Robust Multilayer Encryption for Protecting Healthcare Data in Cloud Computing

Mohammad Bani-Hani, Mohammed Al-Husainy[*], Member, IAENG, Ala'eddin Al-Zu'bi, Ghayth Al-Asad, Sara Albatienh and Hazem Abuoliem

Abstract— Cloud computing has become integral to various organizations, including healthcare facilities medical records contain sensitive information, such as treatment plans, diagnoses, X-ray images, and patients' medical histories. Ensuring the confidentiality and integrity of these records fosters and strengthens the trust between patients, healthcare providers, and organizations. However, the challenge of providing adequate security for user-related information persists, as current encryption algorithms struggle to keep pace with evolving threats. Cybercriminals continuously develop new methods to breach encrypted systems. Therefore, a multi-layer encryption algorithm capable of addressing these sophisticated threats is essential for enhancing the security of user-related data. This work suggests a multi-layer encryption algorithm that employs the patient's password as an initial key, a pseudo-random number generation (PRNG) algorithm, and different hash functions to encrypt sensitive patient information. They are used to represent patient data differently in each layer and to get the keys required for the encryption process. It is necessary to determine that the parameters of the multi-layer encryption algorithm were evaluated with the help of the approved metrics and compared with the characteristics of the other known encryption methods. The experiments revealed that the suggested multi-layer encryption algorithm enhances the protection of the patient's data and the defense mechanisms of this data against various attacks.

Index Terms— **Multi-layer encryption, Healthcare image security, Cloud computing, Secure hashing algorithm.**

I. Introduction

THE introduction of cloud computing in the healthcare industry has revolutionized the way sensitive patient data is handled and stored. With the implementation of cloud computing, the risk of losing or compromising important healthcare data, such as patient records and medical documents, has significantly decreased. The ability to securely store and access large amounts of healthcare data is one of the key advantages of cloud computing for medical research [1], [2].

Cloud computing offers numerous benefits, including increased flexibility, availability, and storage capacity, allowing healthcare professionals to access and manage critical information anytime and anywhere. However, ensuring data integrity, privacy, and security in the healthcare cloud environment is essential to maintain trust and encourage the adoption of cloud-based solutions [3, 4].

In today's digital age, the security of user-related information is of utmost importance. Encryption algorithms play a crucial role in safeguarding sensitive data from unauthorized access. Since the strength of any encryption algorithm primarily depends on the use of a strong key. Moreover, using more than one key in the encryption algorithm and making these keys as random as possible will help make the encryption algorithm resistant to attacks and provide a high level of protection for the encrypted data. Therefore, many recently developed encryption algorithms use different tools to randomly generate the required keys to be used in the encryption process [5]-[7].

However, with the advancement of technology, traditional single-layer encryption methods may be vulnerable to hacking attempts. Therefore, there is a need for the development of more robust and secure encryption algorithms [8], [9].

The Secure Hash Algorithm (SHA) is frequently used in encryption techniques. The set of cryptographic hash algorithms known as SHA was created to provide effective and secure data integrity checks. The SHA function generates a unique, fixed-size hash value for any size of input data. Among the basic properties of hash functions, one can mention the following: The size of the hash value is expressed in bits and depends on the version of SHA. There are several members of the SHA family that are widely utilized, including SHA-1, SHA-224, SHA-256, SHA-384, and SHA-512. Where the hash value sizes are 160, 244, 256, 384, and 512 bits, respectively [10], [11].

Another advantage that comes with the use of a multi-layer encryption algorithm is the ability to safely secure an organization's valuable data. Thus, the use of multiple layers of encryption, each with keys as well as algorithms different from the other, provides a more substantive security of data. Although the first layer of encryption is breached, the attackers are still faced with several layers that they must penetrate to reach the protected data. These layers of encryption not only make the process of decryption more complex but also increase the layers of protection in case of

Manuscript received September 16, 2024; revised June 13, 2025.

Mohammad Bani-Hani is a network administrator at Jadara Research Center, Jadara University, Irbid, Jordan (email: Mbbanihani@gmail.com).

M. A. Al-Husainy is a professor of Computer Science and Cybersecurity, Irbid National University, Irbid, Jordan (Corresponding author to provide phone: 00962796846119; email: DrAlHusainy@gmail.com).

Ala'eddin Al-Zu'bi is a programmer at the Exams Department, Ministry of Education, Irbid, Jordan (email: Alaaalzoubi1985@yahoo.com).

Ghayth Al-Asad is a director of training and institutional development at the Ministry of Local Administration, Amman, Jordan (email: ghayth.thelover@gmail.com).

Sara Albatienh is a postgraduate student at Irbid National University, Irbid, Jordan (email: Batainehsara96@yahoo.com).

Hazem Abuoliem is a postgraduate student at Irbid National University, Irbid, Jordan (email: Hazemabuoliem@gmail.com).

a breach. Further, multi-layered encryption algorithms are stronger and less susceptible to different sorts of cyber threats; for this reason, they are widely used by organizations that work with protected data. Multi-layer encryption algorithms have proved to be a proactive and efficient measure, especially now that data insecurity haunts almost every organization and business entity. [9].

II. Related Works

The main goal of cryptography researchers is to combine different approaches to produce a strong encryption algorithm that is resistant to most types of attacks. This is usually done using a variety of proven tools as well as innovative ones.

Qin et al. [12] proposed a new image encryption technique that integrates dynamic wavelet decomposition with scrambling and diffusion processes to achieve both spatial and frequency domain encryption. The initial value for a hyperchaos system (denoted as SHA-512) is used to create a chaotic key matrix. The algorithm includes block scrambling, dynamic wavelet decomposition based on Hamming distance and plaintext, dynamic rotation of the scrambling matrix, and applying the Zigzag transform to generate a key matrix. It also involves bitwise XOR operations between the wavelet coefficient matrix, chaotic key matrix, and key matrix to achieve diffusion. Simulation experiments demonstrate strong encryption/decryption quality and resistance to various attacks.

Shraida & Younis suggested a diffusion methodology based on the SHA-256 hash function, one-dimensional logistic map, three-dimensional Lorenz, and DNA encoding and computation for image encryption techniques that work. Encrypting adopted the secret key, which was obtained by using the SHA-256 algorithm on the original image with 256-bit features. These secret keys are then employed to make the initial parameters of the one-dimensional logistic map and the three-dimensional Lorenz system. The work enhanced the security of the encryption algorithm by integrating DNA computing, coding, and the characteristics of a chaotic map. As concluded herein, the suggested encryption algorithm is more secure and dependable than previous image encryption algorithms in terms of information entropy and correlation coefficients [13].

Baagyere et al. presented an innovative approach that combines steganography and cryptography using features that include genetic algorithm (GA) operators: a combination of crossover, mutation, and selection of the residue number system (RNS). Its goal is to build and implement an efficient, multiple-layered architecture that will counter the growing capabilities of computer processing and cyber threats. The main advantages of this approach are, therefore, its strength and efficiency. The approach proved to be invulnerable to attackers and also consumed less power than other similar methods by utilizing GA and RNS. The use of the multi-layered steganography method enables added layers of encryption on the steady image, hence improving their safety [8].

Lin et al. suggested encryption as the best way of protecting the reliability, availability, safety, and confidentiality of stored images for web-based processing platforms. The general idea behind the research study is just to employ the mechanism of two-round image encryption through the application of a Multilayer Convolutional Processing Network, or MCPN for short. In MCPN layers, the researchers adopted 2D spatial convolutional operations to extract image data and subsequently perform encryption operations. Further, pseudorandom numbers have been used in the present work to establish a secret key by using the sine-power chaotic map (SPCM) as the key generator for the balanced networks. This diffusion was later incorporated during the first techniques of encrypting an image by altering the pixels of the image. Data entropy, pixel change ratio, mean integrated variable size, structural similarity index, and peak signal-to-noise ratio are some of the metrics that were used [14].

Sabir & Guleria developed a novel multi-layer image color encryption technique that solves the challenge of securely transmitting personal image data across insecure methods. There are three stages in the method of encryption. In the initial stage, a random matrix matching cipher (RMAC) is used within this stage to protect the coordinate system in the geometric domain. The reality-preserving 2D discrete fractional Hartley transform (RP2DFrHT) is included in the next stage to provide real-valued encryption image data suitable for display by removing the complex value components, storage, and transmission in the digital domain. The third stage uses a 2D Arnold map to enhance security and expand the key space. The strengths of the proposed technique lie in its ability to simultaneously provide security in the geometric, coordinate, frequency, and time domains. However, the security of the technique relies on the secret keys and their correct arrangement, which may represent a potential security vulnerability [15].

III. Proposed Multilayer Algorithm

The proposed multi-layer encryption algorithm uses the patient's password as an initial key, a pseudorandom number generation algorithm, and various SHA hash functions as tools to encrypt confidential patient data. These tools are used to represent the patient's data differently at each layer and to generate the keys needed to encrypt the confidential patient data. Multi-layer encryption is implemented by dividing the source data into several blocks at each layer. The length of the blocks in each layer is different from the other layers; the length of the blocks is determined based on the number of bytes in the hash value in that layer. The type of SHA hash function used in each layer is randomly selected from Table I using a pseudorandom number generation algorithm and using the patient's password as the seed for the algorithm.

Table I
SHA Type

#	SHA Type	No. of Bytes
1	SHA-1	160bits=20bytes
2	SHA-224	224bits=28bytes
3	SHA-256	256bits=32bytes
4	SHA-384	384bits=48bytes
5	SHA-512	512bits=64bytes

To make it easier for readers to understand how the proposed algorithm works, some terms and data structures are presented below:

<u>**Inputs:**</u>

- **Source Data (SD):** confidential patient data that will be encrypted using multi-layer encryption. The encryption algorithm treats the **SD** as a file containing bytes.
- **Initial key (IK)**: the patient's password that will be used to calculate the **Seed** value of the pseudorandom number generation algorithm (PRNGA) used in the proposed encryption system.

<u>**Output:**</u> Encrypted Data (**ED**): encrypted patient data generated after encrypting the **SD** using the proposed encryption algorithm.

A. Preparation Stage

- Calculate the **Seed** value using Equation (1):

$$Seed = \sum_{i=0}^{\substack{Length\ of \\ IK-1}} \begin{pmatrix} ASCII\ code\ value\ of \\ each\ character\ of\ IK_i \end{pmatrix} \quad (1)$$

- Use **PRNGA** with the **Seed** value to get the following parameters:
  - A random value **N** with a value between (0…15) that represents the length of the table that is generated in the next point.
  - A table **HFTable** that contains a random sequence of different types of **SHA** hash functions (shown in Table II). For example:

TABLE II
HFTABLE

#	Hash Function	No. of Bytes
1	SHA-224	28
2	SHA-384	48
3	SHA-1	20
4	SHA-224	28
5	SHA-512	64
:	…	…
N	SHA-1	20

  - A vector **V** of random bytes of length equal to **N**, is to be used as the initial value for the first hash function in **HFTable**. For example:

	0	1	2	…	N-1
V	E7	69	A4	…	14

B. Encryption Stage

- For **Layer=1** to **N**, perform the following encryption process:
  - Split **SD** into several blocks whose length is equal to the number of bytes in the **third** column in the **HFTable** in row number equal to **Layer**. For example: if **Layer=2**, and **HFTable[2, 3]=5**.

	0	1	2	3	4	0	1	2	3	4		0	1	2	3	4
SD	13	F3	92	0A	78	22	00	CA	5E	65	…	A5	90	E1	56	89
			Block1					**Block2**						**Blockn**		

  - Call a corresponding hash function in the second column in the **HFTable** in row number **Layer** and use **V** as input data for the function to produce a new hash value **H**. For example:

	0	1	2	3	4
H	13	F3	92	0A	78

  - Now, for each generated block in the previous step, perform the following steps:
    - ➢ Call the corresponding hash function in the **second** column in the **HFTable** in row number **Layer** and use the last hash value produced as input data for the function to produce a new hash value **H**.

	0	1	2	3	4
H	E7	69	A4	9B	14

    - ➢ XOR every byte in the new hash value with the corresponding byte in the current block of SD. For example:

	0	1	2	3	4
H	E7	69	A4	9B	14
XOR					
	0	1	2	3	4
Block1	13	F3	92	0A	78
↓					
	0	1	2	3	4
Block1	F4	9A	36	91	6C

    - ➢ Arrange the bytes in **H** (in ascending order) and arrange the bytes in the corresponding block in **SD** in the same order as the bytes in **H**.

	0	1	2	3	4			0	1	2	3	4
H	E7	69	A4	9B	14	→	**H**	14	69	9B	A4	E7
	0	1	2	3	4			0	1	2	3	4
Block$_1$	F4	9A	36	91	6C	→	**Block$_1$**	6C	9A	91	36	F4

- Construct the encrypted data ED from the last produced encrypted blocks from SD.

IV. EXPERIMENTS AND PERFORMANCE EVALUATION

For the initial performance evaluation of the proposed algorithm, X-ray and MRI images were used as confidential patient data in the experiments. The images used were obtained from the “Kaggle” dataset, which contains various color and grayscale images of different sizes. Examples of these images are shown in Fig. 1. The data in any image file is processed as a sequence of bytes.

A comparison was made with well-known encryption algorithms such as AES and 3DES using several metrics, including Normalized Mean Absolute Error (NMAE), Encrypted Images, Peak Signal to Noise Ratio (PSNR), Entropy, Key Size, Correlation Coefficient, Number of Layers, Encryption Time, Histogram, and Avalanche Effect.

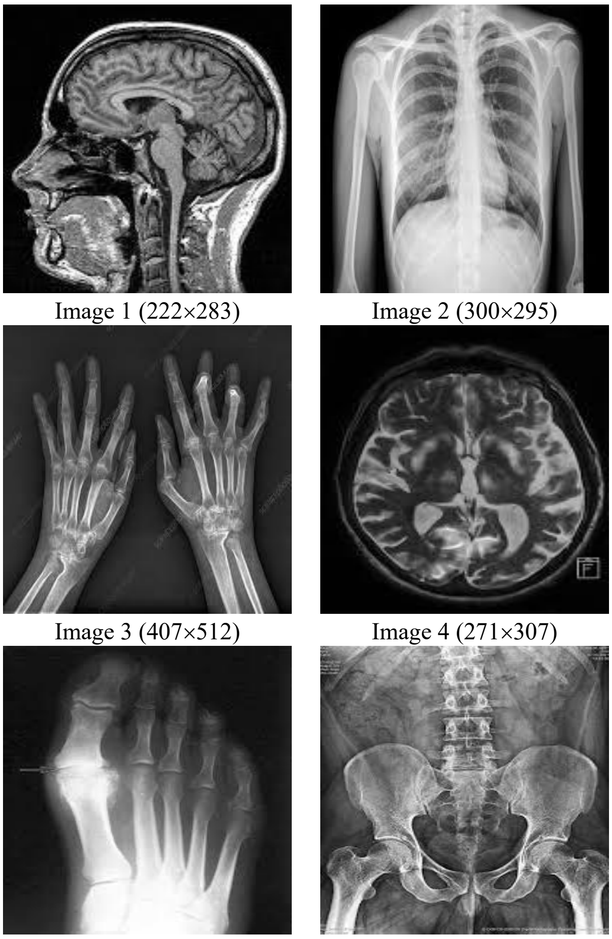


Image 1 (222×283) Image 2 (300×295)

Image 3 (407×512) Image 4 (271×307)

Image 5 (244×263) Image 6 (294×358)

Fig. 1. Examples of images used in the experiments.

A. Normalized Mean Absolute Error (NMAE)

While comparing the original data with encrypted data, Normalized Mean Absolute Error (NMAE) was used in experiments for assessing the effectiveness of the proposed multi-layer encrypted algorithm AES and 3DES, which is represented in Equation (2) [16].

$$\mathrm{NMAE} = \frac{\sum_{k=1}^{N} |S_k - E_k|}{\sum_{k=1}^{N} S_k} \times 100 \tag{2}$$

Where S represents the source data and E represents the encrypted data.

An efficient encryption method will be the one to get the maximum value of NMAE. Table III is the NMAE that has been obtained in experiments between the proposed multi-layer encryption method, AES, and 3DES on six test images. The proposed multi-layer encryption method outperformed other encryption methods, providing strong data protection.

TABLE III
NMAE VALUES FOR ENCRYPTION METHODS (PROPOSED, AES, AND 3DES).

Encryption Method	NMAE (%)						
	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	Average
Proposed	83.832	80.959	49.500	54.601	83.399	62.987	69.213
AES	83.663	80.748	49.439	54.631	83.365	62.954	69.133
3DES	83.733	80.949	49.317	54.453	83.391	62.923	69.128

B. Encrypted Images

Achieving a high distortion ratio in the encrypted image indicates the efficiency of the encryption method in producing unrecognizable images. Fig. 2 shows the encrypted images of the source images (image 3 and image 6) presented in Fig. 1 that were produced using the proposed multi-layer, AES, and 3DES methods. A visual comparison of these encrypted images demonstrates the proposed multi-layer method's effectiveness in producing fully distorted encrypted images similar to the well-known recommended methods AES and 3DES.

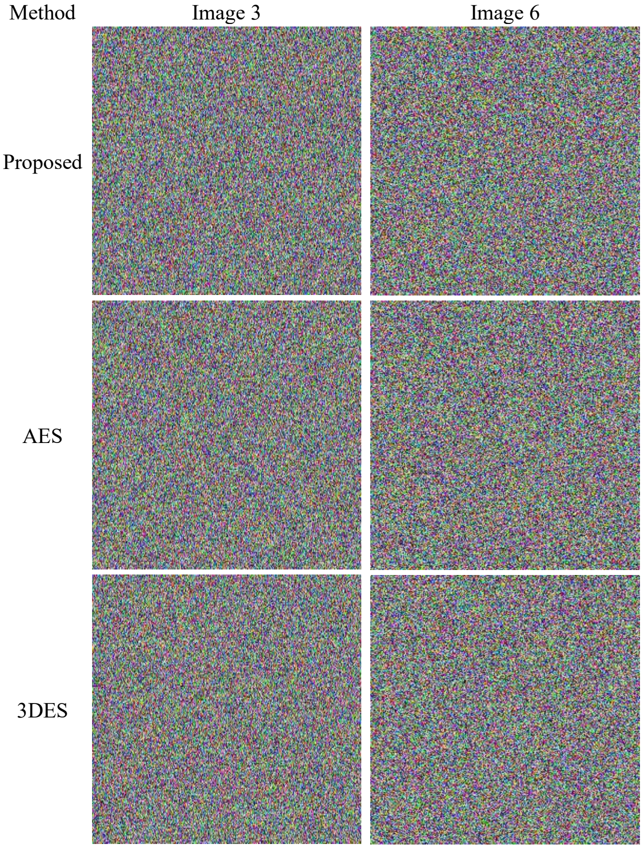


Fig. 2. Encrypted images generated from the source images (image 3 and image 6) in Fig. 1.

C. Peak Signal-to-Noise Ratio (PSNR)

PSNR is another metric measure of the quality of the resulting encrypted image and is used to determine the level of protection achieved by comparing the source data with the encrypted data, as shown in Equation (3). A lower PSNR value indicates better quality of the encrypted image and more efficient encryption [17]:

$$\mathrm{PSNR} = 10.\log_{10}\left(\frac{Max_S^2}{NMAE}\right) \tag{3}$$

Where S represents the source data, and $MaxS$ is the maximum possible byte value of S.

Table IV shows the PSNR values for three encryption methods: proposed multi-layer encryption, AES, and 3DES, calculated for six images with their average values. It is clear from Table IV that the proposed multi-layer encryption method showed the lowest average of PSNR, which means the best performance compared to other methods.

TABLE IV
PSNR VALUES FOR ENCRYPTION METHODS (PROPOSED, AES, AND 3DES).

Encryption Method	PSNR (dB)						
	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	Average
Proposed	6.658	5.520	6.880	7.312	6.797	6.629	6.633
AES	6.656	5.518	6.578	7.306	6.791	6.638	6.581
3DES	6.654	5.531	6.596	7.326	6.796	6.634	6.590

D. Entropy

Entropy is a fundamental mathematical concept that quantifies the randomness of a system. It serves as a metric to measure uncertainty and unpredictability. In essence, entropy assesses how much the outcome of an experiment can be predicted by observing previous outcomes of the same experiment. In cryptography, the entropy value is calculated using Equation (4) [18], [19]:

$$\text{Entropy} = \sum_{i=1}^{n} P_i . log_2(P_i) \tag{4}$$

Where n is the number of different data values and P_i is the occurrence probability of the data value.

Table V shows the entropy values for three encryption methods: proposed multi-layer encryption, AES, and 3DES. The consistently high entropy values across the test images indicate that the proposed multilayer encryption method effectively produces random and unpredictable encrypted data. However, the superior average entropy value of the proposed multilayer encryption method indicates that it may provide a higher level of security and data protection than AES and 3DES.

TABLE V
ENTROPY VALUES FOR ENCRYPTION METHODS (PROPOSED, AES, AND 3DES).

Encryption Method	Entropy						Average
	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	
Proposed	7.99920	7.99979	7.99929	7.99945	7.99896	7.99916	7.99931
AES	7.99918	7.99975	7.99922	7.99941	7.99809	7.99907	7.99912
3DES	7.99920	7.99977	7.99929	7.99935	7.99895	7.99911	7.99928

E. Key Size and Key Space

When proposing cryptography techniques, it is worth underlining that the key used here is one of the crucial arguments, which defines the strength of the proposed methods. This means that the incorporation of a large key to the method increases its strength in ensuring that an attacker will not penetrate it by attempting to guess the code through trial and error. The main key size that had been used in the proposed method is calculated using Equation (5) [7]:

$$\text{Key Size (in bits)} = \text{N} + \text{T} \tag{5}$$

Where N is the number of characters in the initial key entered by the user, and T is the total number of bytes in all hash values generated using the SHA hash functions in all layers.

Table VI displays the key size and key space for the proposed multilayer encryption algorithm, AES, and 3DES, and calculates the average for each. In the case of the key size shown in Table VI, the proposed multilayer encryption method is seen to be much larger than AES and 3DES. This could suggest increased security due to the larger key space.

The proposed multilayer encryption algorithm uses a variable key size depending on the input data, ranging from 1235 bits to 1897 bits, much larger than the 256-bit and 168-bit fixed keys used by AES and 3DES, respectively. It is an innovative and unique feature of this algorithm that represents a significant improvement over the smaller key sizes used in current encryption standards, positions it as a highly promising technique for secure image encryption applications, and makes brute-force attacks on encryption keys significantly more difficult.

TABLE VI
KEY SIZE AND KEY SPACE FOR ENCRYPTION METHODS (PROPOSED, AES, AND 3DES).

Encryption Method	Key Size (bits)							Key space
	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	Average	
Proposed	1327	1559	1378	1406	1235	1897	1467	2^{1467}
AES	256	256	256	256	256	256	256	2^{256}
3DES	168	168	168	168	168	168	168	2^{168}

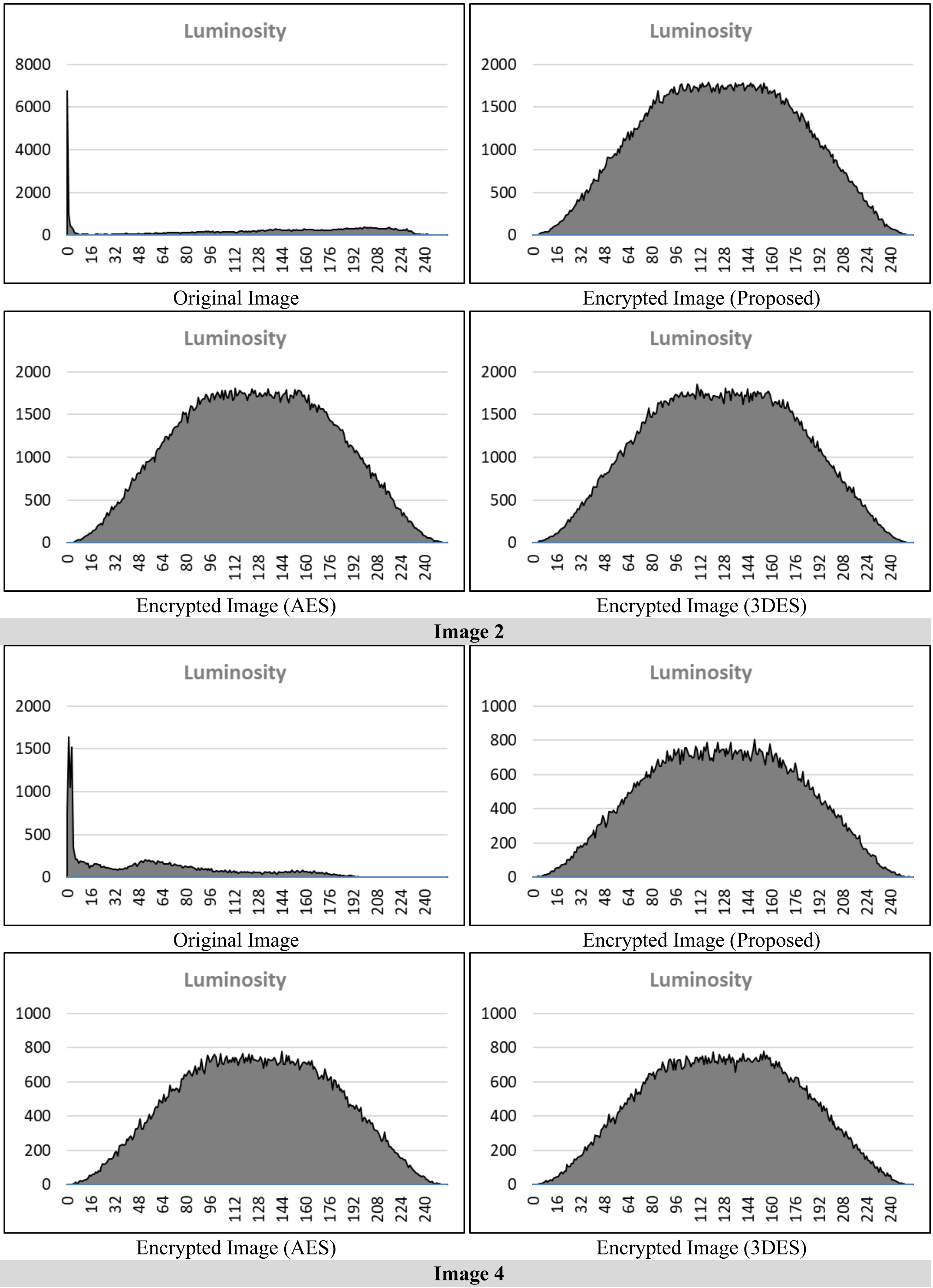
F. Histogram

Histogram analysis is a method used in image encryption to assess the statistical properties of the encrypted image and compare these properties with those of the original image. This involves evaluating pixel distribution and intensity levels. This analysis is essential for assessing the strength and security of image encryption algorithms, ensuring that encrypted images can resist various attacks and exhibit uniform distribution and high entropy levels. Recent advancements in image encryption, including chaotic maps and deep learning techniques, have significantly improved the security and efficiency of encrypted images. These new methods have successfully tackled issues concerning pixel correlation and histogram analysis, making it more difficult for potential attackers to exploit statistical patterns in encrypted images [6].

Fig. 3 presents the histogram of the original image alongside the histograms of their encrypted versions created using three different encryption methods: the proposed multilayer encryption, AES, and 3DES. The pixel distribution in the histograms of the encrypted images generated by the proposed multilayer encryption method is more uniform, similar to that of the AES and 3DES methods. This uniformity results in an approximately equal probability of occurrence for each intensity level. The histograms of Image 2 and Image 4 are given in Fig. 3 as examples, and the histograms of the other encrypted images are similar in shape.

G. Correlation Coefficient

The correlation coefficient quantifies the degree of relation in the encrypted data of consecutive bytes and is an implication of the amount of randomness provided by an encryption method. A lower value of the correlation coefficient means that inter-byte correlations have been reduced by encryption techniques, improving the security of data.



Original Image

Encrypted Image (Proposed)

Encrypted Image (AES)

Encrypted Image (3DES)

Image 2

Original Image

Encrypted Image (Proposed)

Encrypted Image (AES)

Encrypted Image (3DES)

Image 4

Fig. 3. Histograms of the original Images (Image 2 and Image 4) and their encrypted images.

To measure the strength and direction of the linear dependency of two values, Pearson's correlation coefficient is used, the value of which ranges between -1 and 1 [20]. The correlation coefficient is calculated using Equation (6).

$$C = \frac{N\sum_{j=1}^{N}(X_j \times Y_j) - \sum_{j=1}^{N} X_j \times \sum_{j=1}^{N} Y_j}{\sqrt{\left(N\sum_{j=1}^{N} X_j^2 - \left(\sum_{j=1}^{N} X_j\right)^2\right) \times \left(N\sum_{j=1}^{N} Y_j^2 - \left(\sum_{j=1}^{N} Y_j\right)^2\right)}} \quad (6)$$

Where N is the total number of pixels in the encrypted image, X and Y are the pixel values of two neighboring pixels in the encrypted image.

According to the obtained results shown in Table VII, the correlation values of the proposed multilayer encryption method, AES, and 3DES for six test images are presented, and the average correlation values of each encryption method are also calculated.

TABLE VII
CORRELATION VALUES FOR ENCRYPTION METHODS (PROPOSED, AES, AND 3DES).

Encryption Method	Correlation						Average
	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	
Proposed	0.03260	0.03300	0.03110	0.02030	0.02340	0.03450	0.02915
AES	0.03290	0.03420	0.04530	0.02030	0.02810	0.04250	0.03388
3DES	0.05870	0.03360	0.03480	0.02630	0.03210	0.04540	0.03848

H. Number of Layers

The number of encryption layers for each image is determined randomly based on the characters of the initial key entered by the user, as explained in the preparation stage of the proposed method. The randomly generated layers for the images in Fig. 1 are listed in Table VIII. Using a variable number of layers, as opposed to a fixed number, is another design feature that enhances the security of the proposed multi-layer encryption approach.

TABLE VIII
THE RANDOMLY GENERATED LAYERS FOR THE IMAGES IN FIG. 1.

Encryption Method	Initial Key	Number of Layers
Image 1	6$Ta	4
Image 2	%q7H!	2
Image 3	H3W9	5
Image 4	^5G8A	3
Image 5	&U2K89	5
Image 6	M5#s1	3

I. Encryption Time

The speed of the encryption process is an important metric for evaluating the performance of an encryption method. The same images were encrypted using the proposed multilayer encryption technique as well as other known encryption methods, such as AES and 3DES [5], [21].

Table IX compares the encryption times of the proposed multi-layer method, AES, and 3DES. The proposed multilayer encryption method generally has longer encryption times compared to the other two algorithms, likely due to the additional computation required for the multiple encryption layers. But this might be generally accepted for greater security.

TABLE IX
ENCRYPTION TIME FOR ENCRYPTION METHODS (PROPOSED, AES, AND 3DES).

Encryption Method	Encryption Time (Sec.)						
	Image 1	Image 2	Image 3	Image 4	Image 5	Image 6	Average
Proposed	0.491	1.622	0.570	1.201	0.543	0.506	0.822
AES	0.204	0.679	0.194	0.354	0.247	0.242	0.320
3DES	0.231	0.759	0.255	0.384	0.228	0.243	0.350

J. Avalanche Effect

The avalanche effect in casing means that if one bit of input is changed, then more than a 50% change in the encrypted data. This property is used to assess the effectiveness of cryptographic methods to corrupt data with diffusion and make it challenging for the attacker to find patterns or predict output [5].

Fig. 4 shows the recovered source images from the encrypted images (Image 1 and Image 5) in Fig. 1, using the proposed multi-layer method, after altering 1 and 3 bits in the initial key.

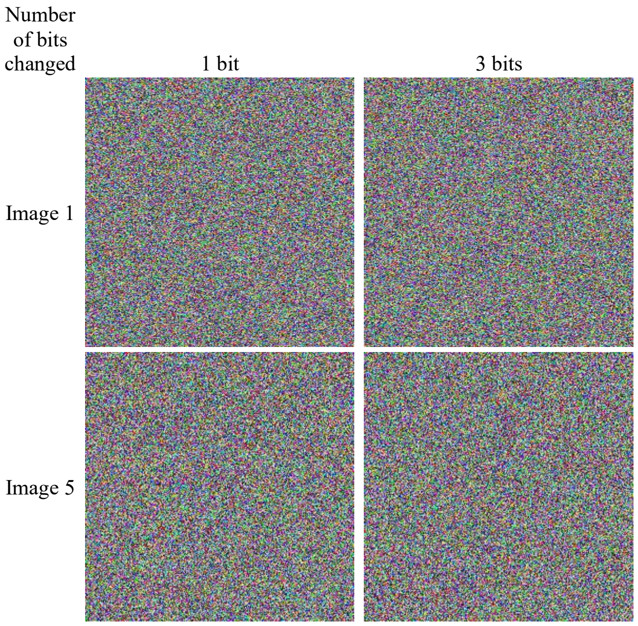


Fig. 4. Recovered images (image 1 and image 5) after changing some bits in the initial key.

V. CONCLUSIONS

This work introduced an algorithm for encrypting images that utilizes multiple layers of encryption. The number of encryption layers is randomly chosen depending on the user-supplied key, increasing complexity and unpredictability to boost the technique's security. Utilizing a variable number of encryption layers that are dynamically determined increases uncertainty and enhances resilience against cryptanalytic attacks like brute-force or differential attacks.

The multi-layer encryption method being suggested has undergone a comprehensive assessment and comparison with AES and 3DES on different criteria, including entropy, key size, NMAE, PSNR, Correlation, number of encryption layers, encryption time, histogram, and Avalanche effect. These thorough assessments showcase the method's strength and efficiency in securely encrypting images, comprehensively evaluating its performance, and security features. The results indicate that while the proposed multi-layer encryption method may have some trade-offs in encryption time, it could offer enhanced security features due to its utilization of multiple encryption layers and variable parameters.

ACKNOWLEDGMENT

The authors would like to thank Irbid National University, Irbid, Jordan.

REFERENCES

[1] Ahmed, S. T., Hammood, D. A., Chisab, R. F., Al-Naji, A., & Chahl, J., "Medical image encryption: a comprehensive review," Computers, vol. 12, no. 8, pp160-205, 2023.

[2] Naeem, U. H., Bilal, M., Syed, F., Rasheed, K., & Saad, S, "A Multilayer encryption model to protect healthcare data in cloud environment," In 2022 International Conference on Data Analytics for Business and Industry (ICDABI), pp. 42-48, 2022.

[3] Altowaijri, S. M., "An architecture to improve the security of cloud computing in the healthcare sector," Smart Infrastructure and Applications: Foundations for Smarter Cities and Societies, pp 249-266, 2020.

[4] Aouissaoui, I., Bakir, T., & Sakly, A., "Robustly correlated key-medical image for DNA-chaos-based encryption," IET Image Processing, vol. 15, no. 12, pp 2770-2786, 2021.

[5] Al-Husainy, M. A. F., Al-Sewadi, H. A., & Sayed, A. M., "Using the 3D protein structure as key to encrypt images," Journal of Information and Organizational Sciences, vol. 47, no. 2, pp 333-354, 2023.

[6] Al-Hyari, A., Obimbo, C., & Altaharwa, I., "Generating powerful encryption keys for image cryptography with chaotic maps by incorporating collatz conjecture," IEEE Access, 2024.

[7] Al-Shargabi, B., & Al-Husainy, M. A. F., "A new DNA-based encryption algorithm for internet of things," In International Conference of Reliable Information and Communication Technology, pp 786-795, 2020.

[8] Baagyere, E. Y., Agbedemnab, P. A. N., Qin, Z., Daabo, M. I., & Qin, Z., "A multi-layered data encryption and decryption scheme based on genetic algorithm and residual numbers," IEEE Access, vol. 8, pp 100438-100447, 2020

[9] Oanta, Emil M., Iustin Priescu, and Catalin Apostolescu. "Multi-layer encryption flexible integrating algorithm," In Advanced Topics in Optoelectronics, Microelectronics, and Nanotechnologies XI, vol. 12493, pp 482-488, 2023

[10] Chethana, S., Charan, S. S., Srihitha, V., Radha, D., & Kavitha, C. R., "Comparative analysis of password storage security using double secure hash algorithm," In 2022 IEEE North Karnataka Subsection Flagship International Conference (NKCon), pp 1-5, 2022

[11] Zhou, S., He, P., & Kasabov, N., "A dynamic DNA color image encryption method based on SHA-512," Entropy, vol. 22, no. 10, pp 1091-1114, 2020

[12] Qin, Q., Liang, Z., Liu, S., Wang, X., & Zhou, C., "A dual-domain image encryption algorithm based on hyperchaos and dynamic wavelet decomposition," IEEE Access, vol. 10, pp 122726-122744, 2022

[13] Shraida, G. K., & Younis, H. A. "An efficient diffusion approach for chaos-based image encryption and DNA sequences," Iraqi Journal for Electrical and Electronic Engineering, vol. 18, no. 2, pp 69-74, 2022.

[14] Lin, C. H., Wen, C. H., Lai, H. Y., Huang, P. T., Chen, P. Y., Li, C. M., & Pai, N. S., "Multilayer convolutional processing network-based cryptography mechanism for digital images. Infosecurity," Processes, vol. 11, no. 5, pp 1476-1496, 2023

[15] Sabir, S., & Guleria, V., "A novel multi-layer color image encryption based on RSA cryptosystem, RP2DFrHT and generalized 2D Arnold map," Multimedia Tools and Applications, vol. 82, no. 25, pp 38509-38560, 2023

[16] Al-Shargabi, B., & Al-Husainy, M. A. F., "Multi-round encryption for COVID-19 data using the DNA key," International Journal of Electrical & Computer Engineering, vol. 12, no. 1, pp 2088-8708, 2022.

[17] Abduljaleel, I. Q., Abdul-Ghani, S. A., & Naji, H. Z., "An image of encryption algorithm using graph theory and speech signal key generation," Journal of Physics: Conference Series, vol. 1804, no. 1, pp 012005-012016, 2021.

[18] Abbas Fadhil Al-Husainy, M., AA Al-Sewadi, H., & Al-Shargabi, B., "Image encryption using a binary search tree structure-based key," International Journal of Computing and Digital Systems, vol. 12, no. 1, pp 823-836, 2022

[19] Upadhyaya, A., Rai, C. S., & Aithal, G., "Residue number system-based S-box generation and its applications in AES for image encryption," IAENG International Journal of Applied Mathematics, vol. 54, no. 9, pp 1867-1881, 2024

[20] Wenzhao Teng, and Yujun Zhang, "STRay: A Model for prohibited item detection in security check images," Engineering Letters, vol. 32, no. 10, pp 1854-1861, 2024,

[21] Mniai, A., & Jebari, K., "Credit card fraud detection by improved SVDD," In Proceedings of the World Congress on Engineering, 2022, July 6-8, London, U.K., pp 6-8