IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received December 13, 2018, accepted January 7, 2019, date of publication January 23, 2019, date of current version April 2, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2894295

Matrix Coding-Based Quantum Image Steganography Algorithm

ZHIGUO QU[1,2], ZHENWEN CHENG[3], AND XIAOJUN WANG[4]

[1]Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science and Technology, Nanjing 210044, China
[2]Jiangsu Collaborative Innovation Center of Atmospheric Environment and Equipment Technology, Nanjing University of Information Science and Technology, Nanjing 210044, China
[3]School of Electronic and Information Engineering, Nanjing University of Information Science and Technology, Nanjing 210044, China
[4]School of Electronic Engineering, Dublin City University, Dublin 9, Ireland

Corresponding author: Zhiguo Qu (qzghhh@126.com)

This work was supported in part by the National Natural Science Foundation of China under Grant 61373131, Grant 61601358, Grant 61672290, Grant 61232016, and Grant 61501247, in part by the Six Talent Peaks Project of Jiangsu Province under Grant 2015-XXRJ-013, in part by the Natural Science Foundation of Jiangsu Province under Grant BK20171458, in part by the Natural Science Foundation of the Higher Education Institutions of Jiangsu Province, China, under Grant 16KJB520030, in part by the Sichuan Youth Science and Technique Foundation under Grant 2017JQ0048, in part by the NUIST Research Foundation for Talented Scholars under Grant 2015r014, and in part by the PAPD and CICAEET Funds.

ABSTRACT Embedding secret information into quantum carrier image for covert communication is one of significant research fields of quantum secure communication. Using good imperceptibility and high embedding efficiency of matrix coding, this paper proposes a novel matrix coding-based quantum steganography algorithm for quantum color images. In order to better apply matrix coding in actual demand, two different embedding methods are proposed. One embedding method is single pixel-embedded (1, 3, 2) coding, called SPE (1, 3, 2) coding for short. This method embeds two qubits of secret information into three least significant qubits (LSQbs) of a single pixel of quantum carrier image, and at most only one LSQb would be changed. The other embedding method is the multiple pixels-embedded (1, 3, 2) coding, called MPsE (1, 3, 2) coding, in which three LSQbs of multiple carrier pixels are utilized to embed two secret qubits. On account of experimental simulation obtained in the MATLAB environment, it shows that the new algorithm has good performance in the imperceptibility, the security, the embedding efficiency, and the embedding capacity.

INDEX TERMS Quantum image steganography, matrix coding, quantum color images, imperceptibility, embedding efficiency.

I. INTRODUCTION

It is well known that Heisenberg uncertainty principle, measurement collapse principle and quantum non-cloning principle belong to three fundamental principles of quantum mechanics [1]. Based on these fundamental principles, quantum secure communication [2]–[6] plays an extremely significant role in information communication. As an important branch of quantum secure communication, quantum steganography [7]–[15] realizes covert communication by embedding secret information into quantum multimedia carrier and transmitting it in the public quantum channel. Based on various quantum image representation models [16]–[21] and the mature quantum image processing techniques (QIPT [22], [23]), quantum image-based steganography [24]–[30] has been developing rapidly in recent years. For a monochrome image, the flexible representation of quantum images (FRQI [17]) encodes the gray information into 1 qubit, while the novel enhanced quantum representation (NEQR [18]) encodes this information into 8 qubits. For a color image, the novel quantum representation of color digital images (NCQI [20]) encodes the RGB information into 24 qubits correspondingly. Since large redundancy of quantum image can be used to embed secret information, it is widely recognized that quantum image steganography has good prospect for quantum secure communication.

In 2015, Jiang *et al.* [24] proposed a novel strategy for quantum image steganography based on Moire pattern. When repetitive structures (such as screens, grids or gratings) are

The associate editor coordinating the review of this manuscript and approving it for publication was Giovanni Angiulli.

superposed or observed relative to each other, the Moire effect occurs, which is an optical phenomenon [31]. The embedding process of this algorithm starts with selecting an initial Moire grating as the carrier image. Then the secret image is embedded into the initial Moire grating and the deformed Moire grating is the Moire pattern. The extracting process restores the secret image by operating the initial Moire grating and the Moire pattern. In the same year, Jiang *et al.* [25] also proposed a quantum image steganography algorithm based on the least significant bit (LSB [32]). Two different embedding methods are given according to the selection regions of quantum carrier image. One embedding method is plain LSB that the gray information's LSB of quantum carrier image is substituted by one secret qubit. Plain LSB steganography is simple, however its security is poor. Many image processing techniques, such as filtering, noising and compressing, can easily remove the hidden secret information. The another embedding method is block LSB which improves imperceptibility and security by embedding one secret qubit into a number of pixels of a image block. But the capacity of block LSB steganography is only $1/2^q$. In 2016, Qu *et al.* [26] put forward a novel self-adaptive quantum steganography algorithm to embed secret information into quantum watermark image and quantum carrier image simultaneously. This embedding method requires quantum watermark image to ensure the security of quantum stego image obtained by embedding secret information into quantum carrier image. In 2017, Heidari *et al.* [27] presented a quantum red-green-blue image steganography. Three different embedding methods are provided based on the characteristic of quantum color images that the RGB information is encoded by three channels, i.e., Red channel, Green channel and Blue channel. The first embedding method utilizes only one of the image's channels to embed secret information. The second embedding method uses the LSB XORing technique to cover secret information. And the last embedding method employs two channels to hide secret information. Later, Heidari and Farzadnia [28] also presented a novel quantum LSB-based steganography method using the Gray code for quantum color images. The Gray code [33], also known as the reflected binary code (RBC), is an approach to encode an integer in the 2^n-ary numeral system into an n-bit binary sequence. Comparing with the traditional binary code, two successive values in the Gray code differ merely one bit. This algorithm has a considerable embedding capacity for using the Gray code to simultaneously embed two secret qubits into three LSQbs of each carrier pixel according to the reference tables. In 2018, Zhou *et al.* [29] brought forward a novel quantum image steganography scheme based on LSB. The sizes of quantum carrier image and the original secret image are assumed to be $4m \times 4m$ and $m \times m$, respectively. The embedding process of this algorithm begins with scrambling the original secret image by using the bit-plane scrambling method. Then the scrambled secret image is expanded into the same size as quantum carrier image by utilizing the key, which is only known to the sender and the receiver. Next, the Arnold scrambling method [34] is used to scramble the expanded secret image and obtain the meaningless secret image. Finally, the meaningless secret image is embedded into quantum carrier image by the LSB technique. In 2018, Qu *et al.* [30] proposed a novel quantum image steganography algorithm based on exploiting modification direction (EMD [35]). The EMD embedding uses a pixel-group containing n carrier pixels to embed one secret digit in the $(2n + 1)$-ary notational system, and only one carrier pixel may be changed or all carrier pixels unchanged.

According to the existing quantum image steganography algorithms [24]–[30] mentioned above, it's easy to know that many quantum image steganography algorithms [25], [27]–[29] are related to the LSB technique. Moreover, the LSB technique is the simplest embedding method in matrix coding [36]. As an effective technique to improve imperceptibility of communication protocols, matrix coding was proposed by Crandall in 1998. Applied in the information hiding system based on the LSB substitution, matrix coding has two obvious advantages:

(1) It can avoid embedding secret information into sensitive positions of carrier data for better imperceptibility;

(2) It can effectively reduce modifications to carrier data for higher embedding efficiency.

In order to achieve better imperceptibility and higher embedding efficiency than quantum image steganography algorithms [24]–[30] discussed above, this paper proposes a novel matrix coding-based quantum image steganography algorithm based on quantum color images. According to the number of pixels of quantum carrier image used to embed secret information, two different embedding methods are proposed. One embedding method is SPE (1, 3, 2) coding that embeds two secret qubits into three LSQbs of a single carrier pixel, and at most only one LSQb changed. The other embedding method is MPsE (1, 3, 2) coding that three LSQbs of multiple carrier pixels are utilized to embed two secret qubits by also at most only one LSQb changed. In addition, a universal quantum circuit for matrix coding and a dedicated quantum circuit for (1, 3, 2) coding are designed to illustrate the embedding and extracting processes of the new algorithm for practice.

The rest of this paper is organized as follows. Brief introductions about matrix coding and its application in communication protocols, and the NCQI representation for quantum color images are given in Section II. In Section III, the embedding and extracting processes of the new algorithm are presented in detail. The simulation results and the related performance analysis are given in Section IV. Finally, the conclusion is provided in Section V.

II. PRELIMINARIES

A. MATRIX CODING AND ITS APPLICATION IN COMMUNICATION PROTOCOLS

As a well-known technique of steganographic coding, matrix coding [36] has advantages of good imperceptibility and high embedding efficiency. Moreover, (1, n, k) coding is one of

common methods of matrix coding applied in communication protocols. In $(1, n, k)$ coding, at most 1 LSB in n carrier data will be changed to embed k bits of secret information, where $n = 2^k - 1$. Let's suppose that those LSBs of n carrier data are $a_1, a_2, \cdots, a_i, \cdots, a_{2^k-1}$ $(1 \le i \le 2^k - 1)$, and k secret bits are $x_1, x_2, \cdots, x_j, \cdots, x_k$ $(1 \le j \le k)$. The rule of $(1, n, k)$ coding can be presented as follows.

Step1 First, according to the order of n carrier data, the position of the i_{th} carrier data is encoded as in (1).

$$\begin{aligned} i =& (b_{i,k} b_{i,k-1} \cdots b_{i,j} \cdots b_{i,1})_2, \\ & b_{i,j} \in \{0, 1\}, i \in \left[1, 2^k - 1\right], j \in [1, k] \end{aligned} \tag{1}$$

Step2 Next, the value of c_j is calculated according to (2),

$$c_j = \begin{cases} 0, x_j = \bigoplus_{i=1}^{2^k-1} \left(a_i \cdot b_{i,j}\right) \\ 1, x_j \ne \bigoplus_{i=1}^{2^k-1} \left(a_i \cdot b_{i,j}\right) \quad 1 \le j \le k \end{cases} \tag{2}$$

where $\bigoplus_{i=1}^{2^k-1}$ indicates recursive XOR operations.

Step3 Then, it's assumed that

$$C = \sum_{j=1}^{k} c_j \cdot 2^{j-1} \tag{3}$$

If $C = 0$, all of $a_1, a_2, \cdots, a_{2^k-1}$ will be kept intact; otherwise, the value of a_C will be changed. In this way, k secret bits can be successfully embedded into n carrier data.

Step4 Finally, the j_{th} secret bit can be extracted according to (4).

$$\begin{aligned} x_j &= \bigoplus_{i=1}^{2^k-1} \left(a_i' \cdot b_{i,j}\right) \\ &= \left(a_1' \cdot b_{1,j}\right) \oplus \left(a_2' \cdot b_{2,j}\right) \oplus \cdots \oplus \left(a_{2^k-1}' \cdot b_{2^k-1,j}\right) \end{aligned} \tag{4}$$

From the above steps, the modification rate $D(k)$, the embedding rate $R(k)$ and the embedding efficiency $W(k)$ of $(1, n, k)$ coding can be calculated in terms of (5), (6) and (7), respectively.

$$D(k) = \frac{1}{n+1} = \frac{1}{2^k} \tag{5}$$

$$R(k) = \frac{k}{n} = \frac{k}{2^k - 1} \tag{6}$$

$$W(k) = \frac{R(k)}{D(k)} = \frac{k \cdot 2^k}{2^k - 1} \tag{7}$$

Equations (5), (6) and (7) show that these performance parameters of $(1, n, k)$ coding are closely related to k. According to the different values of k, the trend of these performance parameters is obtained, as shown in Table 1. It can be seen from Table 1 that the modification rate $D(k)$ and the embedding rate $R(k)$ are decreased, while the embedding efficiency $W(k)$ is increased when k is increased.

Taking $k = 2$ and $n = 3$ for example, the embedding process of $(1, 3, 2)$ coding is to embed two secret bits (x_1 and x_2) into three LSBs (a_1, a_2 and a_3) by matrix coding. If

$$x_1 = a_1 \oplus a_3, \; x_2 = a_2 \oplus a_3 \tag{8}$$

TABLE 1. Performance parameters of $(1, n, k)$ coding with respect to k.

k	n	The modification rate $D(k)$ (%)	The embedding rate $R(k)$ (%)	The embedding efficiency $W(k)$
1	1	50.00	100.00	2.00
2	3	25.00	66.67	2.67
3	7	12.50	42.86	3.43
4	15	6.25	26.67	4.27
5	31	3.12	16.13	5.16
6	63	1.56	9.52	6.09
7	127	0.78	5.51	7.06
8	255	0.39	3.14	8.03
9	511	0.20	1.76	9.02

it does not change values of a_1, a_2 and a_3. If

$$x_1 \ne a_1 \oplus a_3, \; x_2 = a_2 \oplus a_3 \tag{9}$$

it should change the value of a_1. If

$$x_1 = a_1 \oplus a_3, \; x_2 \ne a_2 \oplus a_3 \tag{10}$$

it should change the value of a_2. If

$$x_1 \ne a_1 \oplus a_3, \; x_2 \ne a_2 \oplus a_3 \tag{11}$$

it should change the value of a_3. The extracting process of $(1, 3, 2)$ coding to extract two secret bits can be determined by (12).

$$a_1' \oplus a_3' = x_1, \quad a_2' \oplus a_3' = x_2 \tag{12}$$

It also can be seen from Table 1 that $(1, 3, 2)$ coding has higher embedding efficiency than $(1, 1, 1)$ coding. Furthermore, $(1, 3, 2)$ coding has higher embedding rate than $(1, 7, 3)$ coding. Therefore, this paper proposes a novel quantum image steganography algorithm mainly based on $(1, 3, 2)$ coding.

B. THE NCQI REPRESENTATION FOR QUANTUM COLOR IMAGES

In 2016, the novel quantum representation of color digital images (NCQI [20]) was first proposed by Sang *et al.*. The NCQI representation employs two entangled qubit sequences so that the RGB information and the position information of each pixel can be encoded together. And the whole image is stored in the superposition of the two qubit sequences. As a result, a $2^n \times 2^n$ quantum color image can be represented as (13),

$$|I\rangle = \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} |h(i)\rangle \otimes |i\rangle \tag{13}$$

where $\otimes$ denotes the tensor product. The i_{th} pixel's RGB information $|h(i)\rangle$ is encoded by three color component channels, as shown in (14).

$$\begin{aligned} |h(i)\rangle &= \bigotimes_{j=0}^{7} \left|R_j^i\right\rangle \bigotimes_{j=0}^{7} \left|G_j^i\right\rangle \bigotimes_{j=0}^{7} \left|B_j^i\right\rangle \\ &= \left|R_7^i R_6^i \cdots R_0^i\right\rangle \left|G_7^i G_6^i \cdots G_0^i\right\rangle \left|B_7^i B_6^i \cdots B_0^i\right\rangle, \\ & R_j^i, G_j^i, B_j^i \in \{0, 1\}, \quad h(i) \in \left[0, 2^{24} - 1\right] \end{aligned} \tag{14}$$

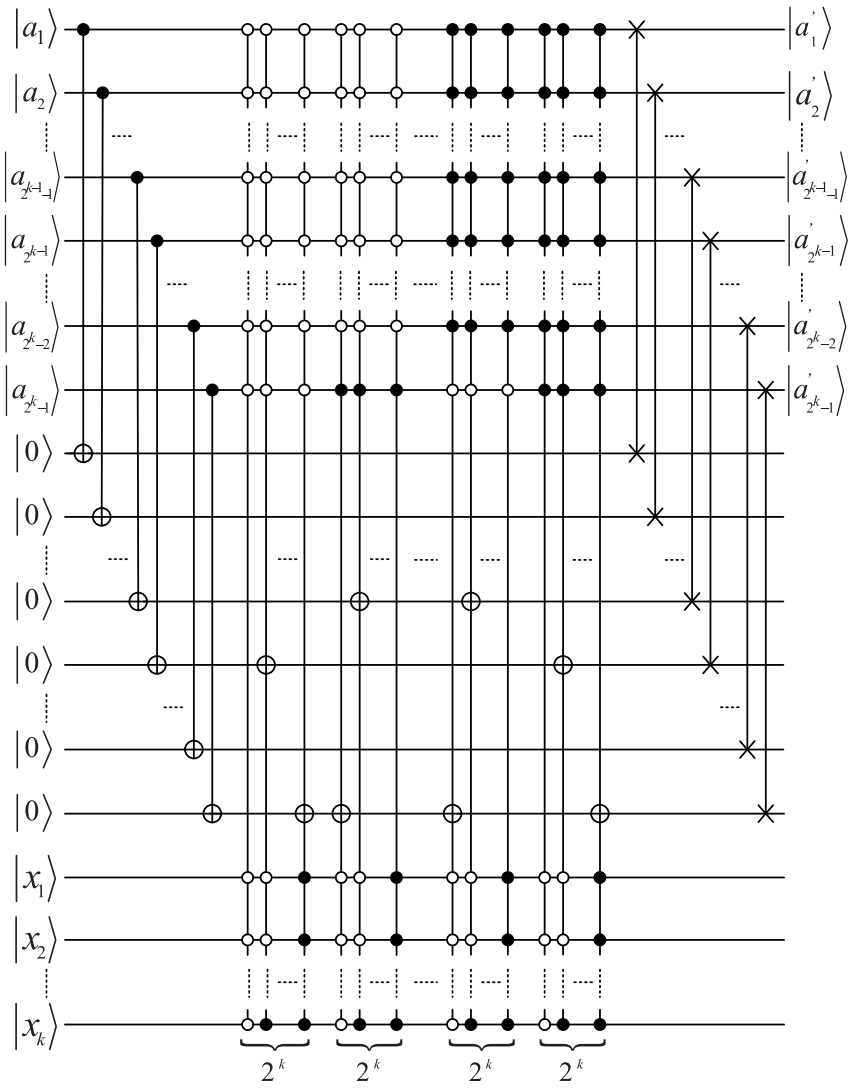


FIGURE 1. A universal quantum circuit for embedding secret information based on (1, *n*, *k*) coding.

The subscript j of $\left|R_j^i\right\rangle$ denotes the j_{th} qubit in 8 qubits of the Red information. In addition, the i_{th} pixel's position information $|i\rangle$, including the vertical information and the horizontal information, can be defined as in (15).

$$|i\rangle = |y\rangle\,|x\rangle = |y_{n-1}y_{n-2}\cdots y_0\rangle\,|x_{n-1}x_{n-2}\cdots x_0\rangle$$
$$y \in \left[0, 2^n - 1\right], \quad x \in \left[0, 2^n - 1\right], \; i \in \left[0, 2^{2n} - 1\right] \tag{15}$$

III. QUANTUM IMAGE STEGANOGRAPHY ALGORITHM BASED ON MATRIX CODING

According to the rule of (1, n, k) coding introduced in Section II, universal quantum circuits for embedding and extracting secret information based on (1, n, k) coding are designed and shown in Figures 1 and 2, respectively. The symbols "•", "○", "⊕" and "×" in Figure 1 represent "one control", "zero control", "NOT operation" and "swap operation", respectively. Meanwhile, dedicated quantum circuits for embedding and extracting secret information based on (1, 3, 2) coding are also designed and shown in Figures 3 and 4, respectively.

In order to achieve better performance in imperceptibility and the embedding efficiency than that of previous quantum image steganography algorithms, this paper proposes a novel quantum image steganography algorithm based on (1, 3, 2) coding, which has better performance than (1, 1, 1) coding and (1, 7, 3) coding in matrix coding. The flow chart of the proposed (1, 3, 2) coding algorithm is shown in Figure 5.

In (1, 3, 2) coding, at most 1 LSB in 3 carrier data will be changed to embed 2 bits of secret information. According to the number of pixels of quantum carrier image used to embed secret information, two different embedding methods based on (1, 3, 2) coding are proposed in this paper, i.e., single

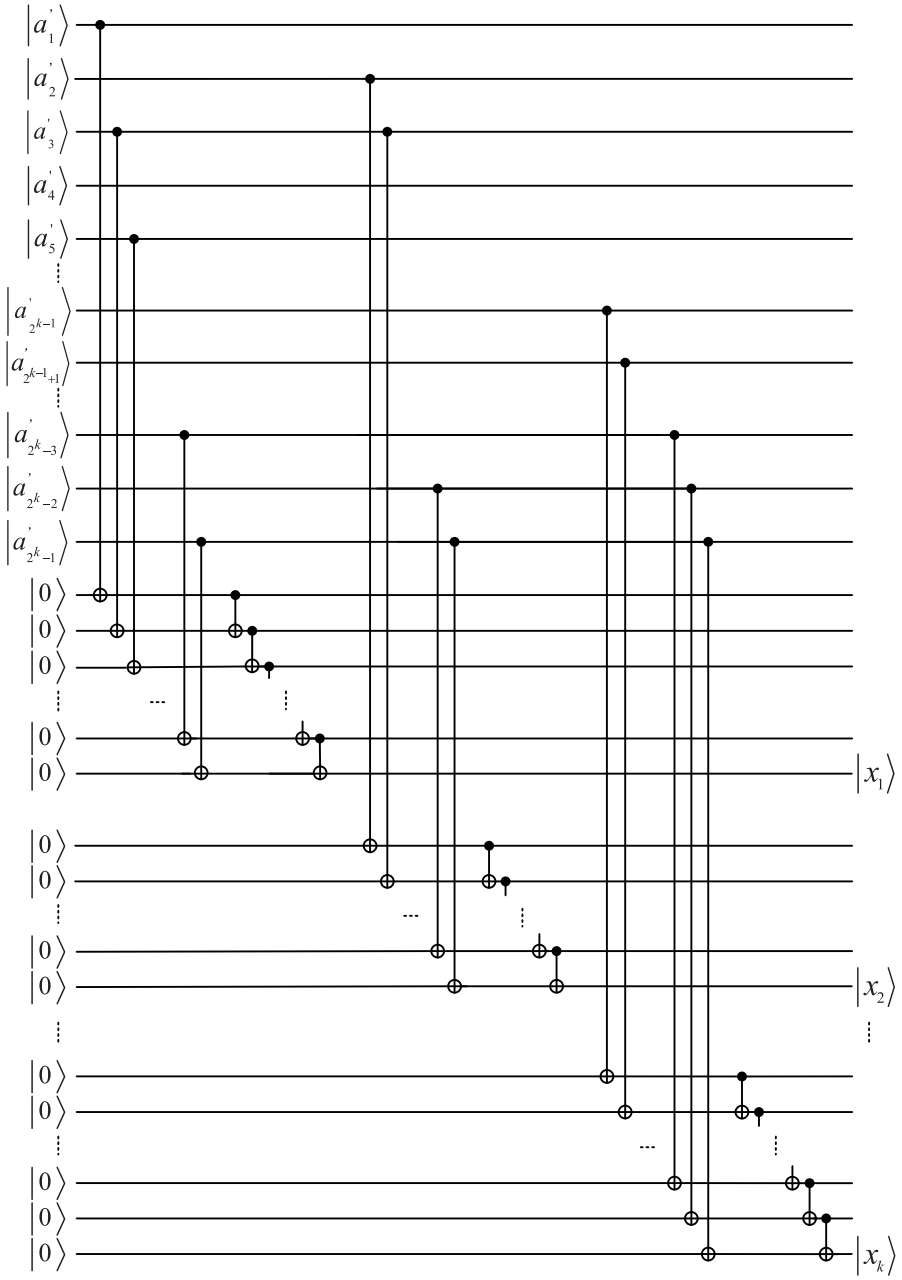


FIGURE 2. A universal quantum circuit for extracting secret information based on (1, *n*, *k*) coding.

pixel-embedded (1, 3, 2) coding (called SPE (1, 3, 2) coding for short) and multiple pixels-embedded (1, 3, 2) coding (called MPsE (1, 3, 2) coding for short).

A. QUANTUM IMAGE STEGANOGRAPHY ALGORITHM BASED ON SPE (1, 3, 2) CODING

SPE (1, 3, 2) coding is to embed 2 secret qubits into 3 LSQbs encoded by three color component channels of a single pixel. The detailed steps of SPE (1, 3, 2) coding are presented as follows.

Step1 At first, in the NCQI representation, a color image of size $2^n \times 2^n$ can be expressed as (16).

$$|C\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}\left(\left|R_7^iR_6^i\cdots R_0^i\right\rangle_{1-8}\left|G_7^iG_6^i\cdots G_0^i\right\rangle_{9-16}\left|B_7^iB_6^i\cdots B_0^i\right\rangle_{17-24}|i\rangle\right) \quad (16)$$

The i_{th} pixel's RGB information of quantum color image $|C\rangle$ has 3 LSQbs, i.e., $|R_0^i\rangle_8$, $|G_0^i\rangle_{16}$ and $|B_0^i\rangle_{24}$.

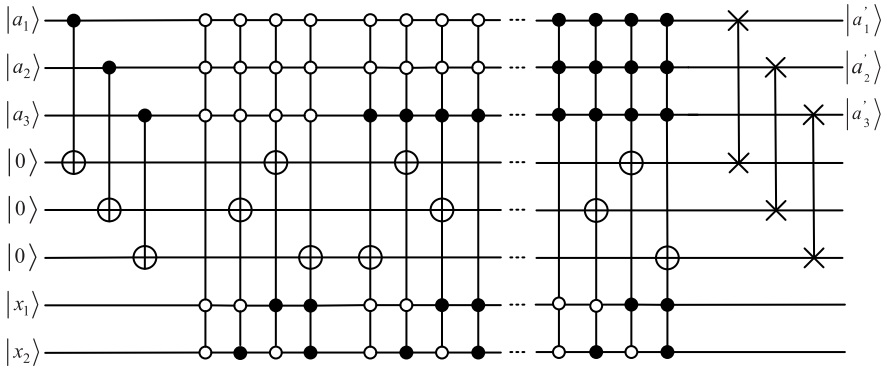


FIGURE 3. A dedicated quantum circuit for embedding 2-qubits secret information based on (1, 3, 2) coding.

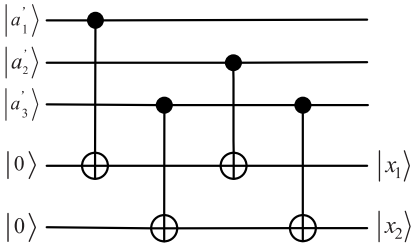


FIGURE 4. A dedicated quantum circuit for extracting 2-qubits secret information based on (1, 3, 2) coding.

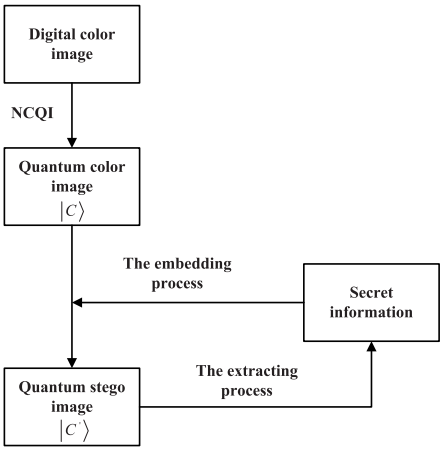


FIGURE 5. Flow chart of the proposed (1, 3, 2) coding algorithm.

Step2 Next, the $2i_{th}$ secret qubit $|x_{2i}\rangle$ and the $(2i+1)_{th}$ secret qubit $|x_{2i+1}\rangle$ are embedded into $\left|R_0^i\right\rangle_8 \left|G_0^i\right\rangle_{16} \left|B_0^i\right\rangle_{24}$ by (1, 3, 2) coding, which can be realized by the dedicated quantum circuit shown in Figure 3. After embedding all secret information into the corresponding pixels by recursively implementing this method, quantum color image $|C\rangle$ becomes quantum stego image $\left|C'\right\rangle$.

$$\left|C'\right\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}\left(\left|R_7^iR_6^i\cdots R_0^{i'}\right\rangle_{1-8}\left|G_7^iG_6^i\cdots G_0^{i'}\right\rangle_{9-16}\left|B_7^iB_6^i\cdots B_0^{i'}\right\rangle_{17-24}|i\rangle\right) \quad (17)$$

In this way, the embedding process is completed.

Step3 Finally, the extracting process is basically the reverse of the embedding process. The detailed steps are given as follows.

(1) Quantum stego image $\left|C'\right\rangle$ is a complex vector in Hilbert Space of size 2^{24+2n}. Let's decompose the vector $\left|C'\right\rangle$ into the direct product of the RGB information and corresponding position information given as (18).

$$\left|C'\right\rangle = m_0 \otimes \begin{pmatrix}1\\0\\\vdots\\0\\0\end{pmatrix}_{2^{2n}\times 1} + m_1 \otimes \begin{pmatrix}0\\1\\\vdots\\0\\0\end{pmatrix}_{2^{2n}\times 1} + \cdots + m_{2^{2n}-1} \otimes \begin{pmatrix}0\\0\\\vdots\\0\\1\end{pmatrix}_{2^{2n}\times 1} \quad (18)$$

Obviously, this operation can be realized because the vector $\left|C'\right\rangle$ and the binary sequence of all pixels' position information are known.

(2) All pixels' RGB information of $m_0, m_1, \cdots, m_{2^{2n}-2}$ and $m_{2^{2n}-1}$ are respectively encoded into the appropriate binary sequence which consists of 24 qubits. Then, the 8_{th} qubit, the 16_{th} qubit and the 24_{th} qubit of the i_{th} pixel's RGB binary sequence are extracted to obtain values of $\left|R_0^{i'}\right\rangle_8$, $\left|G_0^{i'}\right\rangle_{16}$ and $\left|B_0^{i'}\right\rangle_{24}$. In the same way, all of $\left|R_0^{0'}\right\rangle_8$, $\left|G_0^{0'}\right\rangle_{16}$, $\left|B_0^{0'}\right\rangle_{24}$, $\cdots$, $\left|R_0^{(2^{2n}-1)'}\right\rangle_8$, $\left|G_0^{(2^{2n}-1)'}\right\rangle_{16}$ and $\left|B_0^{(2^{2n}-1)'}\right\rangle_{24}$ are also obtained. Those values form a initial binary string with the length of 3×2^{2n}.

(3) Each of 3 qubits of the initial binary string are taken as a group to extract 2 secret qubits by (1, 3, 2) coding. In this way, a new binary string of length 2^{2n+1} is formed. According to the length of secret information, the redundant part of the new binary string is removed to obtain the final binary string of secret information.

With this, the extracting process is also completed.

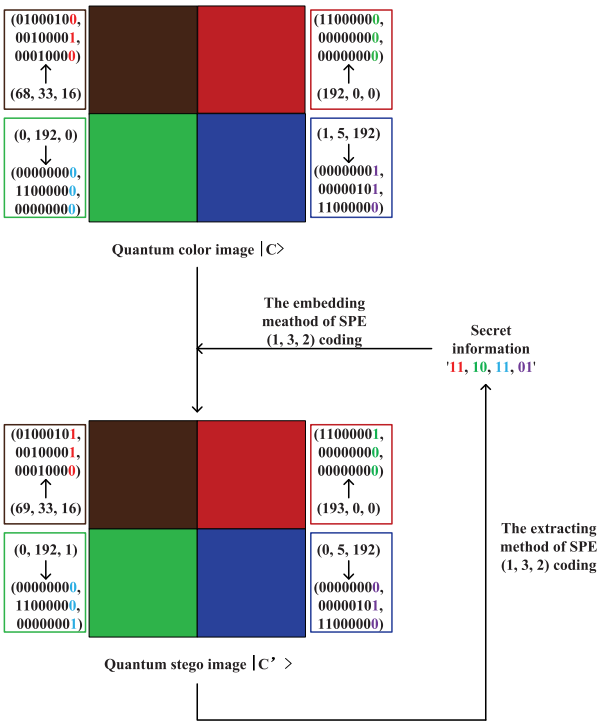


FIGURE 6. A quantum image steganography algorithm based on SPE (1, 3, 2) coding.

From the process of SPE (1, 3, 2) coding described above, it can be calculated that the embedding efficiency of SPE (1, 3, 2) coding is 2.67, and the embedding capacity of secret information is less than 2^{2n+1}. Moreover, the number of the embedded secret qubits in each pixel of quantum color image is 2. Figure 6 shows the process that using quantum color image of size $2^1 \times 2^1$ embeds secret information '11101101' by SPE (1, 3, 2) coding.

Similarly, the process of SPE (1, 1, 1) coding is that three successive secret qubits $|x_{3i}\rangle$, $|x_{3i+1}\rangle$ and $|x_{3i+2}\rangle$ are respectively embedded into $|R_0^i\rangle_8$, $|G_0^i\rangle_{16}$ and $|B_0^i\rangle_{24}$ of the i_{th} carrier pixel by using the LSB technique. In contrast, SPE (1, 7, 3) coding embeds 3 secret qubits into $|R_2^i\rangle_6$, $|R_1^i\rangle_7$, $|R_0^i\rangle_8$, $|G_1^i\rangle_{15}$, $|G_0^i\rangle_{16}$, $|B_1^i\rangle_{23}$ and $|B_0^i\rangle_{24}$ encoded by the i_{th} carrier pixel.

B. QUANTUM IMAGE STEGANOGRAPHY ALGORITHM BASED ON MPSE (1, 3, 2) CODING

MPsE (1, 3, 2) coding can embed 2 secret qubits into 3 LSQbs encoded by one color component channel belonging to multiple pixels. The detailed steps of MPsE (1, 3, 2) coding are provided as follows.

Step1 According to the NCQI representation in Equation (16), a color image of size $2^n \times 2^n$ can be expressed as quantum color image $|C\rangle$. Three LSQbs $\left|R_0^{3j}\right\rangle_8$, $\left|R_0^{3j+1}\right\rangle_8$ and $\left|R_0^{3j+2}\right\rangle_8$ are respectively encoded by the $3j_{th}$ carrier pixel, the $(3j+1)_{th}$ carrier pixel and the $(3j+2)_{th}$ carrier pixel of the Red channel, where $j \in \left[0, 2^{2n}/3\right]$. Three LSQbs $\left|G_0^{3j}\right\rangle_{16}\left|G_0^{3j+1}\right\rangle_{16}\left|G_0^{3j+2}\right\rangle_{16}$ in the Green channel and three LSQbs $\left|B_0^{3j}\right\rangle_{24}\left|B_0^{3j+1}\right\rangle_{24}\left|B_0^{3j+2}\right\rangle_{24}$ in the Blue channel are similar to that of it. In addition, $\left|B_1^{3j}\right\rangle_{23}\left|B_1^{3j+1}\right\rangle_{23}\left|B_1^{3j+2}\right\rangle_{23}$ in the Blue channel are considered as the indicator named "flag" that can be used in the embedding and extracting processes. According to the value of $\left|B_1^{3j}\right\rangle_{23}\left|B_1^{3j+1}\right\rangle_{23}\left|B_1^{3j+2}\right\rangle_{23}$, one of $\left|R_0^{3j}\right\rangle_8\left|R_0^{3j+1}\right\rangle_8\left|R_0^{3j+2}\right\rangle_8$, $\left|G_0^{3j}\right\rangle_{16}\left|G_0^{3j+1}\right\rangle_{16}\left|G_0^{3j+2}\right\rangle_{16}$ and $\left|B_0^{3j}\right\rangle_{24}\left|B_0^{3j+1}\right\rangle_{24}\left|B_0^{3j+2}\right\rangle_{24}$ is chosen as the embedding location of secret information.

–If the value of $\left|B_1^{3j}\right\rangle_{23}\left|B_1^{3j+1}\right\rangle_{23}\left|B_1^{3j+2}\right\rangle_{23}$ is $|000\rangle$ or $|111\rangle$, $\left|R_0^{3j}\right\rangle_8\left|R_0^{3j+1}\right\rangle_8\left|R_0^{3j+2}\right\rangle_8$ will be chosen;

–If the valve of $\left|B_1^{3j}\right\rangle_{23}\left|B_1^{3j+1}\right\rangle_{23}\left|B_1^{3j+2}\right\rangle_{23}$ is $|010\rangle$ or $|101\rangle$, $\left|G_0^{3j}\right\rangle_{16}\left|G_0^{3j+1}\right\rangle_{16}\left|G_0^{3j+2}\right\rangle_{16}$ will be chosen;

–Otherwise, $\left|B_0^{3j}\right\rangle_{24}\left|B_0^{3j+1}\right\rangle_{24}\left|B_0^{3j+2}\right\rangle_{24}$ will be chosen.

Step2 Next, if $\left|B_1^{3j}\right\rangle_{23}\left|B_1^{3j+1}\right\rangle_{23}\left|B_1^{3j+2}\right\rangle_{23} = |110\rangle$, two successive secret qubits $|x_{2j}\rangle$ and $|x_{2j+1}\rangle$ will be embedded into $\left|B_0^{3j}\right\rangle_{24}\left|B_0^{3j+1}\right\rangle_{24}\left|B_0^{3j+2}\right\rangle_{24}$ by (1, 3, 2) coding. Then, all secret information are embedding into the corresponding pixels, quantum color image $|C\rangle$ becomes quantum stego image $\left|C''\right\rangle$.

$$\left|C''\right\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}\left(\left|R_7^iR_6^i\cdots R_0^{i''}\right\rangle_{1-8}\left|G_7^iG_6^i\cdots G_0^{i''}\right\rangle_{9-16}\left|B_7^iB_6^i\cdots B_0^{i''}\right\rangle_{17-24}|i\rangle\right) \quad (19)$$

In this way, the embedding process is completed.

Step3 Finally, the extracting process is given as follows.

(1) Decompose the vector $\left|C''\right\rangle$ into the direct product of the RGB information and corresponding position information as in (20).

(2) All pixels' RGB information of l_0, $\cdots$, l_{3j}, l_{3j+1}, l_{3j+2}, $\cdots$, $l_{2^{2n}-2}$ and $l_{2^{2n}-1}$ are respectively encoded into the appropriate binary sequence which consists of 24 qubits. Then, the 23_{th} qubit of the i_{th} pixel's RGB binary sequence is extracted to obtain the value of $|B_1^i\rangle_{23}$. Similarly, $|B_1^0\rangle_{23}, \ldots, \left|B_1^{3j}\right\rangle_{23}$, $\left|B_1^{3j+1}\right\rangle_{23}$, $\left|B_1^{3j+2}\right\rangle_{23}, \ldots, \left|B_1^{2^{2n}-2}\right\rangle_{23}$ and $\left|B_1^{2^{2n}-1}\right\rangle_{23}$ are obtained. The value of $\left|B_1^{3j}\right\rangle_{23}\left|B_1^{3j+1}\right\rangle_{23}\left|B_1^{3j+2}\right\rangle_{23}$ can be used to get the embedding location of secret information. According to the embedding location, all the corresponding stego qubits can be extracted from the corresponding pixels' RGB binary sequence, and those qubits will form an initial binary string with the length of 2^{2n}.

(3) Each of 3 qubits of the initial binary string are divided into a group to extract 2 secret qubits by (1, 3, 2) coding. In this way, a new binary string of length $2^{2n+1}/3$ is formed. Finally, according to the length of secret information, the redundant part of the new binary string is removed to obtain the final secret information.

As mentioned above, the extracting process is also completed.

$$\begin{aligned}|C''\rangle = l_0 \otimes \begin{pmatrix}1\\0\\\vdots\\0\\0\\\vdots\\0\\0\end{pmatrix}_{2^{2n}\times 1} + \cdots + l_{3j} \otimes \begin{pmatrix}0\\0\\\vdots\\1\\0\\0\\\vdots\\0\\0\end{pmatrix}_{2^{2n}\times 1} \\ + l_{3j+1} \otimes \begin{pmatrix}0\\0\\\vdots\\0\\1\\0\\\vdots\\0\\0\end{pmatrix}_{2^{2n}\times 1} + l_{3j+2} \otimes \begin{pmatrix}0\\0\\\vdots\\0\\0\\1\\\vdots\\0\\0\end{pmatrix}_{2^{2n}\times 1} \\ + \cdots + l_{2^{2n}-1} \otimes \begin{pmatrix}0\\0\\\vdots\\0\\0\\0\\\vdots\\0\\1\end{pmatrix}_{2^{2n}\times 1}\end{aligned} \tag{20}$$

From the above steps, it can be seen that the embedding efficiency of MPsE (1, 3, 2) coding is also 2.67, and the embedding capacity of secret information is less than $2^{2n+1}/3$. In addition, the number of embedded secret qubits in each pixel of quantum color image is only 0.67. A quantum color image of size $2^1 \times 2^1$ used to embed secret information '10' is shown in Figure 7 to illustrate the secret information embedding and extracting processes of MPsE (1, 3, 2) coding.

Similarly, the process of MPsE (1, 1, 1) coding is to embed 1 secret qubit into one of $\left|R_0^j\right\rangle_8$, $\left|G_0^j\right\rangle_{16}$ and $\left|B_0^j\right\rangle_{24}$ according to the "flag". In addition, MPsE (1, 7, 3) coding embeds three successive secret qubits $\left|x_{3j}\right\rangle$, $\left|x_{3j+1}\right\rangle$ and $\left|x_{3j+2}\right\rangle$ into one of 7 LSQbs' $\left|R_0^{7j}\right\rangle_8 \left|R_0^{7j+1}\right\rangle_8 \cdots \left|R_0^{7j+6}\right\rangle_8$, 7 LSQbs' $\left|G_0^{7j}\right\rangle_{16} \left|G_0^{7j+1}\right\rangle_{16} \cdots \left|G_0^{7j+6}\right\rangle_{16}$ and 7 LSQbs' $\left|B_0^{7j}\right\rangle_{24} \left|B_0^{7j+1}\right\rangle_{24} \cdots \left|B_0^{7j+6}\right\rangle_{24}$ according to the "flag".

IV. EXPERIMENT RESULTS AND PERFORMANCE ANALYSIS

In general, for achieving covert communication, a qualified quantum image steganography algorithm has the following attributes.

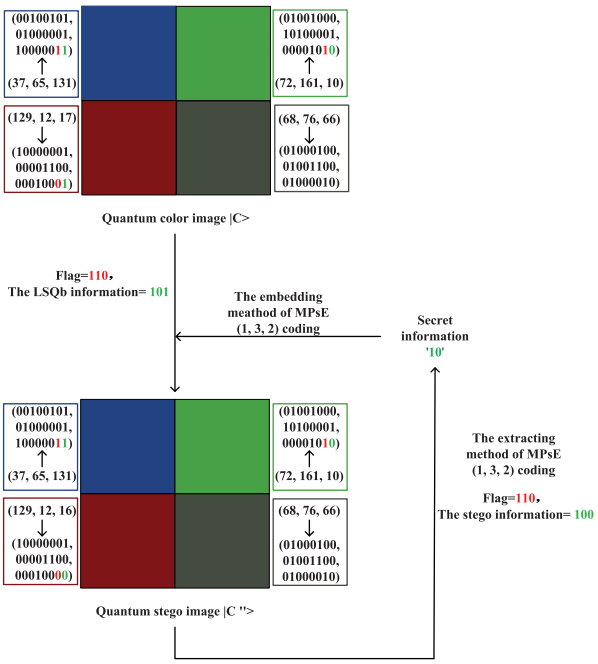


FIGURE 7. A quantum image steganography algorithm based on MPsE (1, 3, 2) coding.

(1) Good imperceptibility. Imperceptibility is one of the most significant parameters to evaluate the performance of a quantum image steganography algorithm. Good imperceptibility can ensure that an eavesdropper (named as "Eve") could not detect or nearly unable to find out the existence of any secret information.

(2) High security. If a legitimate receiver wants to correctly extract secret information from the stego image, a quantum image steganography algorithm should reduce the influence of quantum channel noises on the stego image and prevent Eve modifying the stego image.

(3) High embedding efficiency. The embedding efficiency is capable of reflecting transparency of steganographic methods, which is the ratio between embedded secret qubits and distortion energy caused by data embedding. When embedding secret information into quantum carrier image, fewer modifications to quantum carrier image means higher embedding efficiency, vice versa.

(4) Large embedding capacity. On the premise of not affecting normal use of quantum carrier image, the embedding capacity represents the maximum payload of secret information that can be embedded into quantum carrier image. Under this condition, the more secret information is embedded into quantum carrier image, the larger the embedding capacity will be.

In order to analyze the performance of the new proposed algorithm from the aforementioned four parameters, a number of simulation-based experiments in classical computer MATLAB R2012a environment are conducted in this section. Six color images "Lena", "Airplane", "Vegetables", "Baboon", "Stone" and "University" of size

TABLE 2. PSNR values of the simulation results, the embedding efficiency and the embedding capacity of six embedding methods based on matrix coding and the other embedding algorithms ([25], [26], [28], [30]).

The embedding method	Carrier color images for calculating PSNR values (dB)						The embedding efficiency	The embedding capacity[1]	The embedding capacity[2] ($qubit/pixel$)
	Lena	Airplane	Vegetables	baboon	Stone	University			
SPE (1, 1, 1) coding	48.564	48.784	48.955	49.212	48.601	49.042	2.00	3×2^{2n}	3
SPE (1, 3, 2) coding	51.258	51.765	52.096	52.144	51.976	51.865	2.67	2^{2n+1}	2
SPE (1, 7, 3) coding	47.366	47.454	47.841	47.594	47.657	48.214	3.43	3×2^{2n}	3
MPsE (1, 1, 1) coding	52.246	52.553	53.065	52.449	52.847	52.019	2.00	2^{2n}	1
MPsE (1, 3, 2) coding	57.145	57.852	57.457	57.695	57.047	57.343	2.67	$2^{2n+1}/3$	0.67
MPsE (1, 7, 3) coding	59.144	59.254	59.883	59.201	59.878	59.664	3.43	$3 \times 2^{2n}/7$	0.29
Jiang Nan et al. [25]	50.167	51.134	50.648	50.492	51.017	51.273	2.00	2^{2n}	1
Qu Zhiguo et al. [26]	51.247	51.673	51.376	51.742	52.142	51.834	2.00	2^{2n}	1
Heidari et al. [28]	55.423	55.846	55.703	55.462	55.354	55.246	2.67	2^{2n+1}	2
Qu Zhiguo et al. [30]	56.533	56.143	56.438	56.175	56.814	56.267	2.5	2^{2n}	1

[1] The first expression of the embedding capacity is the maximum number of secret qubits embedded into a $2^n \times 2^n$ quantum carrier image without affecting its normal use.

[2] The second expression of the embedding capacity is defined as the ratio of the number of secret qubits and the number of quantum carrier image's pixels.

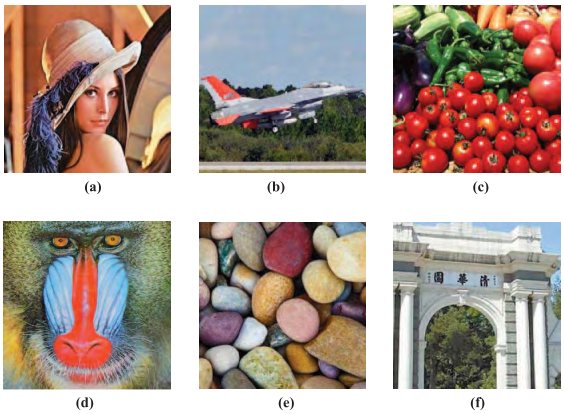


FIGURE 8. Carrier color images used in experiments. (a) Lena. (b) Airplane. (c) Vegetables. (d) Baboon. (e) Stone. (f) University.

$2^8 \times 2^8$ are used as carrier images in experiments, as shown in Figure 8.

A. IMPERCEPTIBILITY

1) PEAK SIGNAL TO NOISE RATIO (PSNR)

For a quantum image steganography algorithm, if the stego image still owns good image quality for its normal use, it implies the algorithm has good imperceptibility. So far, PSNR is widely used to evaluate image quality in digital image processing.

PSNR and MSE (Mean Squared Error) are defined as (21) and (22), respectively.

$$PSNR = 20\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \tag{21}$$

$$\begin{aligned} MSE = \frac{1}{3mn}\sum_{x=0}^{2^n-1}\sum_{y=0}^{2^n-1}\Big\{&[I(x,y,R) - J(x,y,R)]^2 \\ &+ [I(x,y,G) - J(X,Y,G)]^2 \\ &+ [I(X,Y,B) - J(x,y,B)]^2\Big\} \end{aligned} \tag{22}$$

Here I and J are two different images, and MAX_I is the maximum pixel of image I. In the new proposed algorithm, I and J correspond to the original carrier image and the stego image, respectively. Besides, $I(x, y, R)$ represents the Red information of the $(x, y)_{th}$ pixel of image I.

Table 2 lists PSNR values of six embedding methods based on matrix coding and other embedding methods ([25], [26], [28], [30]), which stego images are obtained by embedding the same secret information into different carrier images. It can be seen from Table 2 that PSNR values of the new algorithm are much higher than the image quality standard of 38 dB, which proves that stego images have high image quality. Because three secret qubits are embedded into one carrier pixel, PSNR values of SPE (1, 1, 1) coding and SPE (1, 7, 3) coding are a little lower than that of other algorithms ([25], [26], [28], [30]). Besides, PSNR values of SPE (1, 3, 2) coding, MPsE (1, 1, 1) coding and two other algorithms ([25], [26]) are similar because one LSQbs of a carrier pixel may be changed to embed secret information. Obviously, owing to low modification rate that at most only one pixel may be changed in multiple carrier pixels to embed the same number of secret information, PSNR values of MPsE (1, 3, 2) coding and MPsE (1, 7, 3) coding have higher than that of other algorithms ([25], [26], [28], [30]).

As shown in Figure 9, it is easy to know that differences between carrier images and the corresponding stego images are impossible to be identified by the naked eye of human beings. Therefore, the new algorithm has good imperceptibility.

2) THE HISTOGRAM ANALYSIS

As another tool commonly used in digital image processing, the image histogram can show the frequency of different pixel levels, in which the abscissa contains all gray levels of the image, and the ordinate represents the frequency of different gray levels.

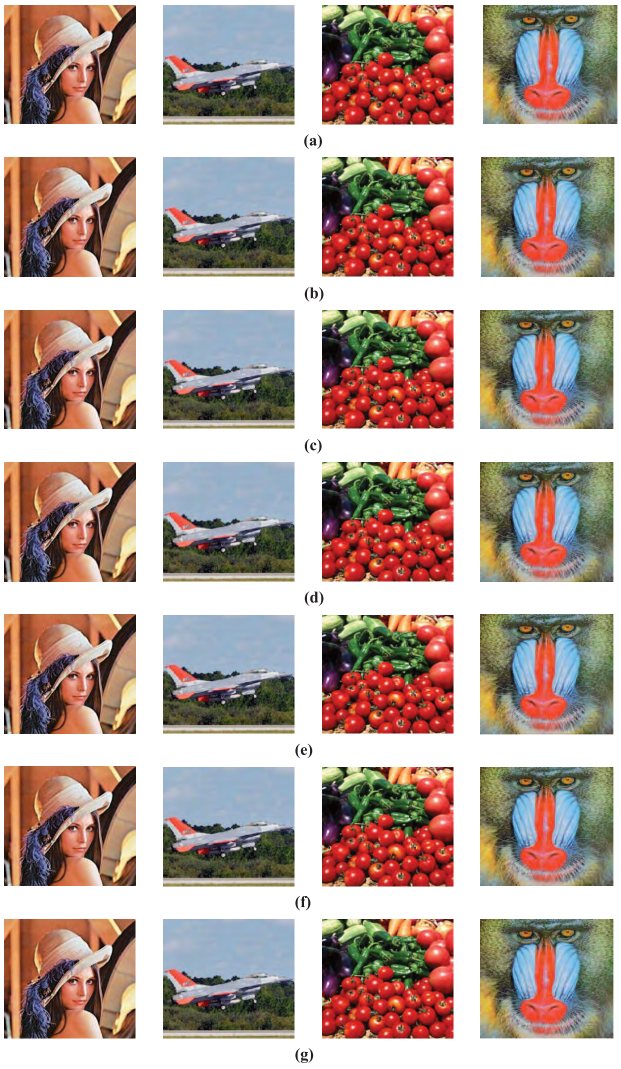


FIGURE 9. Image quality comparison of carrier images and the corresponding stego images. (a) Carrier color images. (b) Stego images based on SPE (1, 1, 1) coding. (c) Stego images based on SPE (1, 3, 2) coding. (d) Stego images based on SPE (1, 7, 3) coding. (e) Stego images based on MPsE (1, 1, 1) coding. (f) Stego images based on MPsE (1, 3, 2) coding. (g) Stego images based on MPsE (1, 7, 3) coding.

In the new proposed algorithm, when the naked eye of human beings cannot detect differences between the carrier image and the corresponding stego image, one can judge whether these two images match or not by comparing their histograms.

Figures 10 and 11 give a number of histograms of carrier images and the corresponding stego images obtained by SPE (1, 3, 2) coding and MPsE (1, 3, 2) coding, respectively. It can be seen from Figures 10 and 11 that each histogram has three different colored lines, with which each line represents one of three color component channels. For example, the red line represents the Red channel. According to Figures 10 and 11, the histogram of the stego image is in adequate agreement with the histogram of the carrier image. Therefore, the new algorithm based on matrix coding has good performance in imperceptibility.

B. SECURITY

In order to ensure security of a quantum image steganography algorithm, it is necessary to reduce the interference of quantum channel noises on the stego image and prevent Eve from obtaining any secret information in the stego image. Thus, the new proposed algorithm's security is analyzed from two aspects. One aspect is from the effect of quantum channel noises and the other aspect is from the influence of Eve attacks.

1) THE EFFECT OF QUANTUM CHANNEL NOISES

In an open quantum channel interacted with external environment, the transmitted qubits are susceptible to the noise. This section will only analyze the effect on a single qubit, because different quantum channel noises are more likely to occur on a single qubit. In general, there are four types of quantum channel noises, namely the bit-flip noise, the phase-flip (phase-damping) noise, the depolarizing noise and the amplitude-damping noise. σ_I, σ_X, σ_Y and σ_Z expressed in (23) belong to Pauli matrices, which are indispensable in the quantum channel noise analysis.

$$\sigma_I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \sigma_X = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \\ \sigma_Y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \sigma_Z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{23}$$

Herein, σ_I is a unit matrix and it means that there is no noise effects on the qubit. σ_X and σ_Z are the bit-flip noise and the phase-flip noise, respectively. $\sigma_Y = i\sigma_X\sigma_Z$ is the superposition of σ_X and σ_Z excepting a global phase of $e^{\frac{\pi}{2}i}$. For the sake of brevity and comprehension, the embedding method of SPE (1, 3, 2) coding is taken as an example to analyze the influence that four quantum channel noises effect on quantum stego image $|C'\rangle$.

In the quantum noisy environment, a pure state will be transformed into a mixed state, which is more convenient to be represented by the density operator rather than the vector state. So the density operator ρ of the i_{th} pixel information of quantum stego image $|C'\rangle$ can be written as (24).

$$\rho = \left(\left| R_7^i \cdots R_0^{i'} G_7^i \cdots G_0^{i'} B_7^i \cdots B_0^{i'} \right\rangle_{1-24} |i\rangle \right. \\ \left. \cdot \langle i| \left\langle R_7^i \cdots R_0^{i'} G_7^i \cdots G_0^{i'} B_7^i \cdots B_0^{i'} \right|_{1-24} \right) \tag{24}$$

(1) The bit-flip noise: Simply speaking, the effect of this noise is to change the state of a qubit from $|0\rangle$ to $|1\rangle$ or $|1\rangle$ to $|0\rangle$ with probability λ which is the noise factor. And Kraus operators [37] of the bit-flip noise are defined as follows.

$$E_0 = \sqrt{1-\lambda}\sigma_I, \quad E_1 = \sqrt{\lambda}\sigma_X, \ 0 \le \lambda \le 1 \tag{25}$$

When ρ is affected by the bit-flip noise $E_q^{(t)}$ (the subscript q is 0 or 1, and the superscript t represents that the

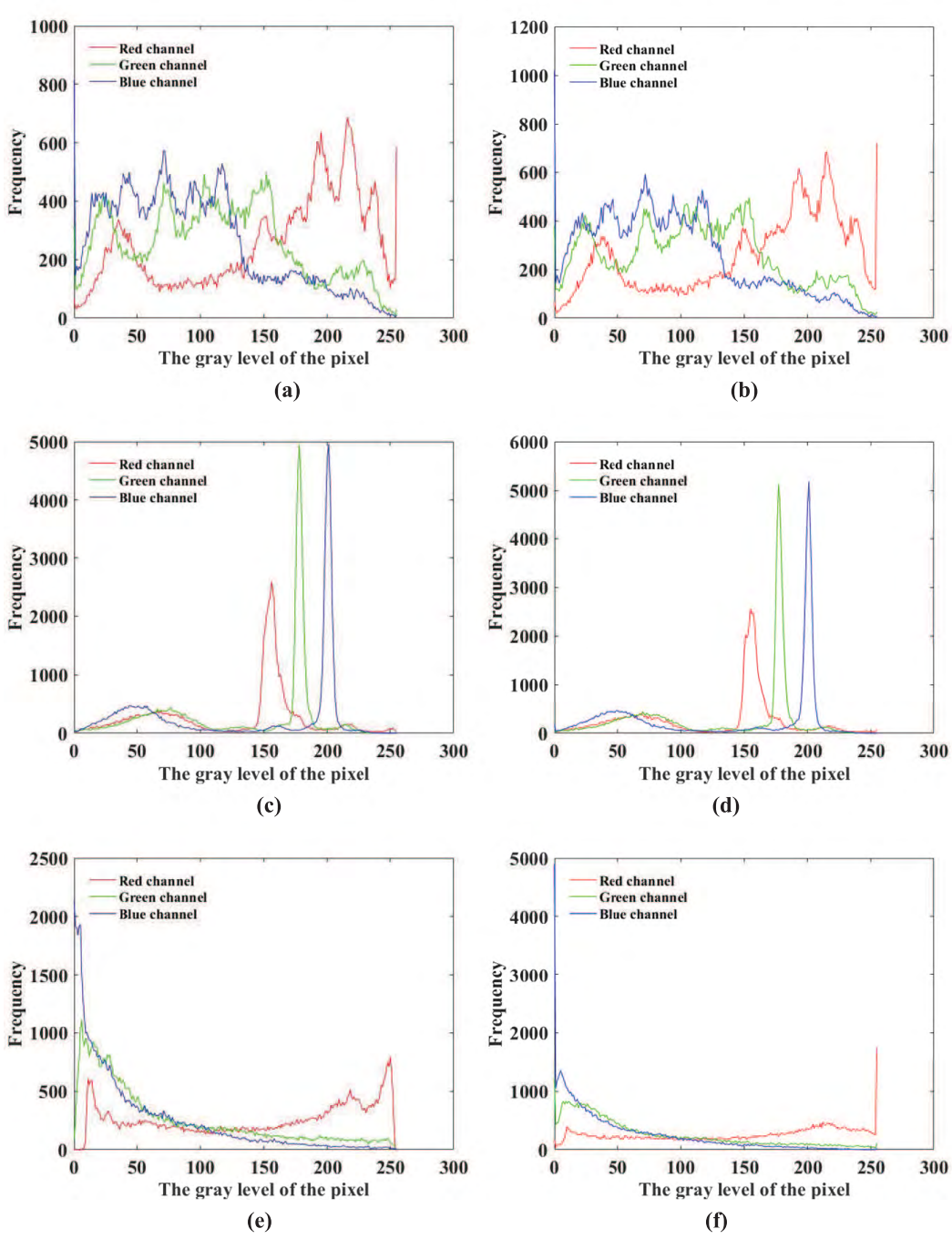


FIGURE 10. The histograms of carrier images and the corresponding stego images obtained by SPE (1, 3, 2) coding. (a) The original carrier image Lena. (b) The corresponding stego image Lena. (c) The original carrier image Airplane. (d) The corresponding stego image Airplane. (e) The original carrier image Vegetables. (f) The corresponding stego image Vegetables.

t_{th} qubit of the RGB information will be affected by the noise), the density operator ε can be obtained as follows.

$$\begin{aligned}\varepsilon &= \sum_{q=0}^{1} E_q^{(24)} \rho E_q^{(24)\dagger} \\ &= E_0^{(24)} \rho E_0^{(24)\dagger} + E_1^{(24)} \rho E_1^{(24)\dagger} \end{aligned} \tag{26}$$

If $\left|B_0^{i'}\right\rangle_{24} = 0$, Equation (26) can be rewritten as:

$$\begin{aligned}\varepsilon_0 = \Big[&(1-\lambda) \left|R_7^i \cdots R_0^{i'} \cdots G_0^{i'} \cdots B_1^i 0\right\rangle_{1-24} |i\rangle \\ &\cdot \langle i| \left\langle R_7^i \cdots R_0^{i'} \cdots G_0^{i'} \cdots B_1^i 0\right|_{1-24} \Big] \\ &+ \Big(\lambda \left|R_7^i \cdots R_0^{i'} \cdots G_0^{i'} \cdots B_1^i 1\right\rangle_{1-24} |i\rangle \\ &\cdot \langle i| \left\langle R_7^i \cdots R_0^{i'} \cdots G_0^{i'} \cdots B_1^i 1\right|_{1-24} \Big) \end{aligned} \tag{27}$$

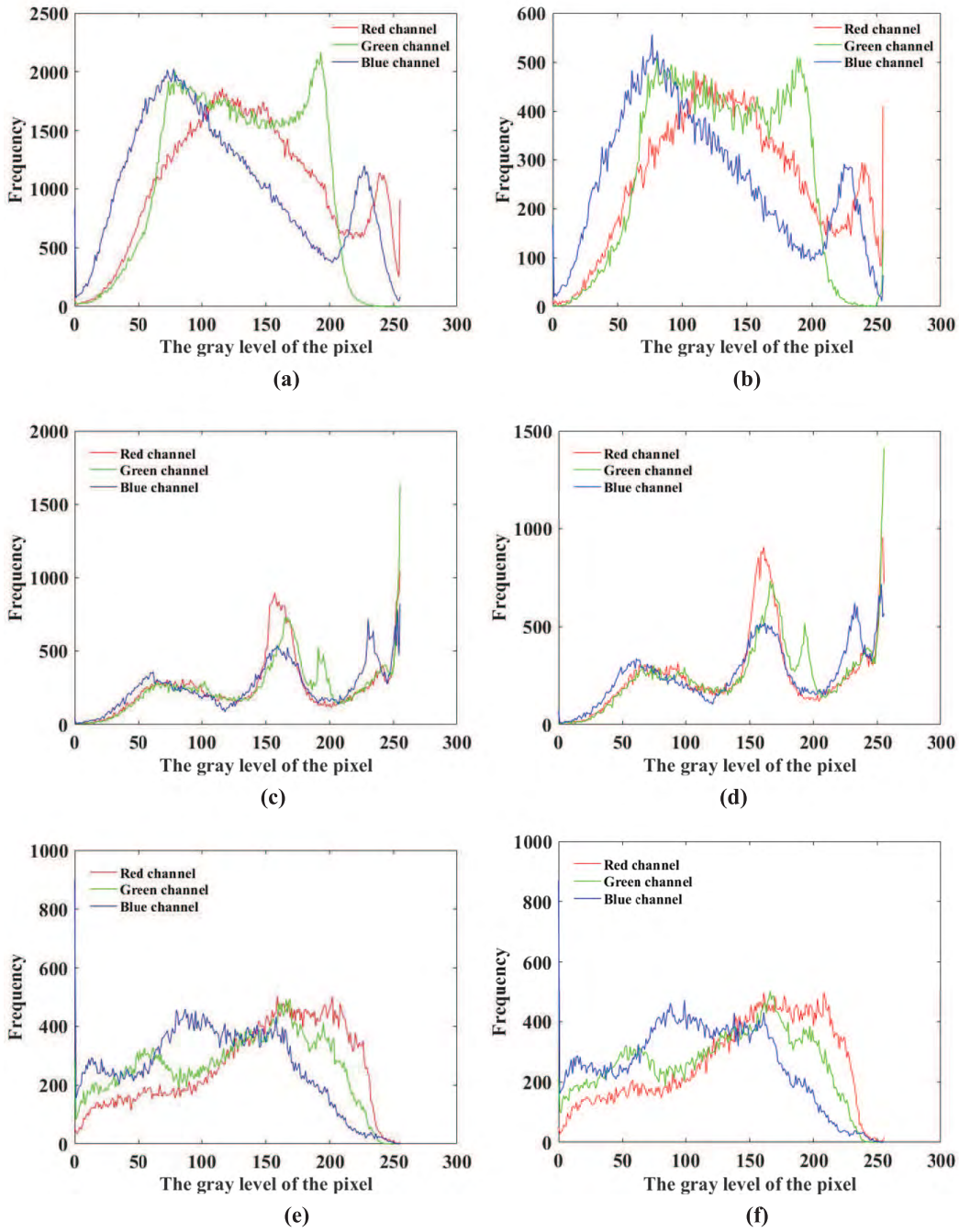


FIGURE 11. The histograms of the another carrier images and the corresponding stego images obtained by MPsE (1, 3, 2) coding. (a) The original carrier image Baboon. (b) The corresponding stego image B. (c) The original carrier image University. (d) The corresponding stego image University. (e) The original carrier image Stone. (f) The corresponding stego image Stone.

Then, the fidelity F_0 between ρ and ε_0 is:

$$\begin{aligned} F_0 &= \left| \langle i| \left| R_7^i \cdots R_0^{i'} \cdots G_0^{i'} \cdots B_1^i 0 \right|_{1-24} \varepsilon_0 \right. \\ &\quad \left. \cdot \left| R_7^i \cdots R_0^{i'} \cdots G_0^{i'} \cdots B_1^i 0 \right\rangle_{1-24} |i\rangle \right| \\ &= 1 - \lambda \end{aligned} \tag{28}$$

If $\left|B_0^{i'}\right\rangle_{24} = 1$, the density operator ε_1 and the fidelity F_1 between ρ and ε_1 are given by (29) and (30), respectively.

$$\begin{aligned} \varepsilon_1 = \Big[&(1-\lambda) \left| R_7^i \cdots R_0^{i'} \cdots G_0^{i'} \cdots B_1^i 1 \right\rangle_{1-24} |i\rangle \\ &\cdot \langle i| \left| R_7^i \cdots R_0^{i'} \cdots G_0^{i'} \cdots B_1^i 1 \right|_{1-24} \Big] \end{aligned}$$

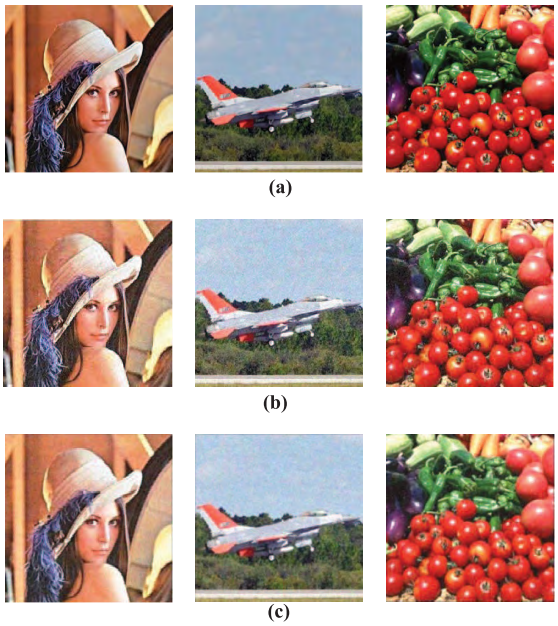


FIGURE 12. The influence of Gauss noise on stego images obtained by SPE (1, 3, 2) coding. (a) The original stego images. (b) The affected stego images subjected by Gauss noise. (c) The treated stego images processing by Gaussian filter.

$$+\left(\lambda\left|R_7^i\cdots R_0^{i'}\cdots G_0^{i'}\cdots B_1^i 0\right\rangle_{1-24}|i\rangle\right.$$
$$\left.\cdot\langle i|\left\langle R_7^i\cdots R_0^{i'}\cdots G_0^{i'}\cdots B_1^i 0\right|_{1-24}\right) \quad (29)$$

$$F_1 = \left|\langle i|\left\langle R_7^i\cdots R_0^{i'}\cdots G_0^{i'}\cdots B_1^i 1\right|_{1-24}\varepsilon_1\right.$$
$$\left.\cdot\left|R_7^i\cdots R_0^{i'}\cdots G_0^{i'}\cdots B_1^i 1\right\rangle_{1-24}|i\rangle\right| = 1-\lambda \quad (30)$$

It can be found from Equation (28) that F_0 keeps increasing with the decreasing of λ, so is F_1. It also shows that the bit-flip noise has weak influence to the new algorithm when λ is small. For clarity, Gauss noise is used to further illustrate the effect of the bit-flip noise on the new algorithm.

In the classical channel, the digital image transmitted may be inevitably disturbed by Gauss noise, which is one of the most common noises. Based on SPE (1, 3, 2) coding, Figure 12 shows the original stego images subjected by Gauss noise and the treated stego images processing by Gaussian filter. It proves that Gaussian filter can reduce the influence of Gauss noise on the new algorithm for the treated stego images having high image quality. Thus, by performing Gaussian filtering beforehand, the new algorithm has good security to effectively resist on the bit-flip noise.

(2) The phase-flip noise: The effect of this noise changes the phase of a qubit from $|1\rangle$ to $-|1\rangle$ with probability λ, and its Kraus operators are defined as follows.

$$E_0 = \sqrt{1-\lambda}\sigma_I, \quad E_1 = \sqrt{\lambda}\sigma_Z,\ 0 \le \lambda \le 1 \quad (31)$$

It is worth noting that the phase-flip noise is equivalent to the phase-damping noise, which describes the loss of quantum information without energy dissipation. Due to all pixels of quantum image are encoded by binary sequences, the phase-flip noise will not have substantial effect on quantum stego image. As a result, the new algorithm can resist on the phase-flip noise.

(3) The depolarizing noise: The effect of this noise is to take a qubit and replace it by a completely mixed state $\sigma_I/2$ with probability λ, and its Kraus operators are defined as follows.

$$E_0 = \sqrt{1-\lambda}\sigma_I, E_1 = \sqrt{\frac{\lambda}{3}}\sigma_X,$$
$$E_2 = \sqrt{\frac{\lambda}{3}}\sigma_Y, E_3 = \sqrt{\frac{\lambda}{3}}\sigma_Z, 0 \le \lambda \le 1 \quad (32)$$

Equation (32) can be understood that ρ is retained with probability $1-\lambda$, and three operators σ_X, σ_Y and σ_Z all act on ρ with probability $\lambda/3$, respectively.

$\sigma_Y = i\sigma_X\sigma_Z$ is the superposition of σ_X and σ_Z excepting a global phase of $e^{\frac{\pi}{2}i}$. As mentioned above, the phase-flip noise σ_Z has no substantial effect on quantum stego image, while only the bit-flip noise σ_X can affect quantum stego image. So, the influence of σ_Y can be simplified to be that of the bit-flip noise.

Consequently, the relevant simulation and analysis of the bit-flip noise also can prove that the new algorithm has good security to resist on the depolarizing noise.

(4) The amplitude-damping noise: This noise describes the energy dissipation effect due to energy loss from a quantum system, and it can be described by Kraus operators as follows.

$$E_0 = \begin{bmatrix} 1 & 0 \\ 0 & \sqrt{1-\lambda} \end{bmatrix}, \quad E_1 = \begin{bmatrix} 0 & \sqrt{\lambda} \\ 0 & 0 \end{bmatrix}, \quad \le \lambda \le 1 \quad (33)$$

It is noted that there is no linear combination of E_0 and E_1 to create a new operator that is direct proportional to the operator σ_I. The operator E_0 keeps $|0\rangle$ unchanged with reduced amplitude of $|1\rangle$. The operator E_1 changes $|1\rangle$ to $|0\rangle$ accompanied by the physical process of losing quantum energy to the environment. Therefore, the new algorithm can better resist on the amplitude-damping noise.

In conclusion, the new algorithm can achieve good security to resist on quantum channel noises.

2) THE INFLUENCE OF EVE ATTACKS

In quantum steganography, intercept-measure-resend attack, entanglement-measure attack and DoS (Denial of Service) attack are several common quantum attacks that Eve will adopt.

(1) Intercept-measurement-resend attack: The procedure of this attack is that Eve intercepts the stego image transmitted in the quantum channel and measures it. Then, Eve sends the intercepted quantum image to the legitimate receiver. It can be seen from Equations (17) and (19) that all information of the stego image is expressed in a superposition state. If the stego image is collapsed into a monochrome image once Eve measures it, the receiver will notice the presence of Eve and

abort the communication. Thus, the new algorithm is resilient to intercept-measurement-resend attack.

(2) Entanglement-measure attack: The procedure of this attack is as follows. Eve uses the unitary operation to entangle her own auxiliary particles with the stego image to generate the new image. Then, Eve sends the new image back to the receiver. Finally, Eve tries to obtain secret information from her own auxiliary particles and the new image. In Section III, the process of extracting secret information based on SPE (1, 3, 2) coding is presented in detail. It also can be seen from Equation (18) that the receiver will be conscious of the difference in the number of qubits between the stego image and the new image. In other words, Eve cannot solve the entanglement between her own auxiliary particles with the new image. Therefore, the new algorithm can resist on entanglement-measure attack.

(3) DoS attack: Although Eve cannot get secret information from the stego image in some cases, she could interfere with the communication so that the receiver cannot obtain secret information. DoS attack is one of the most powerful attacks, in which the purpose is not eavesdropping but preventing the communication. Generally, most quantum image steganography algorithms can detect DoS attack but weak in defending against it. However, to launch DoS attack, Eve needs to find out the communication channel first. Fortunately, MPsE (1, 3, 2) coding has good imperceptibility of embedding 2 secret qubits into one of 3 LSQbs' $\left|R_0^{3j}\right\rangle_8 \left|R_0^{3j+1}\right\rangle_8 \left|R_0^{3j+2}\right\rangle_8$, 3 LSQbs' $\left|G_0^{3j}\right\rangle_{16} \left|G_0^{3j+1}\right\rangle_{16} \left|G_0^{3j+2}\right\rangle_{16}$ and 3 LSQbs' $\left|B_0^{3j}\right\rangle_{24} \left|B_0^{3j+1}\right\rangle_{24} \left|B_0^{3j+2}\right\rangle_{24}$, which is determined by the value of $\left|B_1^{3j}\right\rangle_{23} \left|B_1^{3j+1}\right\rangle_{23} \left|B_1^{3j+2}\right\rangle_{23}$. From this point of views, unless Eve attempts to cut off all communication channels at a great cost, the ability of the new algorithm to resist DoS attack can be guaranteed by its good imperceptibility.

In summary, the new algorithm has good security to resist on Eve attacks.

C. THE EMBEDDING EFFICIENCY AND THE EMBEDDING CAPACITY

The embedding efficiency is an important parameter to evaluate the performance of a quantum image steganography algorithm. Random linear matrix coding can be used to approximate the upper bound of the embedding efficiency, which was proved by Andreas [38] in 2001. It can be seen from Table 1 that the embedding efficiency of (1, 3, 2) coding is 2.67, which is considerable. Moreover, the embedding process of SPE (1, 3, 2) coding is simpler than that of MPsE (1, 3, 2) coding, which needs a "flag" to determine the embedding location of secret information.

The embedding capacity of a quantum image steganography algorithm is assessed in two different ways. The first way is the maximum number of secret qubits embedded into quantum carrier image without affecting its normal use. Taking a $2^n \times 2^n$ quantum carrier image for example, the embedding capacities of SPE (1, 3, 2) coding and MPsE (1, 3, 2) coding are 2^{2n+1} and $2^{2n+1}/3$, respectively.

The second way is defined as the ratio of the number of secret qubits and the number of quantum carrier image's pixels. For example, the embedding capacity of SPE (1, 3, 2) coding is calculated as follows.

$$C = \frac{2^{2n+1}}{2^{2n}} = 2qubit/pixel \tag{34}$$

Similarly, the embedding capacity of MPsE (1, 3, 2) coding is 0.67 $qubit/pixel$. It's proved that SPE (1, 3, 2) coding has a higher embedding capacity than MPsE (1, 3, 2) coding.

Table 2 also gives the embedding efficiency and the embedding capacity of six embedding methods based on matrix coding and other embedding methods ([25], [26], [28], [30]), respectively. Compared with the other quantum image steganography algorithms ([25], [26], [28], [30]), it can be seen that the new algorithm based on matrix coding has better performance in terms of the embedding efficiency and the embedding capacity except MPsE (1, 7, 3) coding.

V. CONCLUSION

This paper proposes a novel quantum image steganography algorithm based on matrix coding for quantum color images. According to the number of carrier pixels that are selected to embed secret information, two different embedding methods are proposed. One embedding method is SPE (1, 3, 2) coding that embeds two secret qubits into three LSQbs of a single carrier pixel, and only one LSQb may be changed or three LSQbs unchanged. The other embedding method is MPsE (1, 3, 2) coding that three LSQbs of multiple carrier pixels are used to embed two secret qubits. Furthermore, this paper designs a universal quantum circuit for matrix coding and a dedicated quantum circuit for (1, 3, 2) coding to better understand the processes of embedding and extracting secret information. By observing the image quality comparison between carrier images and the corresponding stego images, calculating their PSNR values, comparing their histograms, and analyzing the effects of quantum channel noises and Eve attacks, simulation results based on MATLAB demonstrate that the new algorithm has good performance in imperceptibility and security. In addition, the embedding efficiency and the embedding capacity of SPE (1, 3, 2) coding are 2.67 and 2^{2n+1} respectively, and MPsE (1, 3, 2) coding are 2.67 and $2^{2n+1}/3$, which are impressive.

REFERENCES

[1] D. Deutsch, "Quantum theory as a universal physical theory," *Int. J. Theor. Phys.*, vol. 24, no. 1, pp. 1–41, Jan. 1985.

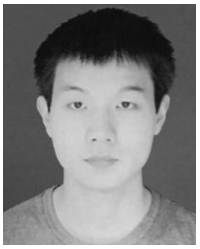
[2] J. F. Du *et al.*, "Experimental realization of quantum games on a quantum computer," *Phys. Rev. Lett.*, vol. 88, no. 13, Apr. 2002, Art. no. 137902.

[3] X.-B. Chen, Z. Dou, G. Xu, C. Wang, and Y.-X. Yang, "A class of protocols for quantum private comparison based on the symmetry of states," *Quantum Inf. Process.*, vol. 13, no. 1, pp. 85–100, Jan. 2014.

[4] G. Xu, X.-B. Chen, Z. Dou, Y.-X. Yang, and Z. Li, "A novel protocol for multiparty quantum key management," *Quantum Inf. Process.*, vol. 14, no. 8, pp. 2959–2980, Aug. 2015.

[5] J. Li, X.-B. Chen, G. Xu, Y.-X. Yang, and Z.-P. Li, "Perfect quantum network coding independent of classical network solutions," *IEEE Commun. Lett.*, vol. 19, no. 2, pp. 115–118, Feb. 2015.
[6] Z. Qu, J. Keeney, S. Robitzsch, F. Zaman, and X. Wang, "Multilevel pattern mining architecture for automatic network monitoring in heterogeneous wireless communication networks," *China Commun.*, vol. 13, no. 7, pp. 108–116, Jul. 2016.
[7] Y. Cao, Z. Zhou, X. Sun, and C. Gao, "Coverless information hiding based on the molecular structure images of material," *Comput. Mater. Continua*, vol. 54, no. 2, pp. 197–207, Feb. 2018.
[8] A. Pradeep, S. Mridula, and P. Mohanan, "High security identity tags using spiral resonators," *Comput. Mater. Continua*, vol. 52, no. 3, pp. 185–195, Dec. 2016.
[9] R. H. Meng, S. G. Rice, J. Wang, and X. Sun, "A fusion steganographic algorithm based on faster R-CNN," *Comput., Mater. Continua*, vol. 55, no. 1, pp. 1–16, Jan. 2018.
[10] Q. Nie, X. Xu, B. Feng, and L. Y. Zhang, "Defining embedding distortion for intra prediction mode-based video steganography," *Comput. Mater. Continua*, vol. 55, no. 1, pp. 59–70, Apr. 2018.
[11] Q. Zhou *et al.*, "Steganography using reversible texture synthesis based on seeded region growing and LSB," *Comput. Mater. Continua*, vol. 55, no. 1, pp. 151–163, Apr. 2018.
[12] Z. G. Qu, T. C. Zhu, J. W. Wang, and X. J. Wang, "A novel quantum stegonagraphy based on Brown states," *Comput. Mater., Continua*, vol. 56, no. 1, pp. 47–59, Jul. 2018.
[13] J. Gea-Banacloche, "Hiding messages in quantum data," *J. Math. Phys.*, vol. 43, no. 9, pp. 4531–4536, 2002.
[14] T. Mihara, "Quantum steganography embedded any secret text without changing the content of cover data," *J. Quantum Inf. Sci.*, vol. 2, no. 1, pp. 10–14, Mar. 2012.
[15] Z.-H. Wei, X.-B. Chen, X.-X. Niu, and Y.-X. Yang, "The quantum steganography protocol via quantum noisy channels," *Int. J. Theor. Phys.*, vol. 54, no. 8, pp. 2505–2515, Aug. 2015.
[16] S. E. Venegas-Andraca and J. L. Ball, "Processing images in entangled quantum systems," *Quantum Inf. Process.*, vol. 9, no. 1, pp. 1–11, 2010.
[17] P. Q. Le, F. Dong, and K. Hirota, "A flexible representation of quantum images for polynomial preparation, image compression, and processing operations," *Quantum Inf. Process.*, vol. 10, no. 1, pp. 63–84, Feb. 2010.
[18] Y. Zhang, K. Lu, Y. Gao, and M. Wang, "NEQR: A novel enhanced quantum representation of digital images," *Quantum Inf. Process.*, vol. 12, no. 8, pp. 2833–2860, 2013.
[19] Y. Zhang, K. Lu, Y. Gao, and K. Xu, "A novel quantum representation for log-polar images," *Quantum Inf. Process.*, vol. 12, no. 9, pp. 3103–3126, Sep. 2013.
[20] J. Sang, S. Wang, and Q. Li, "A novel quantum representation of color digital images," *Quantum Inf. Process.*, vol. 16, no. 2, p. 42, Feb. 2017.
[21] Z. Qu, Z. Cheng, M. Luo, and W. Liu, "A robust quantum watermark algorithm based on quantum log-polar images," *Int. J. Theor. Phys.*, vol. 56, no. 11, pp. 3460–3476, Nov. 2017.
[22] S. E. Venegas-Andraca and S. Bose, "Storing, processing, and retrieving an image using quantum mechanics," *Proc. SPIE*, vol. 5105, pp. 1–11, Aug. 2003.
[23] J. Wang, N. Jiang, and L. Wang, "Quantum image translation," *Quantum Inf. Process.*, vol. 14, no. 5, pp. 1589–1604, May 2015.
[24] N. Jiang and L. Wang, "A novel strategy for quantum image steganography based on moiré pattern," *Int. J. Theor. Phys.*, vol. 54, no. 3, pp. 1021–1032, Mar. 2015.
[25] N. Jiang, N. Zhao, and L. Wang, "LSB based quantum image steganography algorithm," *Int. J.Theor. Phys.*, vol. 55, no. 1, pp. 107–123, 2016.
[26] Z. Qu, H. He, and S. Ma, "A novel self-adaptive quantum steganography based on quantum image and quantum watermark," in *Proc. Int. Conf. Cloud Comput. Secur.*, 2016, pp. 394–403.
[27] S. Heidari, M. R. Pourarian, R. Gheibi, M. Naseri, and M. Houshmand, "Quantum red-green-blue image steganography," *Int. J. Quantum Inf.*, vol. 15, no. 5, Aug. 2017, Art. no. 1750039.
[28] S. Heidari and E. Farzadnia, "A novel quantum LSB-based steganography method using the gray code for colored quantum images," *Quantum Inf. Process.*, vol. 16, no. 10, p. 242, Oct. 2017.
[29] R.-G. Zhou, J. Luo, X. Liu, C. Zhu, L. Wei, and X. Zhang, "A novel quantum image steganography scheme based on LSB," *Int. J. Theor. Phys.*, vol. 57, no. 6, pp. 1848–1863, Jun. 2018.
[30] Z. Qu, Z. Cheng, W. Liu, and X. Wang, "A novel quantum image steganography algorithm based on exploiting modification direction," *Multimedia Tools Appl.*, pp. 1–21, Aug. 2018. doi: 10.1007/s11042-018-6476-5.
[31] I. Amidror, *The Theory of the Moiré Phenomenon* (Computational Imaging and Vision). Dordrecht, The Netherlands: Springer, 2009.
[32] K. Patel, S. Utareja, and H. Gupta, "Information hiding using least significant bit steganography and blowfish algorithm," *Int. J. Comput. Appl.*, vol. 63, no. 13, pp. 24–28, Feb. 2013.
[33] C.-C. Chen and C.-C. Chang, "LSB-based steganography using reflected Gray code," *IEICE Trans. Inf. Syst.*, vol. E91-D, no. 4, pp. 1110–1116, Apr. 2008.
[34] N. Jiang and L. Wang, "Analysis and improvement of the quantum Arnold image scrambling," *Quantum Inf. Process.*, vol. 13, no. 7, pp. 1545–1551, Jul. 2014.
[35] X. Zhang and S. Wang, "Efficient steganographic embedding by exploiting modification direction," *IEEE Commun. Lett.*, vol. 10, no. 11, pp. 781–783, Nov. 2006.
[36] R. Crandall, "Some notes on steganography," in *Posted Steganography Mailing List*. Berlin, Germany: Springer, 1998.
[37] X.-T. Liang, "Classical information capacities of some single qubit quantum noisy channels," *Commun. Theor. Phys.*, vol. 39, no. 5, pp. 537–542, Oct. 2002.
[38] A. Westfeld, "F5-A steganographic algorithm," in *Proc. Int. Workshop Inf. Hiding*, in Lecture Notes in Computer Science, vol. 2137. Pittsburgh, PA, USA: Springer, Oct. 2001, pp. 289–302.

ZHIGUO QU received the Ph.D. degree in information security from the Beijing University of Posts and Telecommunications, in 2011. He is currently an Associate Professor with the School of Computer and Software, Nanjing University of Information Science and Technology, China. His research interests include quantum secure communication and quantum information hiding.



ZHENWEN CHENG is currently pursuing the master's degree in electronics and communication engineering with the Nanjing University of Information Science and Technology, China, in 2016. His research interests include quantum watermarking and quantum steganography.

XIAOJUN WANG received the M.Eng. degree in computer applications from BUPT, in 1987. He did his Ph.D. research at the School of Engineering, Staffordshire University (Staffordshire Polytechnic), England, U.K., from 1989 to 1992. He joined the School of Electronic Engineering, Dublin City University, as an Assistant Lecturer, in 1992, and a Permanent Staff, in 1995, where he was the Head of China Affairs with Dublin City University, from 2002 to 2007, and is currently an Associate Professor. His research interest includes quantum secure communications. He received the Ph.D. Scholarship from the Sino-British Technical Cooperation Training Award, in 1989.