Jestr

Journal of Engineering Science and Technology Review 13 (2) (2020) 199 - 205

JOURNAL OF
Engineering Science and Technology Review

Research Article

www.jestr.org

Reversible Data Hiding for Quantum Images using Quantum Controlled-NOT Gate Operation

Gaofeng Luo[1], Ling Shi[2,*], Zijuan Shi[1,3] and Liang Zong[1]

[1]*College of Information Engineering, Shaoyang University, Shaoyang 422000, China*
[2]*Department of Information Technology and Creativity, Shaoyang Polytechnic, Shaoyang 422000, China*
Faculty of Education, University of Malaya, Kuala Lumpur 59200, Malaysia

Received 2 January 2020; Accepted 13 March 2020

Abstract

At present, quantum image data hiding technology is restricted by high fidelity and embedding capacity, which frequently leads to permanent distortion of carrier images. A reversible data hiding method based on quantum controlled-NOT (CNOT) gate operation was proposed in the present study to satisfy the requirements of embedding capacity and visual quality and recover the original carrier image without loss. First, the hidden and carrier images were represented by a novel enhanced quantum representation of digital images. The hidden images were then encrypted and scrambled by employing chaos method. The quantum secret image was embedded into the relevant bit plane of the quantum carrier image considering quantum CNOT gate operation. The quantum key image was also generated. Finally, the current work not only extracted the quantum secret image without error but also recovered the carrier image without loss via inverse quantum CNOT gate operation. Simulation experiments were conducted to analyze embedding concealment and visual quality of the embedded steganographic images. Results demonstrate that the quantum circuit based on quantum CNOT gate operation not only enhances the embedding concealment but also improves the peak signal-to-noise ratio at the embedding capacity of 2 bits per pixel by 10% compared with the traditional least significant bit method. Thus, this operation achieves the lossless recovery of the original quantum carrier image. This study also provides certain theoretical importance and practical value for the security authentication and protection of quantum images.

Keywords: Quantum image, Reversible data hiding, Controlled-NOT gate

1. Introduction

The design of efficient quantum algorithms for complicated problems in the classical field of data processing has achieved remarkable performance improvement with the ongoing development of quantum information technology [1-2]. Specifically, the application of quantum computation to image processing, namely, quantum image processing [3-4], by utilizing the superposition and entanglement characteristics of quantum, has been warmly welcomed by scholars. Quantum image data hiding is an important branch of quantum image processing. Research on this aspect can improve the efficiency of image security processing and analysis. Such a mechanism can also be used for security authentication and copyright protection of quantum data.

However, image processing and application in special fields, such as medical and military images, has strict requirements on image quality and timeliness of processing with the invention and development of novel technologies, such as big data and sensors. Existing literature reported that traditional quantum data hiding will result in the permanent distortion of the original carrier when embedded. Consequently, the application requirements are unsatisfied, thereby introducing challenges to the research on quantum image data hiding technology.

Therefore, scholars employ the emerging quantum computation technique to conduct relevant studies on image security technologies, such as image encryption, watermarking, and steganography [5-8]. Encryption is mainly used as the pre-processing operation in quantum data hiding technology, whereas watermarking and steganography are two research branches of quantum image information hiding technology. The design of these algorithms mainly begins with scrambling, encryption, embedding, and extraction of secret images. The algorithm performance mainly considers embedding visual quality and capacity. However, the permanent distortion of the quantum carrier image is inevitable during embedding of the secret data with the quantum image as the carrier. Therefore, the reversibility in the process of quantum image data hiding must be urgently addressed to extract the quantum secret image correctly while recovering the original carrier image without loss.

This study employs novel enhanced quantum representation (NEQR) of digital images [9] based on the above-mentioned analysis to design the basic framework of reversible data hiding for quantum images. Quantum controlled-NOT (CNOT) gate operation is also utilized to construct the quantum circuit, thus embedding and extracting quantum secret images. Subsequently, embedding capacity, visual quality, and lossless recovery of quantum images are analyzed to further provide references for security authentication and copyright protection of quantum images.

*E-mail address: ling_shi@163.com
ISSN: 1791-2377 © 2020 School of Science, IHU. All rights reserved.
doi:10.25103/jestr.132.24

2. State of the art

At present, scholars are mainly concerned with two aspects of quantum data hiding technology, including quantum image watermarking and steganography, focusing on quantum image embedding algorithm, embedding capacity, and visual quality of embedded carrier images.

Iliyasu [10] studied quantum image watermarking and authentication by using a flexible representation of quantum images (FRQI) for the constrained geometric transformation of quantum images. However, the author failed to provide the watermark embedded in quantum circuits. The application of the proposed method was limited because the FRQI model cannot accurately obtain pixel color information. Miyake [11] utilized the NEQR of digital images as a basis and proposed a quantum watermarking scheme using only small-scale quantum circuits. This scheme directly embedded the watermark image into the lowest 2-bit plane of the carrier pixel through XOR operation. However, the visualization quality was insufficiently decent after embedding. Heidari [12] investigated quantum color image watermarking and quantum data copyright protection and used electronic signature as the embedded object. The application was confined due to data-based copyright protection. Naseri [13] proposed a security scheme for quantum watermarking based on the least significant bit (LSB) and most significant bit methods in classical image processing. Similarly, this scheme was deficient because it uses multiple keys, thereby complicating the algorithm and corresponding quantum circuits to a certain extent. Luo [14] analyzed and studied the encryption of multiple quantum images by using the quantum CNOT and exchange gate operations to solve the shared encryption of multiple images. However, this method only achieved the encryption of multiple quantum images, which was applied to the preprocessing of data hiding for quantum images.

Heidari [15-16] examined quantum image steganography by using Gray code and LSB methods, mainly concentrating on hiding information based on different color channels of color images. However, the author failed to consider the recovery of the original carrier images after embedding. El-latif [17-18] proposed a quantum data hiding method for remote medical image sharing and a new technique for image steganography based on quantum substitution boxes. These algorithms were mainly designed from two aspects: steganographic capacity and fidelity. Similarly, the recovery of an original carrier image was neglected. Wang [19] explored the least significant qubit (LSQb) data hiding algorithm for quantum image and determined the corresponding unitary transformation because data hiding based on image frequency domains can enhance security. Nevertheless, Wang did not provide the embedding and extraction of quantum circuits. Qu [20] exploited the modification direction and investigated quantum image steganalysis with an unsatisfactory embedding capacity. Xiang [21] conducted a preliminary study on the reversible data hiding for quantum images in combination with the difference expansion technique. Nevertheless, the corresponding quantum circuit complexity is relatively high.

The above-mentioned studies are mainly centered on exploring data hiding techniques based on quantum images from the following two perspectives: watermarking and steganography. Such studies aimed to design an effective quantum algorithm and the corresponding quantum circuits, enhance the embedding capacity of data hiding, and reduce the image distortion of carrier images. Although the above-mentioned research attained good robustness, they neglected the study of image recovery after distortion. To date, few studies in the domain of data hiding for quantum images can not only meet the general requirements of data hiding and embedding but also recover the carrier image without loss. The present study aims to establish the reversible data hiding framework of quantum images through the quantum image representation model NEQR and analyze the embedding and extraction methods of quantum secret images. The reversibility of the algorithm and the lossless recovery of carrier images are studied to provide a reference for the further optimization of quantum data hiding.

The remainder of this study is organized as follows. Section 3 establishes a reversible data hiding framework for quantum images, analyzes one and two hidden quantum binary images, and designs the embedding circuit. Section 4 verifies the embedding visual quality through simulation experiments and analyzes the reversibility of this method, that is, the original carrier image can be recovered without loss. Section 5 summarizes the entire study and provides some relevant conclusions.

3. Methodology

3.1 Quantum image model and preprocessing

The sizes of the carrier image (grayscale 256), that is, the binary image, is assumed to be hidden, and the blank image used as the key image is $2^n \times 2^n$. The new quantum images are used to represent the NEQR. Accordingly, these images are represented as follows:

$$|C\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|C_{YX}\rangle|YX\rangle, C_{YX} = c_{yx}^{7}\ldots c_{yx}^{1}c_{yx}^{0}, c_{yx}^{i} \in \{0,1\} \quad (1)$$

$$|S\rangle == \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|S_{YX}\rangle|YX\rangle, \quad S_{YX} \in \{0,1\} \quad (2)$$

$$|E\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|E_{YX}\rangle|YX\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|0\rangle|YX\rangle \quad (3)$$

where $|C\rangle$, $|S\rangle$, and $|E\rangle$ represent the quantum carrier, quantum binary, and quantum key images, respectively, and $|YX\rangle$ represents the coordinate value of the quantum image.

A simple chaos sequence encryption method is adopted to optimize the security performance of hiding, which is defined as follows:

$$X_{\delta+1} = \mu X_{\delta}(1 - X_{\delta}) \quad (4)$$

where $\delta = 0,1,\ldots,n$, $X_0 \in [0,1]$ refers to the initial value, and $0 \le \mu \le 4$. When $3.57 \le \mu \le 4$, the mapping generates a pseudo-random number $(0,1)$. Therefore, a suitable initial value is selected to generate a binary sequence $B = \{b_1, b_2, \ldots b_{2^{2n}}\}$. Quantum CNOT gate operation is later conducted for each pixel of the quantum binary image to obtain $|S'_{YX}\rangle = |S_{YX}\rangle \oplus |B\rangle$. All pixels of an image are stored in superposition in accordance with the quantum

superposition state principle, and color transformation of all pixels is simultaneously completed. Therefore, the encrypted quantum binary image is represented as follows:

$$|S'\rangle == \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|S'_{YX}\rangle|YX\rangle,\quad S'_{YX}\in\{0,1\} \tag{5}$$

The quantum image model NEQR completed image transformation from classical to quantum storage. Fig. 1 presents the basic framework of reversible data hiding based on quantum image.

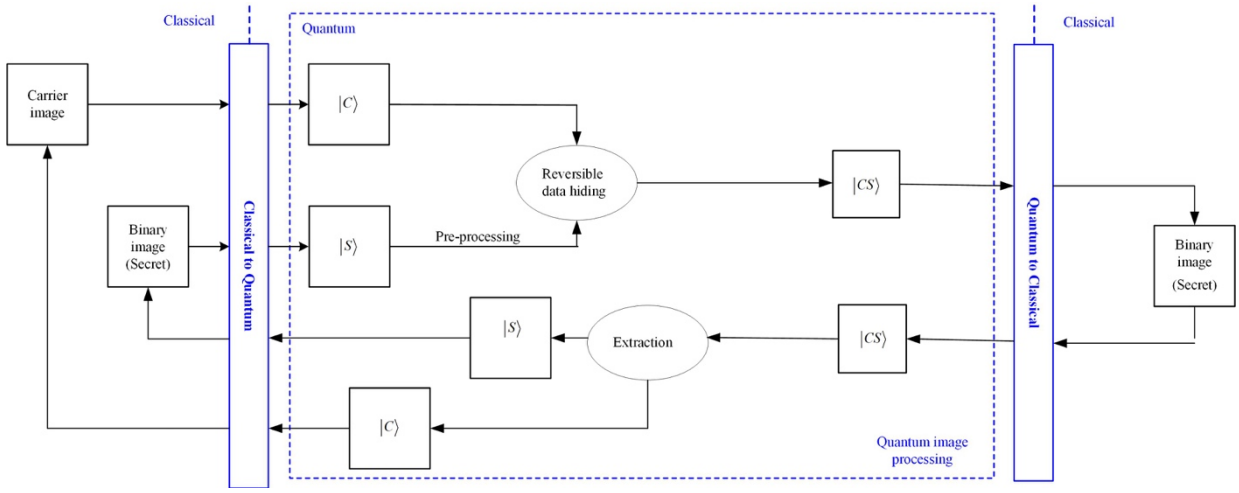
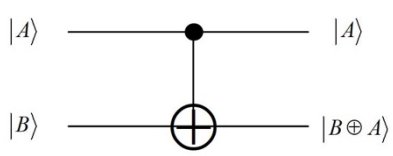


Fig. 1. Quantum reversible data hiding framework

3.2 Embedding of a single quantum binary image

Data hiding essentially rests with the embedding of the secret data. In the course of information hiding with quantum gray images as the carrier, the choice of pixels where the quantum carrier image is embedded can directly perform the replacement or modification operation through a certain type of operation. The simple LSB algorithm has been constantly used in quantum image watermarking and steganography because the low-order plane of the image has the least effect on human vision. However, data embedding simply avoids operation on the lowest level plane because data hiding attackers can easily conduct a steganographic analysis of data embedding according to the LSB statistical characteristics.



$$U_c = \begin{bmatrix} 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

Fig. 2. CNOT gate and control matrix

Quantum CNOT gate has two input qubits: the control and target qubits. Fig. 2 shows the circuit diagram and control matrix of the qubits. If the control qubit is zero, then the target qubit remains unchanged; if the control qubit is one, then the target qubit is flipped, and its principle is represented in the following equation:

$$|00\rangle\to|00\rangle,|01\rangle\to|01\rangle,|10\rangle\to|11\rangle,|11\rangle\to|10\rangle \tag{6}$$

The figure demonstrates that CNOT is an extension of the classical XOR gate. When the control and target qubits perform the XOR operation, the results are stored in the target qubit. Hence, $t = c_{yx}^7 \oplus c_{yx}^6 \oplus \ldots c_{yx}^0$, $c_{yx}^i \in \{0,1\}$, and $sum = \sum_{i=0}^{7} c_{yx}^i$ are assumed in the classical XOR operation. Specifically, when the sum is odd, t = 1; when the sum is even, t = 0. With a non-gate operation on one of the digits, the value of T is flipped. Modification of the LSB of the lowest three bits of the image pixel will not result in significant changes in the image visual quality. Hence, quantum CNOT gate operation is adopted to the lowest 3-bit plane of the quantum carrier image to achieve $|c_{yx}^2\rangle \oplus |c_{yx}^1\rangle \oplus |c_{yx}^0\rangle$ whose result is expressed as $|r\rangle$. The corresponding pixel values of the encrypted quantum binary images $|S'_{YX}\rangle$ is compared with $|r\rangle$. When the two pixel values are equal, that is, $|0\rangle$ or $|1\rangle$, no change in the lowest 3-bit plane of the quantum carrier image can be observed. Considering $|r\rangle = |c_{yx}^2\rangle \oplus |c_{yx}^1\rangle \oplus |c_{yx}^0\rangle \neq |S'_{YX}\rangle$, $|r\rangle = |0\rangle$, $|S'_{YX}\rangle = |1\rangle$, and the sum is even are supposed. The bit plane should be flipped in accordance with the principle of priority of the lowest qubit plane to ensure that the sum is odd, such as $|000\rangle\to|001\rangle$ and $|011\rangle\to|010\rangle$, and the blank key image is $|0\rangle$. If $|r\rangle = |1\rangle$, $|S'_{YX}\rangle = |0\rangle$, then the sum is odd. Thus, considering embedding concealment, the LSB plane of the second bit should be flipped to ensure that the sum is even, such as $|001\rangle\to|011\rangle$ and $|100\rangle\to|110\rangle$. The pixel value of the key image $|E_{YX}\rangle$ is flipped to $|1\rangle$. The steganographic image after embedding is as follows:

$$|CS'\rangle = \frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|CS'_{YX}\rangle|YX\rangle, CS'_{YX} = cs'^7_{yx}\ldots cs'^0_{yx} \tag{7}$$
$$cs'^i_{yx}\in\{0,1\}$$

The embedding procedures are as follows.

Step 1: The difference or value of the lowest 3-bit plane of the image pixel of the quantum carrier can be determined

considering quantum CNOT gate operation (i.e., $|r\rangle=|c^2_{yx}\rangle\oplus|c^1_{yx}\rangle\oplus|c^0_{yx}\rangle$).

Step 2: When the corresponding coordinates of the quantum carrier and binary images to be hidden are equal, $|S'_{YX}\rangle$ and $|r\rangle$ should be compared. If the coordinates are the same, then no modification is required.

Step 3: When $|r\rangle=|0\rangle$ and $|S'_{YX}\rangle=|1\rangle$, $|cs'^0_{yx}\rangle=|\overline{c^0_{yx}}\rangle$ and $|E_{YX}\rangle=|0\rangle$.

Step 4: When $|r\rangle=|1\rangle$ and $|S'_{YX}\rangle=|0\rangle$, $|cs'^1_{yx}\rangle=|\overline{c^1_{yx}}\rangle$ and $|E_{YX}\rangle=|1\rangle$.

Fig. 3 shows the embedding circuit.

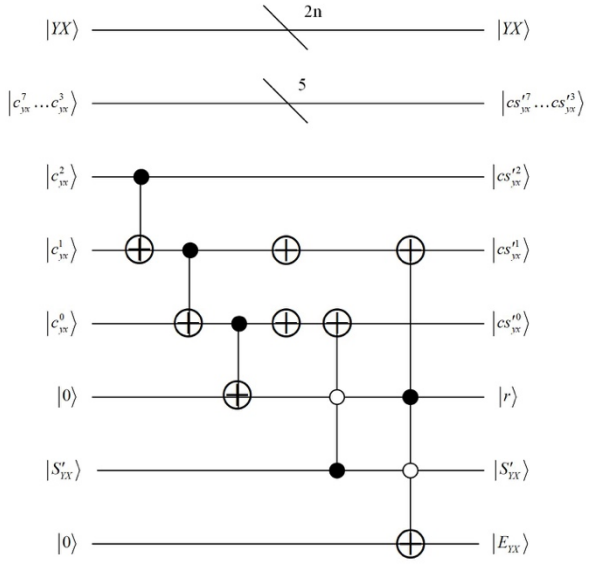


Fig. 3. Embedding circuit of a single quantum binary image

3.3 Embedding of two quantum binary images

Although the above-mentioned 1-bit method can achieve embedding, this method has an overt limitation of circumscribed embedding quantity. In this part, the case wherein two quantum binary images are simultaneously embedded into the quantum carrier image will be considered. Herein, the expressions of two quantum binary images be presented as follows:

$$\begin{aligned}|S^1\rangle&=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|S^1{}_{YX}\rangle|YX\rangle,\quad S^1{}_{YX}\in\{0,1\}\\|S^2\rangle&=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|S^2{}_{YX}\rangle|YX\rangle,\quad S^2{}_{YX}\in\{0,1\}\end{aligned}\tag{8}$$

Two binary images are constructed into a quantum image with a grayscale of four through quantum image interpolation. The quantum secret image is also obtained by using the above-mentioned encryption method whose expression is as follows:

$$|S''\rangle=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|S''_{YX}\rangle|YX\rangle,\quad S''_{YX}=s''^1_{yx}s''^0_{yx}\tag{9}$$

The quantum CNOT gate is used to process the lowest 3-bit planes of the quantum carrier image. If $|t_1\rangle=|c^2_{yx}\rangle\oplus|c^1_{yx}\rangle$ and $|t_0\rangle=|c^2_{yx}\rangle\oplus|c^0_{yx}\rangle$, then these values will be compared with those of the 2-bit planes of the quantum secret image, namely, $|s''^1_{yx}\rangle$ and $|s''^0_{yx}\rangle$. The results can be divided into the following four cases:

(1) When $|s''^1_{yx}\rangle=|t_1\rangle$ and $|s''^0_{yx}\rangle=|t_0\rangle$, modification is unnecessary in the course of embedding.

(2) When $|s''^1_{yx}\rangle\neq|t_1\rangle$ and $|s''^0_{yx}\rangle\neq|t_0\rangle$, $|c^2_{yx}\rangle$ should be flipped.

(3) When $|s''^1_{yx}\rangle=|t_1\rangle$ and $|s''^0_{yx}\rangle\neq|t_0\rangle$, $|c^0_{yx}\rangle$ should be flipped.

(4) When $|s''^1_{yx}\rangle\neq|t_1\rangle$ and $|s''^0_{yx}\rangle=|t_0\rangle$, $|c^1_{yx}\rangle$ should be flipped.

The image expression after embedding is as follows:

$$\begin{aligned}&|CS''\rangle=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|CS''_{YX}\rangle|YX\rangle, CS''_{YX}=cs''^7_{yx}\ldots cs''^0_{yx}\\&cs''^i_{yx}\in\{0,1\}\end{aligned}\tag{10}$$

The quantum key image is still necessary herein to recover the original quantum carrier image. The above-mentioned analysis indicated that unlike the embedding of a single quantum binary image, the quantum key image must be extended; that is, the pixel gray level is four, and its expression is as follows:

$$|E'\rangle=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|E'_{YX}\rangle|YX\rangle=\frac{1}{2^n}\sum_{Y=0}^{2^n-1}\sum_{X=0}^{2^n-1}|e'^1_{yx}e'^0_{yx}\rangle|YX\rangle\tag{11}$$

The embedding procedures and methods are as follows.

Step 1: The quantum CNOT gate operation is conducted on the lowest 3-bit planes of the quantum carrier image to obtain $|t_1\rangle=|c^2_{yx}\rangle\oplus|c^1_{yx}\rangle$ and $|t_0\rangle=|c^2_{yx}\rangle\oplus|c^0_{yx}\rangle$.

Step 2: When the corresponding coordinates of the quantum carrier and secret images to be hidden are equal, and if $|s''^1_{yx}\rangle=|t_1\rangle$ and $|s''^0_{yx}\rangle=|t_0\rangle$, then $|cs''^2_{yx}\rangle=|c^2_{yx}\rangle$, $|cs''^1_{yx}\rangle=|c^1_{yx}\rangle$, $|cs''^0_{yx}\rangle=|c^0_{yx}\rangle$, and the key image $|e'^1_{yx}e'^0_{yx}\rangle$ is $|00\rangle$.

Step 3: Provided that $|s''^1_{yx}\rangle\neq|t_1\rangle$ and $|s''^0_{yx}\rangle\neq|t_0\rangle$, then $|cs''^2_{yx}\rangle=|\overline{c^2_{yx}}\rangle$, $|cs''^1_{yx}\rangle=|c^1_{yx}\rangle$, $|cs''^0_{yx}\rangle=|c^0_{yx}\rangle$ and the key image $|e'^1_{yx}e'^0_{yx}\rangle$ is $|11\rangle$.

Step 4: Provided that $|s''^1_{yx}\rangle=|t_1\rangle$ and $|s''^0_{yx}\rangle\neq|t_0\rangle$, then $|cs''^2_{yx}\rangle=|c^2_{yx}\rangle$, $|cs''^1_{yx}\rangle=|c^1_{yx}\rangle$, $|cs''^0_{yx}\rangle=|\overline{c^0_{yx}}\rangle$ and the key image $|e'^1_{yx}e'^0_{yx}\rangle$ is $|01\rangle$.

Step 5: Provided that $|s''^1_{yx}\rangle\neq|t_1\rangle$ and $|s''^0_{yx}\rangle=|t_0\rangle$, then $|cs''^2_{yx}\rangle=|c^2_{yx}\rangle$, $|cs''^1_{yx}\rangle=|\overline{c^1_{yx}}\rangle$, $|cs''^0_{yx}\rangle=|c^0_{yx}\rangle$ and the key image $|e'^1_{yx}e'^0_{yx}\rangle$ is $|10\rangle$.

Step 3 is taken as an example, and Fig. 4 shows its corresponding embedded quantum circuit. The two embedded bits of information are unequal to the XOR value of the lowest 3-bit of the carrier image. At this point, $|c^2_{yx}\rangle$ is

flipped, and $\left|e'^{1}_{yx}e'^{0}_{yx}\right\rangle$ is flipped to $\left|11\right\rangle$. Notably, the quantum circuit in other embedding cases can be obtained by the same method.

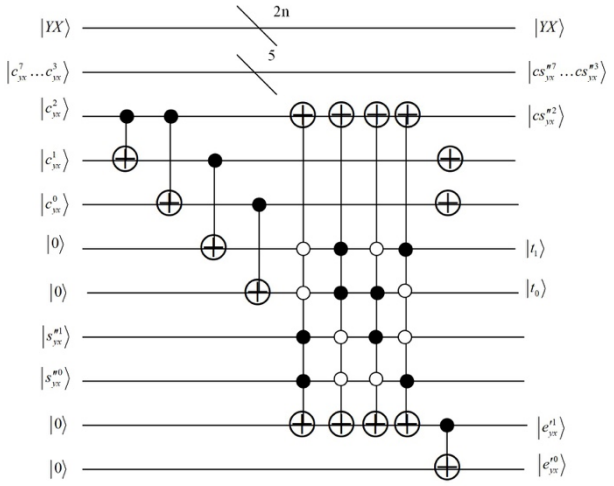


Fig. 4. Example of embedded quantum circuit

3.4 Hidden information extraction

The above-mentioned analysis manifests two types of hidden information extraction.

On the one hand, the hidden information is supposed to be a single quantum binary image. Quantum CNOT gate operation is directly applied to the lowest 3-bit plane of the embedded quantum carrier image (steganographic image) $\left|CS'\right\rangle$, that is, $\left|cs'^{2}_{yx}\right\rangle\oplus\left|cs'^{1}_{yx}\right\rangle\oplus\left|cs'^{0}_{yx}\right\rangle$. The result is the encrypted quantum binary image $\left|S'\right\rangle$. The chaos sequence is generated and $\left|S'\right\rangle$ is decrypted using the same initial value and key, and the quantum binary image $\left|S\right\rangle$ is obtained.

On the other hand, when the hidden information comprises two quantum binary images, the quantum CNOT gate operation is directly applied to the embedded quantum carrier image (steganographic image) $\left|CS''\right\rangle$, that is, $\left|cs''^{2}_{yx}\right\rangle\oplus\left|cs''^{1}_{yx}\right\rangle$, $\left|cs''^{2}_{yx}\right\rangle\oplus\left|cs''^{0}_{yx}\right\rangle$. In this case, the results are the values of the 2-bit planes of the hidden image, namely, $\left|s''^{1}_{yx}\right\rangle$ and $\left|s''^{0}_{yx}\right\rangle$. Subsequently, the quantum secret image $\left|S''\right\rangle$ is decrypted, and the original two quantum binary images $\left|S^{1}\right\rangle$, $\left|S^{2}\right\rangle$ are obtained considering the inverse scaling of the quantum image.

The above-mentioned extraction process reveals that the hidden information extraction is the inverse operation of the embedding process. The extraction method is concise and has no requirement on the auxiliary and key of the original carrier image. Thus, such a method can accurately extract the embedded quantum secret image information.

4. Result analysis and discussion

4.1 Simulation experiments and results

At present, the proposed method in this study relied on the assistance and support of the classical computer because no universal quantum computer is available. MATLAB 2014b was used for the simulation experiments, and its computer hardware was configured with Intel (R) Core (TM) i5-7200u CPU with 2.70 GHz and 8.00 Gb RAM. In the simulation process, four grayscale images ("Lena," "Cameraman," "Airplane," and "Peppers") with a grayscale of 256 and two binary images ("Pirate" and "Mandril") with a grayscale of 256 were chosen as the quantum carrier and secret images to be embedded, respectively. Fig. 5 shows all the test images. Figs. 6 (a)-1 and (b)-1 demonstrate the embedding effect after a single binary image, that is, Mandril, has been embedded into carrier images Lena and Cameraman. Figs. 6 (a)-2 and (b)-2 present the embedding effect after two binary images, namely, Pirate and Mandril, have been embedded.

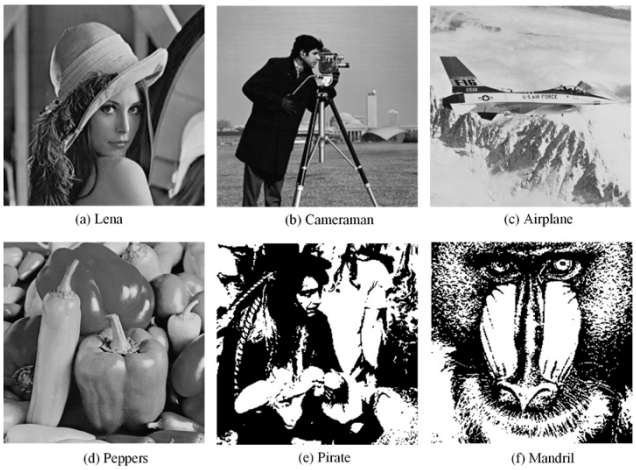


Fig. 5. Text images

Fig. 6. Image carriers after embedding

4.2 Visual quality and concealment analysis

The peak signal-to-noise ratio (PSNR) is adopted to evaluate the effect of information hiding, that is, visual quality, and algorithm imperceptibility. The PSNR in the two carrier images I with size $m\times n$ and the corresponding carrier images J embedded with watermark is defined as follows:

$$PSNR=10\log_{10}\frac{MAX_I^2}{MSE}=20\log\frac{MAX_I}{\sqrt{MSE}} \tag{12}$$

where MAX_I is the maximum gray value of the image color,

and MSE is the mean squared error, which is defined as follows:

$$MSE = \frac{1}{mn}\sum_{i=0}^{m-1}\sum_{j=0}^{n-1}[I(i,j) - I(i,j)]^2 \quad (13)$$

In the simulation experiment, four carrier images were taken as objects, and the PSNR value in the case of embedding a binary image, that is, embedding 1 bit/pixel, was calculated. The results were compared with those of the simple LSB substitution method (Fig. 7). The figure demonstrates that the PSNR value calculated via the method proposed in this study is slightly low. In this method, the embedded bit not only changed the least bit plane but also modified and substituted the second LSB; thus, the PSNR value was slightly lowered. However, hiding information in different bit planes demonstrates good security considering the concealment of information hiding. Accordingly, attackers will have difficulty in directly attacking via the least bit plane analysis.

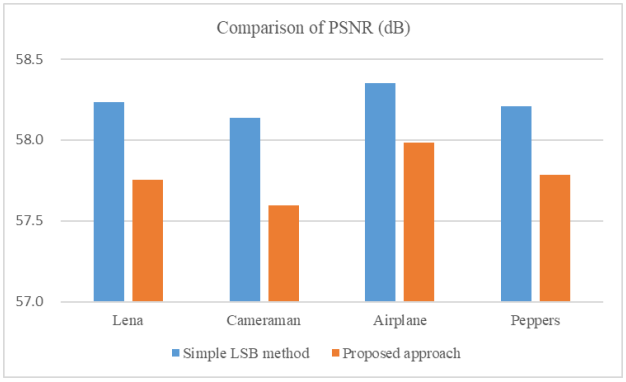


Fig. 7. Comparison of PSNR after embedding one qubit

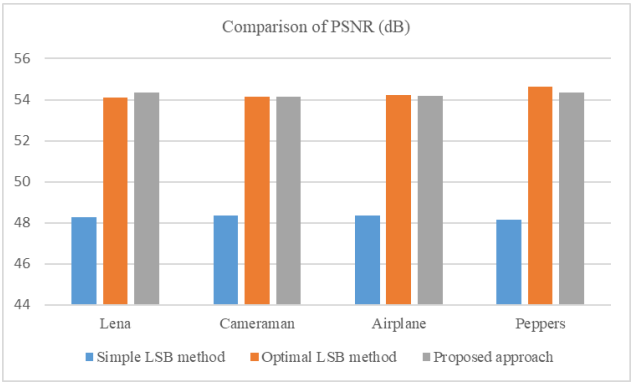


Fig. 8. Comparison of PSNR after embedding two qubits

Second, the PSNR value in the case of embedding two binary images, that is, embedding 2 bits/pixel, was calculated. The results were compared with those of the simple LSB substitution and the optimization methods in literature [22] (Fig. 8). The figure demonstrates that the PSNR value of the optimized method and the proposed method in this study increased by approximately 10% compared with the simple substitution. Both methods also obtained good PSNR value (approximately 54 dB). This finding further indicates the high fidelity of the embedded carrier image of this information hiding method. This method also employed quantum CNOT gate operation on the lowest 3-bit planes and inverted 1 bit at most. This method possesses better steganographic security and robustness compared with direct embedding in the lowest 2-bit planes.

4.3 Analysis of reversibility

The above-mentioned analysis indicated that the proposed quantum image data hiding method can realize the embedding and error-free extraction of quantum secret images. However, the proposed method inevitably leads to the permanent distortion of carrier images. Therefore, this section analyzes and discusses the reversibility of the algorithm, that is, the lossless recovery of the original carrier image.

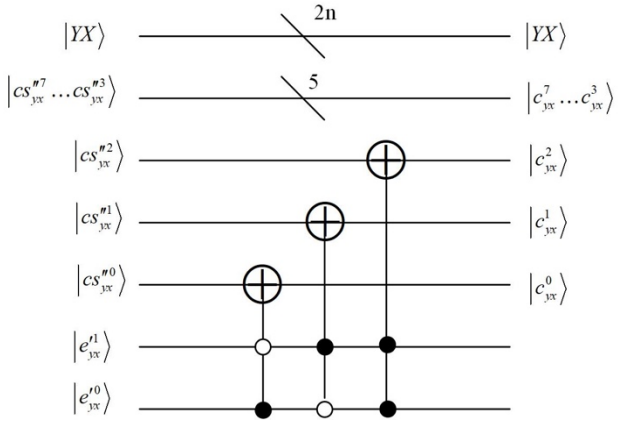


Fig. 9. Quantum circuit of carrier image recovery

Fig. 10. Carrier image after recovery

First, the generated key image $|E\rangle$ in the embedding process is a binary image because the embedded image is a single binary image. Fig. 3 shows that when the pixel value is $|0\rangle$, the pixel value of the corresponding carrier image remains constant. When the pixel value is $|1\rangle$, the second LSB of the carrier image is flipped in the course of embedding. At this point, the recovery of the original carrier image via the CNOT gate operation is feasible.

Similarly, when the embedded image comprises two quantum binary images, 2 bits were embedded in each pixel, thereby generating four types of pixel values $|e'^1_{yx}e'^0_{yx}\rangle$ of the key image (i.e., $|00\rangle$, $|01\rangle$, $|10\rangle$, and $|11\rangle$ $|E'\rangle$. These

values corresponded to no qubit flipping, $\left|c_{yx}^{0}\right\rangle$, $\left|c_{yx}^{1}\right\rangle$, and $\left|c_{yx}^{2}\right\rangle$ in the embedding process. Hence, the operation is only required in the case of relevant bit plane of steganographic image in the process of carrier image recovery. Fig. 9 presents the carrier image recovery quantum circuit. Considering the four carrier images in Fig. 5, the quantum secret images were embedded and then recovered. Fig. 10 demonstrates the recovered carrier images. A slight difference can be observed between the corresponding carrier images in Figs. 10 and 5. Furthermore, the PSNR values of the original and recovered carrier images were calculated, which turned out to be PSNR = Inf. This finding indicates the lossless recovery of the original carrier image and the reversibility of the hiding algorithm.

5 Conclusions

The NEQR and quantum CNOT gate operation were employed to analyze the embedding, extraction, and carrier image recovery in terms of the quantum image data hiding. Such an undertaking is conducted for information hiding and extraction based on quantum carrier image to recover the original carrier image without loss. Finally, the following conclusions can be drawn.

(1) A simple quantum CNOT-gate is used to design the quantum image embedding circuit. The embedding position of this algorithm is variable compared with the fixed LSB bit embedding, and the embedding concealment is optimized.

(2) The embedded carrier image has high fidelity and achieves the blind extraction of secret information.

(3) In the embedding process, the quantum key image is generated to ensure that the original carrier image is recovered without loss through the key image. Accordingly, the reversible data hiding based on the quantum image is realized.

Overall this study adopted the novel quantum image representation model NEQR in combination with emerging technologies of quantum computation. The present study also conducted theoretical research and simulation experiments considering image information hiding technology. This study determined a basic framework of reversible data hiding for quantum images. A reversible data hiding algorithm for quantum carrier images based on quantum CNOT gate operation has also been proposed in this study. This algorithm provides references for the follow-up study of quantum image security authentication and protection.

Acknowledgments

This work was supported by the Research Foundation of Education Bureau of Hunan Province, China (Grant Nos. 18B420 and 19B512).

This is an Open Access article distributed under the terms of the Creative Commons Attribution License

References

1. P. W. Shor, “Algorithms for quantum computation: discrete logarithms and factoring”. In: *Proceedings of 35th Annual Symposium on Foundations of Computer Science*, Santa Fe, NM, USA: IEEE, 1994, pp. 124-134.
2. L. K. Grover, “A fast quantum mechanical algorithm for database search”. *In: Proceedings of the 28th Annual ACM symposium on the Theory of Computing*, New York, USA: ACM, 1996, pp. 212-219.
3. Y. Cai, X. Lu, and N. Jiang, “A Survey on quantum image processing”. *Chinese Journal of Electronics*, 27(4), 2018, pp. 718-727.
4. X. W. Yao, H. Wang, Z. Liang *et al.*, “Quantum image processing and its application to edge detection: theory and experiment”. *Physical Review X*, 7(3), 2017, pp.031041.
5. Y.-G. Yang, J. Tian, H. Lei, Y.-H. Zhou, and W.-M. Shi, “Novel quantum image encryption using one-dimensional quantum cellular automata”. *Information Sciences*, 345, 2016, pp. 257-270.
6. T. Zhang, B. Abd-el-atty, M. Amin, and A. A. A. El-latif, “QISLSQb: a quantum image steganography scheme based on least significant qubit”. In: *International Conference on Mathematical, Computational and Statistical Sciences and Engineering*, Shenzhen, China: DEStech Publications, Inc., 2016, pp. 40-45.
7. X. Song, S. Wang, A. A. Abd El-Latif, and X. Niu, “Dynamic watermarking scheme for quantum images based on Hadamard transform”. *Multimedia Systems*, 20(4), 2014, pp. 379-388.
8. Y.-G. Yang, Q.-X. Pan, S. Sun, and P. Xu, “Novel image encryption based on quantum walks”. *Scientific Reports*, 5, 2015, pp. 7784.
9. Y. Zhang, K. Lu, Y. Gao, and M. Wang, “NEQR: a novel enhanced quantum representation of digital images”. *Quantum Information Processing*, 12(8), 2013, pp.2833-2860.
10. A. M. Iliyasu, P. Q. Le, F. Dong, and K. Hirota, “Watermarking and authentication of quantum images based on restricted geometric transformations”. *Information Sciences*, 186(1), 2012, pp. 126-149.
11. S. Miyake and K. Nakamae, “A quantum watermarking scheme using simple and small-scale quantum circuits”. *Quantum Information Processing*, 15(5), 2016, pp.1849-1864.
12. S. Heidari, R. Gheibi, M. Houshmand, and K. Nagata, “A robust blind quantum copyright protection for colored images based on owner’s signature”. *International Journal of Theoretical Physics*, 56(8), 2017, pp.2562-2578.
13. M. Naseri, S. Heidari, M. baghfalaki *et al.*, “A new secure quantum watermarking scheme”. *Optik*, 139, 2017, pp.77-86.
14. G. Luo, R.-G. Zhou, and W.-W. Hu, “Novel quantum secret image sharing scheme”. *Chinese Physics B*, 28(4), 2019, pp. 040302.
15. S. Heidari and E. Farzadnia, “A novel quantum LSB-based steganography method using the Gray code for colored quantum images”. *Quantum Information Processing*, 16(10), 2017, pp.242.
16. S. Heidari, M. R. Pourarian, R. Gheibi, M. Naseri, and M. Houshmand, “Quantum red-green-blue image steganography”. *International Journal of Quantum Information*, 15(5), 2017, pp.1750039.
17. A. A. A. El-latif, B. Abd-el-atty, and M. S. Hossain, “Efficient quantum information hiding for remote medical image sharing”. *IEEE Access*, 6, 2018, pp.21075-21083.
18. A. A. A. El-latif, B. Abd-el-atty, and S. E. Venegas-andraca, “A novel image steganography technique based on quantum substitution boxes”. *Optics and Laser Technology*, 116, 2019, pp. 92-102.
19. S. Wang, J. Sang, X. Song, and X. Niu, “Least significant qubit (LSQb) information hiding algorithm for quantum image”. *Measurement*, 73, 2015, pp.352-359.
20. Z. Qu, Z. Cheng, W. Liu, and X. Wang, “A novel quantum image steganography algorithm based on exploiting modification direction”. *Multimedia Tools and Applications*, 78(7), 2019, pp.7981-8001.
21. S. Xiang, H. Li, and T. Song, “Reversible data hiding algorithm in NEQR quantum images (in Chinese)”. *Journal of Cyber Security*, 3(6), 2018, pp. 78-91.
22. R.-G. Zhou, W. Hu, G. Luo, P. Fan, H. Ian, and P. Swap, “Optimal LSBs-based quantum watermarking with lower distortion”. *International Journal of Quantum Information*, 16(5), 2018, pp. 1850058.

.