picture encryption, this research presents several new criteria. It was created so that needs for higher levels of safety and higher levels of performance could be met. First, the pixels in the image are diffused to randomly mix them up and disperse them all over the screen. Rather than using rounds, the suggested technique utilizes a cascaded-looking composition of F-functions in a quadrate architecture. The proposed F-function architecture is a three-input, three-output Type-3 AES-Feistel network with additional integer parameters representing the subkeys in use. The suggested system makes use of the AES block cipher as a function on a Type-3 AES-Feistel network. Blocks in the proposed system are 896 bits in length, whereas keys are 128 bits. The production of subkeys is encrypted using a chain of E8- algorithms. The necessary subkeys are then generated with a recursion. The results are reviewed to verify that the new layout improves the security of the AES block cipher when used to encrypt medical images in a computer system.

Keywords: *Cryptography; Block Cipher; AES; Medical image; Chaotic map, Image Encryption.*

INTRODUCTION

By providing cutting-edge tools for remote diagnosis and speedier administration of first aid, telemedicine technologies are transforming many facets of the healthcare industry. Digital images play a key role in these applications, which aim to deliver faster and better healthcare. These digital images are frequently shared via public networks between hospitals, doctors, and patients, despite the fact that they often contain private and patient diagnostic data. In order to protect the patient's confidentiality, they must be safely stored and transported. However, traditional cryptographic techniques are insufficient to provide adequate security when encrypting digital image data due to its special qualities, such is the image's huge size and significant redundancy and correlation between its pixels. As the standard algorithms lose their effectiveness, there is a growing demand for more refined and specific picture encryption methods [1]. There are currently a lot of widely-used standard algorithms for conventional encryption. The vast majority of these can be stored in a text document. Strong nearby pixel correlations make it difficult to directly

[1] How to cite the article: Mahdi G.S., Jassim M.F., Ali M.Q..; August 2024; Encryption of Medical Image Based on Cascaded Design of AES Block Algorithm and Chaotic Map; *International Journal of Research in Science and Technology*, Vol 14, Issue 3, 1-12, DOI: http://doi.org/10.37648/ijrst.v14i03.001

apply these techniques to photos or movies. The level of detail decreases as the correlation between neighboring pixels decreases [2].

Both the Advanced Encryption Standard (AES) and the Data Encryption Standard (DES) formed the backbone of conventional image encryption techniques. The security and efficiency of conventional approaches are being pushed to new tests by the ever-increasing computational capacity of computers [3]. Many novel ideas, including chaos theory and quantum mapping theory, have been included into encryption systems [4] to boost the safety and use of picture cryptography. Encryption schemes inspired by chaos theory have attracted the attention of many scientists because of their shared characteristics with chaotic systems, such being their long-term uncertain repetitive trajectories and their sensitivity to initial conditions. [5], [6].

The mathematical and physical foundations of chaos theory date back to the 1960s, and the area is just now reaching full maturity. Pseudo randomness, unpredictability, and a high sensitivity to beginning values and parameters are hallmarks of chaos theory, giving it a leg up in the competitive field of picture encryption. Numerous researchers have proposed hybrid technological/ideological image encryption methods [7] that are grounded in chaos theory.

The following are the significant contributions of the proposed algorithm:

- Using Type-3 Feistel network. Since the proposed algorithm has a block length of 896 bits and the internal word-size is 32 bits. Along with the variety of network-structures which are able of management three subblocks of 128 bits as input to Type-3 AES-Feistel network.
- There are six rounds in the suggested algorithm design of Type-3 AES-Feistel network; where in each round one subblock of 128 bits is utilized to modify all the other subblocks, because of this, this architecture offers significantly improved diffusion qualities at only a small additional expense. Hence, To get the same strength, fewer rounds need to be used. Also, a Type-3 AES-Feistel network has an advantage over structures that use many subblocks "at once" to alter other subblocks because these structures are typically considerably more difficult to evaluate.
- As increasing the input block size of the proposed algorithm, the exhaustive "key search" and the "matching ciphertext" attack were infeasible.
- In the proposed encryption algorithm further complex reversible mixing and scrambling algorithm has been used which was required to provide the necessary decorrelation for image bytes randomly. Also, another gain behind the scrambling is to make the relationship complex between the original image and encrypted image to decrease attempts to infer the key.

This paper is organized into VI sections. Section II discusses the related works. Section III explains AES block cipher, while section IV explains the architecture of the proposed system in detail. Section V shows the experimental results. Section VI focuses on the conclusions and further scope of the proposed work..

RELATED WORKS

The utilization of Advanced Encryption Standard (AES) is employed to perform encryption of pixel data about medical imaging in adherence to the Digital Imaging and Communications in Medicine (DICOM) standard. To prevent unauthorized modifications during transmission, it is imperative to utilize encrypted network protocols when dealing with sensitive information. Hence, ongoing research is being conducted to assess the efficacy of encryption techniques in safeguarding medical images and explore potential avenues for enhancement. In a study conducted in 2018, HUA et al. proposed a novel method for encrypting medical images, which involved high-speed scrambling and adaptive diffusion techniques [8]. In 2018, Bhogal et al. [9] introduced a novel approach that combines a chaotic map with the AES. This technique was subjected to a comprehensive evaluation, comparing its performance to that of the original AES through several tests. By contrasting the two, it became evident that the utilization of the chaotic map had a discernible impact on the overall efficacy of the encryption mechanism. The unique methodology, called CAT-AES, involves the iterative application of Arnold's cat map before performing encryption a certain number of times. In contrast, the conventional AES encryption algorithm does not incorporate such iterations.

In 2020, Manjula and Mohan [10] proposed a solution based on employing an improved AES algorithm to send encrypted patient information and concealed medical images across a network. A new dynamic S-Box is spawned using a Hash function to ensure robust security. By decreasing encryption processing time and improving stego picture quality, the proposed security framework aims to improve performance. The evolution of medical picture encryption technologies was examined by Muhammed et al. [11] in 2020. Both the histogram and the correlation coefficient can be used to examine the relationship between pixels in an image by comparing the distribution of values and the number of pixels in the original and processed images.

A chaotic image encryption system based on the combination of the Arnold's Cat Map and the 2D Logistic-Sine-Coupling Map(2D-LSCM) was proposed by K. Jain et al. [1] in 2021 to improve the randomness and security of encrypted images. Ashwaq et al. [2] in 2021 used a quadratic map-based approach as a preprocessing step to remove the association between pixels and increase the entropy. Confidentiality is achieved through the use of AES image encryption, which causes some degree of confusion and spreads the information around. The results of the security study show that the robustness of the secret key is crucial to the success of the sensitive encryption and decryption procedures.

In 2022, the chaos-based picture encryption and block cipher approaches were constructed and assessed by Chaudhary et al. [12]. The native chaotic and hybrid chaotic approaches are an Arnold cat map and a logistic map, while the block cipher approach is the advanced encryption standard (AES). The results demonstrate that the hybrid chaotic map is more resistant to differential attacks and selected plain text attacks due to its higher NPCR and UACI values. When compared to the other two methods, the Arnold cat map has the lowest computing cost. However, AES is more resistant to statistical attacks since it has a lower PSNR value (7.53 to 11.93) and more fluctuation between the histograms of the original and cipher images.

In the year 2022, Aarthi and colleagues [13] introduced a novel chaotic architecture that utilizes the Advanced Encryption Standard (AES) in conjunction with a Poisson regression model to secure the encryption of color medical images. The sender transmits a concluding image to the recipient, which exhibits a normalized pixel count rate (NPCR) of 99.0174 and an average unified average changing intensity (UACI) of 33.0690. The results obtained from the experimental study and subsequent security evaluations indicate that this picture encryption method has potential for use in encrypting and transmitting medical images. In 2023, Qiang et al. created a medical image encryption method with a unique hyperchaotic map [14]. In this study, we construct a 2D Logistic-Gaussian hyperchaotic map (2D-LGHM) with multiple hyperchaotic behaviors, then proceed to demonstrate the enhanced ergodicity and unpredictability of this map by the utilization of performance test measures.

ADVANCE ENCRYPTION STANDARD (AES)

AES is an iterative replacement of Feistel cipher. It is based on substitution and permutation networks (SPN), which are widely used for both encryption and decryption. In block cipher methods, SPN entails a number of mathematical processes [15]. As a fixed plaintext block size, AES could handle 128 bits (16 bytes). AES operates on a matrix of bytes, which is represented here as a 44 matrix of these 16 bytes. AES's number of rounds is also an important design choice. The number of rounds is depending on the length of key. The AES algorithm may encrypt and decode data using keys of 128, 192, or 256 bits in length. The number of rounds in a cryptographic algorithm like AES is determined by the size of the key being used; for example, 10 rounds are used for 128-bit keys, 12 rounds for 192-bit keys, and 14 rounds for 256-bit keys (Figure 1). [16].

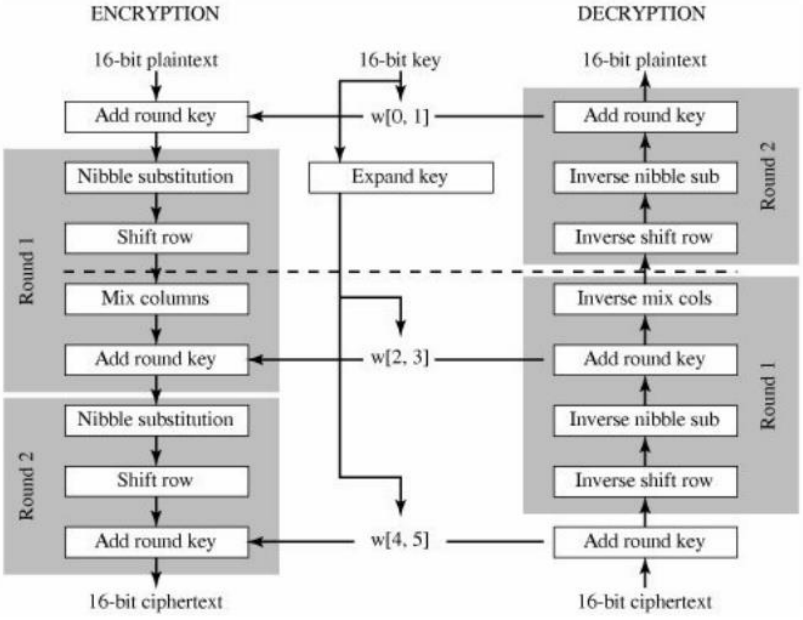

Figure 1. Basic Structure of AES.

QUADRATIC MAP

The non-asymptotic behaviour of reiterations at n+, proven by the quadratic map's basic mathematical formulations, corresponds to the map's immensely intricate dynamic properties [17]. Furthermore, the value of parameter a can have a substantial impact on the features. This is associated with the fact that for large values of n, the dependence on x is tremendously polynomial and intricate. In this approach, quadratic mapping can be applied to capture these dynamics thoroughly. Think about this quadratic equation:.

$$Xn + 1 = a - xn2 \quad for\ 0 < a < 2 \qquad (1)$$

Where the fixed points are xn.

PROPOSED ALGORITHM

It is advocated that medical photographs be encrypted to prevent their illicit duplication and alteration and to increase overall image security. The proposed picture encryption is split into two parts: a chaotic map-based permutation phase and an upgraded AES-based diffusion phase. The proposed architecture entails a Type-3 Feistel network that accepts three inputs and generates three outputs, accompanied with integer parameters that reflect the employed sub-keys. A singular iteration of the AES block encryption can effectively represent the cascading process. The system under consideration has a block size of 896 bits. The suggested system employs 128-bit keys. Subkeys are generated using an E6-chained encryption system. The necessary subkeys are then generated via recursion.

A. Image Permutation

In the permutation phase the input medical image is distributed into seven blocks randomly based on new indices that is generated based on chaotic map. The aimed of this phase is to decorrelate the pixel adjacency of input image. Figure 2 depicts the block diagram of the proposed permutation phase. And the Algorithm 1 illustrates the steps of image permutation.

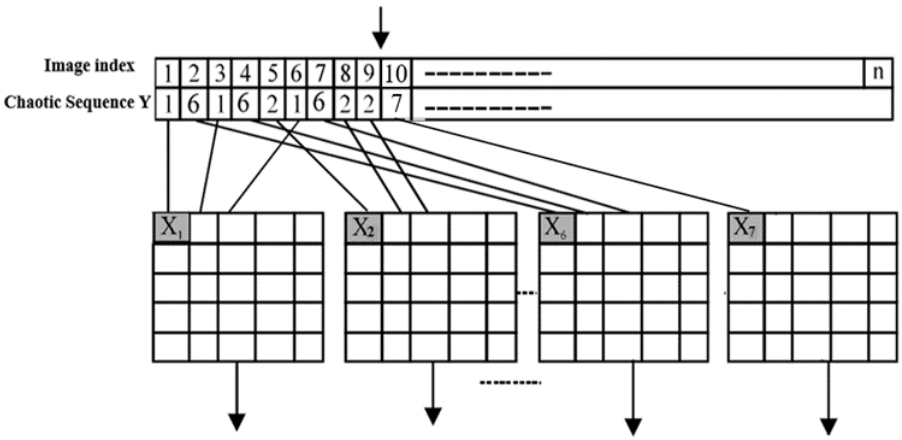

Figure 2. The proposed image permutation.

Algorithm 1: Image Permutation.
Input: MI \\ Medical image
X0, a \\ quadratic map parameters.
t, \\ t is the number of blocks
M, N \\ Medical image dimensions.

Output: Pi i=1,..,t, where t=7\\ Permuted blocks.
Step1: Convert input image into 1D array of length n=M×N
Step2: Initialize b as a sequence of length n:
Step 2.1: For I= 1→ n
b[I]=I mod t
EndFor
Step 2.2: Apply the quadratic map to create a permutation sequence with a secret chaotic key to permute the pixels.
Let a =0.5, X0=0.15,
X0 = a ×X02
For i = 1 to n
Xi= a ×Xi-1 2
End for i

Step 2.3: Normalize the chaotic map X array in the range [1,n].
Step3: Divide IM into t blocks.
For j=1 → n
z=X[j]
If (z <> 1)
z=z× n / t
no=count[z]+1
b=z+ no
Y[b]=IM[j]
End For
Step4: Permute the MI into t blocks according to the random chaotic index to generate permuted blocks Pi i=1,..,7 such as following:
Pi(I) = Y(J) where I=1,..,n, J=1,..n and i=1,..,t

B. Image Diffusion

In diffusion phase the P1..P7 are 128 bits blocks of 896 bits plaintext. The C1..C7 are 128 bits blocks, which in assemble give 896 bits ciphertext. F-function is a procedure with 6 parameters. Three parameters are 128 bits input blocks and there are three 128 bits output blocks. And additionally, two parameters are several sub-keys to be used. The practical aim of the proposed system was to satisfy as many goals as potential for image encryption at the same time keeping the cipher straightforward. The block diagram of the proposed algorithm is depicted in Figure (3). Decryption can be represented using the same diagram with all arrows reversed.

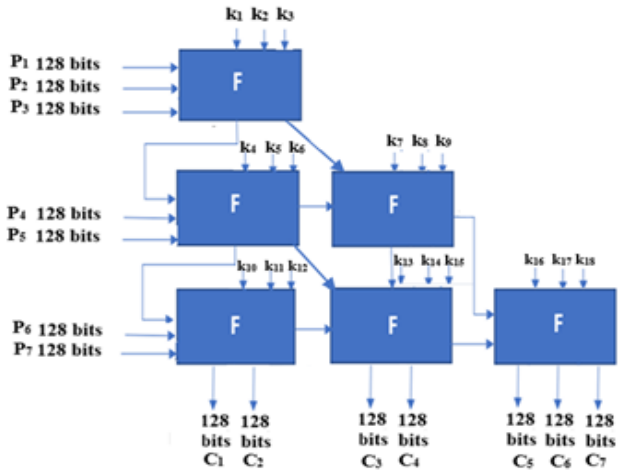

Figure 3. The block diagram of the proposed diffusion algorithm.

The block diagram of the F function is shown in Figure (4). The design of F function is a Type-3 AES-Feistel network. The total key length for each F function is 384 bits (i.e., 128×3) Algorithm 2 illustrates the steps of diffusion process.

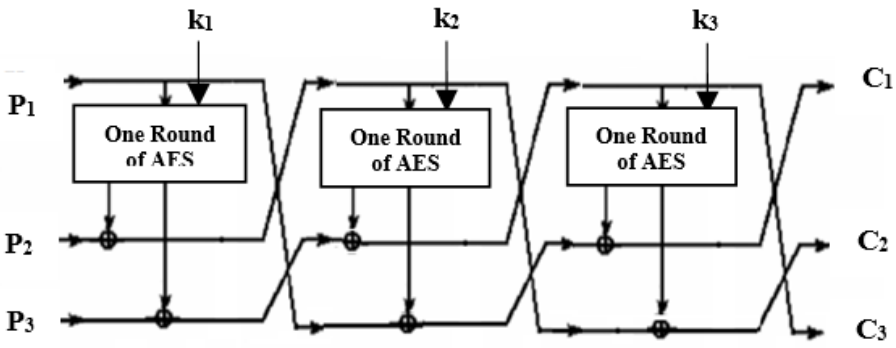

Figure 4. The block diagram of F function.

Algorithm 2: Image Diffusion
Input: Pi // Permuted blocks.
M, N // Medical image dimensions.
Output: E // Encrypted image.
Step1: let n=M×N, t=7
Step2: Take blocks bki
for i=1,..,t of size128 bits from Pi blocks:
For h=0,..,n-1 step t
i=1,..t
j=1,..t
bki(j)=Pi(j)
EndFor j
EndFor i
F (bk1, bk2, bk3, e1, e2, e3, k1, k2,k3)
F (bk4, bk5,e1, e4, e5,e6)
F (bk6, bk7 ,e4, C1,C2,e7)

C. Sub keys Generations

The input key size of the proposed system is 128 bits. Three rounds have been required in each proposed Type-3 AES-Feistel network design. Each round required three 128 bits sub keys. Also the total sub keys are k1,k2,…,k18 each of which is 128 bits. E8- chained encryption utilized for sub keys generation. Let k be an inserted key. Then a recursion has been used to generate required subkeys such as following:

k1 = k, ki+1 = E(ki) i=1,..18 (2)

EXPERIMENTAL RESULTS

A. Security Analysis

The external parameters of the cipher system limit the additional protection obtained by applying encryption. For example, a malicious party with knowledge of the plaintext's redundancy can locate the key by a thorough key search. The work factor of this attack is only dependent on the key length m when expressed in terms of encryptions. When an opponent gains temporary access to a block encryptor or decryptor, they can use it to encrypt or decrypt a specific plaintext or ciphertext. For the used key, this can be regarded as a partial table reconstruction. In the future, encryptions can use this incomplete table to learn more about the plaintext. This attack's chances of success solely depend on the block length, n. Black box cryptanalysis refers to the class of assaults that do not use the cipher's internal structure, which includes both of these cases.

The block length n and the key length m are the two external parameters of a block cipher. It is stated that 3-WAY is BB-secure in relation to its external parameter n (= 896), and key length m (=128).

The proposed system used type-3 Feistel network in cascaded design. The optimal trade-off between speed, strength, and analytical appropriateness is offered by a type-3 Feistel network. A desirable characteristic of an encryption algorithm is that a minor alteration to the plaintext or the key ought to result in a substantial alteration to the ciphertext.

B. Analysis of Key Sensitivity and Key Space

The secret keys in the encryption algorithm should be very sensitive, and the key space should be large enough to prevent brute-force attacks. One of the most essential features in any encryption scheme is the key space. A significant key space provides resistance against a brute force attack. The proposed system makes use of the two independent variables X0 and a. As a result, these symbols represent the key space [18]; however, the number of distinct values exceeds the value of 1014 because these variables are double-precision numbers. Specifically, the key space for one proposed algorithm is ((1014)2 =1028 ≈ 293. Further, the proposed algorithm has a user key of length 512 bits. Subsequently, the total key space is 293× 2128= 2221, while the key space of AES is 2128

Remarkably, the key space of the employed algorithm is larger than that of the AES algorithm. This indicates that our technique is highly resilient to brute-force attacks. Furthermore, the input sequence of the encryption system in this technique is generated by the nonlinear chaotic system. The chaotic system is strong enough to withstand linear attacks because of its innate nonlinearity, unpredictability, and pseudo-randomness.

An encrypted image cannot be accurately decrypted if there is a slight alteration in the keys used for encryption and decryption. Referred to this phenomenon as sensitivity to secret keys. To decrypt the encrypted image, the suggested approach in this research is to try various key values that differ from the original key by one digit. The output image is totally different from the original image. we use Lena256 as the encryption object to test the key sensitivity of our encryption system. During the test, we used the original key as: a=0.5, and x0=0.15. We add 10^{-10} to the above keys respectively and use the modified key to decrypt the ciphertext in the decryption process. The decryption result is shown in Figure 5. From Figure 5, we can see that even if the key changes 10^{-10}, the wrong key cannot decrypt the ciphertext correctly, proving our encryption scheme is highly sensitive to the key. This result demonstrates how sensitive the suggested approach is to modifications made to the secret key.

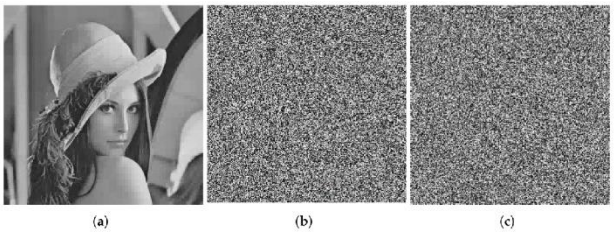

Figure 5. Key sensitivity analysis. (a) Correct key. (b) x0+10-10 (c) a++10-10.

*C. **Statistical Analysis***

This section presents the results of our experiments designed to evaluate the cryptographic properties of our proposed algorithm. various aspects will be examined like histogram analysis, correlation, information entropy, and analysis of differential attacks.

*D. **Histogram Analysis***

An image histogram is a graphical representation of the number of pixels in an image as a function of their intensity. If an attacker analyses the information of the histogram, the original image might possibly be decrypted. Thus, the method is exposed to statistical attacks from hackers. Figure (5) shows the encrypted images with their histograms.

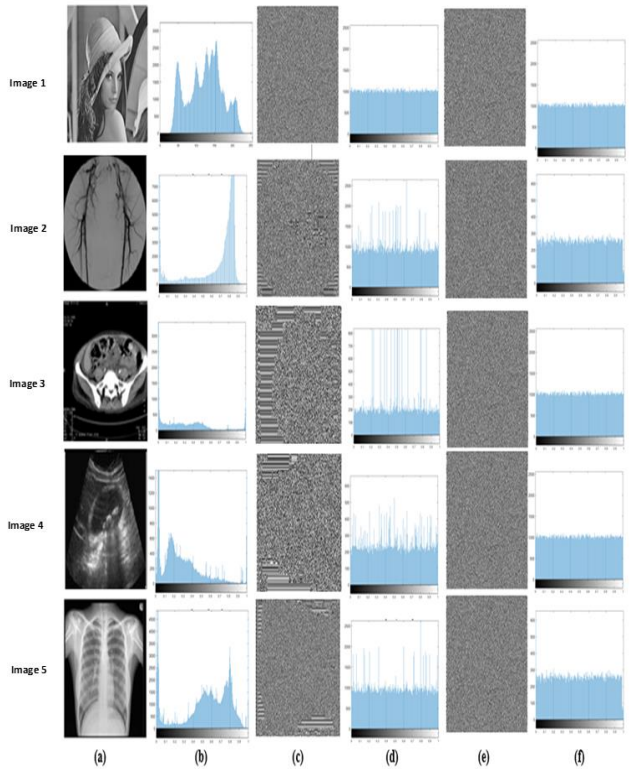

Figure 6. Encryption and decryption image. (a) Original image, (b) Histogram of the original image, (c) Encrypted image by AES (d) Histogram of the encrypted image by AES (e) Encrypted image by the proposed method, (f) Histogram of the encrypted image by the proposed system.

Figure 6 shows that there is no resembling of sensory perception between the original images and their ciphered counterparts with the proposed algorithm while AES encryption algorithm still some information can be inferred from the encrypted images.

However, the histograms of images encoded by the proposed algorithm show uniform distributions, lacking discernible characteristics, and therefore, it is necessary not to reveal or disclose any details or data related to the underlying image under any circumstances or conditions. This observation highlights the efficiency of the proposed algorithm against statistical attacks.

*E. **Correlation***

Correlation measures the link between two sets of variables. The following equation represents the cross-correlation coefficient used in this study. (Lui, et al., 2022):

F. $$C = \frac{n\sum_i x_i y_i - \sum_i x_i \sum_i y_i}{\sqrt{(\sum_i x_i^2) - (\sum_i y_i^2)}} \quad (3)$$

Where, C is the cross-correlation coefficient, n is the number of pixels of image, {xi} is pixels values of the original image, {yi} is pixels values of the cipher image [19]. Table (I) shows the correlation between original images and ciphered images AES algorithm and the correlation after applying the proposed method.

TABLE I: The correlation coefficients between original image and their corresponding encrypted images

Image	**Original image**		
	H	**V**	**D**
1	0.9952	0.9978	0.9897
2	0.8575	0.7647	0.7328
3	0.9823	0.9793	0.9605
4	0.9140	0.8956	0.8616
5	0.9815	0.9871	0.9678
Image	**Cipher image by AES**		
	H	**V**	**D**
1	0.0095	0.0072	–0.0093
2	0.0417	0.0263	0.0056
3	0.0135	0.0052	0.0157
4	0.0108	0.0097	0.0152
5	0.0017	0.0051	0.0034
Image	**Cipher image by the proposed algorithm**		
	H	**V**	**D**
1	–0.0135	0.0017	–0.0016
2	0.0017	–0.0071	–0.0084
3	0.0014	0.0023	–0.0056
4	–0.0214	–0.0093	0.0063
5	0.0015	0.0025	–0.0055

The results of correlation coefficients shown in these tables are very small when used proposed algorithm compared with AES algorithm indicates that the plain images and their corresponding cipher images are completely uncorrelated. Figure (7) depicts the correlation distributions of adjacent pixels for original and encrypted images by AES algorithm and proposed algorithm. Table 2 lists the correlation coefficients of Lena image for different related works.

TABLE II: The correlation coefficients between Lena's image, which were encryption using different algorithm

References	H	V	D
Ref [22]	0.0092	0.0203	-0.0073
Ref [23]	0.0086	-0.0027	-0.0013
Ref[24]	-0.0021	0.0027	-0.00032
Ours	–0.0135	0.0017	–0.0016

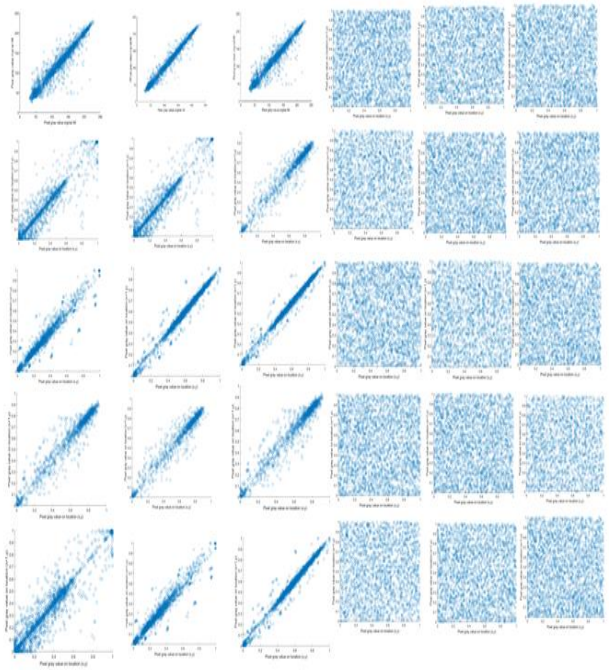

Figure 7. Correlation distributions of adjacent pixels of original image and encrypted images by proposed algorithm.

G. Information Entropy

The main objectives of picture encryption are ambiguity and indeterminacy. One of the most widely used theoretical entropy information measures can represent this limit. Entropy information is defined as follows and represents the degree of uncertainty in the system. [20]:

$$H = -\sum_{k=0}^{G-1} P(k)\log_2(P(k)) \quad (4)$$

Where, H is the entropy, G is the gray scale (=255), and P(k) is the probability of the occurrence of symbol k. Tables (III) shows the entropy between original images and ciphered images using AES and proposed algorithms respectively. From the above results, the proposed algorithm gets higher entropy compared with previous algorithms. Also, by splitting the input image into a number of subblocks made performance even better. Table (IV) lists of the entropy of Lena image compared to some related works compared with proposed algorithm. As we notice from Tables II and V the superior of proposed system.

TABLE III: The entropy values for different ciphered images with AES and proposed algorithms

Image	**Plain Image**	**Cipher Image by AES**	**Cipher Image by proposed algorithm**
1	7.7260	7.8762	7.9987
2	4.1205	6.0129	7.9835
3	5.871	6.7214	7.9945
4	2.3445	6.8682	7.9967
5	5.8712	6.5910	7.9835

TABLE IV: The entropy between Lena's image, which were encryption using different algorithm

References	**Entropy**
A. U. Rehman, et al.	7.9966
L. Teng, et al.	7.9912
AT Hashim, et al.	7.9980
X. Wu, et al.	7.9895
Ours	7.9987

H. Analysis of Differential Attacks

The number of changing pixel rates (NPCR) and Unified Averaged Changed Intensity (UACI) are the performance indicators that have the ability to assess the resilience of cipher against differential attacks [21]. Mathematically they are defined in Eq. (5) and Eq. (6).

$$NPCR = \frac{\sum_{ij} D(i,j)}{N \times M} \times 100\% \qquad (5)$$

$$UACI = \frac{1}{N \times M} \times [\sum_{ij} \times \frac{|C_1(i,j) - C_2(i,j)|}{255}] \times 100\% \qquad (6)$$

In Eq. (6) C1(i,j) and C2(i,j) are two encrypted images obtained from plaintext images that are slightly different. where N is the width, M is the height of the encrypted image and D(i,j) is the difference function between encrypted images. The difference is given as:

Table V : The UACI and NPCR scores for encrypted images by AES and the proposed system.

Image	**NCPR for AES**	**UACI for AES**	**NCPR for proposed algorithm**	**UACI for proposed algorithm**
1	99.4231	33.4620	99.6261	33.6321
2	99.3431	32.4341	99.6531	33.6812
3	99.5309	32.8360	99.6742	33.6310
4	99.3212	32.9812	99.6583	33.6291
5	99.3237	33.1431	99.6542	33.6713

Table 5 lists the UACI and NPCR scores for encrypted images and the results demonstrate that the proposed method is resistant to differential attacks.

CONCLUSIONS

In this paper an enhanced algorithm for image encryption is presented by improving AES encryption algorithm for medical images. Our algorithm includes three fundamental constituents: increased block size, used more complex reversible mixing, and used scramble algorithm d which is required to provide the necessary decorrelation for image bytes randomly, Using Type-3 Feistel network has advantages over structures in which several subblocks are utilized "at once" to change other subblocks, in that these structures are in general much harder to analyze. Based on conducted results; the proposed algorithm has offered high encryption quality by enhancing the security level of the encrypted images. It reduces the correlation among image elements while increasing its entropy value by decreasing the mutual information among the encrypted image variable. As a result, the proposed system is expected to be useful for medical

image encryption and transmission in telemedicine applications. This work can be further extended by increasing block size and number of rounds of F function.

REFERENCES

[1] K. Jain, A. Aji and P. Krishnan, "Medical Image Encryption Scheme Using Multiple Chaotic Maps," *Pattern Recognition Letters*, vol. 152, pp. 356-364, 2021.

[2] A. T. Hashim, J. K. Amira and F. H. Qussay, "Medical image encryption based on hybrid AES with chaotic map," *Journal of Physics: Conference Series*, vol. 1973, no. 1, p. 012037, 2021.

[3] X. Wang and Y. Wang, "Multiple medical image encryption algorithm based on scrambling of region of interest and diffusion of odd-even interleaved points," *Expert Systems with Applications*, vol. 213, no. A, p. 118924, 2023.

[4] Q. Lai, C. Lai, H. Zhang and C. Li, "Hidden coexisting hyperchaos of new memristive neuron model and its application in image encryption," *Chaos, Solitons & Fractals*, vol. 158, p. 112017, 2022.

[5] Z. Hua, F. Jin, B. Xu and H. Huang, "2D Logistic-Sine-coupling map for image encryption," *Signal Processing*, vol. 149, pp. 148-161, 2018.

[6] C. Zou, X. Wang, C. Zhou, S. Xu and C. Huang, "A novel image encryption algorithm based on DNA strand exchange and diffusion," *Applied Mathematics and Computation*, vol. 430, p. 127291, 2022.

[7] M. F. Jassim and A. F. Shimal, "Biometric iris templates security based on secret image sharing and chaotic maps," *International Journal of Electrical & Computer Engineering*, vol. 12, no. 1, pp. 2088-8708, 2022.

[8] Z. Hua, S. Yi and Y. Zhou, "Medical image encryption using high-speed scrambling and pixel adaptive diffusion," *Signal Processing*, vol. 144, pp. 134-144, 2018.

[9] R. S. Bhogal, B. Li, A. Gale and Y. Chen, "Medical image encryption using chaotic map improved advanced encryption standard," *IJ Information Technology and Computer Science*, vol. 8, pp. 1-10, 2018.

[10] G. Manjula and H. S. Mohan, "A secure framework for medical image encryption using enhanced AES algorithm," *International Journal of Scientific & Technology Research*, vol. 9, no. 2, pp. 3837-3841, 2020.

[11] M. W. Malik, D. Husna, I. K. E. Purnama, N. Ingrid , A. N. Hidayati and A. A. P. Ratna, "Development of Medical Image Encryption System Using Byte-Level Base-64 Encoding and AES Encryption Method," in *6th International Conference on Communication and Information Processing*, 2020.

[12] N. Chaudhary, T. B. Shahi and A. Neupane, "Secure image encryption using chaotic, hybrid chaotic and block cipher approach," *Journal of Imaging*, vol. 8, no. 6, p. 167, 2022.

[13] S. Aarthi, K. Geetha, J. Premaladha and V. Nirmala, "Medical color image encryption using chaotic framework and AES through Poisson regression model," in *International Conference on Wireless Communications Signal Processing and Networking*, Chennai, India, 2022.

[14] L. Qiang, H. Genwen, E. Uğur and T. Abdurrahim, "High-efficiency medical image encryption method based on 2D Logistic-Gaussian hyperchaotic map," *Applied Mathematics and Computation*, vol. 442, p. 127738, 2023.

[15] A. A. Mohamed and A. H. Madian, "A Modified Rijndael Algorithm and it's Implementation using FPGA," in *2010 17th IEEE International Conference on Electronics, Circuits and Systems*, 2010.

[16] N. Pramstaller, F. K. Gurkaynak, S. Haene, S, H. Kaeslin, N. Felber and W. Fichtner, "Towards an AES crypto-chip resistant to differential power analysis," in *The 30th European Solid-State Circuits Conference* , 2004.

[17] R. S. Mohammed and S. B. Sadkhan, "Speech scrambler based on proposed random chaotic maps," in *2016 Al-Sadeq International Conference on Multidisciplinary in IT and Communication Science and Applications (AIC-MITCSA)*, 2016.

[18] W. Xiangjun, K. Jürgen and K. Haibin , "A robust and lossless DNA encryption scheme for color images," *Multimedia Tools and Applications*, vol. 77, pp. 12349-12376, 2018.

[19] G. Liu, Wei Li, F. Xingkui, L. Zhuang, W. Yuxuan and M. Hongyang, "An image encryption algorithm based on discrete-time alternating quantum walk and advanced encryption standard," *Entropy*, vol. 24, no. 5, p. 608, 2022.

[20] A. T. Hashim, A. H. Jassem and S. A. Ali, "A novel design of Blowfish algorithm for image security," *Journal of Physics: Conference Series*, vol. 1818, no. 1, p. 012085, 2021.

[21] A. Belazi, M. Khan, A. A. Abd El-Latif and S. Belghith, "Efficient cryptosystem approaches: S-boxes and permutation–substitution-based encryption," *Nonlinear Dynamics*, vol. 87, pp. 337-361, 2017.

AUTHOR BIOGRAPHY

Gaidaa S. Mahdi lecturer at University of Technology-Iraq, Chemical Engineering Department, Baghdad, Iraq. Interesting in Energy & Fuels Nuclear Science & Technology https://orcid.org/0000-0002-2451-5098

M.Fadhel Jassim has graduated in 2008 from the Control and Systems Engineering Department at the University of Technology. She worked as an engineer in the same department from 2008 .In 2015 she took the master degree in the computer engineering from the same department and worked as a university Assistant Lecturer till now.
https://orcid.org/0000-0003-4046-5737

Mr. Mustafa Q. Ali an Assistant Lecturer at University of Baghdad, College of Islamic Sciences from 2008 till now. interesting in renewable energy enhancing of performance, its control techniques, system stability, embedded applications, image processing, and internet of things (IOT). In particular, my future research interests are shaped by the emerging trend towards green mobile technology. My research schedule focuses on the question of how to enhance this technology to continue improving system performance.
ORCID: https://orcid.org/0000-0001-9965-5653