Journal of Applied Physics

RESEARCH ARTICLE | APRIL 25 2025

A quantum image encryption scheme based on quantum Arnold transform and hyper 5D chaotic system

Lishi Liu; Chenhao Yin ; Yumin Dong

J. Appl. Phys. 137, 164404 (2025)
https://doi.org/10.1063/5.0265586

Journal of Applied Physics ARTICLE pubs.aip.org/aip/jap

A quantum image encryption scheme based on quantum Arnold transform and hyper 5D chaotic system

Cite as: J. Appl. Phys. **137**, 164404 (2025); doi: 10.1063/5.0265586
Submitted: 14 February 2025 · Accepted: 5 April 2025 ·
Published Online: 25 April 2025

Lishi Liu, Chenhao Yin, and Yumin Dong[a)]

AFFILIATIONS

College of Computer and Information Science, Chongqing Normal University, Chongqing 401331, China

[a)]**Author to whom correspondence should be addressed:** dym@cqnu.edu.cn. **Also at:** College of Computer and Information Science, Chongqing Normal University.

ABSTRACT

In the wake of the information security era, ensuring the privacy, accuracy, and reliability of images has become imperative. In this paper, a quantum image encryption method combining quantum Arnold transform and a hyper 5D chaotic system is devised. Furthermore, first, a nonlinear color quantization model (NCQI) is used to convert digital images in standard RGB format into quantum color images. Then, based on the size of the converted quantum color image, the corresponding encryption key is generated using the hyper 5D chaotic system. In the encryption stage, we use the key to encrypt the converted quantum color image. This process entails two principal steps: First, we use quantum Arnold transform to scramble the pixel positions in the image and, subsequently, diffuse the pixel values through a carefully designed cyclic shift strategy to achieve the preliminary encryption of the image. To further strengthen the encryption security, we use a quantum rotation gate to perform quantum rotation transformation on the color channel of each pixel point in the encrypted image separately. These well-designed encryption processes, in succession, significantly enhance the security of the image. This paper provides the corresponding quantum circuit design and validates both the efficacy and security of the quantum image encryption scheme through simulation experimental results.

I. INTRODUCTION

With the rapid development of the big data era and multimedia technology, digital color images have been widely used in people's daily lives and multiple industries owing to their high resolution and intuitive expression. While the convenience of image transfer is obvious, it also poses numerous security risks. Hence, an increasing number of researchers are dedicated to exploring more secure encryption strategies in this field. As technology advances and attackers become increasingly sophisticated, the development of reliable and efficient encryption techniques has become paramount in today's society. Furthermore, as the research on traditional image encryption technology delves deeper, its inherent technical limitations, including low encryption efficiency and high time complexity, are becoming increasingly evident. Some widely used image encryption methods are currently facing unprecedented challenges.[1–4] Consequently, researchers have embarked on a quest for more efficient encryption methods.

The unique properties of quantum computing, including quantum entanglement, superposition, and parallel processing capabilities, have inspired researchers to apply quantum technology to the realm of image encryption, leading to the emergence of quantum image encryption technology. Numerous quantum image encryption algorithms have been proposed, making quantum image encryption technology a prominent research trend within the field of information security. Thanks to the concept of superposition states inherent in quantum computing, quantum computers significantly outperform conventional computers in terms of processing efficiency. Furthermore, the inherent unclonability of quantum states ensures the security of quantum image encryption. Therefore, research in the field of quantum image encryption[5–11] has attracted much attention. At the same time, chaotic systems exhibit high sensitivity to the initial conditions and parameters, as well as non-periodicity, and their long-term evolutionary trajectories are inherently uncertain.[12–15] These characteristics, namely,

high key sensitivity, stochastic properties, and sensitivity to plaintexts, are highly compatible with the requirements of image encryption systems. Consequently, image encryption schemes based on chaotic systems have become a hot topic of research. In light of the advancements in quantum computing and the inherent randomness of chaotic systems, the objective of this study is to harness the strengths of both theories and develop a more efficient and secure image encryption scheme.

In 2003, researchers began to explore the application of quantum algorithms to image processing, gradually developing two main directions: Quantum image representation and quantum image processing. In 2005, a study[16] proposed a quantum image representation that converts 2D image pixel values into quantum states in Hilbert space. Since then, various quantum image representations have been introduced, such as Entangled Image,[17] FRQI (Flexible Representation of Quantum Images),[18] and NEQR (Novel Enhanced Quantum Representation).[19] The NCQI (nonlinear color quantization model)[20] model used in this paper is an extension of the NEQR model, overcoming the limitation that NEQR can only represent grayscale images and enable the application of quantum image representation in the field of color images. The NCQI model preserves the color and resolution information of the image by mapping each pixel to a qubit state. It makes full use of the quantum superposition and entanglement properties to optimize the processing and storage of image information, greatly improving the speed and efficiency of image processing and enhancing the security of encryption. Given the various advantages of the NCQI image representation method, our image encryption algorithm will be based on the image represented by the NCQI model.

The key to image encryption technology lies in the construction of its encryption algorithm, and ensuring the security of encrypted images necessitates reliance on cutting-edge image encryption theory. In the existing encryption schemes, whether traditional or emerging quantum image encryption technology, chaotic systems are commonly employed to generate highly random and secure encryption keys, thereby enhancing the complexity and anti-attack capabilities of encryption algorithms. Chaotic systems[21–30] provide a framework for describing the complex dynamic behavior of dynamical systems. They exploit the system's sensitive dependence on initial conditions to exhibit seemingly random properties; this inherent randomness and unpredictability is effectively utilized in the field of information security, particularly in encryption technology, where these properties furnish an important theoretical basis for crafting robust encryption algorithms. Currently, some quantum chaotic systems have been proposed,[31–34] yet most cannot be readily applied in image encryption due to their intricate quantum physics characteristics. Furthermore, quantum chaotic systems typically necessitate quantum computers and other advanced quantum technologies for implementation, which are still in the research and development phase and not readily scalable for widespread adoption. In contrast, classical chaotic systems can be realized on existing computer hardware. To enhance the security of quantum image encryption, this paper employs a novel approach—a hyper 5D chaotic system.[35]

In the context of today's rapid development of information technology, image encryption technology exhibits a trend toward diversification. In particular, the integration of deep learning algorithms and blockchain technology offers more advanced and robust protection strategies for image data security. These emerging technologies not only enhance the complexity and attack resistance of encryption algorithms but also pave new research avenues for image privacy protection and copyright preservation. Lata and Cenkeramaddi[36] investigated various cryptographic strategies for image denoising and enhancement using deep learning models, as well as other aspects of medical image security such as classification, key generation, and target identification. Their study also highlighted the limitations and potential future directions of deep learning models in cryptography. Similarly, other researchers have investigated efficient encryption methods for digital images in the context of deep learning.[37] The review presents a comparative analysis of the performance of different deep learning models in tabular form. Kiya *et al.*[38] investigated learnable color image encryption using deep learning models and evaluated its security and robustness against noise. Meraouche *et al.*[39] conducted a survey to evaluate the performance and security of neural network based encryption techniques. Bao and Xue[40], in their paper, focused on encryption techniques for securing digital images within a deep learning framework and analyzed the encryption performance of the model in terms of compression, target detection, classification, and key generation. Chithraand Aparna[41] introduced a robust blockchain-integrated encryption scheme with steganography for securing image data, enhancing protection through dual-level security by embedding hashed cipher blocks within audio signals. Zhao Feixiang and colleagues[42] have proposed an advanced color image encryption scheme integrating Henon-zigzag mapping and chaotic restricted Boltzmann machines, with a blockchain-enhanced system for secure and verifiable image encryption. Kumari, Singh, and Singh[43] have proposed a novel image encryption model called Multi-Chaotic Maps and Blockchain Encryption (MCBE), which leverages the randomness of logistic and tent maps combined with blockchain's SHA-256 hash function to enhance security and resist brute force attacks, demonstrating improved performance against various cryptographic attacks compared to the existing methods.

In today's increasingly important information security, quantum image encryption technology faces challenges such as low encryption efficiency, insufficient security, loss of color information, and complex key management. Aiming at these problems, this paper innovatively proposes a quantum image encryption method combining quantum Arnold transform and a hyper 5D chaotic system, which significantly improves the encryption speed and meets the real-time demand by designing efficient quantum circuits; at the same time, the method strengthens the security of the encryption algorithm and effectively defends against quantum computing attacks. In addition, the nonlinear color quantization model is adopted to preserve the image color information, ensure the quality of encrypted images, and enhance the practicality of the method by simplifying the key management process. The simulation experiment results confirm the effectiveness and security of the proposed method, which brings new innovations and advances in the field of quantum image encryption.

We propose a novel quantum image encryption method that integrates NCQI image representation, the quantum Arnold transform, a hyper 5D chaotic system, and quantum computing principles. This method offers enhanced encryption efficiency and security compared to some of the currently available image

encryption methods. Initially, we utilize the random function to generate the initial values for the hyper 5D chaotic system. After a predetermined number of iterations, we obtain five encryption keys of appropriate sizes. One of these keys, x_1, is then used to perform an Arnold transform on the position information of the NCQI image. However, merely altering the position information of the image does not fully ensure the security of the encrypted image; therefore, we also encrypt the color information of the image. Initially, we employ the idea of cyclic shift, using key x_2 to individually apply cyclic shifts to each position under the color information, thereby achieving an initial encryption of the image. To further enhance the security of the encrypted image, we then use x_3, x_4, and x_5 as keys, respectively, on the three channels of the NCQI image. This is achieved through the use of the quantum rotation gate to perform quantum rotations for encryption, which significantly improves the security of the encrypted image. Consequently, the innovations of this paper can be summarized as follows:

1. In this study, an advanced quantum image encryption scheme is proposed based on the unique properties of NCQI. This scheme takes advantage of the superiority of quantum computing to realize the quantumization of the image encryption process. Compared with the traditional computing methods, the high efficiency of quantum computing is significantly reflected in this encryption scheme, which significantly improves the speed and security of image encryption.
2. The Arnold transform is employed to scramble the positions of image pixels, while the pixel values are initially diffused through the combination of a cyclic shift strategy. The encryption key, generated by the hyper 5D chaotic system, is utilized to control both the number of Arnold transform iterations and the cyclic shift process, thereby enhancing the complexity and security of the encryption procedure.
3. The key generated by the hyper 5D chaotic system is employed to control the angle of rotation of the quantum rotation gate, facilitating secondary diffusion of the image pixel values. This operation not only intensifies the randomness of the encrypted image but also elevates the sensitivity of the encryption process to the initial conditions, thereby rendering the encryption more resilient to statistical analysis attacks.

In summary, the encryption scheme proposed in this study ingeniously integrates the core principles of quantum computing into the key generation and quantum image encryption processes, thereby harnessing the substantial advantages of quantum technology in the realm of cryptography. Even in scenarios demanding low encryption complexity, this methodology ensures robust security of the encrypted images. Rigorously validated through simulation experiments, the proposed approach demonstrates its efficacy and exhibits exceptional performance in neighboring pixel correlation analysis, information entropy evaluation, and other security assessments.

II. RELATED WORK

A. NCQI

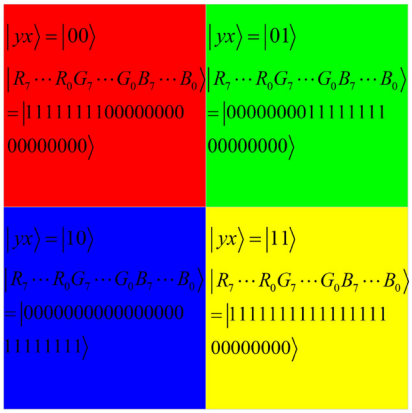
NCQI, innovatively proposed by scholars such as J. Sang and S. Wang in 2017 based on the NEQR framework, is an advanced quantum color image representation specifically designed for quantum computers. While inheriting the advantages of NEQR in efficiently processing image position information, the method achieves accurate encoding of image color information through the introduction of additional qubit dimensions, thereby significantly enhancing the capabilities of quantum image processing. The core advantage of NCQI lies in its natural adaptability and high efficiency for color images. Specifically, it is specially designed for the three color channels (red, green, and blue) unique to color images, each channel being allocated q qubits to precisely represent its color depth, for a total of $3q$ qubits to comprehensively capture and store the color details of the image. This design not only ensures the richness and accuracy of image colors but also reflects the inherent advantages of quantum computing in processing multidimensional data. For the processing of location information, NCQI follows the classical strategy of NEQR, namely, the use of $2n$ qubits to construct an efficient two-dimensional spatial indexing system, which enables the precise localization of the position of each pixel point in the image. This design maintains the simplicity and efficiency of quantum image representation in position encoding, allowing the NCQI model to efficiently perform spatial operations and analysis of images while taking into account the color expression. Therefore, for an image of size $2n \times 2n$ pixels, this model requires $2n + 3q$ qubits to accurately encode all the key information of the image, where $2n$ qubits are dedicated to constructing a two-dimensional spatial index of the image, ensuring that the position of each pixel point can be accurately and unambiguously localized. The other $3q$ qubits are allocated to the three color channels of red (R), green (G), and blue (B), with each channel occupying q qubits to cover a wide color depth range from 0 to 2^{q-1}, thus supporting rich and delicate color expression. In order to achieve a tight integration of positional and color information, the NCQI model cleverly employs the quantum tensor product (QTP) operation. This operation not only effectively entangles the positional quantum state with the color quantum state but also ensures the integrity and consistency of quantum image representation. Through the application of a quantum tensor product, NCQI is able to generate a highly integrated quantum state that contains both the complete spatial layout and detailed color information of the image, thus realizing an efficient and accurate representation of quantum color images. For a quantum color image I of size $2^n \times 2^n$, it can be expressed as follows using the NCQI model:

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

where

$$|C(y,x)\rangle = \left|R_{q-1}\cdots R_0 G_{q-1}\cdots G_0 B_{q-1}\cdots B_0\right\rangle$$
$$|R_i\rangle, |G_i\rangle, |B_i\rangle \in \{0,1\}$$
$$|y\rangle|x\rangle = |y_{n-1}y_{n-2}\cdots y_0\rangle|x_{n-1}x_{n-2}\cdots x_0\rangle, |y_i\rangle|x_i\rangle \in \{0,1\},$$

where $\left|R_{q-1}\cdots R_0 G_{q-1}\cdots G_0 B_{q-1}\cdots B_0\right\rangle$ denotes the color information of the image, which are the values of the red, green, and blue channels. Generally, color images use a color depth of 256 to



$$|I\rangle = \frac{1}{2}\begin{bmatrix} |111111110000000000000000\rangle \otimes |00\rangle + \\ |000000001111111100000000\rangle \otimes |01\rangle + \\ |000000000000000011111111\rangle \otimes |10\rangle + \\ |111111111111111100000000\rangle \otimes |1\rangle \end{bmatrix}$$

FIG. 1. Color image of 2 × 2 size represented by NCQI.

store the colors represented by different channels; so here, we have q=8 and use 24 qubits to store the color information for each of the three channels. $|y\rangle|x\rangle$ represents the position information of the image. Based on the principle of superposition in quantum computing, one qubit can represent two different states simultaneously, and n qubits can have 2^n different states. Therefore, for a quantum color image of size $2^n \times 2^n$, $2n$ qubits can be used to store its position information, where $|y\rangle$ uses n qubits and $|x\rangle$uses n qubits. $|y\rangle$ stores the ordinate (vertical position) information of each pixel of the image, and $|x\rangle$ stores the abscissa (horizontal position) information. The Kronecker product [denoted by (⊗)] can be used to entangle different qubits. Specifically, ⊗ is employed to entangle the image's position information with its color information, ensuring that when the position information of the quantum color image is read, NCQI (presumably a reference to a specific quantum image representation or processing method) can correctly display the color of the pixel at that position. For a color image of size 2 × 2, the representation using NCQI is illustrated in Fig. 1, and its implementation circuit is shown in Fig. 2.

B. Classic 5D chaos system

In order to secure encrypted images, a sufficiently complex key is essential. The uncertainty and high sensitivity of chaotic systems make them indispensable for generating such keys. To obtain a key sufficient to support our encryption algorithm, we studied various chaotic systems and chose to use a hyper 5D chaotic system[35] to generate random keys for encrypting NCQI images. This chaotic system is a hyper 5D chaotic system with stabilized equilibrium points, proposed by Jay Prakash Singh, K. Rajagopal *et al.* in 2018. The specific formulation of this system is given below:

$$\begin{cases} \dot{x}_1 = a(x_2 - x_1) + bx_2x_3 + x_4 + x_5, \\ \dot{x}_2 = -x_1x_3 + cx_2 + x_4, \\ \dot{x}_3 = -4 + x_1x_2 - dx_3, \\ \dot{x}_4 = -ex_2, \\ \dot{x}_5 = -ex_1, \end{cases} \tag{2}$$

where $(x_1, x_2, x_3, x_4, x_5)$ are the state variables of the system, and (a)–(e) are the adjustable parameters of the system. When a = 35, b = 30, c = 17, d = 0.78, and e = 12, the system exhibits hyperchaos. At this time, the finite-time local Lyapunov exponents (LEs) of the system are LEs = (0.6892, 0.1431, 0, −0.4238, −18.944). The positive finite-time local Lyapunov exponents of the system indicate hyper-chaotic behavior. According to the given formula of the chaotic system, we use the given parameter values as the adjustable parameter values of the system. Then, we use a random function to

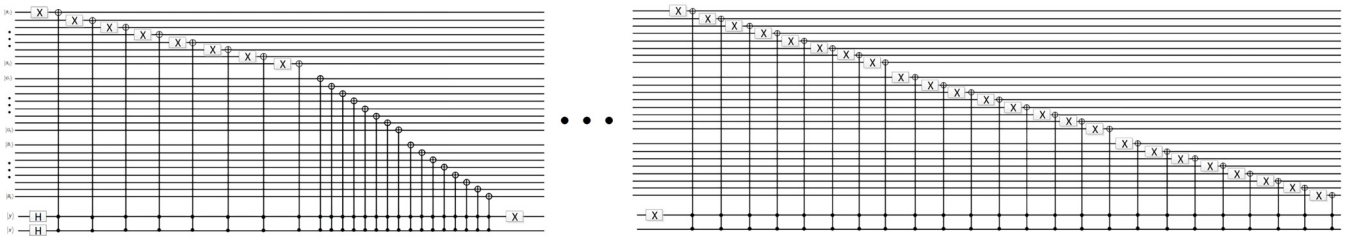


FIG. 2. Implementation circuit for representing 2 × 2 size color image with NCQI.

generate five numbers in the range [0,1] as the initial values of the system state and plot the attractor image of this chaotic system, as shown in Fig. 3. The alignment of the chaotic attractor is sufficiently chaotic, which proves that its randomness is capable of supporting the security of image encryption.

C. Quantum Arnold transform

1. Arnold transformation

The Arnold transformation was established by V. I. Arnold in his study of ergodic theory, while in 1992, Dyson *et al.* applied this transformation as an image disambiguation method in the field of image encryption. The specific operation is as follows: Assume there is an original image I, whose pixel coordinate information is (x, y). We define the Arnold transformation operation on image I as follows:

$$\begin{pmatrix} x_A \\ y_A \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} (modN). \tag{3}$$

This is equivalent to

$$\begin{aligned} x &= (2x_A - y_A) modN, \\ y &= (-x_A + y_A) modN, \end{aligned} \tag{4}$$

where x and y denote the horizontal and vertical coordinates of the original pixel. x_A and y_A denote the horizontal and vertical coordinates of the transformed pixel. N is the side length of the square

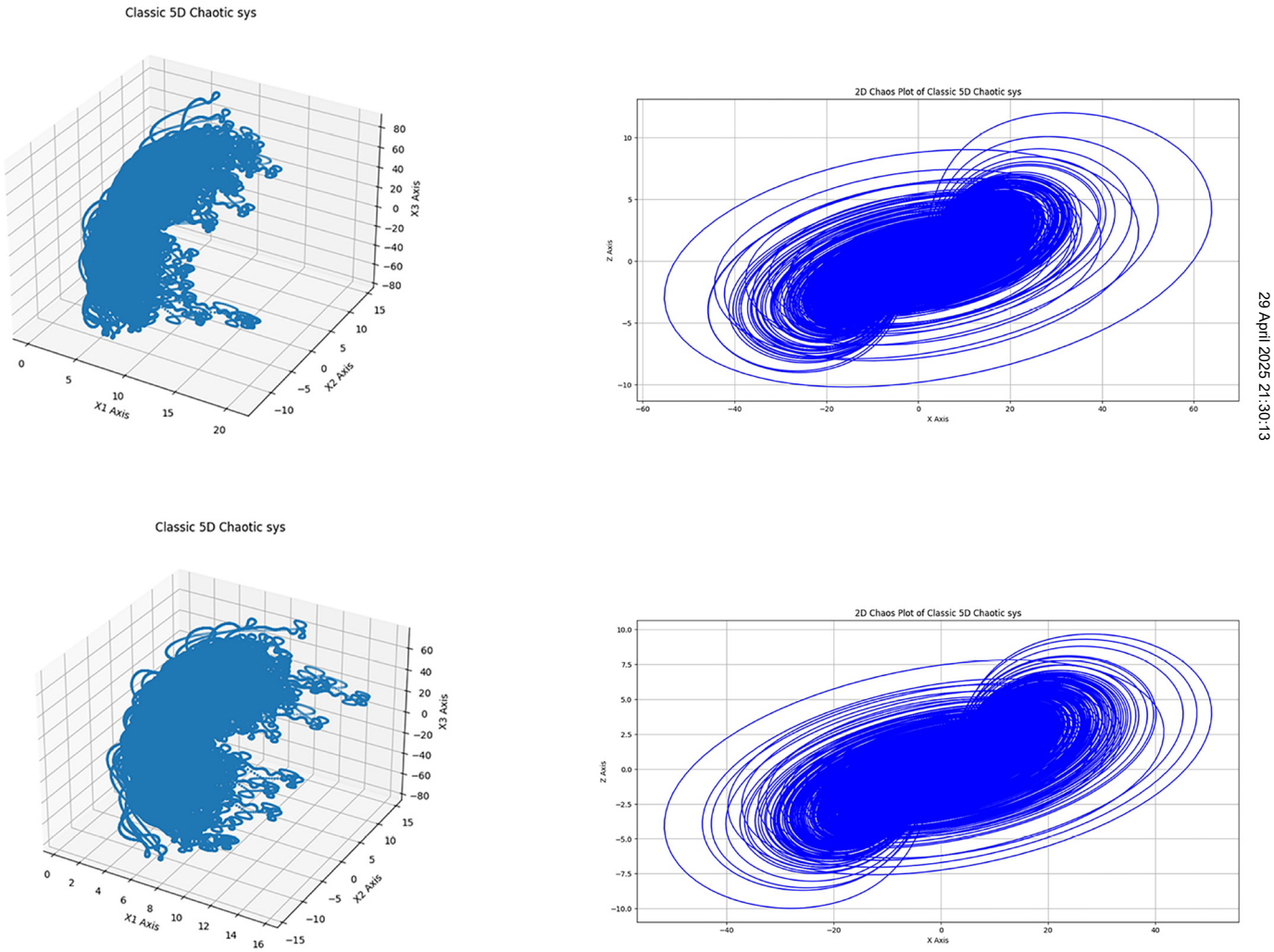


FIG. 3. Attractor diagram of the hyper 5D chaotic system (the upper and lower parts are the attractor diagrams with different initial values. It can be found that a slight change in the initial value will cause the direction of the attractor diagram of the chaotic system to change).

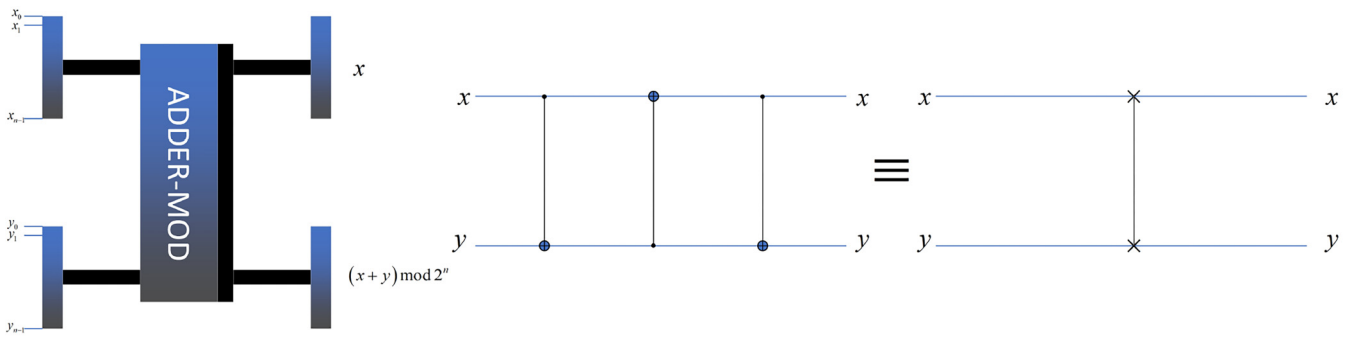


FIG. 4. Adder-mod2^n module and SWAP gate.

image. The restoration process is the inverse transformation, that is,

$$\begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}^{-1} \begin{pmatrix} x_A \\ y_A \end{pmatrix} (modN) = \begin{pmatrix} 2 & -1 \\ -1 & 1 \end{pmatrix} \begin{pmatrix} x_A \\ y_A \end{pmatrix} (modN), \tag{5}$$

which is equivalent to

$$\begin{aligned} x &= (2x_A - y_A) modN, \\ y &= (-x_A + y_A) modN. \end{aligned} \tag{6}$$

Since Arnold's transformation is periodic, it can be employed to transform pixel positions. That is, Arnold transforming an image does not alter the values of the pixels but merely rearranges their positions, ensuring that our encrypted image remains of normal size. Dyson provides an upper and lower bound for the period, specifying that the period for an image of size 256 is 192. This implies that our transformation factor should not be a multiple of 192, as this would render the transformation invalid.

2. Arnold's quantization

In order to quantize the Arnold transformation, we need to utilize the quantum adder modulo (2n) module and the SWAP gate, as illustrated in Fig. 4. The quantum addermod2^n module is capable of realizing the modular addition of two qubits, i.e., $|x, y\rangle$ after the quantum adder-mod2^n module becomes $|x, (x + y)2n\rangle$. The SWAP gate, on the other hand, enables swapping of the positions of two stored qubits, i.e., $|x, y\rangle$ becomes $|y, x\rangle$ after the SWAP operation. For the Arnold transformation introduced earlier, using a adder-mod2^n and SWAP gate processing can be represented as follows: $|x, y\rangle \rightarrow |y, x\rangle \rightarrow |y, (x + y)\rangle \rightarrow |y, (x + 2y)2^n\rangle$, where only the second qubit of $|(x + 2y)2^n\rangle$ is considered, thus obtaining $|y_A\rangle$. Similarly, for $|x, y\rangle \rightarrow |x, (x + y)2^n\rangle$, the operation process is shown in Fig. 5. Only the second qubit is taken, yielding $(x_A = |(x + y)2^n\rangle$. The reduction principle for recovering $|x\rangle$ and $|y\rangle$ from $|x_A\rangle$ and $|y_A\rangle$ is simply the inverse of the above process. For example, $|x_A, y_A\rangle \rightarrow |-x_A, (y_A - x_A)2n\rangle$ and take the second qubit for $|y\rangle$; or $|x_A, y_A\rangle \rightarrow |-y_A, x_A\rangle \rightarrow |y_A, (x_A - 2y_A)2n\rangle$ and then take the second qubit for $|x\rangle$. The operation process is shown in Fig. 6.

D. Quantum rotation gate

The reason why quantum computing has numerous advantages over classical computing is that its various operations are based on qubits, which, unlike classical bits, rely on microscopic particles in quantum physics. Specifically, the states of qubits are indeterminate and irregular. To interpret a qubit, we can refer to the Bloch sphere, as depicted in Fig. 7. The state of a qubit encompasses the entire surface of the Bloch sphere (prior to measurement). Once the qubit is measured, its state becomes determined, either $|0\rangle$ or $|1\rangle$, which correspond to the two poles of the Bloch sphere. By referring to the Bloch sphere, we can understand that, apart from the points lying on the "equator," other points distributed on the sphere's surface will be closer to one of the poles. For this reason, the measurement outcome of a qubit will exhibit different probabilities depending on whether its state is closer to one of the poles. For a qubit, if its state pointer is closer to $|1\rangle$, the probability of measuring it as $|1\rangle$ is greater than that of measuring it as $|0\rangle$, but it is not absolutely certain to be $|0\rangle$ (this reflects the uncertainty principle of quantum computing). The same applies in reverse. For a state located on the "equator," the measurement probabilities of $|0\rangle$ and $|1\rangle$ are equal.

There are three types of quantum rotation gates. One type rotates the state pointer around the x-axis, another rotates it around the y-axis, and the last rotates it around the z-axis.

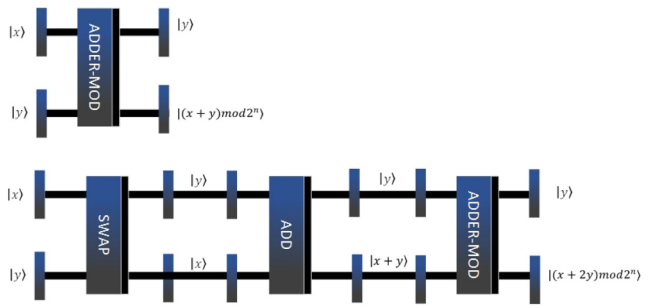


FIG. 5. Diagram of Arnold's quantization process.

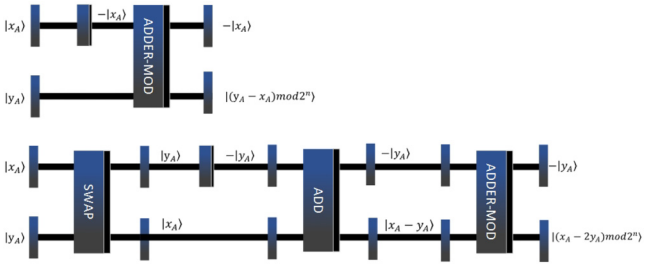


FIG. 6. Diagram of the Arnold reduction quantization process.

Applying these three types of rotation gates will produce different alterations to the state of the qubit, and these alterations have distinct applications in quantum computing. Figure 8 illustrates three different types of quantum rotation gates.

III. ENCRYPTION PROCESS

To achieve the encryption of a quantum color image, our work can be briefly summarized in three steps. In the first step, we need to perform NCQI image preparation on a classical RGB image to obtain a quantum color image. The second step involves preparing the encryption key using the chaotic system mentioned in the article, taking into account the size of the quantum color image prepared in the first step. Last, we encrypt the NCQI image using the key. We will describe these steps in more detail below.

A. Quantum NCQI image preparation

Referring to the principle of NCQI image representation introduced earlier, we can use $2n + 3q$ qubits to store and process color images of size $2^n \times 2^n$ pixels. Here, q qubits are allocated for the color information of each of the R, G, and B channels, respectively;

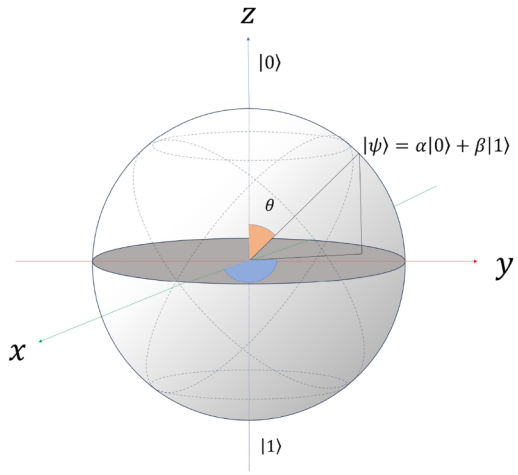


FIG. 7. Bloch Balls.

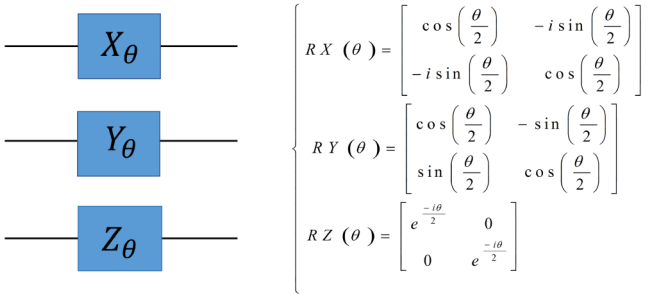


FIG. 8. Three different types of quantum rotation gates (variations in x_θ and y_θ reflect modulation of the vibrational amplitude, while variations in z_θ control the phase shift of the vibrational waveform).

thus, a total of $3q$ qubits are used for color. The remaining n qubits each are used to store information about the horizontal and vertical coordinates of the image pixels (since an unmeasured qubit can be either $|0\rangle$ or $|1\rangle$, n qubits can represent 2^n possible values). Based on these points, for quantum preparation of conventional color images (where the colors of the R, G, and B channels are typically represented with 256 levels, or 8 bits per channel), we can use $2n + 24$ qubits (8-qubits per channel for a total of 24-qubits for color, plus $2n$ qubits for pixel coordinates). First, we need to prepare $2n + 24$ qubits in the initial state $|0\rangle$, which correspond to the arrangement $|R_{q-1}, \cdots, R_0, G_{q-1}, \cdots, G_0, B_{q-1}, \cdots, B_0\rangle \times |y_{n-1}, \cdots, y_0\rangle|x_{n-1}, \cdots, x_0\rangle$ for each qubit's position within the overall state. Subsequently, we perform entanglement operations on these qubits using $\otimes$. Typically, in quantum circuits, we use CNOT gates to entangle different qubits. However, in circuits representing images, we employ a unique approach where the qubit storing pixel position information serves as the control input to the CNOT gate, while the qubit storing color information acts as the target input. Later, we will utilize quantum NOT gates to manipulate the state of the qubits that encode position information, enabling them to represent different positions within the image.

B. Quantum key preparation

Based on the hyper 5D chaotic system introduced earlier, we employ a sequence of five state variables as the encryption key. Upon analyzing the NCQI quantum image representation method, it becomes evident that its structure naturally divides into five distinct parts: Two qubit sequences, $|y\rangle$ and $|x\rangle$, which encode position information, and three qubit sequences, $|R_7, \cdots, R_0\rangle$, $|G_7, \cdots, G_0\rangle$, and $|B_7, \cdots, B_0\rangle$, which store the RGB color channels. We propose using the sequence x_1, x_2, x_3, x_4, x_5 generated by the hyper 5D chaotic system as the key to encrypt this information. The utilization of these five keys can be categorized into two primary functions: Encrypting the NCQI image's position information and encrypting its color information. It is crucial to maintain the original structure of the image during the encryption process. Therefore, for position information, the most appropriate encryption method is to permute and transform the position of each pixel in the image. Consequently, we will use key x_1 to perform a

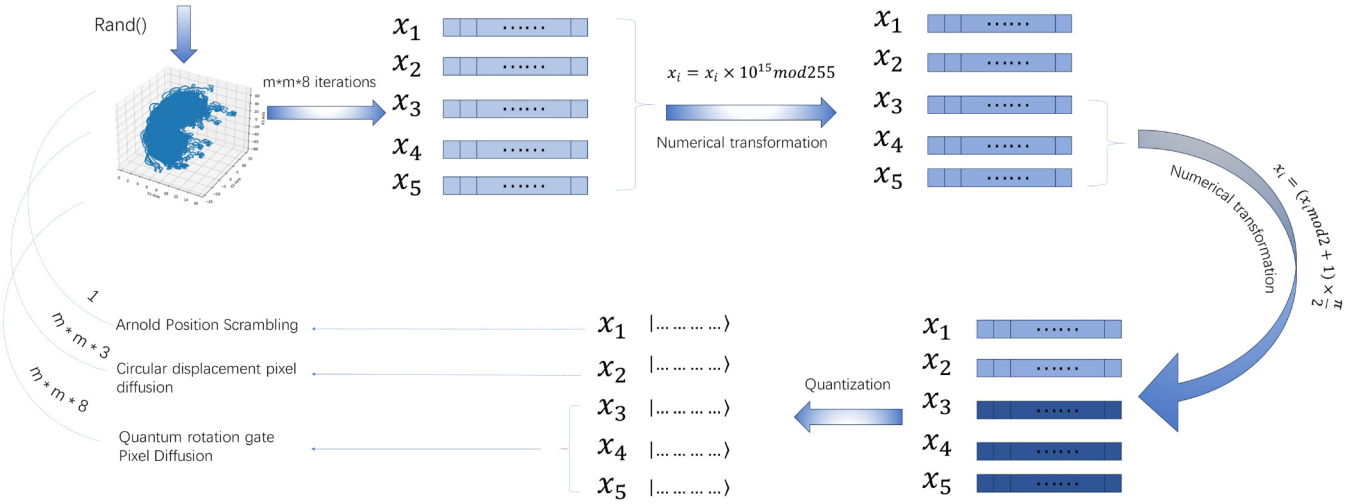


FIG. 9. Flowchart of quantum key preparation.

quantum Arnold transform on the position information $|x\rangle$ and $|y\rangle$ of the NCQI image. However, merely altering the position information of the image is insufficient to guarantee complete security of the encrypted image. Additional measures are necessary to ensure the confidentiality of the color information.

Therefore, we also need to encrypt the color information of the image. We employ the exchange mechanism of the quantum SWAP gate to achieve a transformation akin to code shifting through the swapping operation between qubit circuits. By performing quantum SWAP operations between qubit circuits, we simulate and surpass the code shift transformation used in classical computing, allowing for independent and flexible cyclic shift processing of the color information carried by each pixel in the image. Specifically, key x_2 is used to perform independent cyclic shift transformations for each of the three color channels under each position within the image data. In this process, the quantum SWAP gate not only serves as a medium for information exchange but also significantly enriches the possibilities and complexity of the shift transformation through its inherent non-classical properties, such as superposition and entanglement. Having initially implemented this to encrypt the image, to further enhance the security of the encrypted image, we then use x_3, x_4, and x_5 as keys to encrypt the three RGB channels of the NCQI image through quantum rotation. This is accomplished by utilizing a quantum rotation gate, which applies a rotation to the color values based on the respective keys.

In order to realize the subsequent encryption steps, the preparation of the quantum key is crucial. First, we use the random function to generate initial values for the five state variables of the hyper 5D chaotic system, employing the previously mentioned parameter values as those used by the system. After that, we need to generate a key of reasonable length, based on the size information of the NCQI image, using the hyper 5D chaotic system with each parameter set. Since the key we generate using the hyper 5D chaotic system is a sequence of five classical data points, it cannot be directly used in quantum circuits. This means that we cannot apply the original key directly to perform the quantum Arnold transform or quantum rotation transformation mentioned earlier. Therefore, we still need to prepare the data of the classical key into a quantum state before proceeding to the next step.

For the preparation of the quantum state of the classical data, the simplest method is to use a quantum circuit that refers to the actual classical data to prepare state-specific qubits. Here, we will provide a code example for quantum preparation of classical data of length 8 (the program is implemented based on the Qiskit platform). As Fig. 9 shows, it illustrates how we prepare the quantum key. In order to better explain Sec. III A, we specifically divide the preparation of quantum keys into the following steps: Here, we assume that the size of the NCQI image prepared earlier is $2^n \times 2^n$, and we denote this image by I.

Step 1: According to the size of the image (assuming $M = 2^n$), we use the hyper 5D chaotic system to prepare the key. Since the storage of NCQI images is based on qubits, the key length we need to generate is not determined solely by the number of qubits used in NCQI but rather by "the number of times it should be processed." That is, for $2n$ qubits, each qubit actually encodes two pieces of information, which ensures that $2n$ qubits can represent an image of size $M \times M$. Based on this, we actually need to process these qubits multiple times. For example, suppose we have one qubit, and we initially have a bit-length key that can only process that qubit once. However, by transforming the qubit through the quantum circuit, it can carry another kind of information, so we need to process it again. In other words, the length of the key we need to encrypt an NCQI image does not refer to the number of qubits used by the NCQI model but rather to the total number of encryption bits required for the classical image representation. Where Arnold's transformation is utilized to perform the initial encryption of the interactive pixel position operation,

specifically, the exchange of physical positions $|x\rangle|y\rangle$ of each pixel of the image is controlled by x_1, and x_2 serves as the key to implement the quantum cyclic shift transformation of the color qubits associated with each pixel of the image (this shift operation can be implemented using quantum SWAP gates), essentially effecting the exchange of the positions within the underlying bit sequence. Applying quantum Arnold transform for position exchange necessitates that x_1 specifies the number of times the adder-mod 2^n module is executed. Similarly, using the SWAP gate to shift qubits requires x_2 to dictate the number of times the SWAP operation is executed within each individual pixel's color bit sequence. Since the generation of each state quantity in the chaotic system is homomorphic, we select the size of the longest key as the number of iterations of the chaotic system to obtain the encryption key required. Here, the former approach only requires one data point, whereas the latter necessitates $m \times m \times 3$ data points (given that the image size is $m \times m$, and each pixel has three channels. We need to cyclically shift the qubit sequence in each channel, with a different number of shifts each time, and append a quantum adder after the shift to complicate the color value transformation of the pixel further). For the rotational encryption of pixel color information, we need to utilize three keys, each of length $m \times m \times 8$ (as the color of each channel is rotationally encrypted separately, the length of the qubit sequence storing the color of each channel is 8, and there are a total of $m \times m$ pixels). Comparing the sizes of these required key lengths and referring to the length of the longest key as the number of iterations of the chaotic system, we can see that we need to iterate the hyper 5D chaotic system $m \times m \times 8$ times to generate all the required keys.

Step 2: By iterating the chaotic system, we obtain five keys of appropriate size. However, the values of these keys are generated by the chaotic system, and some of them may not be suitable for our encryption operation or easy to prepare as quantum states. Therefore, we need to transform these original keys numerically before preparing them in a quantum state. During the examination of the chaotic system, we can find that, in fact, most of these values are floating-point numbers with small magnitudes, and these numbers exhibit irregular transformations. In order to make reasonable use of these data, we convert them into integers and then perform modular calculations so that they can be used as encryption data (to make these values more suitable for encryption, we perform modulo 255 operations on them here). The processed x_3, x_4, and x_5 also require modulo 2 processing to convert them into numbers that are either 0 or 1, and then we add 1 to them, meaning they become datasets that contain either 1 or 2. These are then multiplied by $\frac{\pi}{2}$ so that x_3, x_4, and x_5 become random sequences, each containing only the values $\frac{\pi}{2}$,π within its sequence. These random angles will be used as keys to input the quantum rotation gate, in order to realize the rotational encryption of the pixel color information bits. x_1 and x_2 will be used as the number of quantum Arnold transform exchanges and the number of cyclic shifts, respectively, to achieve the initial encryption.

Step 3: Given that the keys generated in step 2 are still essentially of the classical nature, they cannot be directly applied for the efficient operation of quantum circuits. Therefore, in step 3, our core task is to skillfully transform these classical keys into quantum keys.

C. Encryption of NCQI images

Through the above process, we have obtained a quantum color image represented by NCQI and the quantum key necessary for encryption. Next, we will use this key to encrypt the image,

Step 1: We will first apply the x_1 key to perform a quantum Arnold transform on the pixel position information of the NCQI image.

$$\begin{aligned} A(|I\rangle) &= \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}|R_7\cdots R_0G_7\cdots G_0B_7\cdots B_0\rangle \otimes A(|x\rangle|y\rangle) \\ &= \frac{1}{2^n}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}|R_7\cdots R_0G_7\cdots G_0B_7\cdots B_0\rangle \otimes |x_A\rangle|y_A\rangle. \end{aligned} \quad (7)$$

Among them,

$$\begin{aligned} |x_A\rangle &= A(|x\rangle) = |x+y\rangle mod 2^n, \\ |y_A\rangle &= A(|y\rangle) = |x+2y\rangle mod 2^n. \end{aligned} \quad (8)$$

As you can see from the above formula, the quantum Arnold transform for positional information actually uses key x_1 to give the Arnold transform a number of iterations to control quantum-mod 2^n [in order to make sure that the coordinate mapping of the Arnold transform remains valid in the image domain, we introduce the mod 2^n operation to make sure that the transformed pixel coordinates (x_A, y_A) are strictly confined to the integer interval of $[0, 2^n - 1]$]. The quantum circuit diagram for encrypting the location information of NCQI images using the quantum Arnold transform is presented in Fig. 10.

Step 2: Use the x_2 key to encrypt the pixel internal information with a quantum cyclic transform. Specifically, we first extract the internal color information of each pixel by channel, represented as $|R_7, \cdots, R_0\rangle$, $|G_7, \cdots, G_0\rangle$, and $|B_7, \cdots, B_0\rangle$, respectively. We then perform a one-time circular shift operation on each color channel, with the shift length determined by the x_2 key.The length of x_2 is $m \times m \times 3$, divide it into three segments x_2', x_2'', x_2''', and use them to perform SWAP shift operation on $|R_7, \cdots, R_0\rangle$, $|G_7, \cdots, G_0\rangle$, and $|B_7, \cdots, B_0\rangle$, respectively; the number of shifts is provided by each bit in x_2', x_2'', x_2''' . After one shift, the color information is $|R_7', \cdots, R_0'\rangle$, $|G_7', \cdots, G_0'\rangle$, and $|B_7', \cdots, B_0'\rangle$, respectively, but the encryption effect obtained by only performing the shift transformation is not ideal. We continue to use x_2', x_2'', x_2''' and add them with the shifted color information (here, the result of the addition is never separated from the 8-bit quantum bits. It can be regarded as a mode 255 addition), and finally, the encrypted color information can be obtained. The process can be briefly described as follows: $C_{xy} = SWAP(C_{xy}, x_2) + x_2$ (C_{xy} denotes the color value at position (x,y) and x_2 is the key) by step2 will greatly displace the color information of the image. Figure 11 demonstrates how is a quantum circuit using SWAP with a quantum adder to implement cyclic encryption.

Step 3: Use the previously obtained keys x_3, x_4, and x_5 to rotate and encrypt the qubits of the R, G, and B channels of the

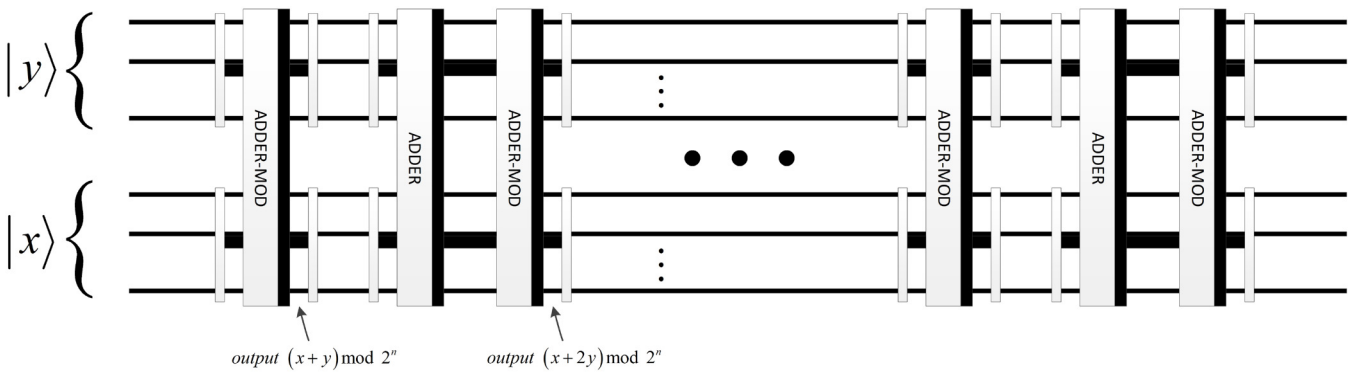


FIG. 10. Quantum circuit diagram of quantum Arnold transform encrypting NCQI image position information.

NCQI image. Define the quantum rotation gate as

$$R(\theta) = \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix}. \tag{9}$$

In fact, the quantum rotation gate is typically either a quantum X-rotation gate or a quantum Y-rotation gate. Referring to the Bloch sphere mentioned earlier, it can be observed that the state of the qubit will indeed change when the vector rotates around the X-axis or the Y-axis, whereas rotating around the Z-axis only affects the phase value. Consequently, the formula for quantum rotation encryption of each pixel in the NCQI image can be derived as follows:

$$\begin{cases} R_1 = \prod_{Y=0}^{y^n-1} \prod_{x=0}^{2^n-1} R_{Y\times R} \\ R_2 = \prod_{Y=0}^{2^2-1} \prod_{x=0}^{2^n-1} R_{Y\times G} \\ R_3 = \prod_{Y=0}^{2^n-1} \prod_{x=0}^{2^n-1} R_{Y\times B}, \end{cases} \tag{10}$$

where

$$\begin{cases} R_{YXR} = (I^{\otimes 8}) \sum_{j=0;i=0}^{2^n-1} \sum_{ji\neq YX}^{2^n-1} |ji\rangle\langle ji| + {R_{YXR}}' \otimes |YX\rangle\langle YX| \\ R_{YXG} = (I^{\otimes 8}) \sum_{j=0;i=0}^{2^n-1} \sum_{ji\neq YX}^{2^n-1} |ji\rangle\langle ji| + {R_{YXG}}' \otimes |YX\rangle\langle YX| \\ R_{YXB} = (I^{\otimes 8}) \sum_{j=0;i=0}^{2^n-1} \sum_{ji\neq YX}^{2^n-1} |ji\rangle\langle ji| + {R_{YXB}}' \otimes |YX\rangle\langle YX| \end{cases} \tag{11}$$

and

$$\begin{cases} {R_{YXR}}' = \otimes_{i=0}^{7} R_{YX}^1 \\ {R_{YXG}}' = \otimes_{i=0}^{7} R_{YX}^2 \\ {R_{YXB}}' = \otimes_{i=0}^{7} R_{YX}^3. \end{cases} \tag{12}$$

In the formula, R_{YX}^1, R_{YX}^2, and R_{YX}^3 correspond to $R((x3, i))$, $R((x4, i))$, and $R((x5, i))$, respectively, where $(x3, i)$ represents the selection of the ith bit of x_3. In this manner, we have achieved the rotation encryption of the color of each channel for each pixel. Figure 12 depicts a quantum circuit diagram for implementing quantum rotation encryption, while Fig. 13 illustrates the overall encryption flowchart of the algorithm for encrypting NCQI images.

IV. DECRYPTION PROCESS

Upon examining the encryption process of NCQI images introduced earlier, we can discern that all operations involved in our encryption scheme are reversible. The various quantum gates employed in quantum computing are inherently unitary matrices. Quantum rotations, for instance, represent unitary transformations. Since unitary transformations are reversible, decrypting the encrypted image simply requires performing the inverse operation using the corresponding key.

V. SIMULATION

In this study, we built an experimental environment for encryption system simulation based on the Windows 10 operating system platform. This experimental environment uses a computer with stable performance, whose core configuration includes a processor with a main frequency of 2.4 GHz and 16 GB of DDR4 memory, which ensures the high efficiency and stability of data processing during the experiment. On the basis of this hardware, we used the Python programming language, combined with its rich scientific computing library, to carefully design and implement an efficient simulation framework for encryption systems. In this study, we chose to use a private dataset rather than a shared dataset based on the following considerations: First, the uniqueness of the private dataset ensures that we can conduct in-depth analysis for a

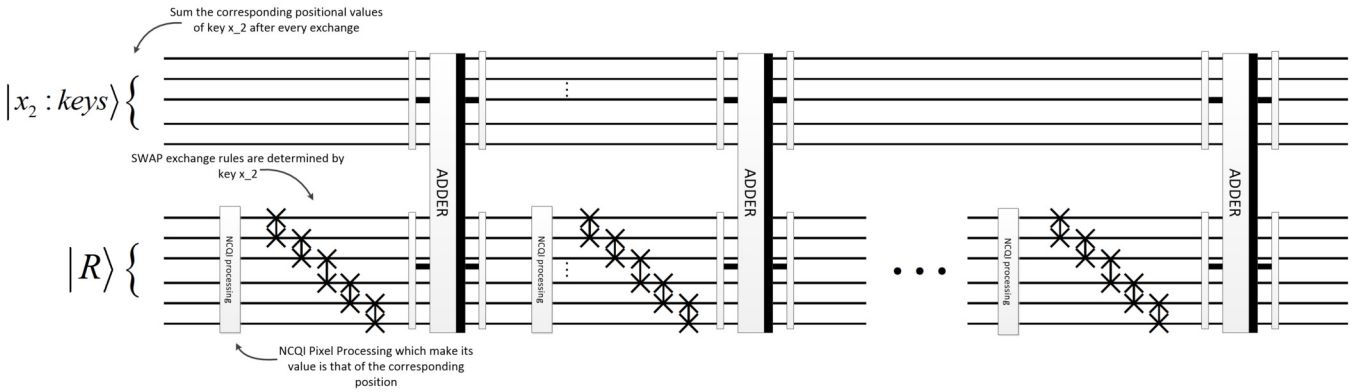


FIG. 11. Circular encryption quantum circuit diagram (since the algorithm strategies adopted for each color channel during the processing process are consistent, in order to maintain the simplicity and clarity of the image processing, this study will only provide a detailed description of a single color channel).

specific research question. Second, considering that the data may contain sensitive information, the use of private datasets helps to maintain the privacy of the research subjects and the confidentiality of the data. Therefore, we chose private datasets for our study.

Through carefully designed algorithms and simulation experiments, we selected four JPG color images with different visual features as the test set (as shown in Fig. 14) to comprehensively evaluate the effectiveness of the encryption technology. Experimental results show that this system-based encryption method exhibits excellent encryption performance: The encrypted image data achieve a high level of visual indistinguishability, exhibiting strong random distribution and complex textures, effectively blocking unauthorized information theft attempts, and significantly improving data security. At the same time, the decryption process also performs well, accurately restoring every detail of the original image. Both the overall visual effect and the local pixel-level information are highly consistent with the original image, without introducing any noticeable distortion or errors. This achievement not only validates the effectiveness of the encryption method in processing color image data but also underscores its application potential and reliability in digital image security. Furthermore, it opens up a novel avenue for exploring quantum security encryption technology, thereby verifying the applicability and reliability of this method specifically in color image encryption.

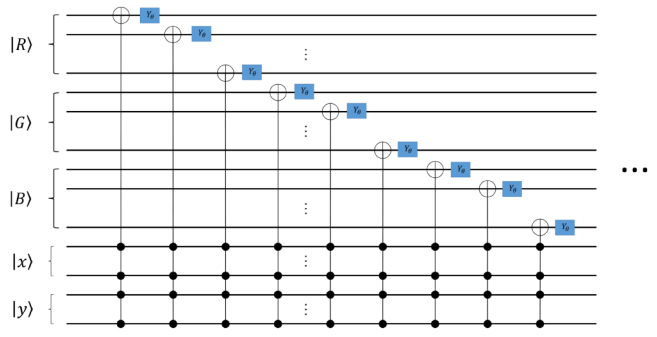


FIG. 12. Quantum circuit diagram for implementing quantum rotation encryption.

A. Keyspace analysis

Expanding the key space not only enhances the complexity and unpredictability of the keys but also effectively mitigates various security threats by significantly increasing the time, computing resources, or costs required for attackers to obtain the correct keys. Consequently, when designing an image encryption algorithm, we must prioritize the adoption of a mathematically robust key generation mechanism that ensures a sufficiently large and evenly distributed key space, thereby maximizing the algorithm's security threshold and safeguarding sensitive image data against unauthorized access

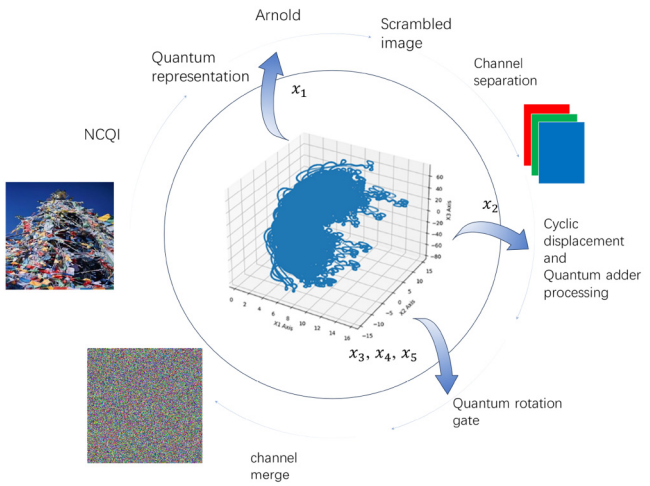


FIG. 13. Overall encryption process.

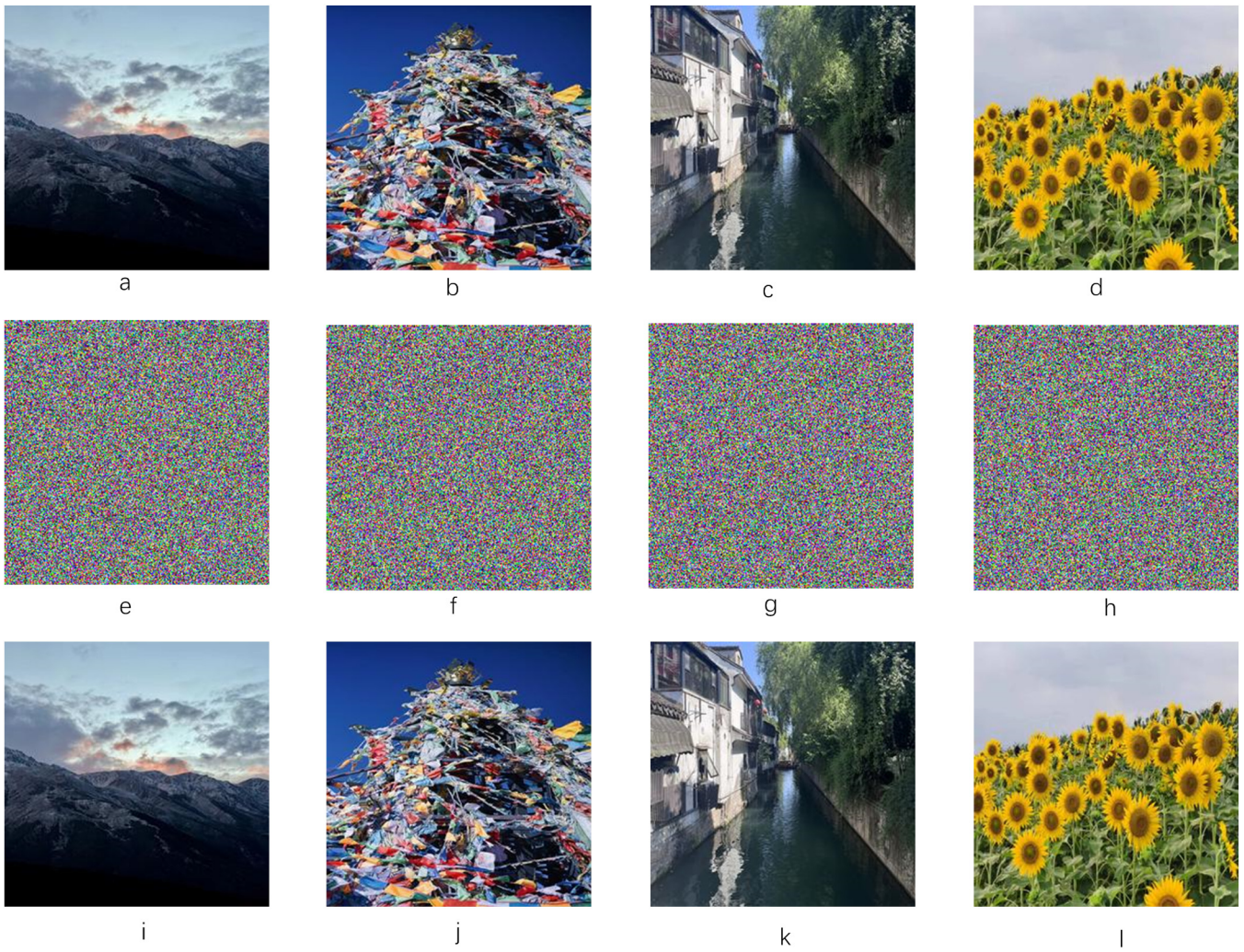


FIG. 14. It illustrates a comparison of images before and after encryption. The plaintext images are labeled as (a)–(d), while the corresponding ciphertext images are shown as (e)–(h). Furthermore, the decrypted images are presented as (i)–(l).

and tampering. This approach constitutes a crucial means of bolstering the overall security of the encryption system. For image encryption algorithms, the key space needs to reach the order of 2^{100} to effectively resist brute force attacks. In this scheme, the output of the random function serves as the input to the hyper 5D chaotic system, and the output of the hyper 5D chaotic system functions as the control key for the encryption process. Consequently, our key comprises the parameters a, b, c, d, e, along with the state variables x_1, x_2, x_3, x_4, x_5. Assuming an effective precision of 10^{14} for the parameters in the nonlinear chaotic system, combined with the experimental data presented in this paper, the key space of this image encryption algorithm can be calculated as $(10^{14})^5 = 10^{70}$, which significantly exceeds 2^{100}. Therefore, this scheme boasts a colossal key space, capable of withstanding brute force attacks and ciphertext-only attacks mounted by both classical computers and even quantum computers.

B. Complexity analysis

The computational complexity of this scheme comes from iterative quantum Arnold transform, quantum cyclic shifts, and quantum rotation gate operations. In the following, the control nongate is used as the base computational unit, and the computational complexity of this scheme is analyzed. One plaintext modulo 2^n adder requires $n-1$ rounding operations, n addition operations, and 1 quantum control nonoperation; thus, iterating the quantum Arnold transform requires $3(28n-12)i$ (i is the number of iterations of the quantum Arnold transform) computational units. The

computational complexity is $O(n)$. The quantum cyclic shift operation requires cyclic shifting of the three-channel color values at each position, which requires a total of $m \times m \times 8 \times 3 \setminus 2$ swap operations, and one swap operation requires three control nongates, i.e., it requires $m \times m \times 8 \times 3 \setminus 2 \times 3 = m \times m \times 36$ control nongate operations, and its time complexity is $O(n^2)$. The quantum revolving door operation is a different rotation operation for $m \times m \times 8 \times 3$ pixel values with a time complexity of $O(n^2)$. In summary, the total computational complexity of this scheme is only $O(n^2)$. For the classical image encryption algorithm, the 2D Arnold transform has a computational complexity of $O(2^{2n})$ just to perform i iterations. It can be seen that the proposed scheme has an exponential speed-up effect in terms of computational complexity compared to the classical image encryption algorithm. It shows that the present encryption algorithm has higher encryption efficiency.

C. Histogram analysis

Histogram analysis is one of the crucial methods for evaluating the security and effectiveness of encryption schemes. It exposes the statistical distribution of pixel values in an image through analysis, potentially offering avenues for attackers to exploit. During encryption, the histogram of a plaintext image often exhibits statistical patterns, such as uneven color distribution, that attackers might leverage for cryptanalysis. Consequently, to bolster encryption security, the histogram of the ciphertext image should strive for a uniform distribution, eradicating discernible statistical patterns.

As shown in Fig. 15, by comparing the histograms of the original and encrypted images, we can visually assess the effectiveness of the encryption technique. Ideally, the histogram of the encrypted image should present a uniform distribution to effectively obfuscate the image data. Observations show that the grayscale features of the original image disappear after encryption and are replaced by a uniform distribution, indicating that the encryption algorithm successfully destroys the color structure. Through quantitative analysis, we find that the histogram uniformity index of the encrypted image is close to the theoretical uniform distribution, confirming the effectiveness of the encryption algorithm in information obfuscation. Meanwhile, the encrypted image performs well in the

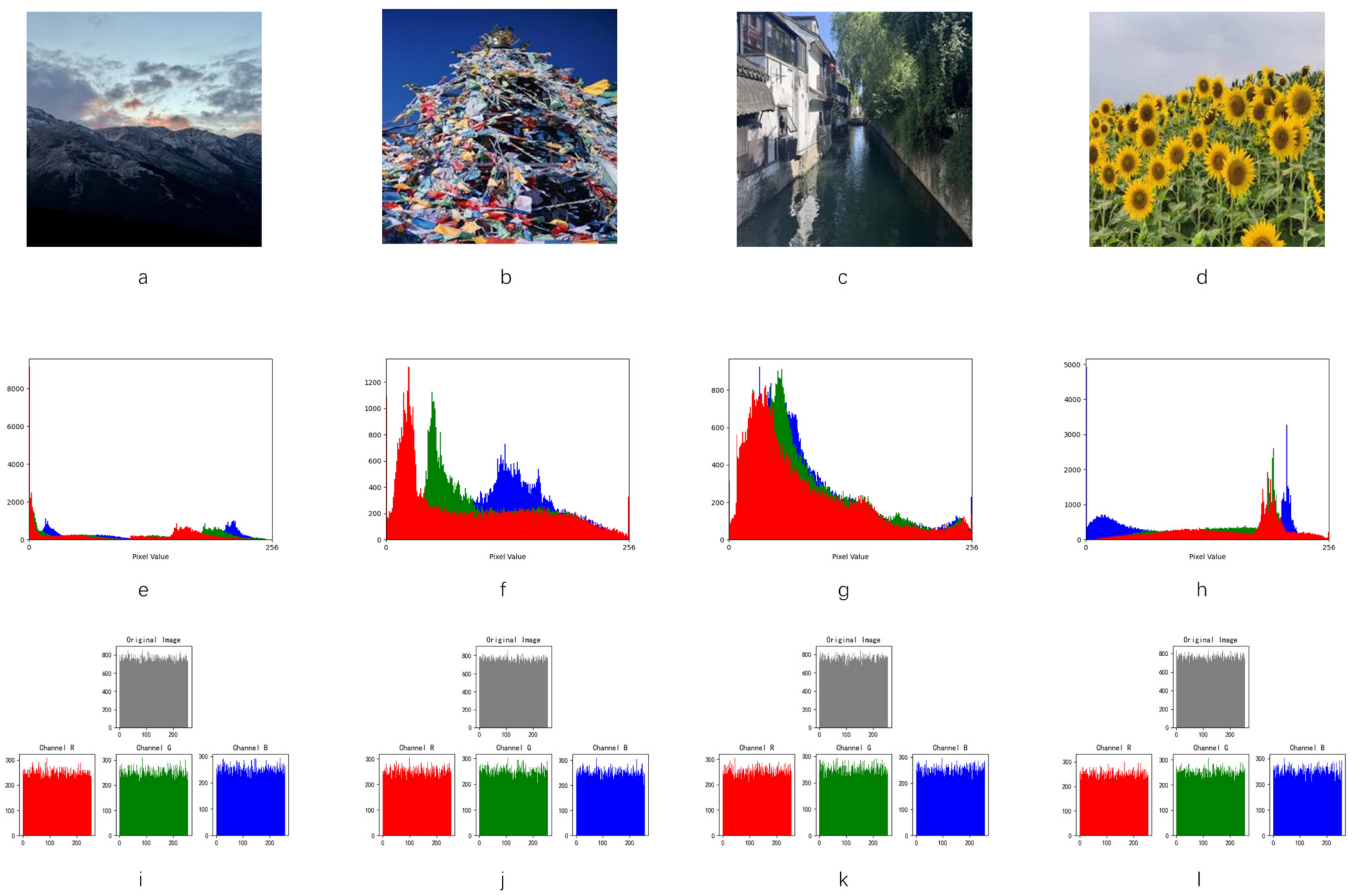


FIG. 15. Histograms comparison before and after encryption(a)–(d) are plaintext images and histograms before encryption are labeled as (e)–(h), while histograms after encryption are shown as (i)–(l).

anti-statistical analysis test, effectively resisting attacks such as histogram equalization and correlation analysis. In summary, this encryption algorithm performs excellently in protecting the original pixel information of the image, enhances image security, and establishes its status as a secure and efficient image encryption scheme.

D. Correlation coefficient analysis

Adjacent pixel correlation analysis, as a specialized technique, is dedicated to measuring the similarity and intrinsic correlation between image regions by precisely calculating and analyzing the correlation among adjacent pixels within the image. However, efficient encryption algorithms effectively weaken this inherent correlation pattern by cleverly disrupting the original layout and values of pixels. Hence, the substantial decrease in correlation among adjacent pixels in the encrypted image serves as a tangible indicator of the encryption algorithm's superior performance and heightened security capabilities. Ideally, the encrypted image should exhibit a correlation coefficient close to zero, indicating minimal exploitable statistical dependence between pixel values. The correlation coefficient, which quantifies the degree of linear relationship between pixel values, is formally defined as follows:

$$R_{xy} = \frac{E[x - E(x)]E[y - E(y)]}{\sqrt{D(x)D(y),}} \tag{13}$$

where $E(x)$, $E(y)$, $D(x)$, and $D(x)$ represent the expectations and variances of x and y, respectively (where x and y represent pixel values). To ensure the security of image encryption, the encryption algorithm must eliminate the condition where the correlation coefficients of adjacent pixels in the original image approach 1 in the horizontal, vertical, and diagonal directions. The encryption algorithm should reduce the correlation between adjacent pixels in all directions of the encrypted image to mitigate the risk of attackers exploiting adjacent pixel correlations to crack the image. We will perform an in-depth data analysis of the neighboring pixels of an image in three key directions: Horizontal, vertical, and diagonal. By comparing the correlation of neighboring pixels in these three directions before and after encrypting the image, we can accurately assess the significance of the encryption effect and the effectiveness of the encryption algorithm. As shown in Fig. 16, this figure visualizes the results of the adjacent pixel correlation analysis of the image before and after encryption. In the original image, neighboring pixels show a high degree of correlation in the horizontal, vertical, and diagonal directions, strongly proving the close interdependence between pixels inside the original image. In contrast, the encrypted image exhibits completely different characteristics: in all directions, the correlation between neighboring pixels is significantly reduced to almost zero, indicating that the encryption algorithm effectively destroys the original dependencies between pixels. The evaluation criteria we use to assess the encryption effect are as follows: First, the degree of correlation reduction, to assess the magnitude of correlation reduction between neighboring pixels in the encrypted image, ideally reducing the correlation to almost zero; second, destruction of pixel dependency, where the encryption algorithm should eliminate the interdependencies between pixels in the original image, thereby ensuring the randomness of the encrypted image. We first calculated the pixel correlation coefficients between the original and encrypted images in three directions. Then, we compared the changes in these coefficients and found that the correlation coefficients of the encrypted image are much lower than those of the original image, indicating that the encryption algorithm effectively reduces the correlation between pixels. This observation strongly verifies the close interdependence between pixels within the original image. In contrast, the encrypted image presents a completely different picture: In all directions, the correlation between adjacent pixels is significantly reduced to an extremely low level, almost reaching an irrelevant state. This significant change not only demonstrates the encryption

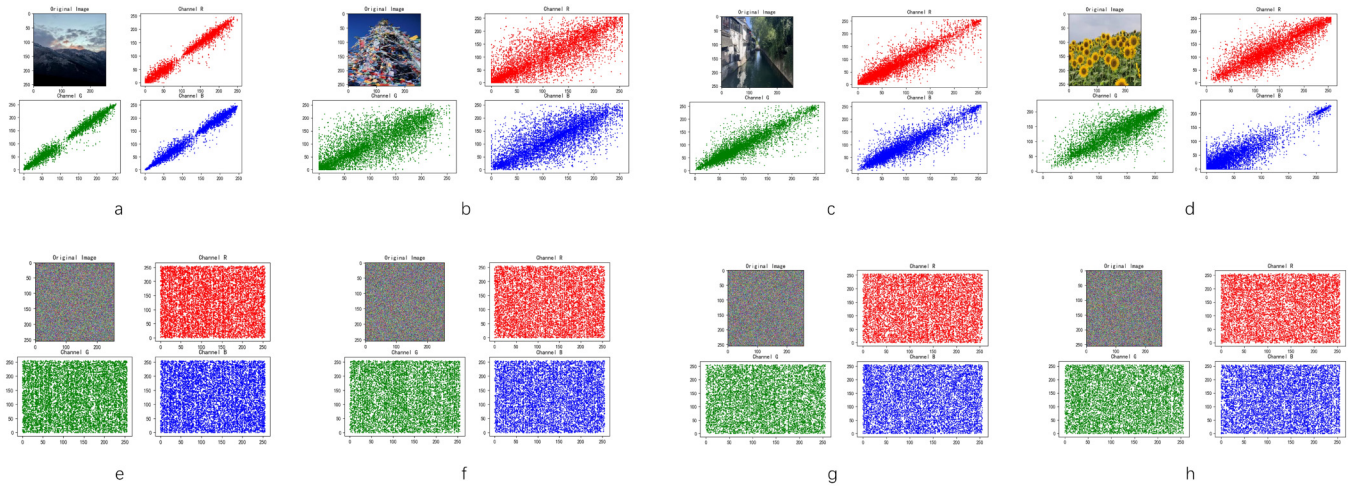


FIG. 16. Correlation analysis of neighboring pixels of images before and after encryption [(a)–(d) represent the correlations of adjacent pixels before encryption, while (e)–(h) correspond to the correlations of adjacent pixels after encryption].

TABLE I. Correlation analysis of adjacent pixels in each direction before and after encryption.

	Explicit			Ciphertext		
Image	H	V	D	H	V	D
Mountain	R:0.9966	R:0.9927	R:0.9928	R:−0.0338	R:−0.0049	R:0.0146
	G:0.9971	G:0.9934	G:0.9928	G:−0.0206	G:−0.0022	G:0.0074
	B:0.9972	B:0.9934	B:0.9927	B:−0.0136	B:−0.0218	B:0.0040
Banner	R:0.9100	R:0.8402	R:0.8251	R:−0.0043	R:0.0233	R:−0.0364
	G:0.8622	G:0.7729	G:0.7358	G:−0.0220	G:0.0197	G:−0.0096
	B:0.8555	B:0.7333	B:0.7003	B:0.0400	B:−0.0155	B:−0.0109
Streams	R:0.9352	R:0.9546	R:0.9217	R:−0.0060	R:−0.0272	R:0.0077
	G:0.9302	G:0.9487	G:0.9054	G:0.0116	G:0.0165	G:−0.0052
	B:0.9284	B:0.9485	B:0.9089	B:−0.0144	B:0.0038	B:0.0094
Sunflower	R:0.8989	R:0.9350	R:0.8702	R:0.0272	R:−0.0054	R:0.0134
	G:0.8842	G:0.9141	G:0.8324	G:0.0044	G:−0.0295	G:0.0117
	B:0.9704	B:0.9774	B:0.9582	B:−0.0130	B:0.0001	B:−0.0088
Lena	R:0.9549	R:0.9761	R:0.9317	R:0.0139	R:0.0070	R:0.0144
	G:0.9351	G:0.9653	G:0.9077	G:0.0210	G:0.0083	G:0.0009
	B:0.9226	B:0.9505	B:0.8952	B:0.0090	B:−0.0064	B:−0.0005

algorithm's excellent ability to disrupt the image information structure but also verifies its success in converting the original image into a series of random, disordered, and difficult-to-parse data sequences, thereby greatly enhancing the image's data security and confidentiality. For the specific data comparison of the correlation analysis of adjacent pixels in each direction before and after encryption using this method, please refer to Table I.

E. Plaintext sensitivity analysis

Image plaintext sensitivity analysis aims to evaluate the content of an unencrypted original image, determining the extent of sensitive information it contains and assessing the potential risk of leakage. In the context of encrypted images, this analysis compares ciphertext images generated from plaintext images encrypted with the same key but having only slight differences. The purpose is to evaluate the sensitivity of the encryption algorithm to small changes in the plaintext. This analysis is a crucial tool for assessing the security of encryption algorithms. A secure encryption algorithm should exhibit extreme sensitivity to minor alterations in the plaintext, ensuring that even slight changes result in significant differences in the ciphertext output. Plaintext sensitivity is typically evaluated using two quantitative indicators: NPCR (Number of Pixels Change Rate) and UACI (Unified Average Change Intensity). NPCR measures the ratio of grayscale value changes between the corresponding pixels in two encrypted images, while UACI quantifies the average magnitude of these changes. Assuming P_1 and P_2 are two plaintext images differing only in the grayscale value of a single pixel at coordinate (i, j), let $C_1(i, j)$ and $C_2(i, j)$ represent the encrypted pixel values of P_1 and P_2 at that coordinate, respectively. The calculation formulas for these indicators are as follows:

TABLE II. Image plaintext sensitivity analysis table.

Image	NPCR	UACI
Lena	R:99.57%	R:33.00%
	G:99.60%	G:30.53%
	B:99.62%	B:27.47%
Mountain	R:99.64%	R:36.22%
	G:99.64%	G:36.92%
	B:99.57%	B:36.26%
Sunflower	R:99.61%	R:31.15%
	G:99.64%	G:29.66%
	B:99.60%	B:37.92%

$$NPCR = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} D(i, j) \times 100\%, \tag{14}$$

$$UACI = \frac{1}{M \times N} \sum_{i=1}^{M} \sum_{j=1}^{N} \frac{|C_1(i, j) - C_2(i, j)|}{255} \times 100\%, \tag{15}$$

$$D(i, j) = \begin{cases} 0, C_1(i, j) = C_2(i, j) \\ 1, C_1(i, j) \neq C_2(i, j). \end{cases}$$

Evaluation Criteria: NPCR: This metric measures the percentage of pixels that have changed between the original and encrypted images. The higher the NPCR value, the higher the plaintext sensitivity. UACI: This metric evaluates the average intensity change of the pixels between the original and encrypted images.The higher the UACI value, the more pronounced the change in pixel values, which is ideal for encryption. Specific result analysis procedure: We performed plaintext sensitivity testing by encrypting multiple test images and comparing the encrypted output with the original

image. We calculated the NPCR and UACI of each test image to quantify the degree of change brought about by the encryption process. The calculated NPCR and UACI values are then compared with the theoretical ideal values, which are 99.6094% for NPCR and 33.4635% for UACI. As shown in Table II, the NPCR and UACI results of our cryptosystem are very close to these theoretical values, showing a high degree of sensitivity to plaintexts. This consistency suggests that even a small change in the plaintext can lead to a significant change in the ciphertext, which is crucial for defending against cryptographic attacks (e.g., chosen-plaintext attacks and known-plaintext attacks).

F. Information entropy

In the evaluation of image encryption technology, image encryption information entropy plays a crucial role. It is a quantitative indicator used to measure the randomness of the pixel values in the encrypted image. In image encryption specifically, the level of encryption information entropy is directly related to the encryption strength of the image . When the encrypted image exhibits a higher information entropy value, it signifies that the distribution of pixel values is more random and unpredictable, which indicates that the encryption algorithm has effectively scrambled and disrupted the image, thereby enhancing its security. Consequently, image encryption information entropy not only furnishes an objective basis for assessing the security performance of image encryption algorithms but also constitutes a scientific criterion for determining the success of the encryption algorithm. Its calculation formula is as follows:

$$H(m) = -\sum_{i=0}^{2^n-1} p(\alpha_i) log_2\, p(\alpha_i), \tag{16}$$

where α_i denotes a pixel point in the image and $p(\alpha_i)$ is the probability of that pixel point appearing in the image, which can be calculated as $\sum_{i=0}^{2^n-1} p(\alpha_i)=1$. It can be seen that for a grayscale image, the maximum possible value of information entropy is $\log_2 256$, corresponding to an equal probability of each of the 256 possible pixel values, i.e., an ideal distribution where each pixel value appears with equal frequency. Table III compares the information entropy of the image before encryption, after encryption using the method proposed in this paper, and after encryption using other methods. Notably, the information entropy of the image after encryption by the present method is closer to its maximum possible value, indicating higher randomness and uncertainty in encrypting image data. Higher information entropy signifies a more even distribution of information in the data, thereby enhancing the resistance of the encrypted data to decryption methods, including brute force decryption.

TABLE III. Comparison of image information entropy after encryption.

Image	Ciphertext entropy
Lena	R:7.992
	G:7.991
	B:7.992
Mountain	R:7.997
	G:7.997
	B:7.997
Sunflower	R:7.997
	G:7.997
	B:7.997

G. Qiskit quantum noise test

In reality, qubits are often subjected to a diverse range of noise factors, including decoherence, mutual coupling, and quantum measurement errors, which can negatively impact the reliability and precision of quantum computing tasks. To better assess the quantum feasibility of our algorithm, we must subject it to quantum noise tests. Qiskit, an open-source quantum computing programming framework developed and maintained by IBM's quantum team, enables users to construct quantum circuits and employ various quantum computing techniques, including quantum noise functions designed to evaluate the resilience of quantum computing methods against interference. Qiskit boasts a comprehensive set of quantum noise functions, such as kraus_error, mixed_unitary_error, pauli_error, ReadoutError, and numerous other noise effects that may occur during quantum computing operations. The main quantum operations involved in encrypting a quantum image using this method can be divided into two parts. One is the quantum Arnold transform of the image information, which is actually exchanging positions of the qubits that contain the image information. This step typically does not introduce significant quantum noise. In addition, we also perform quantum gate encryption on the image information, which involves applying a unitary matrix transformation to the qubits that represent the image. Here, the mixed_unitary_error may occur, so we primarily test the encryption method for resilience against the mixed_unitary_error noise. The specific process involves first constructing the quantum circuit for the NCQI image based on the provided classical image information, then encrypting the image information using quantum gates, applying the mixed_unitary_error during each encryption step to simulate the quantum noise present in the algorithm execution, and finally, decrypting the image and comparing it with the original image to assess the impact of the noise. However, since a 256×256 color image contains a significant amount of information, the quantum circuit required to encode it as quantum information is also relatively complex, and current quantum computers available through Qiskit can only support up to 158-qubits. To address this challenge, we designed a method that first constructs a simplified quantum circuit for executing the quantum rotation process of this algorithm, based on the number of qubits required for the NCQI model of an RGB image of size 256 (an NCQI image of this size requires 40-qubits). Specifically, instead of initializing the full quantum state for this 40-qubit NCQI-structured quantum circuit, we utilize the state transformation probability of a subset of information (e.g., the 24-bit qubits encoding the color of a single pixel) as a proxy for the state transformation probability of the entire image. In other words, the encrypted rotational transformation of the image information undergoes probabilistic transformation due to the

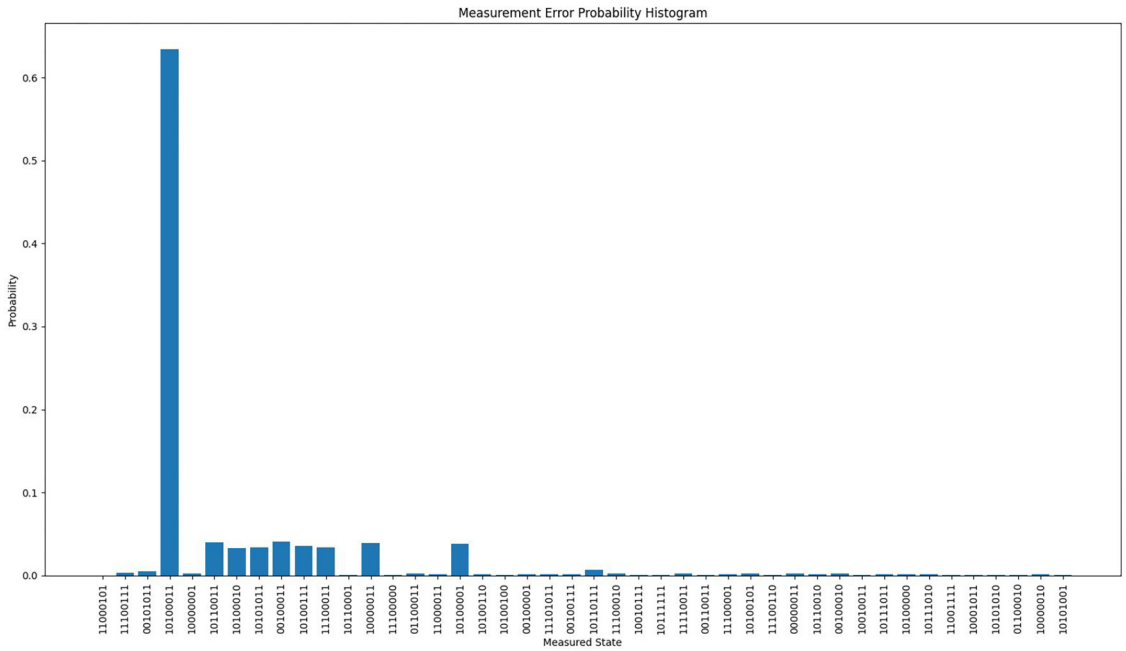


FIG. 17. A probability plot of the measurements for each quantum bit after the introduction of quantum noise.

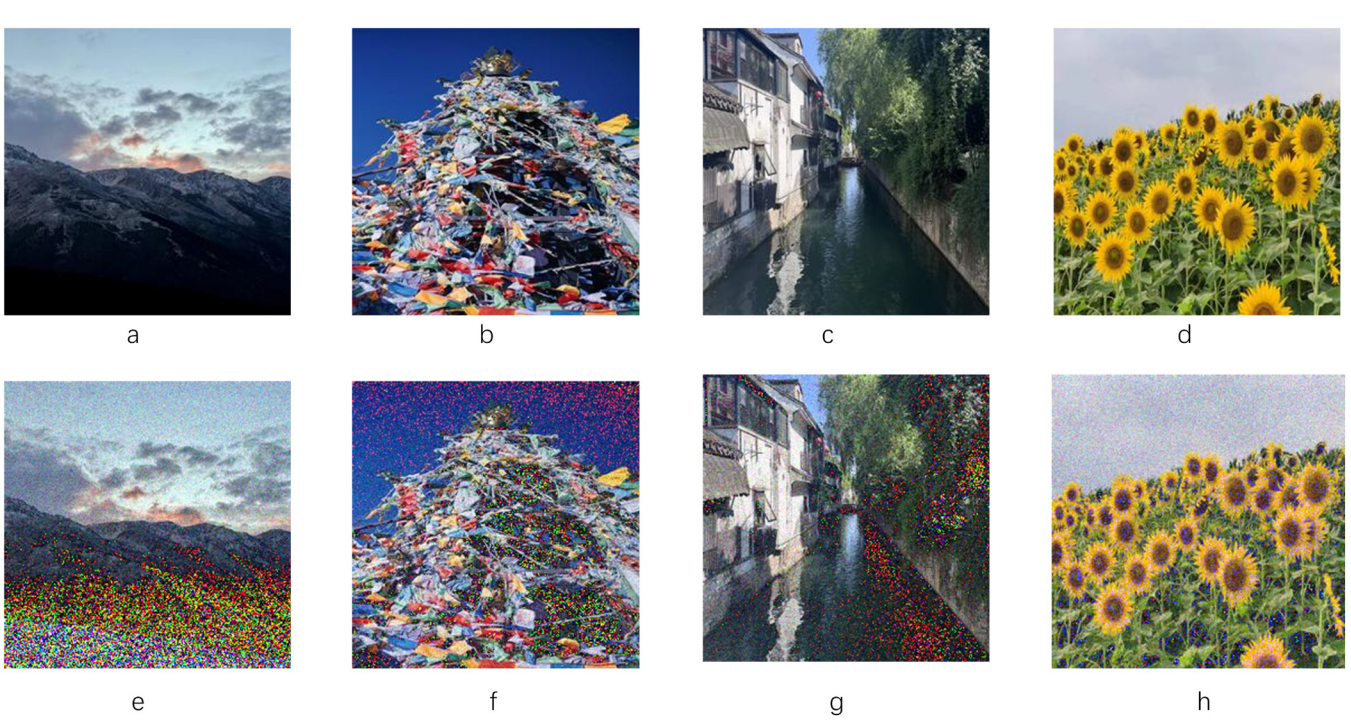


FIG. 18. Comparison of the result after encryption and decryption of the image affected by the noise of the mixed_unitary_error with the original image [the original image is (a)–(d); the image after encryption and decryption of the noise is (e)–(h)].

mixed_unitary_error noise affecting the quantum circuit's output. The resulting probability is then employed to determine the potential state transitions of each pixel in the decrypted image, which is ultimately obtained under the influence of this noise. Figure 17 shows a probability plot of the measurements for each quantum bit after the introduction of quantum noise, while Fig. 18 showcases the decrypted image, affected by the mixed_unitary_error noise, alongside the original image for comparison. It is evident that, despite the presence of noise, the decrypted image retains discernible image information, albeit with some inevitable color distortion. Specifically, in preparing the qubit sequence bits $|101\,00011\rangle$, we observed that, following the You matrix transformation and subsequent data restoration, there is a risk of measurement error. Through numerous repetitive operations and measurements, we accurately obtained an output probability of 0.649, which we utilized as the probability of randomly assigning the correct pixel value to the complete image, perturbed by the noise, to generate Fig. 18. This experiment underscores the quantum noise resistance of our proposed method.

VI. CONCLUSION

In this study, we propose an innovative quantum image encryption scheme that incorporates NCQI-model patterns, quantum Arnold transforms, ultra-five-dimensional chaotic systems, and quantum rotation gate operations. By utilizing sequences generated by a five-dimensional hyperchaotic system, we provide precise control for the execution of quantum Arnold transforms, cyclic shifts, and quantum rotation gates. In addition, the high-dimensional nature of the system significantly enhances the complexity of the key, thereby greatly broadening the key space. The use of this quantum image encryption technique significantly increases the information entropy of the encrypted image, further strengthening the robustness of the encryption. However, it is worth noting that the quantum Arnold transform and the ultra-five-dimensional chaotic system may introduce higher computational complexity, which may result in longer processing times for encryption and decryption. Furthermore, the practical application of quantum encryption algorithms relies on high-performance quantum computers, which may not yet be widely available, given the current state of technology. Therefore, the widespread application of this technology awaits the development of related hardware.

ACKNOWLEDGMENTS

This work was supported by the Open Fund of Advanced Cryptography and System Security Key Laboratory of Sichuan Province (Grant No. SKLACSS–202208), the Science and Technology Research Program of Chongqing Municipal Education Commission (Grant no. KJZD-M202000501), sponsored by The Natural Science Foundation of Chongqing (No. CSTB2023NSCQ-LZX0139) and the National Natural Science Foundation of China (No. 61772295).

AUTHOR DECLARATIONS

Conflict of Interest

The authors have no conflicts to disclose.

Author Contributions

All authors contributed to the study conception and design. Y.D. provided fund support, L.L. conceptualized experiments and wrote the manuscript, and C.Y. performed verification. L.L. and C.Y. are co-first authors with equal contributions. All authors read and approved the final manuscript.

Lishi Liu: Conceptualization (equal); Writing – original draft (equal); Writing – review & editing (equal). **Chenhao Yin:** Validation (equal); Visualization (equal). **Yumin Dong:** Funding acquisition (equal).

DATA AVAILABILITY

The data that support the findings of this study are available from the corresponding author on reasonable request.

REFERENCES

[1]Y. Zhang, C. Li, Q. Li, D. Zhang, and S. Shu, "Breaking a chaotic image encryption algorithm based on perceptron model," Nonlinear Dyn. **69**, 1091–1096 (2012).
[2]C. Li, Y. Liu, T. Xie, and M. Z. Chen, "Breaking a novel image encryption scheme based on improved hyperchaotic sequences," Nonlinear Dyn. **73**, 2083–2089 (2013).
[3]S. Noshadian, A. Ebrahimzade, and S. J. Kazemitabar, "Breaking a chaotic image encryption algorithm," Multimed. Tools Appl. **79**, 25635–25655 (2020).
[4]T. Xie, Y. Liu, and J. Tang, "Breaking a novel image fusion encryption algorithm based on DNA sequence operation and hyper-chaotic system," Optik **125**, 7166–7169 (2014).
[5]N. R. Zhou, T. X. Hua, L. H. Gong, D. J. Pei, and Q. H. Liao, "Quantum image encryption based on generalized Arnold transform and double random-phase encoding," Quantum Inf. Process. **14**, 1193–1213 (2015).
[6]R.-G. Zhou, Q. Wu, M.-Q. Zhang, and C.-Y. Shen, "Quantum image encryption and decryption algorithms based on quantum image geometric transformations," Int. J. Theor. Phys. **52**, 1802–1817 (2013).
[7]Y.-G. Yang, J. Tian, H. Lei, Y.-H. Zhou, and W.-M. Shi, "Novel quantum image encryption using one-dimensional quantum cellular automata," Inf. Sci. **345**, 257–270 (2016).
[8]N. Zhou, W. Chen, X. Yan, and Y. Wang, "Bit-level quantum color image encryption scheme with quantum cross-exchange operation and hyper-chaotic system," Quantum Inf. Process. **17**, 137 (2018).
[9]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 Inf. Process. **16**, 164 (2017).
[10]T. Hua, J. Chen, D. Pei, W. Zhang, and N. Zhou, "Quantum image encryption algorithm based on image correlation decomposition," Int. J. Theor. Phys. **54**, 526–537 (2015).
[11]X.-H. Song, S. Wang, A. A. Abd El-Latif, and X.-M. Niu, "Quantum image encryption based on restricted geometric and color transformations," Quantum. Inf. Process. **13**, 1765–1787 (2014).
[12]M. Zhu and C. Wang, "A novel parallel chaotic system with greatly improved Lyapunov exponent and chaotic range," Int. J. Modern Phys. B **34**, 2050048 (2020).
[13]C. Wang, C. Fan, and Q. Ding, "Constructing discrete chaotic systems with positive Lyapunov exponents," Int. J. Bifurc. Chaos **28**, 1850084 (2018).
[14]P. Zhou, K. Huang, and C.-D. Yang, "A fractional-order chaotic system with an infinite number of equilibrium points," Discrete Dyn. Nat. Soc. **2013**, 910189.
[15]A. Y. Vlasov, "Quantum computations and images recognition," arXiv:quant-ph/9703010 (1997).
[16]J. I. Latorre, "Image compression and entanglement," arXiv:quant-ph/0510031 (2005).

[17]S. E. Venegas-Andraca and J. L. Ball, "Processing images in entangled quantum systems," Quantum Inf. Process. **9**, 1–11 (2010).
[18]P. Q. Le, A. M. Iliyasu, F. Dong, and K. Hirota, "A flexible representation of quantum images for polynomial preparation, image compression and processing operations, quantum inf," Quantum Inf. Process. **10**, 63–84 (2011).
[19]Y. Zhang, K. Lu, Y. Gao, and M. Wang, "NEQR: A novel enhanced quantum representation of digital images," Quantum Inf. Process. **12**, 2833–2860 (2013).
[20]J. Sang, S. Wang, and Q. Li, "A novel quantum representation of color digital images," Quantum Inf. Process. **16**, 42 (2017).
[21]W. Feng, Q. Wang, H. Liu, Y. Ren, J. Zhang, S. Zhang, K. Qian, and H. Wen, "Exploiting newly designed fractional-order 3D Lorenz chaotic system and 2D discrete polynomial hyper-chaotic map for high-performance multi-image encryption," Fractal Fractional **7**, 887 (2023).
[22]A. A. K. Javan, M. Jafari, A. Shoeibi, A. Zare, M. Khodatars, N. Ghassemi, R. Alizadehsani, and J. M. Gorriz, "Medical images encryption based on adaptive-robust multi-mode synchronization of chen hyper-chaotic systems," Sensors **21**, 3925 (2021).
[23]Y. Guo, S. Jing, Y. Zhou, X. Xu, and L. Wei, "An image encryption algorithm based on logistic-fibonacci cascade chaos and 3D bit scrambling," IEEE Access **8**, 9896–9912 (2020).
[24]H. Zhu, J. Ge, W. Qi, X. Zhang, and X. Lu, "Dynamic analysis and image encryption application of a sinusoidal-polynomial composite chaotic system," Math. Comput. Simul. **198**, 188–210 (2022).
[25]Z. Man, J. Li, X. Di, Y. Sheng, and Z. Liu, "Double image encryption algorithm based on neural network and chaos," Chaos, Solitons Fractals **152**, 111318 (2021).
[26]S. Vaidyanathan, "A new eight-term 3-D polynomial chaotic system with three quadratic nonlinearities," Far East J. Math. Sci. **84**, 219–226 (2014).
[27]W. Jie-Zhi, C. Zeng-Qiang, and Y. Zhu-Zhi, "The generation of a hyperchaotic system based on a three-dimensional autonomous chaotic system," Chin. Phys. **15**, 1216 (2006).
[28]Q. Yang and G. Chen, "A chaotic system with one saddle and two stable node-foci," Int. J. Bifurc. Chaos **18**, 1393–1414 (2008).
[29]S. Vaidyanathan, "A new six-term 3-D chaotic system with an exponential nonlinearity," Far East J. Math. Sci. **79**, 135–143 (2013).
[30]C. H. Chen, L. J. Sheu, H. K. Chen, J. H. Chen, H. C. Wang, Y. C. Chao, and Y. K. Lin, "A new hyper-chaotic system and its synchronization," Nonlinear Anal.: Real World Appl. **10**, 2088–2096 (2009).
[31]V. Ivashchuk and V. Melnikov, "Quantum billiards in multidimensional models with fields of forms," Grav. Cosmol. **19**, 171–177 (2013).
[32]M. Santhanam, S. Paul, and J. B. Kannan, "Quantum kicked rotor and its variants: Chaos, localization and beyond," Phys. Rep. **956**, 1–87 (2022).
[33]J. Eisert, M. Friesdorf, and C. Gogolin, "Quantum many-body systems out of equilibrium," Nat. Phys. **11**, 124–130 (2015).
[34]I. Rotter and J. Bird, "A review of progress in the physics of open quantum systems: Theory and experiment," Rep. Prog. Phys. **78**, 114001 (2015).
[35]S. J. Prakash, K. Rajagopal, and R. B. Krishna, "A new 5D hyperchaotic system with stable equilibrium point, transient chaotic behaviour and its fractional-order form," Pramana **91**, 1–10 (2018).
[36]K. Lata and L. R. Cenkeramaddi, "Deep learning for medical image cryptography: A comprehensive review," Appl. Sci. (2076-3417) **13**, 8295 (2023).
[37]K. Panwar, S. Kukreja, A. Singh, and K. Singh, "Towards deep learning for efficient image encryption," Procedia Comput. Sci. **218**, 644–650 (2023).
[38]H. Kiya, A. P. Maungmaung, Y. Kinoshita, S. Imaizumi, and S. Shiota, "An overview of compressible and learnable image transformation with secret key and its applications" (2022).
[39]I. Meraouche, S. Dutta, H. Tan, and K. Sakurai, "Neural networks based cryptography: A survey," IEEE Access **9**, 124727–124740 (2021).
[40]Z. Bao and R. Xue, "Survey on deep learning applications in digital image security," Opt. Eng. **60**, 120901 (2021).
[41]P. L. Chithra and R. Aparna, "Blockchain-based image encryption with spiral mapping and hashing techniques in dual level security scheme," Int. J. Inf. Comput. Secur. **21**, 185 (2023).
[42]Z. Feixiang, L. Mingzhe, W. Kun, and Z. Hong, "Color image encryption via Hénon-zigzag map and chaotic restricted Boltzmann machine over blockchain," Opt. Laser Technol. **135**, 106610 (2021).
[43]T. Kumari, D. Singh, and B. Singh, "Multi-chaotic maps and blockchain based image encryption," Concurr. Comput. Pract. Exp. **36**, e8092 (2024).