Bulletin of Electrical Engineering and Informatics
Vol. 14, No. 3, June 2025, pp. 1912~1924
ISSN: 2302-9285, DOI: 10.11591/eei.v14i3.8887

Hybrid image encryption using quantum bit-plane scrambling and discrete wavelet transform

Eko Hari Rachmawanto[1,2], Ajib Susanto[1,2], Didik Hermanto[1,2], Christy Atika Sari[1,2], Ichwan Setiarso[1], Md. Kamruzzaman Sarker[3]
[1]Study Program in Informatics Engineering, Faculty of Computer Science, Universitas Dian Nuswantoro, Semarang, Indonesia
[2]Research Center for Intelligent Distributed Surveillance and Security, Universitas Dian Nuswantoro, Semarang, Indonesia
[3]Department of Computer Science, Faculty of Science, Bowie State University, Bowie, United States

Article Info

Article history:

Received Jun 21, 2024
Revised Nov 28, 2024
Accepted Dec 25, 2024

Keywords:

Digital image
Discrete wavelet transform
Image encryption
Quality measurement
Quantum bit-plane scrambling

ABSTRACT

Digital image security is increasingly vulnerable to sophisticated attacks, underscoring the urgent need for robust encryption techniques. Traditional encryption methods often fall short in defending against advanced threats, highlighting the importance of innovative solutions to protect digital images. This study tackles these challenges by incorporating quantum computing into image encryption, employing techniques such as bit-plane scrambling, pixel permutation, and bit permutation. These strategies enhance security by introducing complex, non-linear transformations that make decryption attempts significantly more difficult without the correct cryptographic keys. A key configuration based on r=44, μ=2024 is employed to achieve this. The integration of quantum bit-plane scrambling and quantum pixel permutation results in a highly secure encryption method. Experimental results show substantial improvements in entropy levels, along with strong unified average changing intensity (UACI) and number of pixels change rate (NPCR) values across various images. Notably, the "Peppers" image achieved the best performance, with UACI values of 33.5572 and NPCR values of 99.8301. The method proves highly effective, as repeated tests with incorrect keys failed to decrypt the plain image accurately. Future research could explore the addition of a discrete quantum wavelet transform to further enhance the security and efficiency of quantum-based image encryption methods.

Corresponding Author:

Christy Atika Sari
Study Program in Informatics Engineering, Faculty of Computer Science, Universitas of Dian Nuswantoro
Imam Bonjol 207, Semarang, 50131, Central Java, Indonesia
Email: christy.atika.sari@dsn.dinus.ac.id

1. INTRODUCTION

Image encryption is an important technique in information security, aimed at protecting image data from unauthorized access and manipulation [1]. Image encryption involves converting an image to an unrecognizable format using a variety of encryption algorithms, ensuring that only authorized users with the correct decryption key can recover the image to original form [1], [2]. This process is essential to protect sensitive information, such as medical images [3], personal photos [4], and confidential documents [4], transmitted over unsecured channels. However, traditional encryption methods often face challenges such as high computational costs, vulnerability to certain types of attacks, and the need to balance security and image quality. An important issue in image encryption is achieving a robust encryption system that can effectively prevent potential attacks while maintaining computational efficiency and image quality [5], [6]. Traditional methods sometimes do not provide a sufficient level of security against sophisticated attacks and can be computationally intensive, making them impractical for real-time applications. Additionally, the challenge is to ensure that the encrypted image does not reveal useful information about the original image and that the decoding process accurately restores the original image without losing quality [7], [8]. Advanced techniques, such as the stochastic combination of binary fields with bit-plane scrambling and the use of quantum encryption principles, have emerged as promising solutions to solve the problem [9]-[13]. This is by improving the security and efficiency of image encryption.

Numerous studies have explored quantum methods for image encryption. Among these, Guo *et al.* [10] introduced the image encryption algorithm on the basis of a modified Feistel structure, using the new novel enhanced quantum representation (NEQR) model for the quantum computer. This quantum circuit-based algorithm exploits a 128-bit block cipher with sub-keys of 16 bits each, where the whole design was inclined toward characteristics of both Feistel and substitution-permutation networks. It gave a concise quantum circuit design of this encryption algorithm with support from numerical simulations and analyses to prove the efficacy of the method against statistical attack.

Hu *et al.* [11] further extended quantum image encryption by proposing an integrated encryption process. It starts with the Arnold scrambling operations that change the information of the quantum image in the spatial domain. After that, the noised quantum image is decomposed into multi-resolution by quantum wavelet transforms in frequency domain, including the low-frequency components with highly detailed frequency information. Then the wavelet coefficients in every sub-image are encoded by Arnold randomizing operations again. Assign the pixel values to the whole reconstructed quantum image according to the encoded wavelet coefficients by the inverse quantum wavelet transforms. It is relatively easy to decipher an encrypted image since, in principle, all that is needed is just to invert all the quantum operations that are involved in a quantum image encryption process, because all quantum operations are reversible.

Liu and Liu [13] discussed the realm of quantum image encryption using qubit superposition and entanglement features for more efficiency and security. They have developed a new quantum framework for betterment regarding the encryption of images, based on an independent bit-plane permutation scheme. First, grayscale images should be transformed into one of the representation forms of quantum images to enable further operations. Later, the quantum Baker map (QBM) is applied, which permutes the positions of the bits in every bit-plane; hence, the position and value of each pixel change. Besides, partition and iteration parameters are also changed in different bit planes to further extend the key space. Afterward, the permuted image is diffused to form an encrypted image by quantum controlled XOR operations and the newly presented sine chaotification model. Results of experiments and the security analysis guarantee that the proposed quantum image encryption algorithm attains superiority in statistical analysis, key sensitivity, and robustness.

Gao *et al.* [9] proposed with a quantum DNA decoder combined with Hilbert quantum scrambling. Notably, the quantum DNA decoder is utilized for the encoding and decoding process of the pixel color information for the first time in order to influence pixel-level diffusion based on its excellent biological characteristics with much greater space of keys, while the position data of the images are scrambled with Hilbert quantum scrambling to improve encryption efficiency. The permuted image is used as the key matrix for more security in the quantum XOR operation with the original image. As all the quantum operations performed in this paper are invertible, decoding can be performed easily by applying the inverse transformation of the encryption process.

Hamad *et al.* [14] highlighted that scrambling techniques have to be employed in application involving quantum image processing and more so quantum image encryption, where such methods enhance the robustness of the images. The level of encryption whereby the resulting image is non-identifiable or indistinguishable in detail, seeking high entropy and a flat histogram with a peak for the encrypted image. Most research up until now has been about either single-position or single-value shuffling. Only a little research in quantum image shuffling has gone into considering the position and value shuffling together. Therefore, in this paper, modification for quantum logic gates is adapted based on fast and basic schemes for developing one genetic algorithm in consideration of a variety of jamming schemes with a view to deciding on the most suitable item considering the related factor to cost, image, or complexity. It has contributed much towards the research area by providing an integrated platform for automatic scrambling schemes according to the type of image, the method adopted, and the logic circuit.

Thus, this research aims to advance the field of quantum image coding by implementing a hybrid image coding scheme that combines quantum bit-plane scrambling with discrete wavelet transform (DWT). Based on the basic research reviewed, this method integrates the strengths of several methods to improve the security and efficiency of quantum image encryption. Specifically, this research is inspired by the Feistel framework and the researcher's modified NEQR model [10] to use robust block encryption techniques in a quantum framework. In addition, it integrates multi-scale resolution analysis and reversible operations of the Researcher [11] quantum wavelet transform method, ensuring efficient encryption and decoding fruit. In addition, the researcher's independent bit plane permutation scheme and Baker quantile map [13] are used to permute the bit positions, further improving the complexity and security of the encryption. The researcher's use of quantum DNA decoding and quantum Hilbert shuffling techniques [9] contributes to pixel-level diffusion and key space expansion, which are important for strong encryption. Finally, recognizing researcher's [14] emphasis on the importance of image blurring techniques, this study incorporates genetic algorithms to optimize the blurring scheme, ensuring valid high entropy and uniform peak histogram in encrypted images. By synthesizing these state-of-the-art techniques, this research aims to develop a comprehensive and secure quantum image encryption method that exploits both binary plane transform and DWT, thereby significantly improving the strength and efficiency of encryption.

The outline of the presented research will go as follows: section 1 introduces the study by addressing the problem statement of quantum image encryption; it gives an overview of the existing challenges together with their proposed solution and reviews the research which has been done. Section 2 describes the theoretical backgrounds required for setting up the proposed hybrid scheme: an overview of quantum qubits, quantum gates, and DWT, including embedding of a quantum bit-plane scrambling technique. Section 3 discusses in detail the proposed methodology with respect to the flow and integration of these components into the encryption process, shedding light on how quantum principles improved the security and efficiency of the encryption algorithm. Section 4 presents the results of the simulation and analysis that prove the efficiency and robustness in the proposed scheme are better as compared to other schemes. Finally, the paper concludes by summarizing the entire research in section 5 by giving an account of the implications of the findings on quantum image encryption and presenting further research and development in the area.

2. PRELIMINARIES

2.1. Quantum qubits

Quantum qubit [15], [16] is the fundamental unit of information in quantum computing, represented as a superposition of two orthogonal quantum states $|0\rangle$ and $|1\rangle$. each associated with complex probability amplitudes α and β [13], [17], [18] respectively. Mathematically, a general qubit state $|\psi\rangle$ can be expressed as (1), where α and β are complex numbers satisfying the normalization condition $|\alpha|^2+|\beta|^2=1$. This equation illustrates the probabilistic nature of quantum states and their ability to exist in multiple states simultaneously. Quantum gates, such as the Hadamard gate H and Pauli gates $X,\ Y,\ Z$, manipulate qubit states to perform operations essential for quantum computations. Hadamard gate equation can be seen in (2). Which mean the Hadamard gate H converts each basis state $|0\rangle$ and $|1\rangle$ into a linear combination of the two states, scaled by $\frac{1}{\sqrt{2}}$. To provide a more formal representation, we can express the Hadamard transformation in matrix form. The quantum computational basis states $|0\rangle$ and $|1\rangle$ are represented as column vectors, this equation can be seen in (3), Therefore, the Hadamard gate H in matrix equation can be seen in (4), when the Hadamard gate H is applied to a qubit $|\psi\rangle=\alpha|0\rangle+\beta|1\rangle$, the resulting state can be seen in (5).

$$|\psi\rangle=\alpha|0\rangle+\beta|1\rangle \tag{1}$$

$$H|0\rangle=\frac{|0\rangle+|1\rangle}{\sqrt{2}},\ H|1\rangle=\frac{|0\rangle-|1\rangle}{\sqrt{2}} \tag{2}$$

$$|0\rangle=\begin{pmatrix}1\\0\end{pmatrix},\ |1\rangle=\begin{pmatrix}0\\1\end{pmatrix} \tag{3}$$

$$H=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & 1\\1 & -1\end{pmatrix} \tag{4}$$

$$H|\psi\rangle=\frac{1}{\sqrt{2}}\left(\alpha(|0\rangle+|1\rangle)+\beta(|0\rangle-|1\rangle)\right) \tag{5}$$

Thus, the Hadamard gate H generates a superposition of the qubit $|\psi\rangle$ in a new basis that consists of linear combinations of the original basis states $|0\rangle$ and $|1\rangle$. The inherent properties of qubits, including superposition and entanglement, underpin the power of quantum computing by enabling parallelism beyond classical capabilities, thereby facilitating the efficient solution of complex problems in various domains.

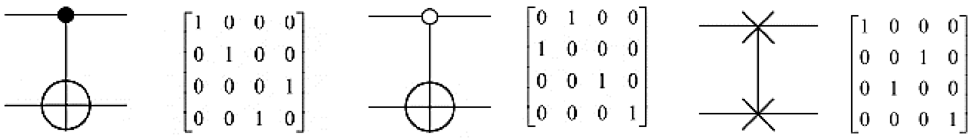
2.2. Quantum gates based on controlled-NOT and SWAP

Quantum gates, such as the controlled-NOT (CNOT) and SWAP gates [19] are fundamental components in quantum computing that enable the manipulation and transformation of qubits [13], [17]. The CNOT gate performs a controlled operation where the target qubit's state is flipped (X gate applied) if and only if the control qubit is in state $|1\rangle$. For equation, the action of CNOT can be seen in (6), where $|c\rangle$ is the control qubit, $|t\rangle$ is the target qubit, $\oplus$ denotes the XOR operation, and the gate applies the X (NOT) gate to the target qubit if the control qubit is $|1\rangle$. The SWAP gate exchanges the states of two qubits. Its action on two qubits

$| q_1\rangle$ and $| q_2\rangle$ can be seen in (7). In matrix form, the CNOT and SWAP gate is represented in Figure 1. The matrix representations of the CNOT and SWAP gates are shown in Figure 1(a) presents the CNOT matrix, which highlights how the gate operates based on the input states of the control and target qubits, while Figure 1(b) displays the SWAP matrix, emphasizing the exchange of states between the two qubits.

$$CNOT \; | c\rangle \, | t\rangle = | c\rangle \, | c \oplus t\rangle \tag{6}$$

$$\mathrm{SWAP} \; | \mathrm{q1}\rangle \, | \mathrm{q2}\rangle = | \mathrm{q2}\rangle \, | \mathrm{q1}\rangle \tag{7}$$

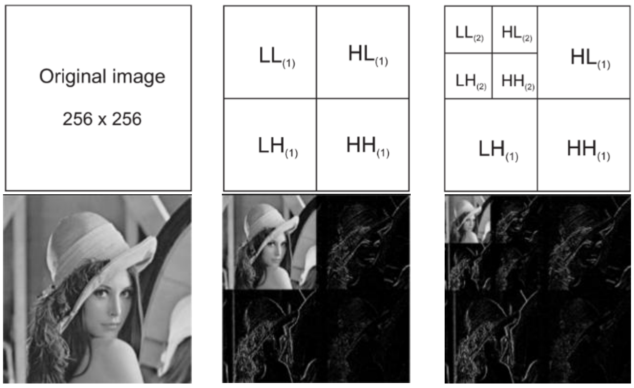


(a) (b)

Figure 1. Matrix representation based on; (a) CNOT matrix and (b) SWAP matrix gates

2.3. Discrete wavelet transform

DWT is a powerful mathematical tool used to analyze and process signals, including digital images, by decomposing them into different frequency components [20], [21]. In DWT, a signal or image passes through a series of filters to capture approximate (low frequency) and detailed (high frequency) components at multiple levels or scales [22]. Each level of decomposition produces subbands represented by the coefficients HL, LH, and HH, which specify the horizontal-low, vertical-low, and diagonal-high frequency components, respectively. At level 1, the original signal or image is passed through one high-pass filter (H_1) and one low-pass filter (L_1), resulting in LL_1 (approximation), HL_1 (horizontal detail), LH_1 (vertical detail), and HH_1 (diagonal detail) coefficients. LL_1 captures the coarsest approximation of the signal's or image's overall structure, while HL_1, LH_1, and HH_1 capture finer details in the horizontal, vertical, and diagonal directions, respectively. At level 2, LL_1 from level 1 undergoes further decomposition using H_1 and L_1, filters, producing LL_2, HL_2, LH_2, and HH_2 coefficients. LL_2 provides a more detailed approximation, while HL_2, LH_2, and HH_2 capture more refined horizontal, vertical, and diagonal details compared to level 1 [23]. The progression of DWT decomposition at different levels can be visualized in Figure 2(a) displays the original image, while Figures 2(b) and (c) illustrate the results of DWT processing at level 1 and level 2, respectively. This breakdown helps in analyzing the image's structural and detailed components across different frequency scales. Based on results of DWT processing each level can be seen in Figure 2.



(a) (b) (c)

Figure 2. Results of DWT processing each level; (a) original image, (b) DWT level 1, and (c) DWT level 2

In DWT, the signal or image is convolved with two types of filters: high-pass (detail) and low-pass (approximation) filters. These filters are typically defined by their coefficients. high-pass filter as $h[n]$ and the low-pass filter as $g[n]$. The length of these filters is N. The decomposition equation based on DWT can be seen in (8)–(11). Where $HL[k]$, $LH[k]$, and $HH[k]$ represent the horizontal, vertical, and diagonal detail coefficients at scale k. And the inverse DWT combines the approximation and detail coefficients to reconstruct the original signal or image, the equation of inverse DWT can be seen in (12).

$$LL[k] \sum_n x[n] \cdot g[2k-n] \tag{8}$$

$$HL[k] \sum_n x[n] \cdot h[2k-n] \tag{9}$$

$$LH[k] \sum_n x[n] \cdot g[2k-n] \tag{10}$$

$$HH[k] = \sum_n x[n] \cdot h[2k-n] \tag{11}$$

$$x[n] = \sum_k LL[k] \cdot g[n-2k] + \sum_k HL[k] \cdot h[n-2k] + \sum_k LH[k] \cdot g[n-2k] + \sum_k HH[k] \cdot h[n-2k] \tag{12}$$

2.4. Novel encryption quantum representation of bit-plane scrambling

Bit-plane scrambling is a cryptographic technique used to enhance the security of digital images by manipulating their binary representations [14]. In an 8-bit grayscale image, each pixel is composed of eight binary bits, denoted as $b7, b6, b5, b4, b3, b2, b1, b0$, representing values from 0 to 255. For example, the pixel value 187 can be represented in binary as 10111011_2, where $b7 = 1$, $b6 = 0$, $b5 = 1$, $b4 = 1$, $b3 = 1$, $b2 = 0$, $b1 = 1$, and $b0 = 1$. Bit-plane scrambling involves applying permutation and transformation operations to these binary bits across all pixels [17]. This can include XOR operations with pseudorandom keys or chaotic maps, which rearrange the bit positions and values within each bit-plane. The scrambling results for each bit-plane of an image can be visualized in Figure 3. Figure 3(a) shows the scrambling of the 7th bit-plane, which contains the most significant bits of the image, while Figure 3(b) represents the scrambled 6th bit-plane. Figure 3(c) illustrates the scrambling of the 5th bit-plane, Figure 3(d) corresponds to the 4th bit-plane, Figure 3(e) represents the 3rd bit-plane, Figure 3(f) shows the 2nd bit-plane, and Figure 3(g) depicts the 1st bit-plane. Finally, Figure 3(h) illustrates the least significant bit-plane. Each bit-plane reflects different levels of detail and structural information about the image, and scrambling them ensures that the image is effectively encrypted across all bit levels.

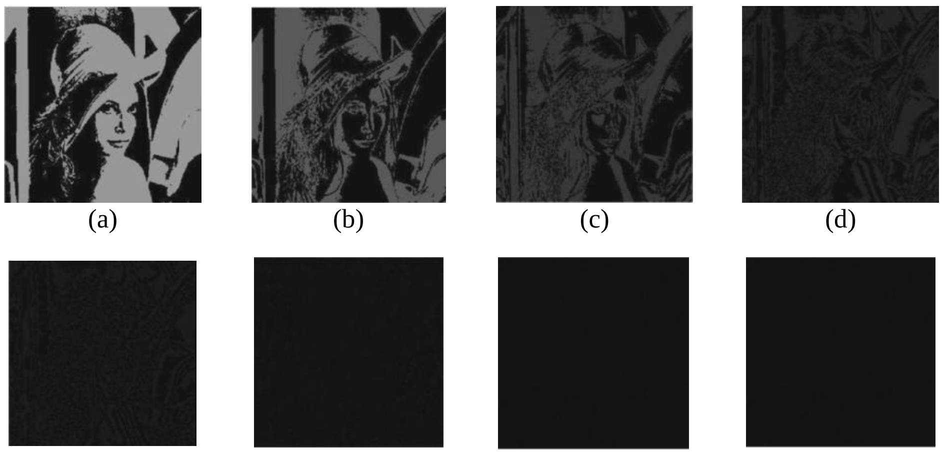


Figure 3. Results of bit-plane scrambling each level; (a) 7th bit-plane, (b) 6th bit-plane, (c) 5th bit-plane, (d) 4th bit-plane, (e) 3rd bit-plane, (f) 2nd bit-plane, (g) 1st bit-plane, and (h) 0 bit-plane

After initializing the bit-plane at each level, the next step is to merge the obtained bit-plane results. This merging allows to reorganize the information from each bit-plane level into a representative data structure. Next, the quantum embedding process is applied to the merging of these bit-plane results and calculate each pixel, as shown in Figure 4.

Figure 4 shows tensor product calculation of bit-plane result. The tensor product is a mathematical operation that takes two vectors or quantum states and combines them into a single vector or state in a higher-dimensional space. For the bit-plane result, the tensor product equation can be seen in (13), where P_{xy} encodes the gray information of the corresponding pixel in the location $|\, yx\rangle$, and the coordinate representation can be detailed as in (14). Where $|\, y\rangle$ and $|\, x\rangle$ are the quantum states representing the y-coordinate and x-coordinate of the pixel, respectively. And the quantum state $|\, yx\rangle$ is formed by concatenating the states $|\, y\rangle$ and $|\, x\rangle$, where each state $|\, y\rangle$ and $|\, x\rangle$ is a binary string of length n (e.g., $|y_n{-}1y_n{-}2\cdots y0\rangle$ and $|x_n{-}1x_n{-}2\cdots$x0$\rangle$).

$$|\, I\rangle = \frac{1}{2^n} \sum_{y=0}^{2^{n-1}} \sum_{x=0}^{2^{n-1}} |\, y\rangle \otimes |\, x\rangle \tag{13}$$

$$| \, yx\rangle = | \, y\rangle \, | \, x\rangle = | \, y_n - 1y_n - 2 \dots \, y0 \,\rangle \, | \, x_n - 1x_n - 2 \dots \, x0 \,\rangle \tag{14}$$

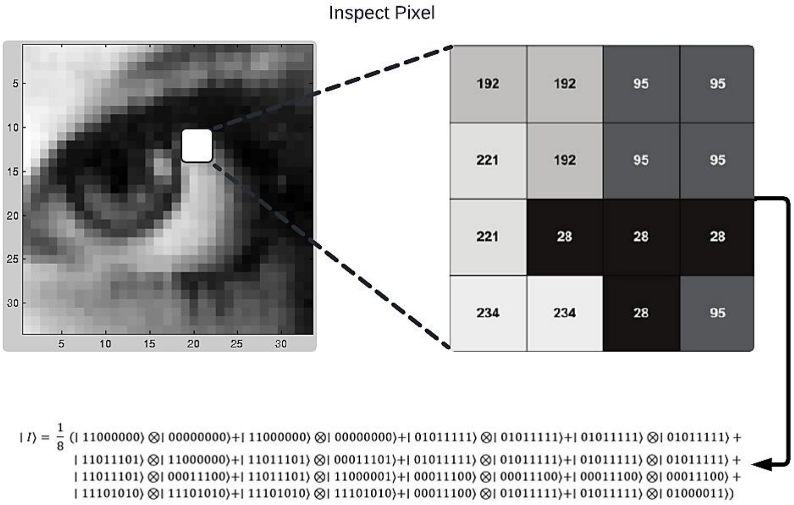


Figure 4. Tensor product calculation of bit-plane result

3. METHOD

This section outlines the proposed method for encrypting images using a hybrid approach that combines pixel permutation, bit permutation, DWT embedding, and chaotic diffusion. The detailed steps of the proposed method are illustrated in Figure 5. Decryption is the process of converting a cipher image back into its original plain image form. This involves reversing the steps applied during encryption to ensure the recovery of the original image. The decryption process includes reversing the chaotic diffusion, performing the inverse discrete wavelet transform (IDWT), undoing the bit permutation, and finally reversing the pixel permutation.

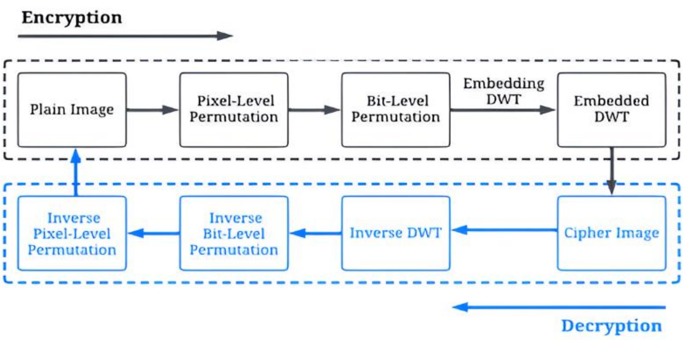


Figure 5. Proposed scheme

In this research, a grayscale image with a resolution of 256×256 pixels is used. This image is converted into a quantum state representation to leverage the principles of quantum computing for enhanced security. The image, denoted as I, is transformed into a quantum state using the tensor product of pixel coordinates and their respective gray values. The quantum state based on plain image can be seen in (15). Where, $\frac{1}{2^n}$ ensures the state is normalized. For an 8-bit grayscale image, n would be 8, which is the number of bits used to represent each pixel value. $\sum_{y=0}^{2^{n-1}-1} \sum_{x=0}^{2^{n-1}-1}$ summations iterate over all possible pixel coordinates (x, y) in the image. Since the image is 256×256 pixels, $n = 8$, and thus $2^{n-1} = 128$. Therefore, the summations run from 0 to 127 for both x and y. Each pixel value is an 8-bit binary number, where p_i^{xy} represents the i^{th} bit of the pixel at position (x, y). For example, if a pixel value is 192, its binary representation is 11000000, and thus p_7^{xy}, p_6^{xy}=0.

$$| \, I\rangle = \frac{1}{2^n} \sum_{y=0}^{2^{n-1}-1} \sum_{x=0}^{2^{n-1}-1} \left(p_7^{xy} p_6^{xy} p_5^{xy} p_4^{xy} p_3^{xy} p_2^{xy} p_1^{xy} p_0^{xy}\right) \otimes | \, yx\rangle \tag{15}$$

3.1. Pixel permutation

Pixel permutation is a step in the image encryption process where the positions of the pixels in the image are shuffled according to a specific permutation function [17], [18]. This operation obscures the spatial structure of the image, making it more difficult to recognize or analyze without the proper decryption key. The initial step involves permuting the pixel positions in the image to obscure its spatial structure. Based (15), to scramble this process can be seen in (16):

$$|I\rangle = \frac{1}{2^n}\sum_{y=0}^{2^{n-1}-1}\sum_{x=0}^{2^{n-1}-1}\left(p_7^{\pi(xy)}p_6^{\pi(xy)}p_5^{\pi(xy)}p_4^{\pi(xy)}p_3^{\pi(xy)}p_2^{\pi(xy)}p_1^{\pi(xy)}p_0^{\pi(xy)}\right)\otimes|\pi(x,y)\rangle \quad (16)$$

Next step, apply the permutation operations to each bit-plane. This involves using quantum gates like the CNOT and SWAP gates to shuffle the pixel positions within each bit-plane. CNOT gate flips the target qubit if the control qubit is 1. The operation of CNOT and SWAP gates can be seen in (17), (18). These gates are fundamental in quantum computing for qubit manipulation and permutation operations. The quantum permutation circuit based on bit-plane permutation can be observed in Figure 6. This figure illustrates the systematic approach of applying quantum gates to rearrange the pixel positions within each bit-plane.

$$\begin{aligned} &CNOT\,|00\rangle = |00\rangle \\ &CNOT\,|01\rangle = |01\rangle \\ &CNOT\,|10\rangle = |11\rangle \\ &CNOT\,|11\rangle = |10\rangle \end{aligned} \quad (17)$$

$$\begin{aligned} &SWAP\,|00\rangle = |00\rangle \\ &SWAP\,|01\rangle = |10\rangle \\ &SWAP\,|10\rangle = |01\rangle \\ &SWAP\,|11\rangle = |11\rangle \end{aligned} \quad (18)$$

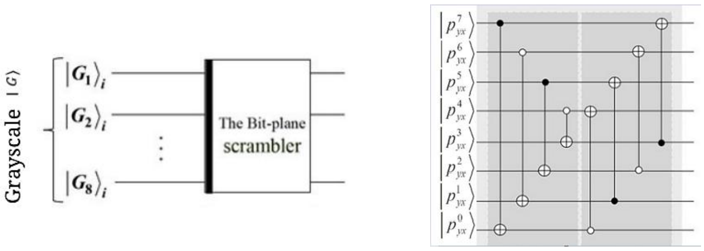


Figure 6. Quantum permutation circuit based on bit-plane permutation

3.2. Bit permutation

Bit permutation is a technique used to shuffle the positions of qubits within each pixel (Y, X) to enhance the security of an encrypted image [13], [17], [18]. The goal is to create a complex and non-linear arrangement of the pixel values, making it difficult for unauthorized parties to decipher the original image. This process involves applying quantum gates such as the CNOT and SWAP gates, which manipulate the positions of the bits within each pixel [18]. Figure 6, which illustrates the quantum permutation circuit based on bit-plane permutation, Figure 7 presents the quantum circuit based on bit-plane shift operation. This circuit demonstrates how each bit-plane undergoes specific shift operations to achieve a scrambled gray level. The scrambling process is carried out using (16), ensuring a high level of security and complexity in the image encryption process.

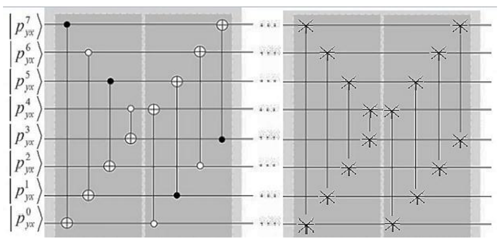


Figure 7. Quantum circuit based on shift operation of bit-plane permutation

The results in Figure 7 are obtained using the calculation according to (19). The sub-operation L_{Y0X0} applied to $|I_1$ can be described with the permutation operator U_{YX} as (19):

$$L_{Y0X0}(|\ I_1)=L_{Y0X0}\ (\frac{1}{2^n}\sum_{y=0}^{2^{n-1}-1}\sum_{x=0}^{2^{n-1}-1}(p_7^{xy}p_6^{xy}p_5^{xy}p_4^{xy}p_3^{xy}p_2^{xy}p_1^{xy}p_0^{xy})\otimes|\ yx\rangle)$$

$$=\frac{1}{2^n}L_{Y0X0}\ (\frac{1}{2^n}\sum_{y=0}^{2^{n-1}-1}\sum_{x=0}^{2^{n-1}-1}(p_7^{xy}p_6^{xy}p_5^{xy}p_4^{xy}p_3^{xy}p_2^{xy}p_1^{xy}p_0^{xy})\otimes|\ yx\rangle)$$

$$=\frac{1}{2^n}\sum_{y=0}^{2^{n-1}-1}\sum_{x=0}^{2^{n-1}-1}(p_7^{xy}p_6^{xy}p_5^{xy}p_4^{xy}p_3^{xy}p_2^{xy}p_1^{xy}p_0^{xy})\otimes|\ yx\ \otimes\ Y_0X_0+\frac{1}{2^n}\ (P_{Y0X0}\ \otimes\ |\ Y_0X_0\ \rangle$$

$$=\frac{1}{2^n}\sum_{y=0}^{2^{n-1}-1}\sum_{x=0}^{2^{n-1}-1}(p_7^{xy}p_6^{xy}p_5^{xy}p_4^{xy}p_3^{xy}p_2^{xy}p_1^{xy}p_0^{xy})\otimes|\ yx\ \otimes\ Y_0X_0+\frac{1}{2^n}U_{XY}P_{Y0X0}\otimes|\ Y_0X_0\rangle \quad (19)$$

Based (19), to change all pixel values in an image, additional operations can be seen in (20). Where L_{YX} represents the quantum permutation and embedding operations applied to each pixel position (y,x) in $|\ I_1$. The product operation $\prod$ signifies the sequential application of these sub-operations across all pixel positions in the image.

$$|\ I_1'\rangle=\prod_{y=0}^{2n-1}\prod_{x=0}^{2n-1}L_{YX}\ \ (|\ I_1\rangle)$$

$$=\prod_{y=0}^{2n-1}\prod_{x=0}^{2n-1}L_{YX}\ \ (\frac{1}{2^n}\sum_{y=0}^{2^{n-1}-1}\sum_{x=0}^{2^{n-1}-1}(p_7^{xy}p_6^{xy}p_5^{xy}p_4^{xy}p_3^{xy}p_2^{xy}p_1^{xy}p_0^{xy})\otimes|\ yx\rangle)$$

$$=\frac{1}{2^n}\sum_{y=0}^{2^{n-1}-1}\sum_{x=0}^{2^{n-1}-1}U_{YX}(|P_{YX}\rangle)\,|Y\rangle\,|X\rangle$$

$$=|\ I_2\rangle) \quad (20)$$

4. EXPERIMENTAL RESULTS

In this section, we present the experimental results obtained from the proposed method. The images used for testing are 256×256 grayscale images, and the simulations were performed using MATLAB 2020a. The effectiveness of the proposed encryption method is demonstrated through various test images, with the results showcasing the robustness and efficiency of the encryption process. The outcomes of these tests, including the encrypted images and their analyses can be seen in Figure 8. Figures 8(a)–(e) is plain image, Figures 8(f)–(j) is encrypted image, and Figures 8(k)–(o) is decrypted image. The results obtained in Figure 8 were achieved using specific key parameters set for the experiment. The key parameters used in the experiment were set to $r=44$ and $\mu=2024$. The encrypted images, as presented in Figures 8(f)–(j), reflect the effectiveness of using these key parameters in the encryption algorithm.

4.1. Histogram measurement

Histogram analysis are performed for the intensity distribution of the pixels of the image before and after encryption. Any good encryption will lead to the flattening histogram of the encoded image in which all pixel values are completely covered, hence concealing any pattern or feature of the original image. This is the uniform distribution where the frequency, intensity, and pixel are uniformly distributed, hence making an encrypted image resistant to statistical attacks due to the difficulty of extracting any meaningful information by the attacker using means. The results of the histogram analysis are presented in Figure 9, which illustrates the intensity distributions for various test images. Figures 9(a) to (e) depict the original, unencrypted images: (a) Cameraman, (b) Rice, (c) Lena, (d) Peppers, and (e) Baboon. These images exhibit distinct intensity distributions, with visible patterns in their respective histograms. Meanwhile, Figures 9(f) to (j) display their corresponding encrypted versions: (f) encrypted Cameraman, (g) encrypted Rice, (h) encrypted Lena, (i) encrypted Peppers, and (j) encrypted Baboon.

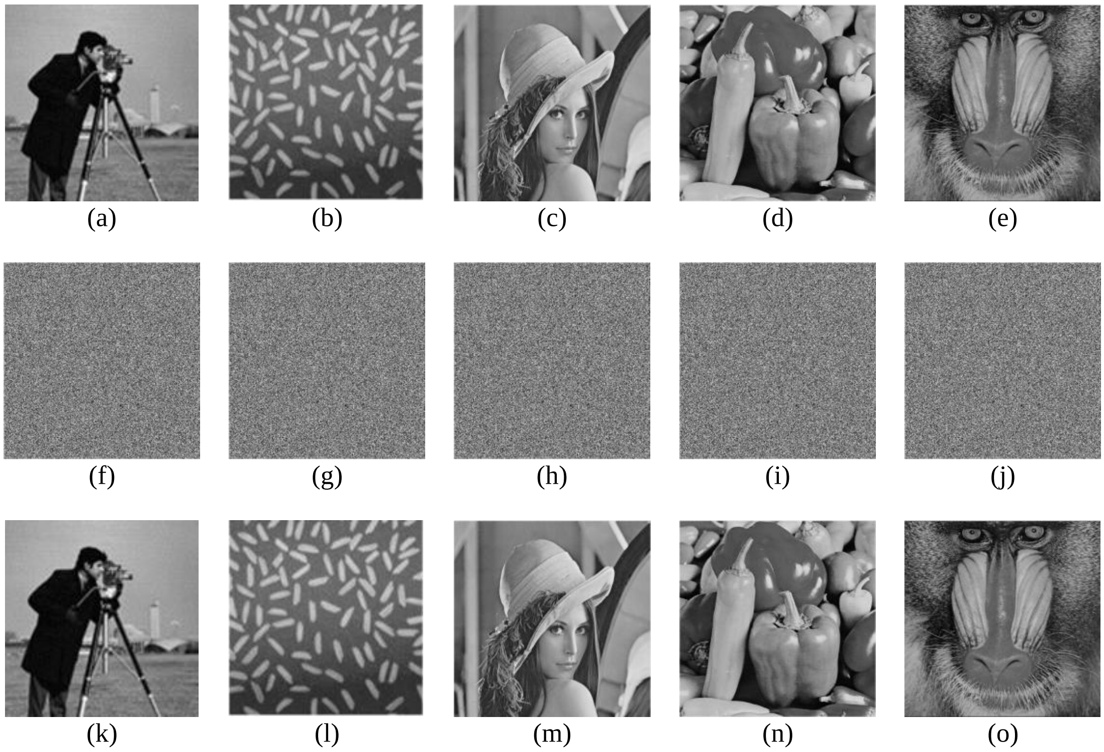


Figure 8. Original, encrypted, and decrypted images using proposed encryption; (a) Cameraman, (b) Rice, (c) Lena, (d) Peppers, (e) Baboon is plain image, (f) encrypted Cameraman, (g) encrypted Rice (h) encrypted Lena, (i) encrypted Peppers, (j) encrypted Baboon is encrypted image, and (k) decrypted Cameraman, (l) decrypted Rice, (m) decrypted Lena, (n) decrypted Peppers, and (o) decrypted Baboon is decrypted image

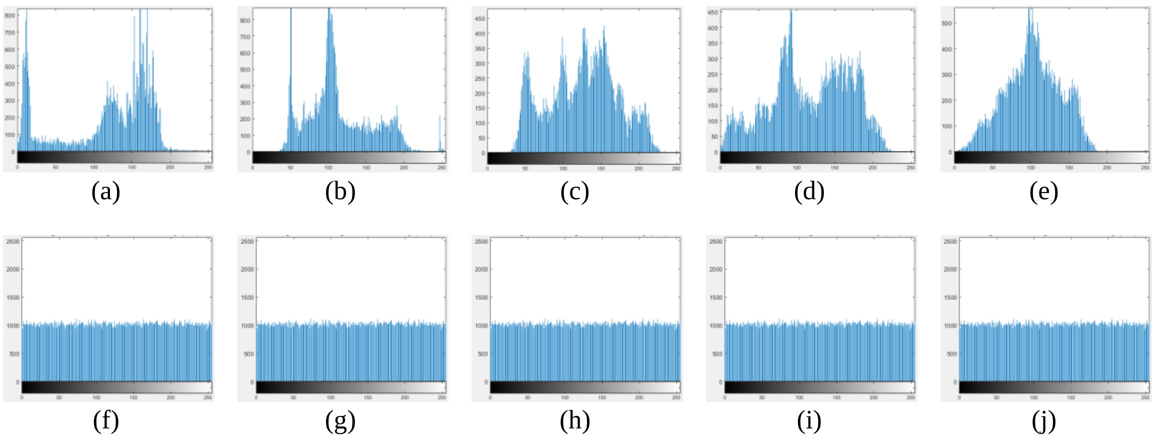


Figure 9. Results of histogram analysis; (a) Cameraman, (b) Rice, (c) Lena, (d) Peppers and (e) Baboon is plain image, (f) encrypted Cameraman, (g) encrypted Rice, (h) encrypted Lena, (i) encrypted Peppers, and (j) encrypted Baboon is encrypted image

4.2. Unified average changing intensity and number of pixels change rate measurement

The most meaningful metrics in analyzing the performance of an image encryption algorithm are unified average changing intensity: number of pixels change rate (NPCR) accounts for the percentage of different pixel values between the original and encrypted images, while unified average changing intensity (UACI) estimates the average intensity change between the two images. Larger values of UACI and NPCR indicate robustness regarding the efficiency of the encryption algorithm to transform the image with more resistance against differential attack. Computed values of UACI and NPCR are shown in Table 1 for some of our experimental tests related to the proposed method.

Table 1. UACI and NPCR measurement

Encrypted image	Researcher	UACI	NPCR
Cameraman	Liu *et al.* [17]	33.5685	99.5804
Peppers		33.5291	99.5300
Cameraman	Wang *et al.* [24]	33.4952	99.7958
Peppers		33.5125	99.7625
Cameraman	Zhou *et al.* [25]	33.5753	99.7325
Peppers		33.4928	99.6982
Cameraman	Our study	33.5688	99.8275
Rice		33.4817	99.8221
Lena		33.5188	99.8237
Peppers		33.5572	99.8301
Baboon		33.4893	99.8244

4.3. Entropy measurement

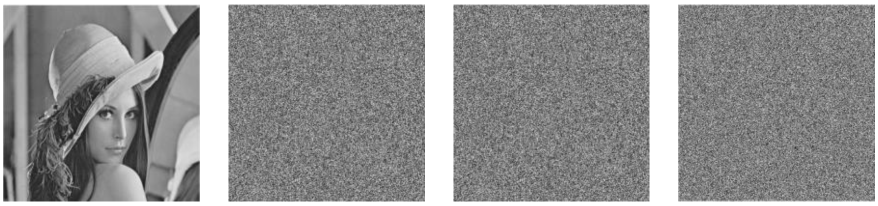
Entropy may be used as a measure to determine the degree of randomness and uncertainty in pixel values of an encrypted image. This indicates that the entropy of the pixels is high, corresponding to a uniform distribution of the pixel values of the input image-one of the good properties in a secure encryption algorithm. Therefore, the encrypted image will not reveal any useful pattern or information about the original image and has a high resistance to different types of cryptanalysis attacks. In this process, entropy of the encrypted image is calculated and reported in Table 2. It can be seen from the results obtained that the proposed encryption method gives an entropy value near the ideal value of 8 for the image. For instance, confirmation to such a highly random and effective method of generating encrypted images can be derived in the 8-bit grayscale.

Table 2. Entropy measurement

Researcher	Plain image	Entropy of plain image	Encrypted image	Entropy of encrypted image
Liu *et al.* [17]	Cameraman	7.0097	Cameraman	7.9970
	Peppers	7.5693	Peppers	7.9973
Wang *et al.* [24]	Cameraman	7.0097	Cameraman	7.9850
	Peppers	7.5693	Peppers	7.9752
Zhou *et al.* [25]	Cameraman	7.0097	Cameraman	7.9956
	Peppers	7.5693	Peppers	7.9962
Our study	Cameraman	7.0097	Cameraman	7.9977
	Rice	7.224	Rice	7.9972
	Lena	7.288	Lena	7.9969
	Peppers	7.5693	Peppers	7.9952
	Baboon	7.208	Baboon	7.9976

4.4. Testing phase

During the experimental phase of this work, some experiments of correct and wrong keys have been done in order to explore the robustness and security of the suggested encryption method. The result is shown in Figure 10, where Figure 10(a) is the test of the correct key, which means that with a correct key, the decryption and reconstructed images are done. Figures 10(b)-(d) in turn reflect the experimental results with imprecise keys.



(a) (b) (c) (d)

Figure 10. Testing phase; (a) correct keys $r = 44, \mu = 2024$, (b) incorrect key $r = 43$ $\mu = 2024$, (c) incorect key $r = 44, \mu = 2023$, and (d) incorect key $r = 38, \mu = 1999$

5. CONCLUSION

This research represents a pioneering approach in integrating quantum computing techniques into image encryption through bit-plane scrambling, pixel permutation, and bit permutation operations. The novel integration of quantum bit-plane scrambling and quantum pixel permutation introduces robust cryptographic methods that significantly improve entropy levels, as evidenced by the measured values: Cameraman (7.9977), Rice (7.9972), Lena (7.9969), Peppers (7.9952), and Baboon (7.9976). Furthermore, the proposed method demonstrates strong performance in terms of UACI and NPCR, with values indicating high encryption effectiveness: Cameraman (33.5688, 99.8275), Rice (33.4817, 99.8221), Lena (33.5188, 99.8237), Peppers (33.5572, 99.8301), and Baboon (33.4893, 99.8244). During the testing phase with incorrect keys ($r = 43$, $\mu = 2024$; $r = 44, \mu = 2023$; $r = 38, \mu = 1999$), none of the attempts successfully decrypted the image, highlighting the algorithm's resilience against decryption without the correct cryptographic key. This research underscores the potential of quantum-inspired encryption techniques in advancing image security, promising further applications in data protection and secure communication systems. For future research, integrating discrete quantum wavelet transform (DQWT) presents a promising direction to enhance the capabilities of quantum-based image encryption methodologies. DQWT offers a powerful toolset for multi-resolution analysis of image data, enabling more efficient representation and manipulation of image features across different scales. The application of DQWT could potentially enhance the encryption algorithm's ability to handle complex image structures while maintaining data integrity and security. Additionally, exploring the synergies between DQWT and quantum permutation techniques could lead to innovative encryption schemes that are robust against various cryptographic attacks.

FUNDING INFORMATION

This research has been funded by Ministry of Education and Culture in the 2024 Fundamental Research Grant in accordance with Decree No. 023/LL6/PgB/AL.04/2024 and 061/A.38-04/UDN-09/VI/2024.

AUTHOR CONTRIBUTIONS STATEMENT

This journal uses the Contributor Roles Taxonomy (CRediT) to recognize individual author contributions, reduce authorship disputes, and facilitate collaboration.

Name of Author	C	M	So	Va	Fo	I	R	D	O	E	Vi	Su	P	Fu
Eko Hari Rachmawanto	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
Ajib Susanto	✓	✓	✓		✓	✓	✓	✓	✓	✓		✓	✓	✓
Didik Hermanto	✓	✓	✓	✓	✓	✓	✓		✓	✓	✓			✓
Christy Atika Sari	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	
Ichwan Setiarso	✓	✓		✓	✓	✓		✓	✓	✓	✓			✓
Md. Kamruzzaman Sarker	✓	✓	✓		✓	✓		✓	✓	✓		✓		

C : **C**onceptualization
M : **M**ethodology
So : **So**ftware
Va : **Va**lidation
Fo : **Fo**rmal analysis
I : **I**nvestigation
R : **R**esources
D : **D**ata Curation
O : Writing - **O**riginal Draft
E : Writing - Review & **E**diting
Vi : **Vi**sualization
Su : **Su**pervision
P : **P**roject administration
Fu : **Fu**nding acquisition

CONFLICT OF INTEREST STATEMENT

Authors state no conflict of interest.

INFORMED CONSENT

We have obtained informed consent from all individuals included in this study.

ETHICAL APPROVAL

The research related to human use has been complied with all the relevant national regulations and institutional policies in accordance with the tenets of the Helsinki Declaration and has been approved by the authors' institutional review board or equivalent committee.

DATA AVAILABILITY

Data availability is not applicable to this paper as no new data were created or analyzed in this study.

REFERENCES

[1] C. Tiken and R. Samli, "A Comprehensive Review About Image Encryption Methods," *Harran Üniversitesi Mühendislik Dergisi*, vol. 7, no. 1, pp. 27–49, Apr. 2022, doi: 10.46578/humder.1066545.

[2] F. A. Alyaqobi, "A Systematic Review on Image Data Protection Methods," *IJIIS: International Journal of Informatics and Information Systems*, vol. 5, no. 3, pp. 131–141, Sep. 2022, doi: 10.47738/ijiis.v5i3.136.

[3] M. Eichelberg, K. Kleber, and M. Kämmerer, "Cybersecurity in PACS and Medical Imaging: an Overview," *Journal of Digital Imaging*, vol. 33, pp. 1527–1542, 2020, doi: 10.1007/s10278-020-00393-3.

[4] M. Ramzan, M. Habib, and S. A. Khan, "Secure and efficient privacy protection system for medical records," *Sustainable Computing: Informatics and Systems*, vol. 35, p. 100717, 2022, doi: 10.1016/j.suscom.2022.100717.

[5] P. Sarosh, S. A. Parah, and G. M. Bhat, "An efficient image encryption scheme for healthcare applications," *Multimedia Tools and Applications*, vol. 81, no. 5, pp. 7253–7270, 2022, doi: 10.1007/s11042-021-11812-0.

[6] S. R. Maniyath and T. V, "An efficient image encryption using deep neural network and chaotic map," *Microprocessors and Microsystems*, vol. 77, p. 103134, 2020, doi: 10.1016/j.micpro.2020.103134.

[7] E. A. Sofyan, C. A. Sari, H. Rachmawanto, and R. D. Cahyo, "High-Quality Evaluation for Invisible Watermarking Based on Discrete Cosine Transform (DCT) and Singular Value Decomposition (SVD)," *Advance Sustainable Science, Engineering and Technology (ASSET)*, vol. 6, no. 1, 2024, doi: 10.26877/asset.v6i1.17186.

[8] C. A. Sari, M. H. Dzaki, E. H. Rachmawanto, R. R. Ali, and M. Doheir, "High PSNR Using Fibonacci Sequences in Classical Cryptography and Steganography Using LSB," *International Journal of Intelligent Engineering and Systems*, vol. 16, no. 4, pp. 568–580, 2023, doi: 10.22266/ijies2023.0831.46.

[9] J. Gao, Y. Wang, Z. Song, and S. Wang, "Quantum Image Encryption Based on Quantum DNA Codec and Pixel-Level Scrambling," *Entropy*, vol. 25, no. 6, Jun. 2023, doi: 10.3390/e25060865.

[10] L. Guo, H. Du, and D. Huang, "A quantum image encryption algorithm based on the Feistel structure," *Quantum Information Processing*, vol. 21, no. 1, Jan. 2022, doi: 10.1007/s11128-021-03364-x.

[11] W. W. Hu, R. G. Zhou, J. Luo, S. X. Jiang, and G. F. Luo, "Quantum image encryption algorithm based on Arnold scrambling and wavelet transforms," *Quantum Information Processing*, vol. 19, no. 3, Mar. 2020, doi: 10.1007/s11128-020-2579-9.

[12] N. Min-Allah *et al.*, "Quantum Image Steganography Schemes for Data Hiding: A Survey," *Applied Sciences (Switzerland)*, vol. 12, no. 20, Oct. 2022, doi: 10.3390/app122010294.

[13] X. Liu and C. Liu, "Quantum image encryption scheme using independent bit-plane permutation and Baker map," *Quantum Information Processing*, vol. 22, no. 6, Jun. 2023, doi: 10.1007/s11128-023-04026-w.

[14] Y. K. Hamad, A. Y. Yousuf, and T. S. Atia, "An Evolutionary Quantum Scrambling Scheme for Medical Image with NEQR Representation," *International Journal of Computing and Digital Systems*, vol. 13, no. 1, pp. 1383–1396, May 2023, doi: 10.12785/ijcds/1301112.

[15] S. S. Gill *et al.*, "Quantum computing: A taxonomy, systematic review and future directions," *Software: Practice and Experience*, vol. 52, no. 1, pp. 66–114, 2022.

[16] Y. Wang, Z. Hu, B. C. Sanders, and S. Kais, "Qudits and high-dimensional quantum computing," *Frontiers in Physics*, vol. 8, p. 589504, 2020.

[17] X. Liu, D. Xiao, and C. Liu, "Quantum image encryption algorithm based on bit-plane permutation and sine logistic map," *Quantum Information Processing*, vol. 19, no. 8, Aug. 2020, doi: 10.1007/s11128-020-02739-w.

[18] J. He, H. Zhu, and X. Zhou, "Quantum image encryption algorithm via optimized quantum circuit and parity bit-plane permutation," *Journal of Information Security and Applications*, vol. 81, p. 103698, 2024, doi: 10.1016/j.jisa.2024.103698.

[19] W.-L. Ma, S. Puri, R. J. Schoelkopf, M. H. Devoret, S. M. Girvin, and L. Jiang, "Quantum control of bosonic modes with superconducting circuits," *Science Bulletin*, vol. 66, no. 17, pp. 1789–1805, 2021, doi: 10.1016/j.scib.2021.05.024.

[20] A. A. Arrasyid, D. R. I. M. Setiadi, M. A. Soeleman, C. A. Sari, and E. H. Rachmawanto, "Image Watermarking using Triple Transform (DCT- DWT-SVD) to Improve Copyright Protection Performance," in *2018 International Seminar on Research of Information Technology and Intelligent Systems (ISRITI)*, IEEE, Nov. 2018, pp. 522–526, doi: 10.1109/ISRITI.2018.8864461.

[21] J. Khandelwal, V. K. Sharma, D. Singh, and A. Zaguia, "Dwt-svd based image steganography using threshold value encryption method," *Computers, Materials and Continua*, vol. 72, no. 2, pp. 3299–3312, 2022, doi: 10.32604/cmc.2022.023116.

[22] F. Yasmeen and M. S. Uddin, "An Efficient Watermarking Approach Based on LL and HH Edges of DWT–SVD," *SN Computer Science*, vol. 2, no. 2, pp. 1–16, Apr. 2021, doi: 10.1007/s42979-021-00478-y.

[23] G. Ardiansyah, C. A. Sari, D. R. I. M. Setiadi, and E. H. Rachmawanto, "Hybrid method using 3-DES, DWT and LSB for secure image steganography algorithm," in *2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE)*, 2017, pp. 249–254, doi: 10.1109/ICITISEE.2017.8285505.

[24] H. Wang, J. Wang, Y. C. Geng, Y. Song, and J. Q. Liu, "Quantum Image Encryption Based on Iterative Framework of Frequency-Spatial Domain Transforms," *International Journal of Theoretical Physics*, vol. 56, no. 10, pp. 3029–3049, Oct. 2017, doi: 10.1007/s10773-017-3469-5.

[25] N. Zhou, Y. Hu, L. Gong, and G. Li, "Quantum image encryption scheme with iterative generalized Arnold transforms and quantum image cycle shift operations," *Quantum Information Processing*, vol. 16, no. 6, Jun. 2017, doi: 10.1007/s11128-017-1612-0.

BIOGRAPHIES OF AUTHORS

Eko Hari Rachmawanto received a Bachelor's degree in Informatic Engineering from the Universitas Dian Nuswantoro, in 2010. He received a Master's double degree Universitas Dian Nuswantoro and Universiti Teknikal Malaysia Malacca (UTeM) in 2010 and 2012. Since 2012, he joined as a Lecturer in Informatics Engineering at the Universitas Dian Nuswantoro, Semarang, Indonesia. Now he serves as Editor in Chief of Accredited Indonesian National Journal. Since 2022 he has supervised the informatics engineering study program in study programs outside the main campus as head of the study program in Kediri, Indonesia. Now he is a member of Security Data Collaboration Research and tasked with developing several researchers regarding data security, and image processing. He can be contacted at email: eko.hari@dsn.dinus.ac.id.

Ajib Susanto is an Associate Professor at the Department of Informatics Engineering, Universitas Dian Nuswantoro, Indonesia. He received his bachelor and master in informatics engineering from Universitas Dian Nuswantoro in 2004 and 2008 respectively. Since 2000 he has joined as lecturer in Universitas Dian Nuswantoro. In 2018 until now, he currently served as chairman of software engineering in Department of Informatics Engineering. Since 2013, he has successively received research grants from the Directorate General of Higher Education (DIKTI). The research field is mobile data security. He can be contacted at email: ajib.susanto@dsn.dinus.ac.id.

Didik Hermanto is served as Deputy Dean of the Computer Science Faculty at UDINUS Kediri. He received Bachelor of Mathematics Education at Muhammadiyah University Surabaya in 1999, Masters in Mathematics Education at PGRI Adi Buana University Surabaya in 2013, and Doctor of Mathematics Education at UNESA Surabaya in 2020. Currently joining the Research Center for Intelligent Distributed Surveillance and Security, Dian Nuswantoro University, Semarang, Indonesia to develop statistical patterns in data security, especially in the development of quantum computing. He can be contacted at email: didik.hermanto@dsn.dinus.ac.id.

Christy Atika Sari received the Master's degree in Informatic Engineering from Dian Nuswantoro University and University Teknikal Malaysia Melaka (UTeM) in 2012. She is currently active as an author in an international journal and conference Scopus indexed. She was also awarded as best author and best paper at a national and international conference in 2019 and 2020 respectively and was awarded by the Indonesian Ministry of Education and Culture Research and Technology as the Indonesian top 50 best researchers in 2020. She's research interest is quantum computing for security data and image processing. She can be contacted at email: christy.atika.sari@dsn.dinus.ac.id.

Ichwan Setiarso received his degree in 1991 from Universitas Pawyatan Daha. In 2011 he received his Master form Universitas Brawijaya, and in 2016 he received his Doctor from Universitas Brawijaya. He served as head of Visual Communication Design Study Program at Universitas Dian Nuswantoro in 2020 until 2022. His research interest is in computation analysis. He can be contacted at email: ichwan.setiarso@dsn.dinus.ac.id.

Md. Kamruzzaman Sarker is Assistant Professor of Computer Science at the Bowie State University. He love to invent new stuff (research), share knowledge (teaching), and at the same time build stuff (software engineering). His research domain spans the broad field of artificial intelligence (AI) and its application. Some specific topics of focus include but are not limited to explainable artificial intelligence, deep learning, knowledge graph, semantic web, and cybersecurity. He can be contacted at email: ksarker@bowiestate.edu.