

Research Article

A Quantum Image Watermarking Scheme Based on Quantum Hilbert Scrambling and Steganography about the Moiré Fringe

Jian-Wei Jiang,¹ Tian Zhang,¹ Wei Li,¹ and Shu-Mei Wang ²

¹School of Information and Control Engineering, Qingdao University of Technology, Qingdao, China

²School of Science, Qingdao University of Technology, Qingdao, China

Correspondence should be addressed to Shu-Mei Wang; wangshumei@qut.edu.cn

Received 6 August 2022; Revised 20 November 2022; Accepted 11 February 2023; Published 7 March 2023

Academic Editor: Yubo Sheng

Copyright © 2023 Jian-Wei Jiang et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

In order to boost the security and confidentiality of information in quantum images, on the foundation of the NEQR model, a novel quantum watermarking scheme combining quantum Hilbert scrambling with steganography based on the Moiré fringe is designed in this paper. First of all, for carrier image, and watermark image, the color information and position information are denoted, respectively, by the NEQR model. Next, the watermark image is converted to a disordered image by quantum Hilbert scrambling, and the message of the original watermark image cannot be gained from the disordered image. At last, the watermark image after scrambling is embedded into the carrier image through the steganography of the Moiré fringe, obtaining the watermarked image. Due to the unitary image of the quantum gate, quantum Hilbert inverse scrambling is the opposite process of quantum Hilbert scrambling. In addition, the watermark image can be completely extracted from the watermarked image. What's more, the experimental simulation and performance analysis of the scheme are done. The experimental simulation proves the feasibility of this algorithm. Visually, there is no difference between the carrier image and the watermarked image. The PSNR between the watermarked image and the carrier image is measured, which quantitatively shows the high similarity. In addition, the time complexity of the quantum circuit is lower than some other quantum image watermarking schemes, which proves the simplicity of this scheme.

1. Introduction

As one of the main carriers of information transmission in modern society, images play a very important role in education, finance, and other fields. At present, protecting the security of image information is one of the research hotspots at home and abroad. The methods of protecting the secret image of an image are roughly divided into two categories: image watermarking [1–5] and image encryption [6–9]. Image watermarking is to embed the pixel data of the watermark image into the carrier image in a certain way, and there is no visual difference between the carrier image and the watermarked image, thus achieving the effect of hiding the watermark image. The essence of the image encryption is to change the value and position of the pixels in a certain method, and the message of the original image cannot be obtained in the encrypted image.

Quantum computing and quantum information have grown rapidly in recent years, guiding new directions for the development of many fields [10–13]. Of course, quantum computing has laid a solid foundation for the rise of quantum imaging. The principle of quantum imaging is to express the image with quantum state, thus bringing a new development direction for the field of image processing. As a result of some inherent characteristics of quantum computing, such as parallelism and entanglement, quantum image processing and performance will be incomparable with classical images. The main advantages of quantum images compared with classical images lie in fast computing speed, high security, and small storage space. After the quantum computer is produced in the future, quantum images can greatly improve people's production and life. Furthermore, the classical algorithm of image steganography has developed to a mature stage, while the related content of

quantum image steganography is very little. In the future, so as to protect greatly the security and confidentiality of information in quantum images, it will be necessary to develop quantum image steganography. First and foremost, we must understand how to store and express images in quantum computer. For the representation of quantum images, domestic and foreign scholars have proposed several methods: Real Ket [14], Qubit Lattice [15], FRQI [16], NEQR [17], MCQI [18, 19], and so on. Among them, the first four are applicable to grayscale images. In the MCQI model, the gray information of the RGB three channels of color image is represented by three entangled quantum states, respectively, extending the expression of grey images to color images. Among the above representation methods of the quantum image, the NEQR is the only one model in which the ground state of qubits is used to express the pixel value, while the probability amplitude of ground state is used to represent the pixel value in other models. Compared with other representation models, the NEQR has the advantage that it will not have the negative effect stem from the collapse of the quantum state during the measurement procedure. It is the most widely used representation model of quantum image now.

Nowadays, the steganography of quantum image is primarily based on frequency domain and spatial domain. The principle of the steganography based on frequency domain is to superimpose the watermark image's information on the frequency domain of carrier image, including quantum Fourier transform (QFT) [20, 21], and quantum wavelet transform (QWT) [22–25]. In 2013, Zhang et al. presented a steganography of quantum images on the foundation of the quantum Fourier transform. Firstly, the carrier image was processed by the quantum Fourier transform, and the watermark image's message was superimposed on the Fourier coefficients of the carrier image to achieve embedding process. There is no visual distinction between the watermarked image with the carrier image [26]. In 2019, on the basis of the FRQI model, Hu et al. put forward a quantum image steganography on the foundation of the Haar wavelet transform. The image is decomposed by the Haar wavelet transform. And the carrier image is decomposed to obtain its diagonal coefficient, and the

diagonal coefficient changes in the light of the information of watermark image, thus realizing the embedding process in the watermark image [27]. The representative algorithms of quantum image steganography based on the spatial domain include the least significant bit algorithm (LSB) [28–31] and the steganography on the basis of the Moiré fringe [32], which embed the message of the watermark image into the carrier image by changing the pixel value of the carrier image. In 2015, on the basis of NEQR, Jiang et al. designed a steganography of quantum images on the foundation of the Moiré fringes and quantum circuits. The processes of embedding and extraction in moiré gratings are achieved by quantum circuits [33]. In 2017, Heidari combined LSB with Gray code and hid two information qubits into the three lowest qubits in the color image by using Gray code, thus completing the embedding process of the watermark image [34].

On the foundation of the NEQR, a novel quantum image steganography combining quantum Hilbert scrambling [35] with information hiding about Moiré fringe is designed in this paper. The context of the article is as follows. The second part introduces the principle of NEQR, quantum Hilbert scrambling, and information hiding about the Moiré fringe. The third part introduces the specific operation process of the algorithm. The simulation experiment and performance analysis of the scheme are introduced in the fourth part. The conclusion is put at the end.

2. Related Work

2.1. NEQR. The NEQR model divides the representation of a quantum image into two sections, including the color information and the position information, and they are expressed by a quantum state, respectively. Therefore, the representation of the whole quantum image is the superposition of two quantum states. With regard to a quantum image of size $2^n \times 2^n$ and pixel value range $[0, 2^{q-1}]$, the color information needs to be represented by q qubits, while the representation of position information requires $2n$ qubits. Thus, the expression of the entire quantum image is as follows:

$$\begin{aligned}
 |P\rangle &= \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |C(X, Y)\rangle |XY\rangle \\
 &= \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} \otimes_{i=0}^{q-1} \otimes_{j=0}^{n-1} |\varphi_{XY}^i\rangle |X_j\rangle |Y_j\rangle, \\
 |C(X, Y)\rangle &= |\varphi_{XY}^0 \varphi_{XY}^1 \cdots \varphi_{XY}^{q-1}\rangle \varphi_{XY}^i \in \{0, 1, 2, \dots, q-1\}, \\
 |X\rangle &= |X_{n-1} X_{n-2} \cdots X_1\rangle |Y\rangle \\
 &= |Y_{n-1} Y_{n-2} \cdots Y_1\rangle |X_j\rangle, |Y_j\rangle \in \{0, 1\},
 \end{aligned} \tag{1}$$

where, $|C(X, Y)\rangle$ represent the color information and $|XY\rangle$ represent the position information.

2.2. Quantum Hilbert Scrambling. In 1870, the Hilbert curve was proposed by G. Peano, which was a special curve that could traverse all points in a set. Using the Hilbert curve for image pixel scrambling can achieve a good scrambling effect, and Hilbert scrambling comes from this. Applying Hilbert scrambling to a matrix M_n with size of $2^n \times 2^n$ can get scrambled matrix F_n . If the elements in F_n are connected in the order before scrambling, the Hilbert curve can be found. Figure 1 is the corresponding Hilbert curve when n takes value from 3 to 5.

The generation of the Hilbert matrix could be completed through step-by-step iteration. The generation iteration formula of the Hilbert matrix is as follows:

$$F_{n+1} = \begin{cases} \begin{pmatrix} F_n & (F_n + 4^n I_n)^T \\ (F_n + 3 \times 4^n I_n)^{PP} & (F_n + 2 \times 4^n I_n)^T \end{pmatrix}, n \text{ is odd,} \\ \begin{pmatrix} F_n & (F_n + 3 \times 4^n I_n)^{PP} \\ (F_n + 4^n I_n)^T & (F_n + 2 \times 4^n I_n)^T \end{pmatrix}, n \text{ is even,} \end{cases} \quad (2)$$

where $F_1 = \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}$, $I_n = \begin{pmatrix} 1 & 1 & \dots & 1 \\ 1 & \ddots & & 1 \\ \vdots & & \ddots & \vdots \\ 1 & 1 & \dots & 1 \end{pmatrix}$. If M_n is

a matrix of size $n \times n$, then M_n^T is the transposed matrix of M_n , and M_n^{PP} is obtained by rotating 180° around the center of M_n .

It can be known from the iterative formula generated by the Hilbert matrix that the Hilbert matrix starts from the initial matrix F_1 and alternately iterates according to whether n is odd or even. Therefore, the generation algorithm of the Hilbert matrix is divided into three parts: initialization, iterative process when n is odd, and iterative process when n is even. The generation iterative formula of the Hilbert matrix as the basis is used to rearrange all pixels of the watermark image in the algorithm of quantum Hilbert scrambling. When rearranging, the watermark image is split into subimages with a size of $2^t \times 2^t$, $t \in [1, n]$, and all image subblocks are rearranged according to the iterative principle of the Hilbert generating matrix. In the whole quantum image scrambling process, t gradually increases from 1 to n ; that is, the size of the image block increases with the raising of t , so the arrangement process of pixel points is divided into n times.

2.3. The Steganography of Quantum Image Based on Moiré Fringe. The steganography based on Moiré fringe comes from the Moiré effect. The Moiré effect is a special optical phenomenon that emerges when two dots or fringes with periodic characteristics are superimposed on each other. It is found that a new pattern will be generated when the two patterns are superimposed on each other under certain conditions. Based on the principle of the above

phenomenon, a scheme for the steganography of images based on Moiré fringe is proposed.

The algorithm of the steganography of the quantum image based on Moiré fringe can be split into three parts, including the embedding process, the denoising process, and the extraction process [31]. The embedding process is to embed the watermark image into the carrier image; the obtained carrier image after the embedding process can be called a prewatermarked image. If the watermark image is directly extracted from the prewatermarked image, the extracted watermark image contains much noise. The function of the denoising process is to remove the noise from the prewatermarked image in order to make sure that the extracted watermark image has no noise. The denoising process can be said to be the optimization process of a watermark image's embedding process. The final step is the extraction process.

3. The Specific Design of the Scheme

Based on the NEQR, a novel quantum image steganography combining quantum Hilbert scrambling with steganography based on the Moiré fringe is designed in this paper. The algorithm can be separated into two parts. One is the scrambling and restoration process of the quantum image based on the quantum Hilbert transformation. Another is the embedding and extraction process of the watermark image on the foundation of steganography which involves the Moiré fringe. Accordingly, quantum circuits are designed for each of the two sections. The principles and quantum circuit diagrams of the two parts are introduced below. The Figure 2 is flow chart of the whole scheme.

3.1. Quantum Circuit Module. According to the quantum Hilbert scrambling principle in Section 2.2, the scrambling process is divided into three parts including initialization, the iterative process when the time of iteration is odd and when the time of iteration is even. When designing quantum circuits for Hilbert scrambling of quantum images, three basic quantum circuit modules including module P , module O , and module E need to be used. The quantum circuit of the initialization is layout based on the module P ; the quantum circuit corresponding to the scrambling process when the time of iterations is odd is generated by the combination of the module P and the module O ; when the time of iterations is an even, the corresponding quantum circuit is generated by module P and module E . The functions and quantum circuit diagrams of the module P , module O , and module E are introduced in .

- (1) The module P can segment the quantum image and realize the generation iteration of the Hilbert matrix. The module P can divide a quantum image with the size of $2^n \times 2^n$ into $2^{n-t-1} \times 2^{n-t-1}$ (t is an integer, and $t \in [0, n-1]$) image subblocks with the size of $2^{t+1} \times 2^{t+1}$. The Figure 3 is the quantum circuit diagram corresponding to this part. The module P firstly swaps x_{n-t-2} and x_{n-t-3} , x_{n-t-3} and x_{n-t-4} , ..., x_1 and x_0 and finally swaps x_0 and y_{n-t-1} .

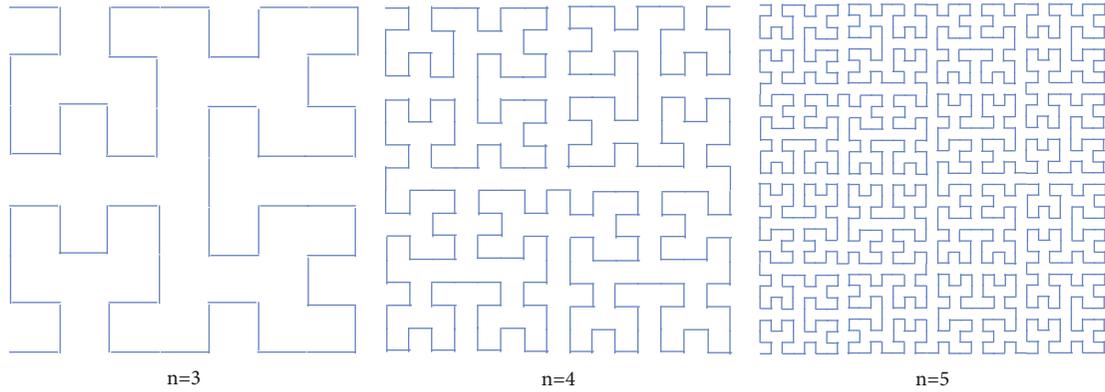


FIGURE 1: The Hilbert curve.

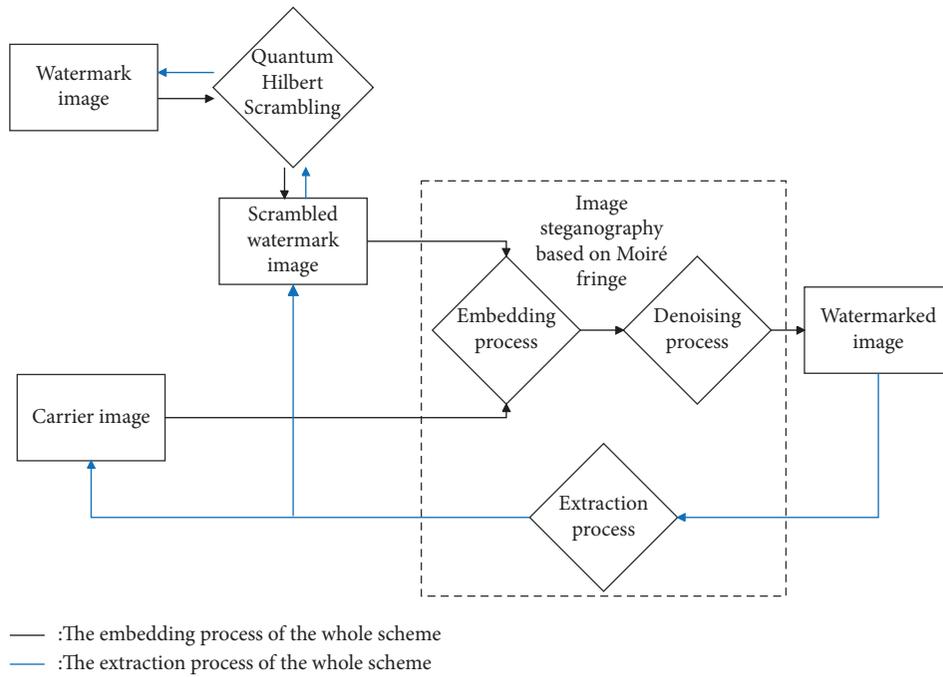


FIGURE 2: Flow chart of the algorithm.

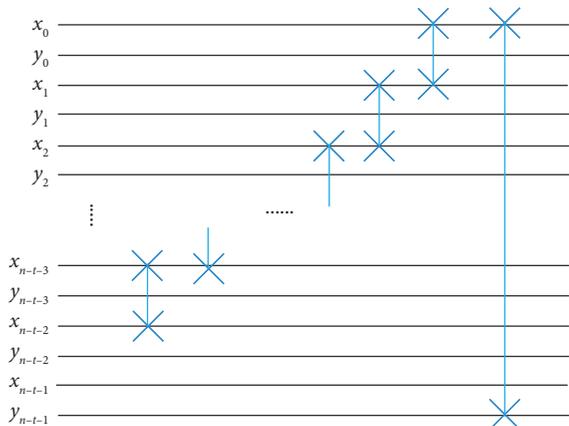


FIGURE 3: The quantum circuit diagram of module P.

- (2) The module O is for the case when the number of iterations is odd in the iterative process of the quantum Hilbert matrix. Assuming that W, X, Y and Z are all matrices of size $2^{t-1} \times 2^{t-1}$, the function of the module O is to convert $\begin{pmatrix} W & X \\ Y & Z \end{pmatrix}$ into $\begin{pmatrix} W & Z^{PP} \\ X^T & Y^T \end{pmatrix}$. The quantum circuit corresponding to this section is clearly demonstrated in Figure 4. Below are the specific quantum circuit process of the module O.
- (1) Swap x_{n-t-1} and y_{n-t-1} with SWAP gate, then add a CNOT gate, where x_{n-t-1} controls y_{n-t-1} .
 - (2) The controlled SWAP gate are used to swap x_{n-1} and y_{n-1} , x_{n-2} and y_{n-2} , ..., x_{n-t} and y_{n-t} , where the control qubit is y_{n-t-1} .

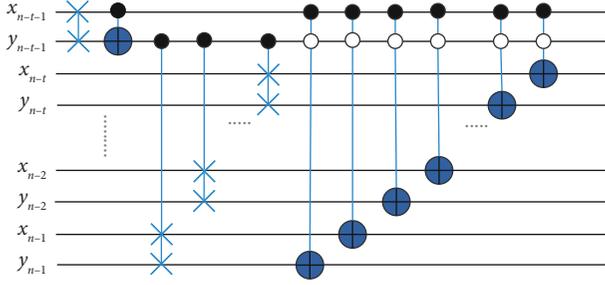


FIGURE 4: The quantum circuit diagram of module O.

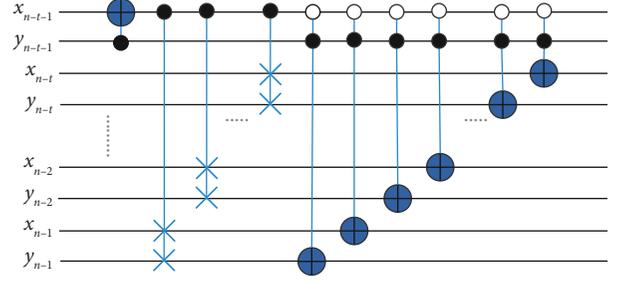


FIGURE 5: The quantum circuit diagram of module E.

- (3) The 2-qubit CNOT gate are used to flip $x_{n-1}, y_{n-1}, x_{n-2}, y_{n-2}, \dots, x_{n-t}, y_{n-t}$, where the control qubit is x_{n-t-1} and y_{n-t-1} .
- (3) The module E is for the case when the number of iterations is even in the iterative process of the quantum Hilbert matrix. Assuming that $W, X, Y,$ and Z are all matrices of size $2^{t-1} \times 2^{t-1}$, the function of the module O is to convert $\begin{pmatrix} W & X \\ Y & Z \end{pmatrix}$ into $\begin{pmatrix} W & X^T \\ Z^{PP} & Y^T \end{pmatrix}$. The Figure 5 is the quantum circuit diagram corresponding to this part. Below are the specific quantum circuit process of the module E.
 - (1) Add a CNOT gate, where y_{n-t-1} controls x_{n-t-1} .
 - (2) The controlled SWAP gate are used to swap x_{n-1} and y_{n-1}, x_{n-2} and y_{n-2}, \dots, x_{n-t} and y_{n-t} , where the control qubit is x_{n-t-1} .
 - (3) The 2-qubit CNOT gate are used to flip $x_{n-1}, y_{n-1}, x_{n-2}, y_{n-2}, \dots, x_{n-t}, y_{n-t}$, where the control qubit is x_{n-t-1} and y_{n-t-1} .

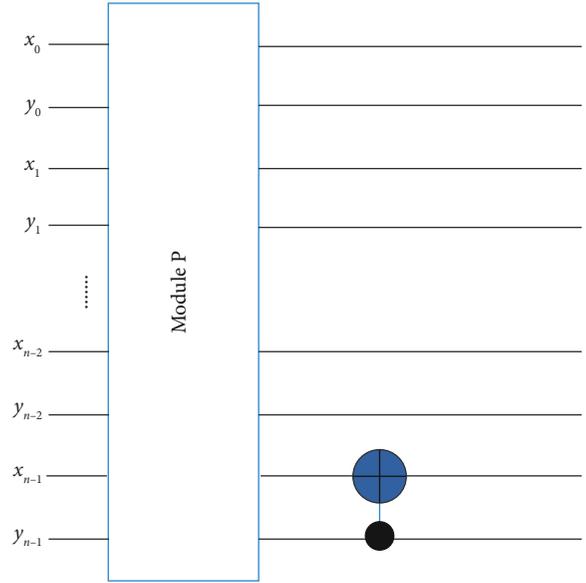


FIGURE 6: The quantum circuit diagram of module initialization.

3.2. *The Quantum Circuit Design of Quantum Hilbert Scrambling.* In Section 3.1, we get the three basic modules of quantum circuits. Next, the three modules are used to design quantum circuits for the three parts of quantum Hilbert scrambling.

3.2.1. *The Mole of Initialization.* The function of initialization is to generate the initial Hilbert matrix $F_1 = \begin{pmatrix} 1 & 2 \\ 4 & 3 \end{pmatrix}$. In this paper, the initialization module on the basis of the module P is designed corresponding to $t = 0$, and just add a CNOT gate between the two lines x_{n-1} and y_{n-1} of module P, where y_{n-1} is the control qubit and x_{n-1} is the controlled qubit. The Figure 6 is the quantum circuit corresponding to the initialization module.

3.2.2. *The Process of Iteration.* When the time of iteration is odd/even, the effect of the corresponding quantum circuit could convert the image block $F_t = \begin{pmatrix} W & X \\ Y & Z \end{pmatrix}$ into $\begin{pmatrix} W & Z^{PP} \\ X^T & Y^T \end{pmatrix} / \begin{pmatrix} W & X^T \\ Z^{PP} & Y^T \end{pmatrix}$. In this paper, the module P and

the module O are combined to form the odd module, and the module P and the module E are combined to form the even module. The quantum circuit of odd module and even module are displayed in Figures 7 and 8, respectively.

According to the analysis of the iterative process of the generation about the Hilbert matrix, the corresponding quantum circuits are designed for each step in the generation process. Combining each unit circuit, the integral quantum circuit about the quantum Hilbert scrambling is displayed in Figure 9. As a result of the unitarity of quantum gate, the inverse circuit of the quantum Hilbert scrambling would be obtained by placing the quantum gates in the entire quantum circuit in reverse order.

3.3. *The Quantum Circuit of the Steganography Based on Moiré Fringe.* The quantum circuit of the steganography based on Moiré fringe is divided into three parts, including the embedding process, the denoising processing, and the extraction process. Firstly, the watermark image is embedded into the carrier image, thus getting the pre-watermarked image. Next, the prewatermarked image is subjected to denoising processing. If there is no the denoise processing, the extracted watermark image will be mixed with noise. At last, the watermark image is extracted from the watermarked

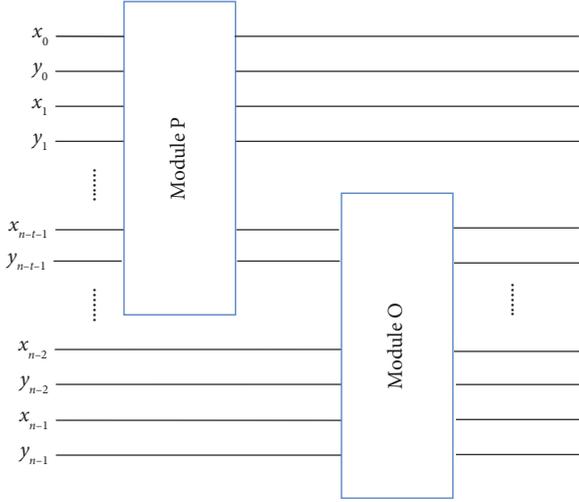


FIGURE 7: The quantum circuit of the odd module (when the time of iterations is odd).

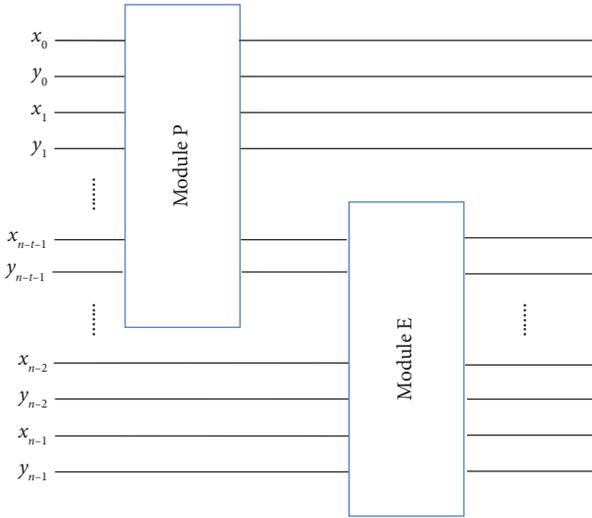


FIGURE 8: The quantum circuit of the even module (when the time of iterations is even).

image. The quantum circuit and design principles of each part are described, respectively, in detail below.

3.3.1. The Embedding Process. The embedding process can achieve embedding the watermark image M into the carrier image Q in a certain way, thus getting the prewatermarked image Q_1 . The principle formula about the embedding process is as follows:

$$Q_1(j, i) = \begin{cases} Q(j, i), & M(j, i) = 0, \\ Q((j-1) \bmod 2^m, i), & M(j, i) = 1. \end{cases} \quad (3)$$

We can draw a conclusion from the above formula that the quantum circuit corresponding to the embedding process is able to be completed by the quantum-controlled exchange gate. If the quantity of qubits controlling the color of the quantum watermark image is m , the message

about color of a pixel is expressed as $C_{M(j,i)}^0 C_{M(j,i)}^1 \cdots C_{M(j,i)}^{m-1}$. That is, the embedding process of watermark images can be achieved through using m quantum-controlled exchange gates. Taking $M(j, i)$ as the control bit, if $M(j, i) = 0$, the corresponding carrier image $Q(j, i)$ remains unchanged; if $M(j, i) = 1$, the carrier image $Q(j, i)$ is replaced by $Q((j-1) \bmod 2^m, i)$. The new matrix $Q(j, i)$ obtained is the matrix $Q_1(j, i)$. The specific quantum circuit is demonstrated in Figure 10, where $C_{(Q(j-1) \bmod 2^m, i)}^\beta$, ($\beta \in 0, 1, \dots, m-1$) is the color information of pixel $Q((j-1) \bmod 2^m, i)$.

3.3.2. The Denoising Process. The function of denoising process is to ensure that the extracted watermark image will not be mixed with noise after extraction. Because in the extraction process, the value of the qubit of the color message about the watermark image depends on whether $Q(j, i)$ and $Q_1(j, i)$ are equal. If they are not equal, $M_1(j, i) = 1$, otherwise, $M_1(j, i) = 0$. If the value of $Q(j, i)$ was originally equal to $Q((j-1) \bmod 2^n, i)$, this would make $M_1(j, i) = 0$, but in fact, $M_1(j, i) = 1$, so that some qubits of the watermark image take the opposite value. The denoising process can prevent this situation. When $M_1(j, i) = 1$, flipping the least significant qubit of the prewatermarked image, that is, $C_{Q_1(j,i)}^{m-1} \rightarrow \overline{C_{Q_1(j,i)}^{m-1}}$. Figure 11 is the quantum circuit corresponding to the denoising process. The embedding process and denoising process can be collectively referred to as the complete embedding process. The quantum circuit corresponding to the complete embedding process is displayed in the Figure 12.

3.3.3. The Extraction Process. The last step is the extraction process. That is, the watermark image M_1 is obtained through the watermarked image Q_1 and the carrier image Q . If $Q(j, i)$ and $Q_1(j, i)$ are equal, then $M_1(j, i) = 0$; otherwise, $M_1(j, i) = 1$, which is given in the following equation:

$$M_1(j, i) = \begin{cases} 0, & Q_2(j, i) = Q_1(j, i), \\ 1, & Q_2(j, i) \neq Q_1(j, i). \end{cases} \quad (4)$$

The design of quantum circuit corresponding to the extraction process is demonstrated in Figure 13.

4. Experimental Simulation and Analysis

Since the quantum computer has not yet come out, we use the classical computer and Matlab to carry out the experimental simulation of the proposed scheme. In addition to the advantage of not having the parallelism of quantum computers, classical computers can follow the processes of the algorithm to achieve the corresponding effect. Eight grayscale images with a size of 512×512 are used in this experimental simulation, of which four images are watermark images and the others are carrier images. The eight images are shown in Figure 14, where (a)–(d) are watermark images and (e)–(h) are carrier images.

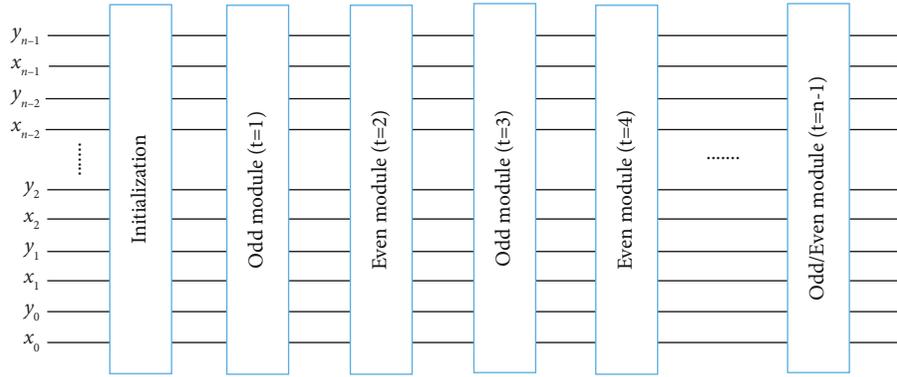


FIGURE 9: The quantum circuit of the quantum Hilbert scrambling.

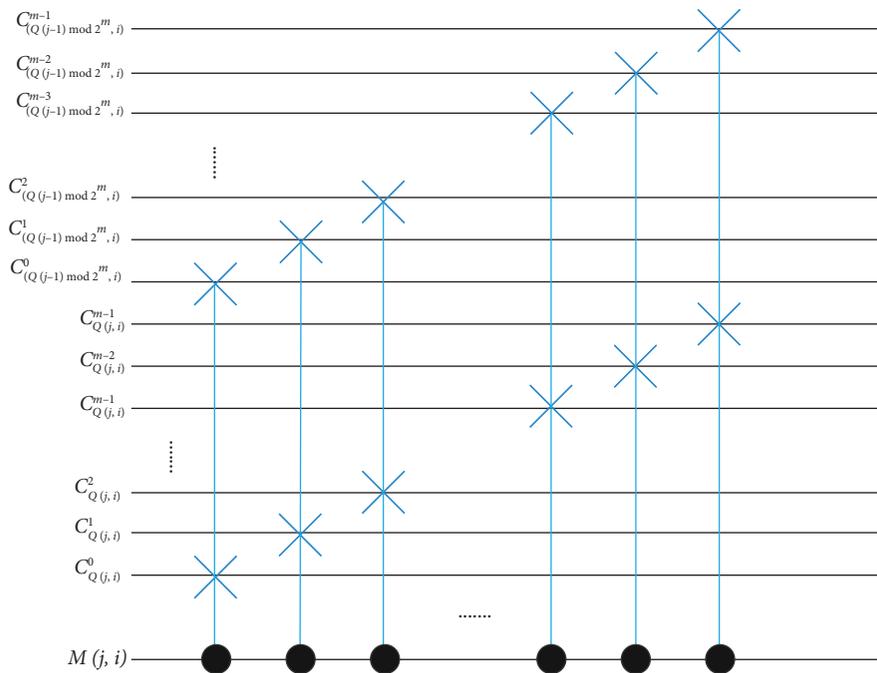


FIGURE 10: The quantum circuit diagrams of the embedding process.

4.1. *Experimental Results.* First of all, perform Hilbert scrambling on the four watermark images in (a)–(d) of Figure 14, and the obtained scrambled watermark images are shown respectively in (a)–(d) of Figure 15. After that, the four scrambled watermark images are embedded into the four carrier images in (e)–(h) of Figure 14 by using the steganography of quantum image based on Moiré fringe. The obtained watermarked image is demonstrated in (a)–(d) of Figure 16. At last, the scrambled watermark image is extracted, and the function of the inverse Hilbert scrambling is to get the original watermark image. The obtained original watermark image is displayed in (a)–(d) of Figure 17.

It can be seen from Figures 14 and 16 that there is no visual difference between the carrier image and the watermarked image, indicating that the watermark image visually does not make a difference to the carrier image. Therefore, from a watermarked image, it is not easy for a third party to detect the existence of the watermark image. The function of

quantum Hilbert scrambling is to scramble the pixel positions of the watermark image. In Figure 15, it is shown that the message of the watermark image cannot be obtained from the scrambled image. Even if a third party finds the existence of a watermark image in the watermarked image, after extracting from the watermarked image, the watermark image’s message cannot be obtained, thereby further ensuring the security of the watermarked image. In Figure 17, it is obvious that the watermark image extracted and subjected to the inverse quantum Hilbert scrambling is identical with the original watermark image. It shows that the entire algorithm process will not change the message of the watermark image, so the entire scheme is feasible.

4.2. *Visual Quality Analysis of the Watermarked Image.* PSNR is usually adopted to assess the similarity of two similar images. The similarity between the two images is

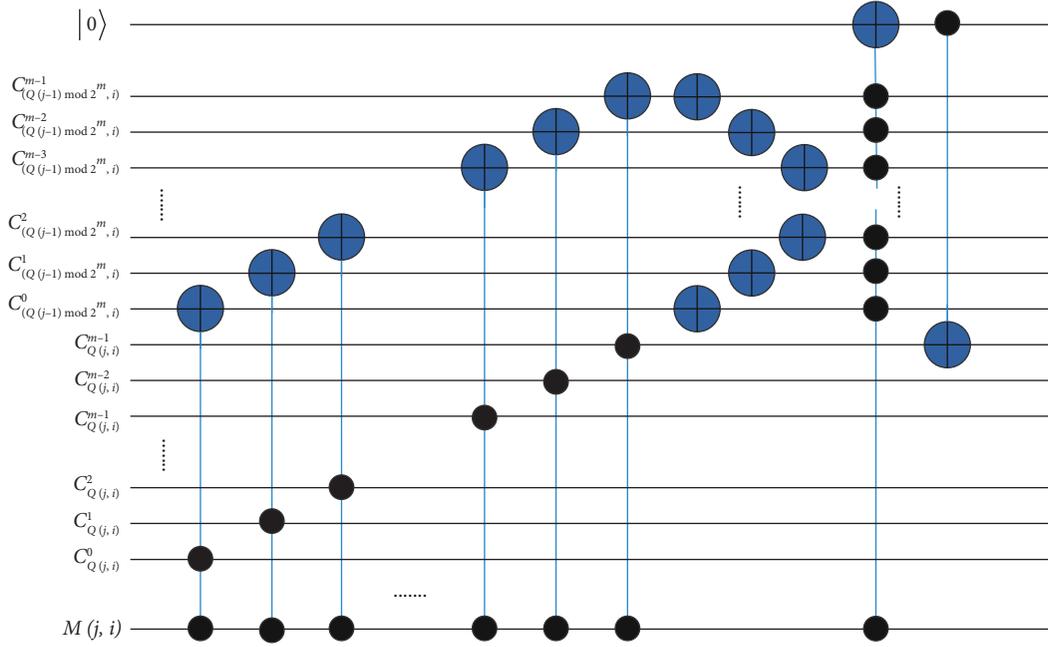


FIGURE 11: The quantum circuit diagram of denoising process.

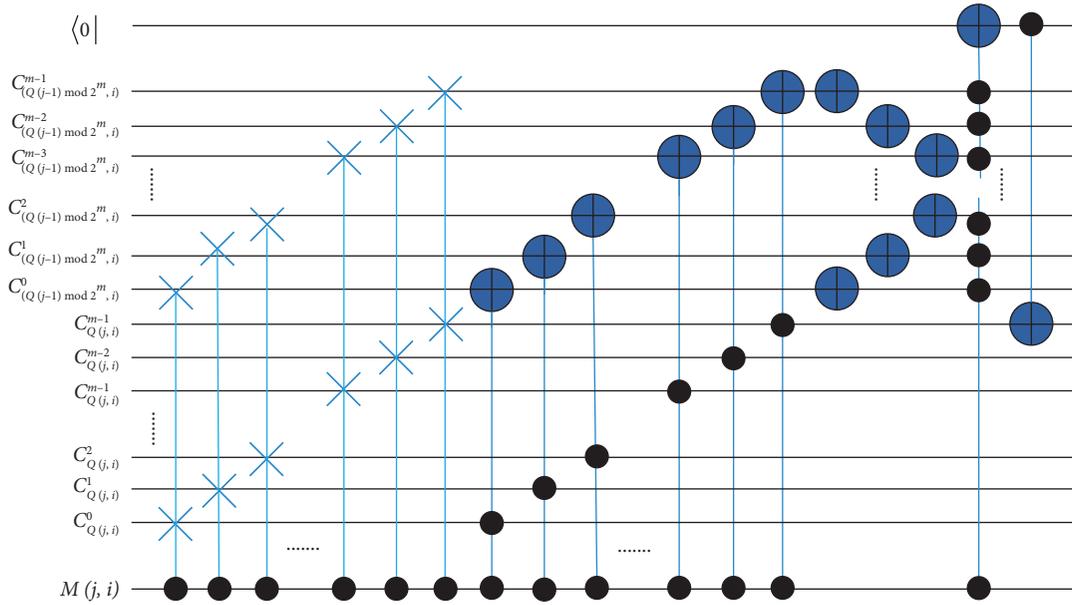


FIGURE 12: The complete quantum circuit of the embedding process.

positively related to the value of PSNR. In order to measure the impact of embedding watermark image on the visual quality of the carrier image, a quantitative analysis by calculating the PSNR value between the watermarked image and the carrier image is done in this paper. For two images of size $2^n \times 2^n$, the calculation equation of PSNR is as follows, where Q is the carrier image, Q_1 is the watermarked image.

$$\text{PSNR} = 20 \log_{10} \frac{V \times 2^n}{\sqrt{\sum_{i=0}^{2^n-1} \sum_{j=0}^{2^n-1} [Q(i, j) - Q_1(i, j)]^2}}, \quad (5)$$

where V is the maximum gray value of the pixel, which is 255. In this paper, PSNR tests are performed on the four groups of watermarks and carrier images used in the experimental simulation. The experimental results obtained are presented in Table 1. The results show that the PSNR values of the measured images are about 51. The PSNR is about 30 in the reference [33], the comparison of PSNR which proves the superiority of this scheme.

4.3. The Time Complexity of Quantum Circuits. The time complexity of a quantum circuit is decided by the number of elementary quantum gates. Basic quantum gates are

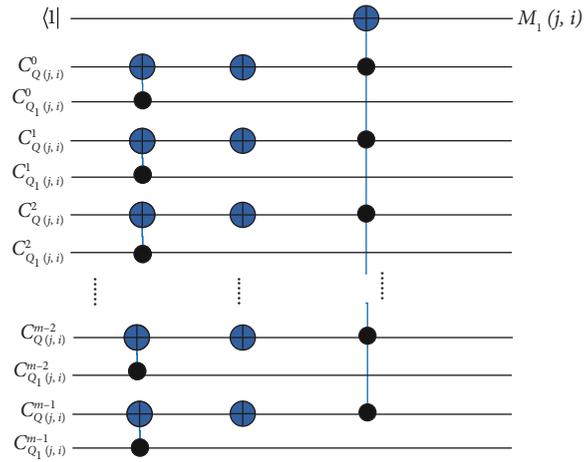


FIGURE 13: The quantum circuit of the extraction process.

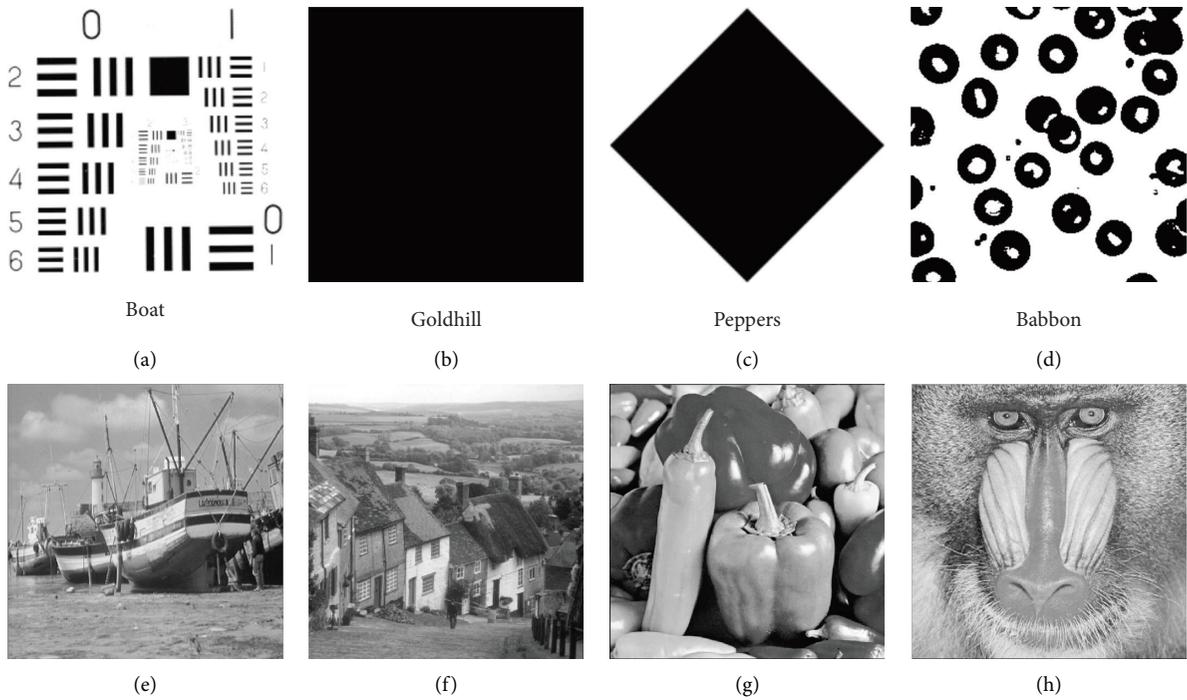


FIGURE 14: The watermark image and the carrier image.

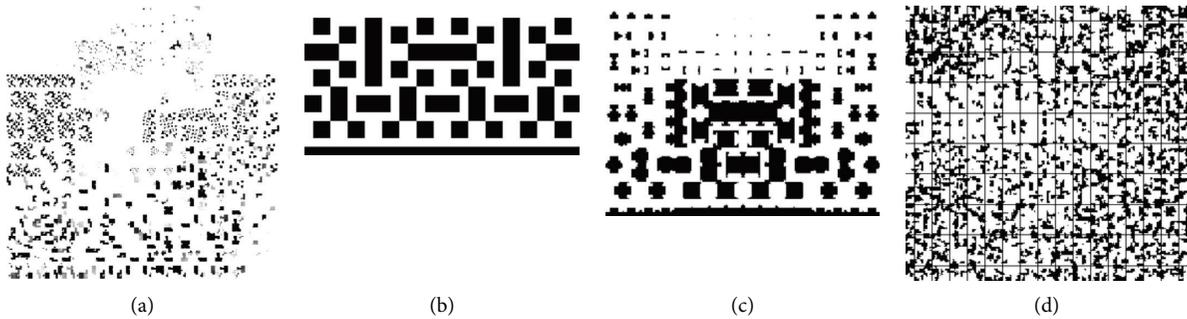


FIGURE 15: The watermark image after quantum Hilbert scrambling.

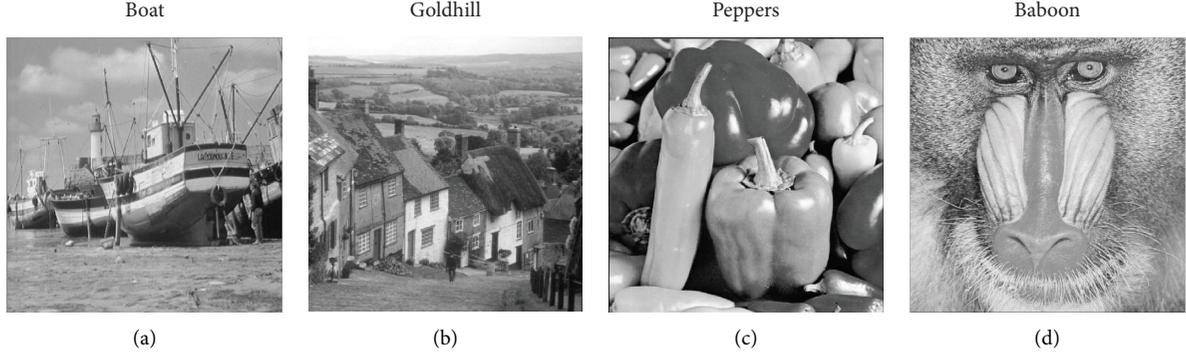


FIGURE 16: The watermarked images. (a) Boat. (b) Goldhill. (c) Peppers. (d) Baboon.

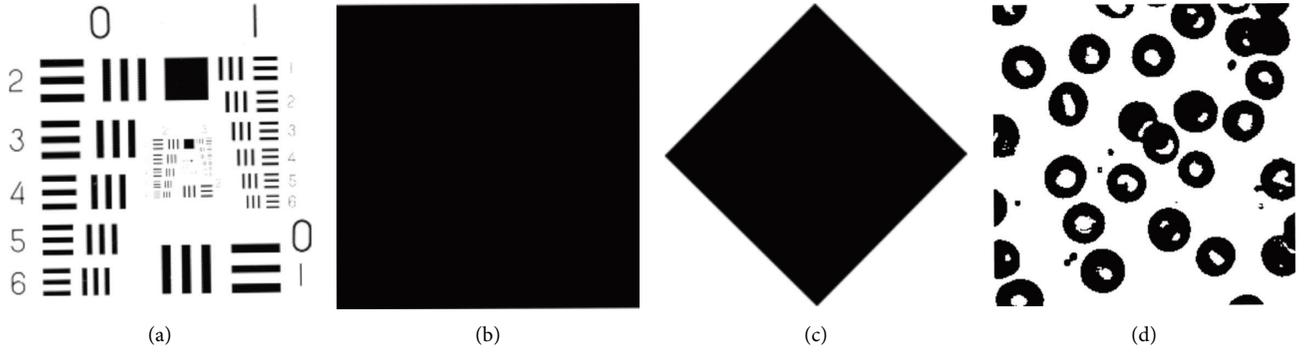


FIGURE 17: The watermark image after extraction and inverse quantum Hilbert scrambling.

TABLE 1: PSNR value of the watermarked image.

Image	Boat	Goldhill	Peppers	Baboon
PSNR	51.2984	51.1485	51.1565	51.1413

quantum gates containing one or two qubits, including NOT gates and CNOT gates. The time complexity of a basic quantum gate is 1.

First of all, the time complexity of the quantum circuit corresponding to the quantum Hilbert scrambling is calculated. The quantum Hilbert scrambling is displayed in Figure 9, which is composed of initialization module, odd module, and even module. The quantum circuits corresponding to the three modules are shown in Figures 6–8 respectively. The initialization module is composed of a Module P and a CNOT gate. The quantum circuit of Module P is presented in Figure 2, it consists of $(n - t - 1)$ SWAP gates, where the value of t is 0. The time complexity of a SWAP gate is equivalent to three CNOT gates, so the time complexity of the initialization is $(3n - 2)$. The odd module consists of module P and module O . The module O is demonstrated in Figure 3. The module O consists of a SWAP gate, a CNOT gate, t controlled SWAP gates, and $2t$ 2-qubit CNOT gates. Because a controlled SWAP gate can be made up of 18 CNOT gates, the time complexity of the SWAP gate is 18. The time complexity of a 2-qubit CNOT gate is 8. As a consequence, the time complexity of the whole odd module is $(34t + 4) + 3(n - t - 1)$. Similarly, the time complexity of even module is $(34t + 1) + 3(n - t - 1)$. So the time

complexity of the whole Hilbert scrambling is $\sum_{t \text{ is odd}} (3n + 31t + 1) + \sum_{t \text{ is even}} (3n + 31t - 2) + 3n - 2 \approx 18(n^2 + n)$. Because of the unitarity of the quantum gate, the time complexity of the quantum circuit about Hilbert inverse scrambling is also $18(n^2 + n)$. So the time complexity of the quantum Hilbert scrambling circuit is $O(n^2)$. However, the complexity of classical Hilbert scrambling is $O(2^{2n})$, so compared with classical scrambling methods, the quantum Hilbert scrambling has certain advantages [35].

Then calculating the time complexity of quantum circuit about the steganography of quantum image based on Moiré fringe. The quantum circuit of this section is divided into three parts, including the embedding process, the denoising process, and the extraction process. For a single pixel, the quantum circuit of the embedding process is demonstrated in Figure 10. It is made up with m controlled SWAP gates, so the time complexity of this part is $18m$. The quantum circuit about denoising processing is shown in Figure 11. It consists of m 2-qubit CNOT gates, m NOT gates, a $(m + 1)$ -qubit CNOT gate, and a CNOT gate. The time complexity of the CNOT gate controlled by x qubits is $(12x - 9)$, so the time complexity of the denoising quantum circuit is $(21m + 4)$. The quantum circuit about the extraction process is shown in Figure 13, and this part consists of m CNOT gates, m NOT gates and a CNOT gate controlled by m qubits, so the time complexity of the quantum circuit about this part is $(14m - 9)$. Hence, the time complexity of the quantum circuit for the steganography of the quantum image's single pixel based on Moiré fringe is $(53m - 5)$. The maximum gray value of the

TABLE 2: Comparison of the circuit complexity.

Method	Reference [36]	Reference [37]	Reference [38]	Our proposed scheme
Complexity	$O(n \cdot 2^{2n} + n)$	$O(n \cdot 2^{2n+2} + n^2)$	$O(n \cdot 2^{2n})$	$O(n \cdot 2^{2n})$

image used in the experimental simulation is 256, so the value of m is 8. For a quantum image of size $2^m \times 2^m$, the time complexity of the quantum circuit is $O(n \cdot 2^{2n})$. To sum up, the complexity of the whole scheme is $O(n \cdot 2^{2n})$. Compared with some other quantum image watermarking algorithms (Table 2) [36–38], the proposed scheme has lower complexity.

5. Conclusion

On the foundation of the NEQR, a quantum watermarking scheme combining quantum Hilbert scrambling with steganography about the Moiré fringe is designed in this paper. First of all, the quantum watermarked image is transformed by quantum Hilbert scrambling, obtaining an encrypted image. The message of the original watermark image cannot be obtained from the scrambled image. Next, the watermarked image after scrambling is embedded into the carrier image using the steganography of the Moiré fringe. At the same time, the quantum Hilbert inverse scrambling and the extraction processes can be completed. Last but not least, we have done a simulation experiment on the algorithm. The watermarked image is visually identical with the carrier image. We also tested the PSNR value of the watermarked image. And compared the results with other references, it is obvious that our scheme has greater performance. In addition, even if the third party found the existence of the watermark image and extracted it from the watermarked image. Because the watermark image is scrambled by quantum Hilbert scrambling, the third party still cannot obtain the message of the watermarked image. Therefore, the proposed algorithm has higher security. Besides, the complexity of the quantum circuit used in this scheme is calculated, which shows that the time complexity of this scheme is lower than some other related schemes.

Data Availability

The data are available upon reasonable request to the corresponding author.

Conflicts of Interest

The authors declare that there are no potential conflicts of interest.

Acknowledgments

This work was supported by the National Natural Science Foundation of China (Grant no. 61772295), Natural Science Foundation of Shandong Province, China (Grant nos. ZR2021MF049 and ZR2019YQ01), and Project of Shandong Provincial Natural Science Foundation Joint Fund Application (ZR202108020011).

References

- [1] N. Fatahi and M. Naseri, “Quantum watermarking using entanglement swapping,” *International Journal of Theoretical Physics*, vol. 51, no. 7, pp. 2094–2100, 2012.
- [2] A. M. Iliyasu, P. Q. Le, F. Dong, and K. Hirota, “Watermarking and authentication of quantum images based on restricted geometric transformations,” *Information Sciences*, vol. 186, no. 1, pp. 126–149, 2012.
- [3] F. Yan, A. M. Iliyasu, B. Sun, S. E. Venegas-Andraca, F. Dong, and K. Hirota, “A duple watermarking strategy for multi-channel quantum images,” *Quantum Information Processing*, vol. 14, no. 5, pp. 1675–1692, 2015.
- [4] S. Miyake and K. Nakamae, “A quantum watermarking scheme using simple and small-scale quantum circuits,” *Quantum Information Processing*, vol. 15, no. 5, pp. 1849–1864, 2016.
- [5] Q. W. Zeng, Z. Y. Wen, J. F. Fu, and N. R. Zhou, “Quantum watermark algorithm based on maximum pixel difference and tent map,” *International Journal of Theoretical Physics*, vol. 60, no. 9, pp. 3306–3333, 2021.
- [6] Y. Ma, N. Li, W. Zhang, S. Wang, and H. Ma, “Image encryption scheme based on alternate quantum walks and discrete cosine transform,” *Optics Express*, vol. 29, no. 18, pp. 28338–28351, 2021.
- [7] W. Yi-Nuo, S. Zhao-Yang, and M. Yu-Lin, “Color image encryption algorithm based on DNA code and alternating quantum random walk,” *Acta Physica Sinica*, vol. 70, no. 23, 2021.
- [8] Z. Liu, T. Xia, and J. Wang, “Image encryption technique based on new two-dimensional fractional-order discrete chaotic map and Menezes-Vanstone elliptic curve cryptosystem,” *Chinese Physics B*, vol. 27, no. 3, Article ID 030502, 2018.
- [9] Y. J. Xian, X. Y. Wang, Y. Q. Zhang, X. Y. Wang, and X. H. Du, “Fractal sorting vector-based least significant bit chaotic permutation for image encryption*,” *Chinese Physics B*, vol. 30, no. 6, Article ID 060508, 2021.
- [10] H. W. Wang, Y. J. Xue, Y. L. Ma, N. Hua, and H. Y. Ma, “Determination of quantum toric error correction code threshold using convolutional neural network decoders,” *Chinese Physics B*, vol. 31, no. 1, Article ID 010303, 2021.
- [11] C. F. Su and C. Y. Chen, “Information hiding method based on quantum image by using Bell states,” *Quantum Information Processing*, vol. 19, no. 1, pp. 1–16, 2020.
- [12] P. Xu, Z. He, T. Qiu, and H. Ma, “Quantum image processing algorithm using edge extraction based on Kirsch operator,” *Optics Express*, vol. 28, no. 9, pp. 12508–12517, 2020.
- [13] J. Song, Z. Ke, W. Zhang, and Y. Ma, “Quantum confidentiality query protocol based on bell state identity,” *International Journal of Theoretical Physics*, vol. 61, no. 3, pp. 1–12, 2022.
- [14] J. I. Latorre, “Image compression and entanglement,” 2005, <https://arxiv.org/abs/quant-ph/0510031>.
- [15] S. E. Venegas-Andraca and J. L. Ball, “Processing images in entangled quantum systems,” *Quantum Information Processing*, vol. 9, no. 1, pp. 1–11, 2010.

- [16] P. Q. Le, F. Dong, and K. Hirota, "A flexible representation of quantum images for polynomial preparation, image compression, and processing operations," *Quantum Information Processing*, vol. 10, no. 1, pp. 63–84, 2011.
- [17] Y. Zhang, K. Lu, Y. Gao, and M. Wang, "NEQR: a novel enhanced quantum representation of digital images," *Quantum Information Processing*, vol. 12, no. 8, pp. 2833–2860, 2013.
- [18] M. Abdolmaleky, M. Naseri, J. Batle, A. Farouk, and L. H. Gong, "Red-Green-Blue multi-channel quantum representation of digital images," *Optik*, vol. 128, pp. 121–132, 2017.
- [19] B. Sun, A. M. Iliyasa, F. Yan, F. Dong, and K. Hirota, "An RGB multi-channel representation for images on quantum computers," *Journal of Advanced Computational Intelligence and Intelligent Informatics*, vol. 17, no. 3, pp. 404–417, 2013.
- [20] Y. G. Yang, J. Xia, X. Jia, and H. Zhang, "Novel image encryption/decryption based on quantum Fourier transform and double phase encoding," *Quantum Information Processing*, vol. 12, no. 11, pp. 3477–3493, 2013.
- [21] Y. G. Yang, X. Jia, P. Xu, and J. Tian, "Analysis and improvement of the watermark strategy for quantum images based on quantum Fourier transform," *Quantum Information Processing*, vol. 12, no. 8, pp. 2765–2769, 2013.
- [22] X. H. Song, S. Wang, S. Liu, A. A. Abd El-Latif, and X. M. Niu, "A dynamic watermarking scheme for quantum images using quantum wavelet transform," *Quantum Information Processing*, vol. 12, no. 12, pp. 3689–3706, 2013.
- [23] Q. Mou, T. Jiang, and J. Liu, "Research on image watermarking algorithm based on quantum haar wavelet transform," *International Journal of Theoretical Physics*, vol. 61, 2015.
- [24] D. Ghai, H. K. Gianey, A. Jain, and R. S. Uppal, "Quantum and dual-tree complex wavelet transform-based image watermarking," *International Journal of Modern Physics B*, vol. 34, no. 04, Article ID 2050009, 2020.
- [25] J. Y. Wu, W. L. Huang, W. M. Xia-Hou, W. P. Zou, and L. H. Gong, "Imperceptible digital watermarking scheme combining 4-level discrete wavelet transform with singular value decomposition," *Multimedia Tools and Applications*, vol. 79, no. 31–32, pp. 22727–22747, 2020.
- [26] W. W. Zhang, F. Gao, B. Liu, Q. Y. Wen, and H. Chen, "A watermark strategy for quantum images based on quantum fourier transform," *Quantum Information Processing*, vol. 12, no. 2, pp. 793–803, 2013.
- [27] W. W. Hu, R. G. Zhou, A. El-Rafei, and S. X. Jiang, "Quantum image watermarking algorithm based on haar wavelet transform," *IEEE Access*, vol. 7, pp. 121303–121320, 2019.
- [28] N. Jiang, N. Zhao, and L. Wang, "LSB based quantum image steganography algorithm," *International Journal of Theoretical Physics*, vol. 55, no. 1, pp. 107–123, 2016.
- [29] S. Wang, J. Sang, X. Song, and X. Niu, "Least significant qubit (LSQb) information hiding algorithm for quantum image," *Measurement*, vol. 73, pp. 352–359, 2015.
- [30] R. G. Zhou, W. Hu, and P. Fan, "Quantum watermarking scheme through Arnold scrambling and LSB steganography," *Quantum Information Processing*, vol. 16, no. 9, pp. 1–21, 2017.
- [31] S. Heidari and M. Naseri, "A novel LSB based quantum watermarking," *International Journal of Theoretical Physics*, vol. 55, no. 10, pp. 4205–4218, 2016.
- [32] G. Lu, L. Saunoriene, S. Aleksiene, and M. Ragulskis, "Optical image hiding based on chaotic vibration of deformable moiré grating," *Optics Communications*, vol. 410, pp. 457–467, 2018.
- [33] N. Jiang and L. Wang, "A novel strategy for quantum image steganography based on moiré pattern," *International Journal of Theoretical Physics*, vol. 54, no. 3, pp. 1021–1032, 2015.
- [34] S. Heidari and E. Farzadnia, "A novel quantum LSB-based steganography method using the Gray code for colored quantum images," *Quantum Information Processing*, vol. 16, no. 10, pp. 1–28, 2017.
- [35] N. Jiang, L. Wang, and W. Y. Wu, "Quantum Hilbert image scrambling," *International Journal of Theoretical Physics*, vol. 53, no. 7, pp. 2463–2484, 2014.
- [36] W. W. Hu, R. G. Zhou, J. Luo, and B. Liu, "LSBs-based quantum color images watermarking algorithm in edge region," *Quantum Information Processing*, vol. 18, no. 1, pp. 1–27, 2019.
- [37] P. Li and X. Liu, "A novel quantum steganography scheme for color images," *International Journal of Quantum Information*, vol. 16, no. 02, Article ID 1850020, 2018.
- [38] G. Luo, R. G. Zhou, W. Hu, J. Luo, X. Liu, and H. Ian, "Enhanced least significant qubit watermarking scheme for quantum images," *Quantum Information Processing*, vol. 17, pp. 299–319, 2018.