

# Strengthening Security and Confidentiality in E-Health Systems through Quantum Encryption of Healthcare Images

Ahmed J. Kadhim<sup>\*</sup>, Tayseer S. Atia<sup>\*\*</sup>

<sup>\*</sup> College of Engineering, Al-Iraqia University, Iraq  
Email: Ahmed.j.kadhim@aliraqia.edu.iq  
<https://orcid.org/0009-0008-9511-2713>

<sup>\*\*</sup> College of Engineering, Al-Iraqia University, Iraq  
Email: tayseer.salman@aliraqia.edu.iq  
<https://orcid.org/0000-0002-1552-569X>

## Abstract

This study presents a pioneering quantum encryption technique, the Generalized Novel Enhancement Quantum Representation (GNEQR), to ensure enhanced security for color medical images in E-health systems. The proposed method is seamlessly integrated into an ASP.NET Web API and Blazor Web Assembly environment. During the encryption process, the GNEQR algorithm utilizes advanced bit-plane scrambling to obscure the original color medical image. A 5D chaotic map is employed to generate an image key, which is then used to create a scrambled version of the key image. Applying an XOR operation between the scrambled image and the key image produces a highly secure quantum-encrypted color image. In the decryption process, the inverse of the encryption steps is implemented, leveraging the 5D chaotic map-generated key to accurately reconstruct the original color medical image. This research aims to significantly enhance E-health security by protecting patient data, including medical images and histories, through quantum encryption. The incorporation of GNEQR within an ASP.NET Web API and Blazor Web Assembly framework facilitates seamless deployment and underscores the potential of this method to revolutionize healthcare data privacy and integrity.

**Keywords-** 5D chaotic map, patient confidentiality, GNEQR, healthcare images, and quantum encryption.

## I. INTRODUCTION

Medical images are crucial in e-health and must be securely protected from unauthorized access. Quantum encryption has emerged as a promising method to enhance e-health security. Recently, a novel technique based on an evolutionary framework was proposed for the secure encryption of color images[1], This technique employs a combination of bit plane scramble, 5D chaotic map, and XOR operations, implemented using C# and the Asp.net Core web API. The encryption system is integrated with the Blazor web assembly to ensure secure medical image transfer.

Several other research investigations have also explored various encryption techniques for medical images. One study introduced a color image encryption system based on hyperchaos and the Hopfield chaotic neural network[2]. Another approach utilized an adaptive DNA code base and a new multi-chaotic map for encrypting medical images[3]. Furthermore, an encryption method drawing edge maps from the source image was proposed[4].

In the context of e-health security and privacy, several related works have contributed valuable insights and solutions. 'eHealth: A Survey of Architectures, Developments in mHealth, Security Concerns, and Solutions' presents an overview of security concerns in e-health, including electronic health record (EHR) security, cloud-based e-health data security, privacy requirements, and cryptographic and non-cryptographic techniques for EHRs[5]. Similarly, 'A Comprehensive Survey on Security and Privacy for Electronic Health Data' identifies security concerns, requirements, solutions, and research gaps for electronic health data security and privacy[6]. 'Investigation of Privacy and Security Challenges in e-Health Clouds' proposes a framework to address data confidentiality, availability, integrity, authentication, authorization, and accountability in e-health clouds[7]. 'Security and confidentiality of electronic health records: issues and obstacles' evaluate various solutions for privacy and security concerns in health organizations[8]. Additionally, 'Is it conceivable for eHealth to offer both security and privacy?' argues the need for organizational, legal, and technical measures to address e-health security and confidentiality concerns.[9]. Lastly, 'Security and Resilience in eHealth Infrastructures and Services' examines Member States' approaches and measures to protect critical healthcare systems.[10]. These related works collectively contribute to the growing efforts to enhance E-health security and privacy, aligning with the aims of this research on quantum encryption using GNEQR in an ASP.NET Web API and Blazor Web Assembly framework.

To structure the paper, Section 2 presents earlier work on the suggested strategy, while Section 3 lays the foundation for secure healthcare media encryption. Section 4 describes a novel method based on Chaotic 9D for producing a key for quantum image encryption and decryption. In Section 5, an analysis of the numerical simulations performed on a conventional computer is presented. Finally, Section 6 provides concluding thoughts on the research's findings and implications.

## II. FRAMEWORK FOR SECURING PATIENT DATA AND IMAGES

The study introduces a quantum image encryption framework developed using C#, ASP.NET Core Web API, and Blazor WebAssembly, aiming to ensure the utmost security and privacy of patient data and medical images in healthcare systems[11]. This framework enables efficient access to web APIs while safeguarding patient data and images through quantum encryption. Implementing this framework represents a significant advancement in healthcare data security, promising enhanced confidentiality and integrity during the data exchange.

Blazor WebAssembly, a widely adopted solution for single-page web applications, follows the typical n-layer pattern of web application development. In this design, the user interface is separated from the business logic and data access, with the latter two typically deployed as an API service. By integrating Blazor WebAssembly into an ASP.NET Core web application using familiar C code files and Razor [12],The framework facilitates the development of a secure and user-friendly web user interface for healthcare applications, As shown in Fig.1.

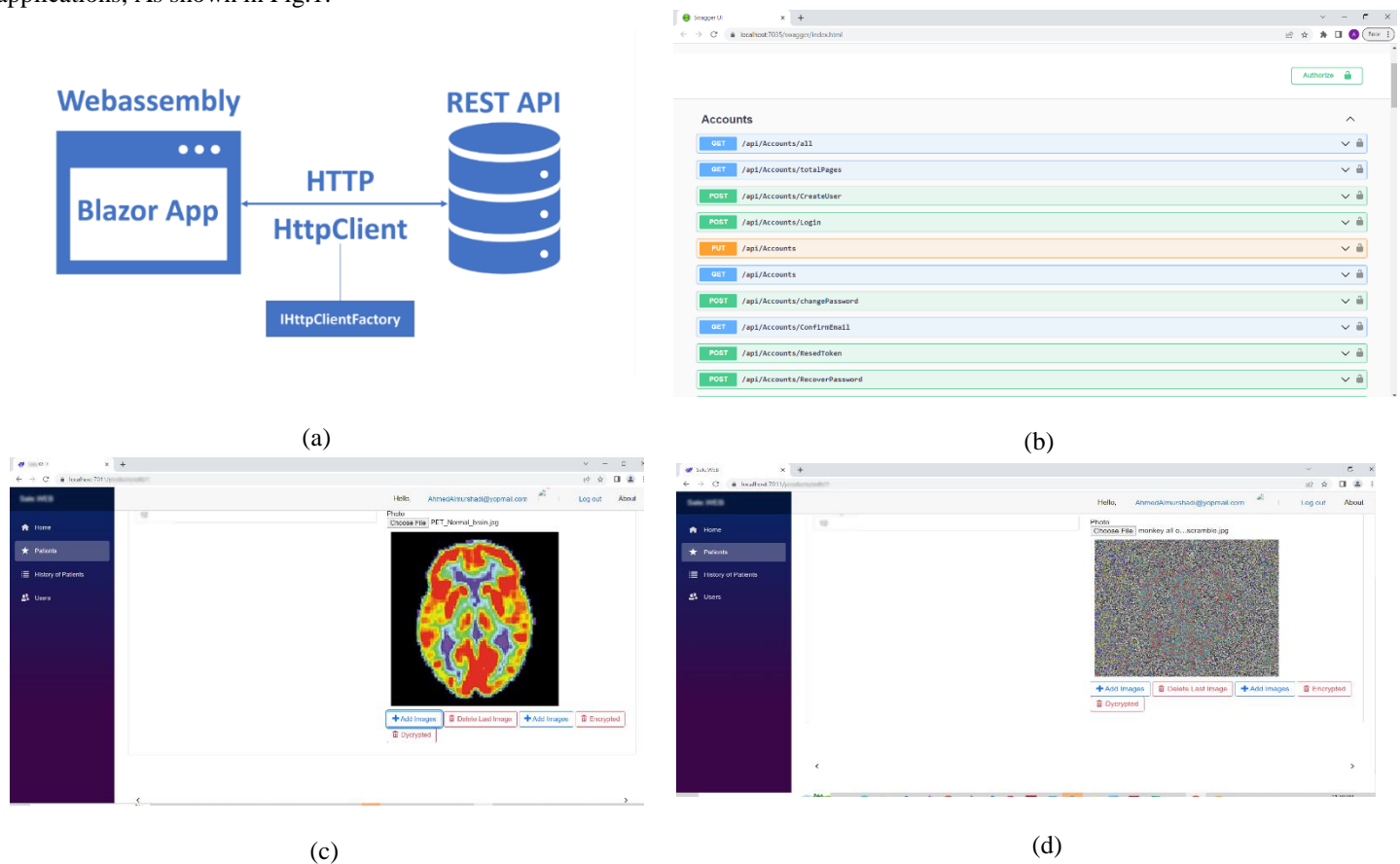


Fig.1. (a)A Comprehensive Framework for Secure Healthcare Data Transfer: Blazor App, Reset API HTTP, and IHttpClientFactory[13] ,(b) ASP.NET Core API, (c) Upload Image to Azure from Blazor WebAssembly,(d) Encrypted Image through Blazor WebAssembly.

Fig.1 illustrates a secure healthcare data transfer process using a Blazor App, a Reset API HTTP block, and an IHttpClientFactory block. The Blazor App serves as a user-friendly single-page web application, enabling healthcare workers to access and manage patient medical photos securely. When users interact with the app, the Reset API HTTP block acts as a middleware, processing HTTP requests and securely communicating with the data source to retrieve relevant medical images and patient data. All data exchange is conducted using HTTPS to ensure confidentiality and integrity. The IHttpClientFactory block facilitates secure client-side HTTP requests, optimizing network resource usage while maintaining connection security. Together, these components create a comprehensive and secure framework for seamless healthcare data transfer.

With the technology built to maintain security and privacy throughout the transfer process to the cloud, healthcare workers can access

patient medical photos from various locations. The proposed method involves patients and healthcare professionals utilizing a quantum encryption system in one place to protect sensitive medical images before transmitting them to the cloud. Subsequently, healthcare participants in another location can access and decrypt the cloud-based photos while ensuring the confidentiality of the patient and the healthcare system throughout the transfer process[14], thanks to the suggested quantum encryption technique. This approach addresses the critical need for secure and private data transfer in the healthcare domain.

### III. SECURE QUANTUM MEDICAL IMAGE ENCRYPTION FRAMEWORK FOR PATIENT DATA AND IMAGES

Fig. 2 illustrates the novel secure quantum medical images encryption framework proposed in this study, specifically designed for cloud-based storage, utilizing Azure Blob Cloud. The framework follows a systematic two-stage process: First, medical images are uploaded from the system to Azure Blob Cloud. Secondly, a Generalized Model of Novel Enhanced Quantum Representation (GNEQR) is applied to construct a quantum state  $|I\rangle$  representing the image. The GNEQR quantum image is generated using a block-based image scrambling scheme. The GNEQR quantum image and its quantum state can then be obtained[15]. The GNEQR quantum image and its quantum state can then be obtained[16], and the quantum state  $|I\rangle$  undergoes scrambling using a robust algorithm to enhance encryption security, along with the generation of a key matrix through a chaotic 5D system [17].

In the second stage, the scrambled quantum state  $|I\rangle$  and the scrambled key matrix  $|K\rangle$  are processed through an XOR operation[18], resulting in a new quantum state  $|O\rangle$  that accurately represents the encrypted image. To ensure precise image restoration, a precise sequence of steps is followed. The quantum state  $|I\rangle$ , representing the original image, is retrieved by performing the XOR operation on the scrambled quantum state  $|O\rangle$  and the scrambled key matrix  $|K\rangle$ . Subsequently, the quantum state  $|I\rangle$  is unscrambled using the inverse of the encryption algorithm, effectively restoring it to its original form. The proposed framework ensures the utmost confidentiality and integrity of patient data and images, particularly color medical images, within cloud-based healthcare systems.

Through the adoption of this secure quantum medical image encryption framework, the study presents a promising approach to bolster the protection of sensitive medical data in cloud-based environments. The framework's potential implications for healthcare systems are significant, as it effectively addresses critical concerns related to data security and privacy, fostering trust and reliability in medical image storage and transfer.

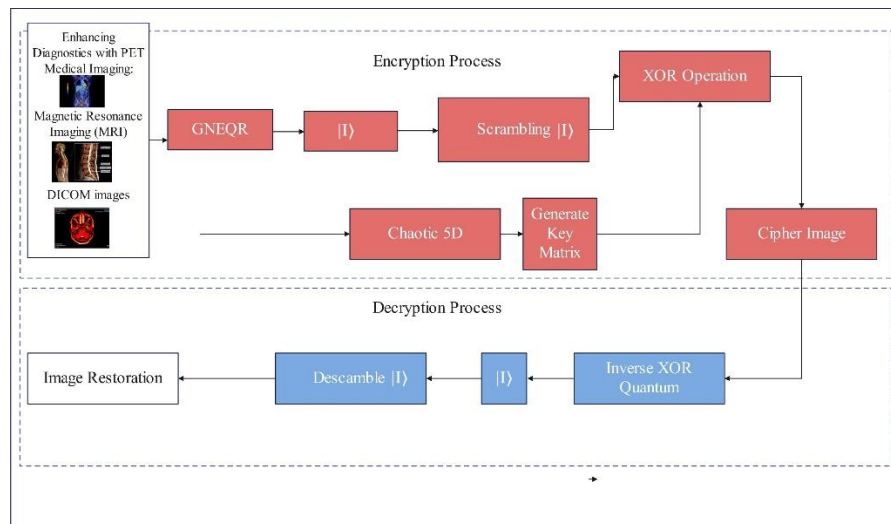


Fig.2. Quantum Encryption for E-Healthcare Images: Block Diagram

### IV. GNEQR (GENERALIZE MODEL OF NOVEL ENHANCEMENT QUANTUM REPRESENTATION)

An image with  $2n \times 2m$  dimensions can be represented by the GNEQR image representation paradigm using  $n + m$  qubits. Three grayscale images are created from an RGB colour image[19].

$$|\Phi_G^r\rangle = \frac{1}{2^{a+b}} \sum_{x=0}^{2^a-1} \sum_{q=0}^{2^b-1} |f_r(x, q)\rangle |x\rangle |q\rangle, \quad (1)$$

$$|\Phi_G^g\rangle = \frac{1}{2^{a+b}} \sum_{x=0}^{2^a-1} \sum_{q=0}^{2^b-1} |f_g(x, q)\rangle |x\rangle |q\rangle, \quad (2)$$

$$|\Phi_G^b\rangle = \frac{1}{2^{a+b}} \sum_{x=0}^{2^a-1} \sum_{q=0}^{2^b-1} |f_b(x, q)\rangle |x\rangle |q\rangle, \quad (3)$$

The Red, Green, and Blue channels of a pixel's colour are represented by the quantum states  $|\Phi_G^r\rangle$ ,  $|\Phi_G^g\rangle$ , and  $|\Phi_G^b\rangle$ , respectively, at the coordinates  $(x, q)$ . Symbols represent these channels. There are three mathematical operators:  $f_r(x, q)$ ,  $f_g(x, q)$ , and  $f_b(x, q)$ . As a result, the GNEQR for  $2n \times 2m$  colour images is computed. The three colour channels of the colour images—R, G, and B—are shown here.

$$|\Phi_c\rangle = \frac{1}{\sqrt{3}} (|\Phi_G^r\rangle|01\rangle + |\Phi_G^g\rangle|10\rangle + |\Phi_G^b\rangle|11\rangle) \quad (4)$$

Utilizing GNEQR, a colored image with dimensions of  $2n \times 2m$  can be produced. This method requires using either  $(n + m + 8)$  or  $(n + m + 10)$  qubits.

Consider the following representation of a 4x4 color image:

```

|R | G | B | R |
|G | B | R | G |
|B | R | G | B |
|R | G | B | R |

```

Each pixel's red, green, and blue channels are denoted as R, G, and B. It must represent this image in GNEQR using the formula (1,2,3) shown before. It must apply GNEQR to each colour channel separately before combining the three channels using equation (4).

The GNEQR for the red channel can be determined as follows:

$$|\Phi_G^r\rangle = \frac{1}{2} * (|0000\rangle |11\rangle + |0100\rangle |10\rangle + |1010\rangle |01\rangle + |1110\rangle |00\rangle)$$

Similar formulas can be used to compute the GNEQR for the green and blue channels:

$$|\Phi_G^g\rangle = \frac{1}{2} * (|0010\rangle |11\rangle + |0110\rangle |10\rangle + |1001\rangle |01\rangle + |1101\rangle |00\rangle)$$

$$|\Phi_G^b\rangle = \frac{1}{2} * (|0001\rangle |11\rangle + |0101\rangle |10\rangle + |1011\rangle |01\rangle + |1111\rangle |00\rangle)$$

The three channels can eventually be combined as follows, using equation (4):

$$|\Phi_c\rangle = \frac{1}{\sqrt{3}} (|\Phi_G^r\rangle|01\rangle + |\Phi_G^g\rangle|10\rangle + |\Phi_G^b\rangle|11\rangle)$$

The Generalized Nested Quantum Representation (GNEQR) technique is used in Algorithm 1's "Representation of the GNEQR," which transforms a 4x4 colour image into a quantum state. It does distinct processing for the red, green, and blue colour channels while figuring out coefficients for every pixel position. Every pixel is given a quantum state, which is then combined to produce an exhaustive quantum representation of the complete image. The resultant quantum state  $|I\rangle$  enables prospective applications in quantum data encoding and picture processing.

---

**Algorithm one:** Representation of the GNEQR

---

**Input:** 4x4 color image represented as a 2D array 'color\_image[4][4]'.

The color image should have pixel values for the red, green, and blue channels at each pixel location  $(x, q)$ .

**Output-** quantum State: an array of complex numbers representing the GNEQR quantum state of the  $|I\rangle$  sequence.

Function GNEQR\_Red\_Channel(image, a, b):

```

red_channel_gneqr = 0
for x from 0 to 2n-1:
    for q from 0 to 2m-1:
        fr = calculate_fr(image[x][q].red, a, b)
        gneqr_state = (1 / (2^(a + b))) * fr * |x>|q>
        red_channel_gneqr += gneqr_state
    End for
End for

```

Function GNEQR\_Green\_Channel(image, a, b):

```

green_channel_gneqr = 0
for x from 0 to 2n-1:
    for q from 0 to 2m-1:

```

---

```
fg = calculate_fg(image[x][q].green, a, b)
gneqr_state = (1 / (2^(a + b))) * fg * |x>|q>
green_channel_gneqr += gneqr_state
End for
End for
return green_channel_gneqr
Function GNEQR_Blue_Channel(image, a, b):
blue_channel_gneqr = 0
for x from 0 to 2n-1:
  for q from 0 to 2m-1:
    fb = calculate_fb(image[x][q].blue, a, b)
    gneqr_state = (1 / (2^(a + b))) * fb * |x>|q>
    blue_channel_gneqr += gneqr_state
  End for
End for
return blue_channel_gneqr
Function GNEQR_Combine_Image(image, a, b):
red_gneqr = GNEQR_Red_Channel(image, a, b)
green_gneqr = GNEQR_Green_Channel(image, a, b)
blue_gneqr = GNEQR_Blue_Channel(image, a, b)
normalization_factor = 1 / sqrt(3)
image_gneqr = normalization_factor * (red_gneqr |01> +
green_gneqr |10> + blue_gneqr |11>)
Return quantum State |I>
```

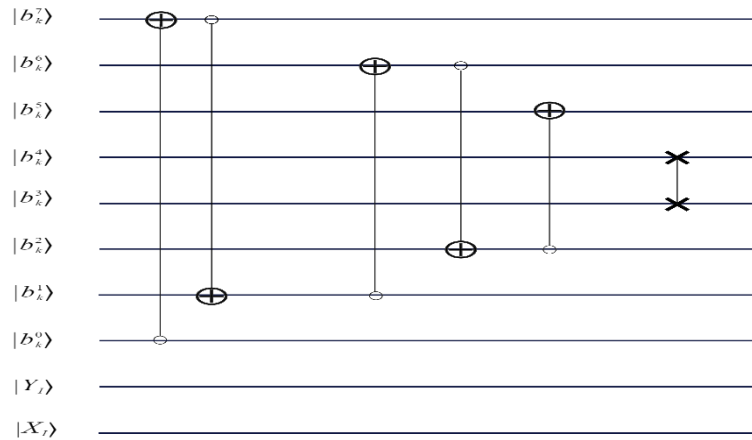
---

## V. QUANTUM IMAGE SCRAMBLE

The scramble image circuit is a quantum circuit implemented in C# that aims to perturb or disorder the information encoded within the qubits of a quantum state. It achieves this by employing a sequence of Controlled-NOT (CNOT) gates and a Swap gate to create a scrambling effect[20]. The principal goal of this circuit is to establish an entangled state characterized by interdependent quantum correlations, thus distributing the encoded information across several qubits in a manner that defies straightforward analysis, as shown in Fig.3. The constituents of the circuit and their respective operations can be summarized as follows:

- 1) CNOT Gate from  $b_0$  to  $b_7$ : The Controlled-NOT gate functions to apply a NOT operation exclusively on the target qubit  $b_7$ : when the control qubit ( $b_0$ ) is in the state  $|1\rangle$ . This operation fosters the entanglement of  $b_0$  and  $b_7$ , thereby enabling the transfer of information from  $b_0$  to  $b_7$ .
- 2) CNOT Gate from  $q_7$  to  $q_1$ : Analogously, the CNOT gate acting from  $b_7$  to  $b_1$  establishes entanglement between  $b_7$  and  $b_1$ , facilitating the exchange of information between these two qubits.
- 3) CNOT Gate from  $b_1$  to  $b_6$ : By means of this CNOT gate,  $b_1$  and  $b_6$  become entangled, resulting in the transfer of information between these two qubits.
- 4) CNOT Gate from  $b_6$  to  $b_1$ : This particular CNOT gate engenders a bidirectional entanglement between  $b_6$  and  $b_1$ , contributing further to the intricate shuffling of information.
- 5) CNOT Gate from  $b_6$  to  $b_2$ : The CNOT gate acting from  $b_6$  to  $b_2$  engenders entanglement between  $b_6$  and  $b_2$ , further enhancing the distribution of information across these qubits.
- 6) CNOT Gate from  $b_2$  to  $b_5$ : Through this CNOT gate,  $b_2$  and  $b_5$  become entangled, thereby enabling the exchange of information between these two qubits.
- 7) Swap Gate between  $b_3$  and  $b_4$ : The Swap gate conducts an exchange of states between  $b_3$  and  $b_4$ , effectively interchanging the information encoded in these two qubits.

As the CNOT and Swap operations are combined within this quantum circuit, it produces a complex and entangled quantum state. The resultant state exhibits a high degree of correlation among the qubits, leading to a sophisticated distribution of information that transcends simple linear arrangements. This scrambling process holds potential significance in quantum information processing, where entanglement and perturbation can offer distinct advantages for various quantum algorithms and protocols.



**Fig .3.** proposed Bit-plane Scramble Method

## VI. GENERATE KEY IMAGE

The chaotic five-dimensional (5D) system is a mathematical model with intricate and unpredictable behavior. It is characterized by a set of differential equations describing the evolution of five variables: A, B, C, W, and U. These variables interact nonlinearly and are governed by parameters including x, y, z, d, e, f, g, h, and i. The system's behavior is extremely sensitive to initial conditions and parameter values, which means that even minor modifications can result in significantly different outcomes[21].

The chaotic 5D system displays intricate patterns and irregular trajectories when simulated or iterated over time. Minor initial conditions or parameter value changes can lead to significantly different outcomes, making long-term predictions practically impossible. This sensitivity to initial conditions gives rise to the system's random-like behavior, which can be harnessed for encryption and essential generation purposes.

$$A = -ax + yz \quad (5)$$

$$B = by - xz \quad (6)$$

$$C = xy - cz + dw(f + 3gu^2) \quad (7)$$

$$W = xy - ew \quad (8)$$

$$U = -z \quad (9)$$

---

### Algorithm two: Generate Image Key

---

Input: Initial values of variables A, B, C, W, and U

Parameter values for x, y, z, d, e, f, g, h, and i

Number of iterations for key generation process

Output- Generated key (final values of A, B, C, W, and U)

Start

Initialize the variables A, B, C, W, and U with the provided initial values.

Set the values for the parameters x, y, z, d, e, f, g, h, and i.

Choose the desired number of iterations for the key generation process.

For each iteration from 1 to the specified number of iterations:

Calculate the derivatives A', B', C', W', and U' using the given equations and the current values of A, B, C, W, and U.

$$dA = -a * A + b * B + U + c * e^A U$$

$$dB = -B + d * A - A * Z - W$$

$$dC = -e * C + A * B + f * e^A U$$

$$dW = g * U - A * B + h * W$$


---

---

$$dU = -h * W + i * B - f * A * Z + e^U$$

Update the values of A, B, C, W, and U by adding the corresponding derivatives multiplied by a small time step.

$$A = A + dA * \text{time\_step}$$

$$B = B + dB * \text{time\_step}$$

$$C = C + dC * \text{time\_step}$$

$$W = W + dW * \text{time\_step}$$

$$U = U + dU * \text{time\_step}$$

End For

Once the iterations are complete, the final values of A, B, C, W, and U represent the generated key.

The generated key can be used for encrypting the image using a suitable encryption algorithm.

---

## VII. XOR OPERATION

The XOR operation is a key component in the proposed secure quantum medical image encryption framework. It plays a pivotal role in enhancing data security by combining the scrambled quantum state representing the medical image and the scrambled key matrix generated through the 5D chaotic system, as shown in Fig.4.. Here is how the XOR operation is applied to produce the encrypted quantum state:

- 1) Scrambling the quantum state: The quantum state representing the medical image is scrambled using a quantum scrambling techniques[22].
- 2) Generating the key matrix: A key matrix is generated through a 5D chaotic system[23].
- 3) Applying the XOR operation: The scrambled quantum state and the key matrix are combined using the XOR operation. This bitwise operation creates an encrypted quantum state[14][22].

By applying the XOR operation, the proposed framework ensures the utmost confidentiality and integrity of patient data within cloud-based healthcare systems. The encrypted quantum state safeguards sensitive medical information from unauthorized access and provides reliable image storage and transfer. The inverse operation of XOR can be used to restore the precise image when needed[23][14].



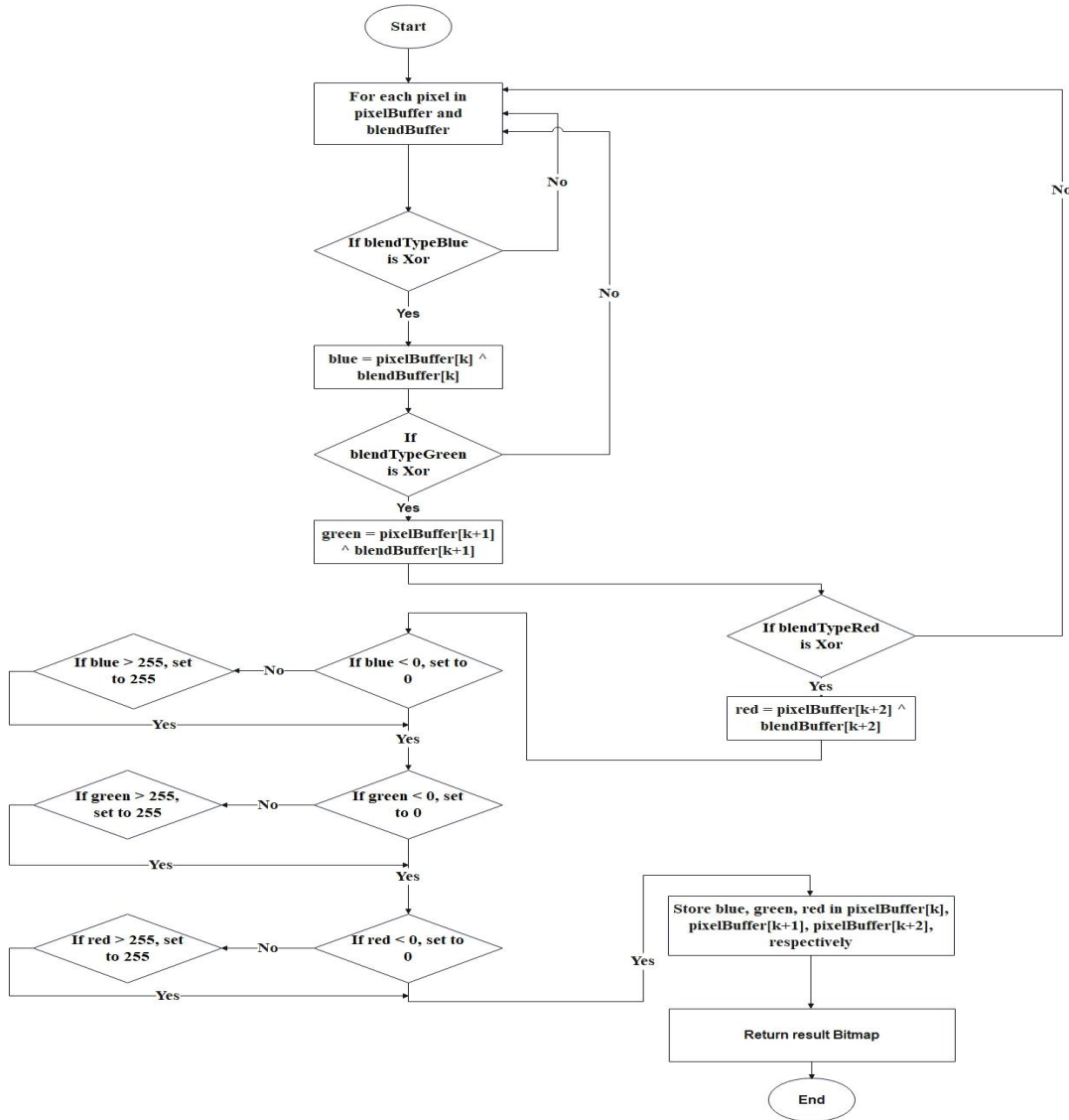


Fig.4. The XOR Operation in Secure Quantum Medical Image Encryption Framework

## VIII. DECRYPTION PROCESS

In the descrambling process of the secure quantum medical image encryption framework, the "inverse operation" refers to reversing the XOR operation applied during encryption. The XOR operation combines the scrambled quantum state  $|I\rangle$  representing the medical image and the scrambled fundamental matrix  $|K\rangle$ , producing the encrypted quantum state  $|O\rangle$ . To restore the original image, the inverse operation involves performing XOR between the encrypted quantum state  $|O\rangle$  and the scrambled key matrix  $|K\rangle$ .

By applying the inverse XOR operation, the framework retrieves the quantum state  $|I\rangle$ , which represents the original medical image before encryption. Subsequently, the quantum state  $|I\rangle$  is unscrambled using the inverse of the encryption algorithm, effectively restoring it to its original form. This process ensures the accurate and faithful restoration of the medical image with the utmost confidentiality and integrity, safeguarding sensitive patient data within cloud-based healthcare systems.

## IX. ANALYSIS AND EVALUATION OF THE PROPOSED APPROACH'S OUTCOMES AND EFFICIENCY








































The development of a patient security data system and the implementation of quantum encryption for medical images using C# and ASP.NET Core web API and Blazor WebAssembly on Visual Studio 2022, with the assistance of a Windows 10 64-bit operating system, an AMD Ryzen 7 processor, and 16 GB of RAM, was a challenging and impressive endeavor. C# and ASP.NET web API are extensively utilized development tools for web applications, including e-health systems. A secure and effective platform for transmitting and storing medical images was developed using these technologies and the Azure cloud platform. A quantum encryption method was also implemented. This achievement demonstrates the



developer's software development skills and capacity to apply their knowledge to real-world healthcare problems.. This achievement demonstrates the developer's software development skills and capacity to apply their knowledge to real-world healthcare problems.

Table 1 shows Medical image encryption involves scrambling and substituting image pixels to protect the distribution of digital medical images[24]. The proposed approach likely involves image scrambling and the use of XOR operations with a key image[25][26]. These encryption techniques play a vital role in ensuring the confidentiality and integrity of sensitive patient data, making the developed platform even more robust and secure. By applying these advanced encryption methods, the system can safeguard medical images during transmission and storage, adhering to the highest data protection standards in the healthcare domain.

**Table1.** Medical Image Encryption Techniques and Approaches.

No	Image	Scrambled Image	XOR operation between Scrambled image and key image
1	CT of the head 		
2	X-ray of the left arm 		
3	x-ray chest 		
4	MRI of the spine 		
5	Tumor on MRI of the brain 		
6	Breast cancer CT scan 		
7	Mammography 2 		
8	CT scan of the abdomen 		
9	CT 2 of the Head 		
10	MRI of Brain 2 		
11	MRI of the Spine, Axial 		
12	X-ray of the left arm 		
13	Second X-ray 		

## X. ENTROPY

Entropy is the standard measure of an encryption algorithm's randomness-based effectiveness [23]. The entropy  $H(s)$  is equal to:

$$\text{Entropy} = \sum p(u_i) \log \frac{1}{p(u_i)} \quad (10)$$

$$\overline{\text{Entropy}}_{k,TB} = \sum_{i=1}^k \frac{\text{Entropy}}{k} \quad (11)$$

Where (Si) represents the blocks and TB represents the pixel, the standard Entropy value is 8.

**Table2.** The entropy of information for the suggested scheme.

No	image	Entropy
1	CT of the head	7.9581
2	X-ray of the left arm	7.9669
3	x-ray chest	7.9521
4	MRI of the spine	7.9702
5	Tumor on MRI of the brain	7.9627
6	Breast cancer CT scan	7.9566
7	Mammography 2	7.9519
8	CT scan of the abdomen	7.9537
9	CT 2 of the Head	7.9553
10	MRI of Brain 2	7.9548
11	MRI of the Spine, Axial	7.9510
12	X-ray of the left arm	7.9631
13	Second X-ray	7.9468
	Average	7.957169

The entropy of the information for the suggested encryption method is displayed in the table. A measure of a data set's randomness is called entropy. The more random the data set, the higher the entropy. The table reveals that the suggested encryption method has an average entropy of 7.957169. This implies that the proposed encryption method generates random data because it is close to the usual number of eight. The information entropy formulas provided show global randomness. This demonstrates that the unpredictability in the data set is widespread rather than merely local. Security benefits from this since it makes it more challenging for an attacker to decrypt the data by identifying patterns in the data.

## XI. ANALYSIS OF HISTOGRAM

The histogram of an image provides a visual representation of the grayscale value distribution within the image. To effectively defend against statistical attacks, the grayscale distribution of the cypher image must be uniform. This can be evaluated through the use of histogram plotting on the cypher image. In addition, the analysis of variance is performed as a numerical evaluation of each variable's histogram properties. According to the source, a lesser variance value indicates greater uniformity in the encrypted image.[27]. The analysis of the histogram variance is conducted about the alteration of the encryption key, and subsequently, it is formulated as an expression.

$$\text{var}(Z) = \frac{1}{L^2} \sum_{m=1}^L \sum_{n=1}^L \frac{1}{2} (z_m - z_n)^2 \quad (12)$$

Histogram values are represented by the vector  $Z$ , where  $Z = z_1, z_2, z_3, \dots, z_{256}$ . The integers  $z_m$  and  $z_n$  represent the total number of pixels in the image, with  $m$  and  $n$  representing the number of visible colors. The letter  $L$  provides the Grayscale in the image. The histograms of the input image and the corresponding encrypted image are shown in Fig .5. It is evident from the figure that the histograms of the suggested encrypted images are highly homogeneous and differ noticeably from the histogram of the input image.

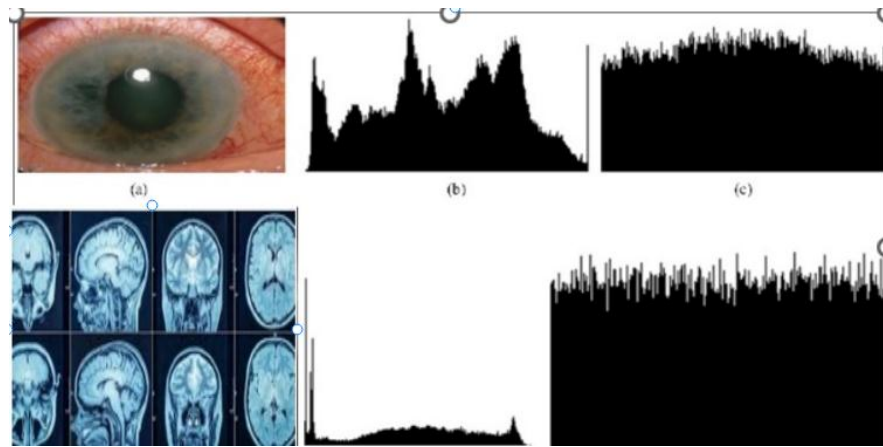


Fig .5. analysis of histograms,(a) source image,(b) histogram of the source image,(c) Encrypted image histogram.

## XII. A STUDYING CORRELATIONS

The correlation between neighboring pixels in an encrypted image is an important measure of the efficacy of an encryption algorithm. A suitable encryption algorithm should generate an encrypted image that exhibits reduced correlation between neighboring pixels. The correlation of adjacent pixels in a painting reflects the connection between them, and due to the high redundancy of image information, the correlation of general photos is very high. A good encryption algorithm should reduce the correlation of adjacent pixels, and the ideal value is 0[28][29]. The equation presented is employed to assess the correlations that exist between neighboring pixels within the encrypted image under consideration:

$$r_{ij} = \frac{D((x-D(x))(y-D(y)))}{\sqrt{P(x)P(y)}} \quad (13)$$

where the terms Expectation and Variance, respectively, are  $D(x)$  and  $P(x)$ . 1000 neighboring pixel pairs are randomly chosen from the encrypted and plain image for the analysis. Table 3 and Fig .6 evaluates the correlation between pixels in the encrypted image generated by the proposed quantum block-based encryption approach. The table presents correlation coefficients for 15 medical images, including CT scans, X-rays, MRIs, and mammography. The correlation coefficients are calculated for the horizontal, vertical, and diagonal directions. The values of the coefficients range from -0.0081 to 0.0139, indicating that the correlation between pixels in the encrypted image is very low, almost zero. The negative values suggest no correlation between the neighboring pixels in the encrypted image.

**Table 3.** Coefficients of correlation.

No	image	Horizontal	Vertical	Diagonal
1	CT of the head	-0.0022	-0.0011	0.0015
2	X-ray of the left arm	0.0048	-0.0010	0.0040
3	x-ray chest	0.0019	-0.0007	-0.0023
4	MRI of the spine	0.0002	0.0060	0.0006
5	Tumor on MRI of the brain	-0.0003	0.0015	0.0051
6	Breast cancer CT scan	-0.0046	0.0004	0.0075
7	Mammography 2	-0.0049	-0.0014	0.0046
8	CT scan of the abdomen	0.0016	0.0088	0.0023
9	CT 2 of the Head	-0.0011	0.0032	-0.0081
10	MRI of Brain 2	0.0005	-0.0024	-0.0038
11	MRI of the Spine, Axial	0.0003	0.0046	-0.0040
12	X-ray of the left arm	0.0049	-0.0072	-0.0003
13	Second X-ray	0.0064	-0.0028	-0.0049
	Average	0.000577	0.000608	0.000169

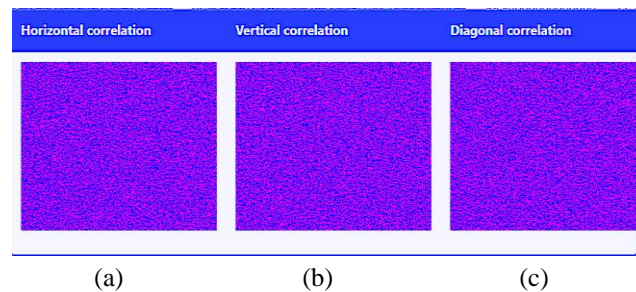


Fig .6. Analysis of correlations. Correlations can be drawn in three different directions: (a) horizontally (b) vertically, and (c) diagonally.

Fig.6. illustrates the correlation plots of neighboring pixels in the cipher image, with subfigures demonstrating horizontal, vertical, and diagonal correlations. The plots show that the pixels in the encrypted image have a weak correlation, which indicates that the proposed encryption approach is effective in securing medical images. The low correlation between the pixels in the encrypted image is an essential feature of an encryption algorithm because it prevents attackers from exploiting statistical patterns to deduce information about the original image.

### XIII. CONCLUSION

The present research introduces a comprehensive framework for achieving secure and efficient quantum encryption of healthcare images within an E-health system. The algorithm implemented in this study incorporates the Generalized Novel Enhancement Quantum Representation (GNEQR) methods, which have been verified through the development of an E-health system and the practical application of quantum encryption techniques for medical images. The encryption process is carried out using C# and ASP.NET Core web API and Blazor WebAssembly on Visual Studio 2022.

The framework employs a two-stage process to ensure the utmost confidentiality and integrity of patient data and images, emphasizing color medical images. In the first stage, medical images are uploaded to Azure Blob Cloud, and a Generalized Model of Novel Enhanced Quantum Representation (GNEQR) is utilized to construct a quantum state  $|I\rangle$  representing the image. The GNEQR quantum image and its quantum state are obtained, followed by additional scrambling using a robust algorithm and a chaotic 5D system to generate a key matrix, enhancing encryption security. In the second stage, the scrambled quantum state  $|I\rangle$  and the scrambled key matrix  $|K\rangle$  undergo an XOR operation, resulting in a new quantum state  $|O\rangle$  representing the encrypted image. Precise image restoration is ensured by following a specific sequence of steps, retrieving the original image's quantum state  $|I\rangle$  through the XOR operation on the scrambled quantum state  $|O\rangle$  and the scrambled key matrix  $|K\rangle$ . The paper's proposed framework showcases promising implications for bolstering the protection of sensitive medical data in cloud-based healthcare systems, addressing critical concerns regarding data security and privacy. By fostering trust and reliability in medical image storage and transfer, this secure quantum medical image encryption framework demonstrates its potential in advancing healthcare systems.

### ACKNOWLEDGMENT

This research was supported by the College of Engineering, Al-Iraqia University. We would like to express our gratitude to Dr. Tayseer S. Atia, Professor at Al-Iraqia University, for her invaluable guidance, expertise, and mentorship throughout the research process. Her profound insights in the field of data security and artificial intelligence, particularly computational intelligence techniques, greatly influenced this research. We are sincerely thankful for her assistance with the implementation of specific techniques and methodologies, which significantly contributed to the success of this study.

### REFERENCES

- [1] X. Man and Y. Song, "Encryption of Color Images with an Evolutionary Framework Controlled by Chaotic Systems," *Entropy*, vol. 25, no. 4, 2023, doi: 10.3390/e25040631.
- [2] Y. Wu, J. Zeng, W. Dong, X. Li, D. Qin, and Q. Ding, "A Novel Color Image Encryption Scheme Based on Hyperchaos and Hopfield Chaotic Neural Network," *Entropy*, vol. 24, no. 10, 2022, doi: 10.3390/e24101474.
- [3] R. I. Abdelfatah and H. M. Saqr, "An efficient medical image encryption scheme for ( WBAN ) based on adaptive DNA and modern multi chaotic map Content courtesy of Springer Nature , terms of use apply . Rights reserved . Content courtesy of Springer Nature , terms of use apply . Rights res," pp. 22213–22227, 2023.
- [4] A. Singh, K. Chatterjee, A. K. Singh, and N. Kumar, "Secure Smart Healthcare Framework using Lightweight DNA Sequence and Chaos for Mobile Edge Computing," *IEEE Internet Things J.*, vol. 10, no. 6, pp. 4883–4890, 2022, doi: 10.1109/IJOT.2022.3219113.
- [5] C. O. Alenoghena *et al.*, "eHealth: A Survey of Architectures, Developments in mHealth, Security Concerns and Solutions," *Int. J. Environ. Res. Public Health*, vol. 19, no. 20, 2022, doi: 10.3390/ijerph192013071.
- [6] S. R. Oh, Y. D. Seo, E. Lee, and Y. G. Kim, "A comprehensive survey on security and privacy for electronic health data," *Int. J. Environ. Res. Public Health*, vol. 18, no. 18, 2021, doi: 10.3390/ijerph18189668.
- [7] R. Alanazi, "Analysis of Privacy and Security Challenges in e-Health Clouds," *Int. J. Adv. Comput. Sci. Appl.*, vol. 13, no. 9, pp. 484–489, 2022, doi: 10.14569/IJACSA.2022.0130955.



- [8] I. Keshta and A. Odeh, "Security and privacy of electronic health records: Concerns and challenges," *Egypt. Informatics J.*, vol. 22, no. 2, pp. 177–183, 2021, doi: 10.1016/j.eij.2020.07.003.
- [9] T. Sahama, L. Simpson, and B. Lane, "Security and Privacy in eHealth: Is it possible?," *2013 IEEE 15th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2013*, no. February 2015, pp. 249–253, 2013, doi: 10.1109/HealthCom.2013.6720676.
- [10] D. Liveri, A. Sarri, and C. Skouloudi, *Security and Resilience in eHealth*. 2015. [Online]. Available: [https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/ehealth\\_sec/security-and-resilience-in-ehealth-infrastructures-and-services](https://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/ehealth_sec/security-and-resilience-in-ehealth-infrastructures-and-services)
- [11] Microsoft, "ASP.NET Core Blazor WebAssembly additional security scenarios." <https://learn.microsoft.com/en-us/aspnet/core/blazor/security/webassembly/additional-scenarios?view=aspnetcore-7.0>
- [12] C. Payette, "How to Integrate Blazor WebAssembly into an Existing ASP.NET Core Web Application", [Online]. Available: <https://www.telerik.com/blogs/integrate-blazor-webassembly-existing-aspnet-core-web-application>
- [13] "HttpClient in Blazor Webassembly", [Online]. Available: <https://www.pragimtech.com/blog/blazor-webAssembly/httpclient-in-blazor-webassembly/>
- [14] A. A. Abd El-Latif, B. Abd-El-Atty, and M. Talha, "Robust Encryption of Quantum Medical Images," *IEEE Access*, vol. 6, pp. 1073–1081, 2017, doi: 10.1109/ACCESS.2017.2777869.
- [15] H. S. Li, X. Chen, S. Song, Z. Liao, and J. Fang, "A block-based quantum image scrambling for gneqr," *IEEE Access*, vol. 7, pp. 138233–138243, 2019, doi: 10.1109/ACCESS.2019.2942986.
- [16] J. Su, X. Guo, C. Liu, and L. Li, "A New Trend of Quantum Image Representations," *IEEE Access*, vol. 8, pp. 214520–214537, 2020, doi: 10.1109/ACCESS.2020.3039996.
- [17] X. Li, J. Zeng, Q. Ding, and C. Fan, "A Novel Color Image Encryption Algorithm Based on 5-D Hyperchaotic System and DNA Sequence," *Entropy*, vol. 24, no. 9, 2022, doi: 10.3390/e24091270.
- [18] C. Li and X. Yang, "An image encryption algorithm based on discrete fractional wavelet transform and quantum chaos," *Optik (Stuttg.)*, vol. 260, no. December 2021, p. 169042, 2022, doi: 10.1016/j.ijleo.2022.169042.
- [19] H. S. Li, X. Chen, H. Xia, Y. Liang, and Z. Zhou, "A Quantum Image Representation Based on Bitplanes," *IEEE Access*, vol. 6, no. c, pp. 62396–62404, 2018, doi: 10.1109/ACCESS.2018.2871691.
- [20] P. Scrambling, "and Pixel-Level Scrambling," pp. 1–16, 2023.
- [21] F. Yu *et al.*, "Chaos-Based Application of a Novel Multistable 5D Memristive Hyperchaotic System with Coexisting Multiple Attractors," *Complexity*, vol. 2020, 2020, doi: 10.1155/2020/8034196.
- [22] N. Bhati, M. Hambir, S. Linganwar, and P. N. Patil, "Securing Medical Images using Quantum Cryptography," vol. 7, no. 2, pp. 2184–2189, 2019.
- [23] T. Janani and M. Brindha, "A secure medical image transmission scheme aided by quantum representation," *J. Inf. Secur. Appl.*, vol. 59, no. April, p. 102832, 2021, doi: 10.1016/j.jisa.2021.102832.
- [24] J. Hu and F. Han, "A pixel-based scrambling scheme for digital medical images protection," *J. Netw. Comput. Appl.*, vol. 32, no. 4, pp. 788–794, 2009, doi: 10.1016/j.jnca.2009.02.009.
- [25] M. Y. M. Parvees and T. Vijayakumar, "Medical image cryptosystem using improved Quadratic Congruential Generator and logistic map," *Meas. Sensors*, vol. 24, no. September, p. 100502, 2022, doi: 10.1016/j.measen.2022.100502.
- [26] S. Madhu and M. Ali Hussain, "Securing Medical Images by Image Encryption using Key Image," *Int. J. Comput. Appl.*, vol. 104, no. 3, pp. 30–34, 2014, doi: 10.5120/18184-9079.
- [27] Y. Q. Zhang and X. Y. Wang, "A symmetric image encryption algorithm based on mixed linear-nonlinear coupled map lattice," *Inf. Sci. (Ny.)*, vol. 273, pp. 329–351, 2014, doi: 10.1016/j.ins.2014.02.156.
- [28] A. B. Abugharsa, A. Samad, B. Hasan, and H. Almangush, "A Novel Image Encryption using an Integration Technique of Blocks Rotation based on the Magic cube and the AES Algorithm," *Int. J. Comput. Sci. Issues*, vol. 9, no. 4, pp. 41–47, 2012.
- [29] J. Xu, B. Zhao, and Z. Wu, "Research on Color Image Encryption Algorithm Based on Bit-Plane and Chen Chaotic System," *Entropy*, vol. 24, no. 2, 2022, doi: 10.3390/e24020186.