Steganography of Quantum Color Images Based on Blocking and Gray Level Difference

Gaofeng Luo¹, Ling Shi²*, Ammar Oad¹,² and Liang Zong¹

¹College of Information Engineering, Shaoyang University, Shaoyang 422000, China
²Department of Information Technology and Creativity, Shaoyang Polytechnic, Shaoyang 422000, China
³Information Technology Center, Sindh Agriculture University Tandojam, Hyderabad, Sindh, Pakistan

Received 13 October 2019; Accepted 5 February 2020

Abstract

Steganography of quantum images is restricted by high fidelity and robustness, which limit hiding capacity and decrease visual quality. To improve the concealment of steganographic embedding of secret messages and enhance embedding capacity, the present study proposed a quantum red-green-blue (RGB) image steganography based on image block and gray level difference. First, digital color images were represented by quantum models and divided into non-overlapping blocks. Second, reference pixels in the blocks were selected, and gray level difference between the reference pixels and the G channel of other pixels was calculated. Third, according to the location of the difference, different bit planes where secret messages were embedded into the R and the B channels of the carrier image were determined. Finally, steganographic image was divided into blocks. The G channel gray difference was calculated, and the original secret message was extracted. Results demonstrate that quantum RGB image steganography has a steganographic capacity of four bits per pixel, and its quantum circuit is less complex. In comparison with other quantum image steganographic methods, the proposed method ensures a large steganographic capacity while realizing satisfactory visual quality and steganographic concealment. The study provides reference significance for exploring data hiding and quantum image security based on quantum RGB image block.

Keywords: RGB image, Quantum image processing, Steganography

1. Introduction

With the development of Internet of Things, 5G, and artificial intelligence, theoretical studies of big data have been transformed to practical applications. However, the increasing value of big data has brought serious information security issues. Due to imperceptibility, information steganography has become important means of information security in the era of big data. With the rapid development of sensors and imaging technology, image sharing has become an important part of human life, attracting widespread attention.

Although image information steganography technology has achieved great success, massive real-time image processing has been beyond the capability of classic computers, which can hardly satisfy growing demands. Quantum computing is considered an influential new computing model [1]. Quantum image processing [2] refers to a new processing technology for classic digital images based on the principle of quantum mechanics. With the superposition and entanglement of quantum, quantum image processing can greatly improve the efficiency of digital image processing. This capability has attracted widespread attention from scholars. Moreover, quantum image processing positively affects image edge detection among others [3].

Scholars have thoroughly studied quantum image representations model [4-5] and the corresponding image steganography technology. Its performance in steganography capacity, visual quality, security, and robustness is poor, and quantum steganography mainly focuses on gray level images. Therefore, quantum color image steganography with high capacity, high fidelity, and strong concealment is needed urgently.

This study used quantum RGB image models [6] to represent color images and divided quantum color images into blocks. The gray level difference of the pixel G channel in the blocks was calculated. According to difference location, secret information was embedded into the qubit planes of the R and the B channels of the carrier images, thus enhancing the concealment and security of secret information, improving embedding capacity, and realizing high visual quality. This study not only develops new ideas and methods for traditional image information steganography study, but it also improves image processing efficiency. The proposed method may be used for information security management in the era of quantum computer. Thus, it has important theoretical significance and application value.

2. State of the art

As a branch of data hiding, quantum image steganography refers to using redundant information in quantum carrier images to conceal secret objects. Scholars carried out numerous studies on steganography technology, taking quantum gray level images and quantum color images as
carriers and investigating the technology’s embedding capacity and steganographic visual quality.

Jiang et al. [7] proposed a quantum image steganography scheme based on Moire pattern. Binary image was embedded, and the embedding capacity was low. To increase the embedding capacity, Miyake et al. [8] designed a quantum steganography scheme using a small-scale quantum circuit, which expanded and embedded a watermark image into a quantum carrier image through quantum controlled-NOT (CNOT) gate. The implementation was not complex, and the carrier image after embedding had low visual quality. Naseri et al. [9] discussed a secure quantum steganography scheme, which used LSB and the most significant bit (MSB) to verify imperceptibility, robustness, and capacity through simulation. Two key images were used in the embedding process, leading to a highly complex quantum circuit. Heidari et al. [10] used the embedding and extraction double-key mechanism to propose a novel quantum image hiding method and designed a copyright protection method for quantum data with high robustness. However, the method was mainly used for quantum image watermarking and copyright protection. A novel quantum image steganography algorithm based on an efficient embedding technique of exploiting modification direction was proposed [11]. However, the embedding rate was low. In frequency domain, a least significant qubit information hiding algorithm was analyzed theoretically [12]. The similarity of the above-mentioned quantum image steganography methods was that the embedded carrier comprised quantum gray level images, and most of which were designed based on LSB. Moreover, these methods had fixed embedding locations and limited steganographic capacity.

Heidari et al. [13] employed Gray code to implement the LSB steganography algorithm for quantum color images, but the quantum circuit complexity was high. Additionally, he proposed three LSB steganography algorithms for quantum color images [14]. These methods used one or two channels of color images to hide secret data. Simple XOR operation was used in the embedding process, leading to limited embedding capacity and poor robustness. El-latif et al. [15] presented a data hiding method for quantum gray level image and embedded a secret image into the carrier image. LSB and MSB were used in the embedding process. However, embedding capacity and position were fixed, and concealment was poor. Li et al. [16-17] proposed a steganography method that embedded secret messages into quantum color images. The Gray code was used in the embedding process, and the embedding capacity was low. Based on Arnold transformation and LSB steganography, Zhou et al. [18] brought forward a quantum steganography algorithm for color images, and such an algorithm can be applied to copyright protection of quantum images. Based on quantum walks, a new technique for image steganography was designed [19]. It could be used with any type of secret message. However, the proposed method was an integrated mechanism between quantum walks and classical data hiding.

The above quantum red-green-blue (RGB) image steganography embedding methods mainly considered embedding capacity and visual quality. LSB was used for embedding, and the embedding position was fixed. Few studies focused on the steganographic embedding of quantum RGB image blocks. The studies of embedding secret data to different qubit planes of carrier images based on the gray-level difference of pixels in blocks were also rare. The current study used RGB image quantum representation model to calculate gray level difference of pixels in blocks based on image blocking. The embedded bit plane was determined according to difference location, which cannot only improve embedding concealment but can also meet the requirements for embedding capacity and visual quality.

The remainder of this study is organized as follows. Section 3 introduces the quantum RGB image model and discusses image blocks and the corresponding preprocessing operation. Moreover, the embedding and extraction methods and the corresponding quantum circuits are presented in the section. Section 4 establishes a simulation model and performs simulations of the steganography method. The results are analyzed and discussed from the aspects of visual quality, embedding capacity, and complexity. Section 5 summarizes this study and draws conclusions.

3. Methodology

This section introduces the quantum RGB image model and relevant image preprocessing operation. The proposed secret message steganography and extraction method is then analyzed and discussed. Fig. 1 shows the quantum RGB image steganographic embedding and extraction process of the proposed method.

3.1 Quantum image representation

For the novel enhanced quantum representation (NEQR) of digital images [5], Abdolmaleky [6] proposed a quantum representation model for RGB images, and the color information was represented by three channels of the red, green and blue. Similar to the novel quantum image representation method, this model uses two quantum entangled sequences to represent the color and the position of pixels. The first quantum sequence represents the color information of RGB of the color image pixels, and the second quantum sequence represents the coordinate information of the pixels. The value range of the three channels of the color images is from 0 to 255. The expression of the RGB image with the size of $2^n \times 2^n$ is as follows:

$$|I\rangle = \frac{1}{2^n} \sum_{i=0}^{2^n} |C_{\text{RGB}}\rangle \otimes |i\rangle$$

(1)

where $\otimes$ represents the tensor product, and $|C_{\text{RGB}}\rangle$ represents the color information of the three channels of RGB of pixel $i$. The definition is as follows:

$$|C_{\text{RGB}}\rangle = |R_i\rangle |G_i\rangle |B_i\rangle$$

(2)

where

$$|R_i\rangle = |r_i^1 r_i^2 \ldots r_i^6\rangle,$$
$$|G_i\rangle = |g_i^1 g_i^2 \ldots g_i^6\rangle,$$
$$|B_i\rangle = |b_i^1 b_i^2 \ldots b_i^6\rangle,$$

$i^r, i^g, i^b \in \{0,1\}$. 
Coordinate position $|y\rangle$ is defined as follows:

$$|y\rangle = |y_1, y_2, \ldots, y_n\rangle = |y_{n-1}, y_{n-2}, \ldots, y_0\rangle$$

where the two $n$-qubit sequences represent the ordinate and abscissa of color images.

3.2 Quantum image blocking and preprocessing

Suppose the size of the quantum color image (carrier) to $2^n \times 2^n$, and the gray levels of the three channels of RGB are 256. The above-mentioned quantum color image representation model is used to express the carrier image as follows:

$$|I\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} |R_{y}\rangle |G_{y}\rangle |B_{y}\rangle \otimes |y\rangle |x\rangle$$

(5)

Some relevant pixels can be selected by fixing certain qubit values of coordinate information, making quantum image blocking possible. Fig. 2 shows a $4 \times 4$ quantum image, with Y-coordinate $|y_{1,0}\rangle$ and X-coordinate $|x_{0,0}\rangle$. $|y_{1,0}\rangle$ is limited to $|0\rangle$, and $|x_{0,0}\rangle$ is limited to $|0\rangle$, which is the $2 \times 2$ block area (block 1) of the upper left corner of the image. In the quantum circuit, $|y_{1,0}\rangle$ and $|x_{0,0}\rangle$ are control qubits. When the values of the control qubits are $|0\rangle$, the $2 \times 2$ area of the upper left corner of the image is processed. According to the image blocking method, the quantum image can be divided into four non-overlapping $2 \times 2$ image blocks (blocks 1, 2, 3, and 4).

Upon dividing the quantum image into blocks, each block is composed of four pixels with the following values: $|f(Y, X)\rangle$, $|f(Y, X+1)\rangle$, $|f(Y+1, X)\rangle$, and $|f(Y+1, X+1)\rangle$. The first pixel is selected as the reference pixel, and the four pixels are divided into three pairs in horizontal, vertical, and diagonal directions, as shown in Fig. 3. Human visual system is highly sensitive to the change of the gray level of G channel. Hence, this study only used the green channel to calculate the gray level difference, and it embedded secret messages into R and B channels.

Set the absolute value set of the three pairs of pixel gray level differences in each block to $\{d_1, d_2, d_3\}$. The quantum module is calculated using the absolute value module [22]:

$$d_1 = |f_G(Y, X) - f_G(Y, X+1)|,$$

$$d_2 = |f_G(Y, X) - f_G(Y+1, X)|,$$

$$d_3 = |f_G(Y, X) - f_G(Y+1, X+1)|.$$  

(6)

where $d_i \in [0, 255]$. Statistical analysis is used to divide the difference between adjacent pixels into high, medium, and low levels, as shown in Fig. 4.

In general, small difference values indicate that the pixels are located in a smooth area, whereas large difference values indicate edge area. Therefore, this study first classifies the difference values and adaptively determines the edge characteristics of the area according to the distribution of the three difference values. Specifically, if the absolute values of the difference values between the three pairs of pixels in the horizontal, vertical, and diagonal directions all belong to the interval $[0, 7]$, then the block is low level. Similarly, the intervals $[8, 15]$ and $[16, 255]$ belong to middle- and high-level blocks, respectively.

Fig.1. Embedding and extraction process

Fig.2. Quantum RGB image blocks
Based on the above analysis, Threshold$_1 = (00001111)_2$ and Threshold$_2 = (00001111)_2$ are predefined to achieve the threshold comparison operation. The threshold comparison quantum circuit of the first threshold is shown in Fig. 5. Qubit $|0\rangle$ is taken as the input auxiliary bit. After $U_T$ operation, if the output qubit satisfies $|\text{Output}\rangle = |1\rangle$, $i = 1,2,3$, namely $d_i \leq (7)_{10}$, then the area belongs to a low-level block.

$$|S\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |S_{yx}\rangle \otimes |yx\rangle = \frac{1}{2^{n+1}} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} \sum_{l=0}^{3} |S_{yx}\rangle \otimes |yx\rangle. \quad (7)$$

To enhance confidentiality, the expanded secret image was subjected to scramble operation, and the quantum bits were conducted with scramble sub-operation $T_{YX}$ through quantum exchange gate unitary operation $U_{YX}$.

$$T_{YX} = I \otimes \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |yx\rangle \langle yx| + U_{YX} \otimes |YX\rangle \langle YX|, \quad (8)$$

where $T_{YX}$ is a unitary matrix, which satisfies $T_{YX}T_{YX}^\dagger = I$ (mod $2^{n+1}$). $T_{YX}^\dagger$ is the conjugate transpose of $T_{YX}$. Therefore, all quantum bits of the $2^n$ pixels of the original secret image was conducted with flat switching operation $T$, which can be realized through $2^n$ sub-operation $T_{YX}$ as follows:

$$T = \prod_{y=0}^{2^n-1} \prod_{x=0}^{2^n-1} T_{YX}. \quad (9)$$

Therefore, through the scrambling method, the scrambled quantum secret image can be expressed as follows:

$$|S'_\rangle = \frac{1}{2} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |S'_{yx}\rangle \otimes |yx\rangle. \quad (10)$$

The scrambling operation is reversible. Hence, its inverse operation $T_{YX}^{-1}$ can be used as reverse scrambling operation after secret message extraction.

### 3.3 Secret message expansion and scrambling

The quantum carrier image was divided into blocks, and the gray channel gray values were calculated and compared. The proposed method then performed necessary expansion and scrambling processing on the secret image to achieve the embedding and security of the secret image. The secret image was set to be embedded as gray level image, with the size of $2^n \times 2^n$ and the gray level of 256. From the above analysis, all pixels of the carrier image with a size of $2^n \times 2^n$ were embedded. Therefore, the secret image was extended. For example, a pixel with a gray value of 200 and a binary form of $(11001000)_2$ was expanded to two pixels in a row-major order (horizontal expansion), namely, $(1100)_2$ and $(1000)_2$. The size of the image is $2^n \times 2^n$, and the gray level is 15. The new quantum image representation is as follows:

$$|S\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |S_{yx}\rangle \otimes |yx\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} \sum_{l=0}^{3} |S_{yx}\rangle \otimes |yx\rangle. \quad (7)$$

3.4 Embedding and extraction methods

According to the above analysis, the flowchart of the embedding method is shown in Fig. 6. The pixels of quantum RGB and secret images of the same size were compared and controlled through the quantum comparator [20]. When the coordinate values of the
two images were equal, the following operation was performed.

The quantum RGB carrier image was blocked. The G-channel gray level difference between adjacent pixels was calculated, and the area was determined. The specific quantum circuit is shown in Fig. 7, where CAV represents the absolute value calculation module, and $U_T$ represents the threshold comparison operation.

Upon determining the area, the embedding algorithm must be used to embed the scrambled secret image into the R and B channels of the carrier image. The steps are as follows.

When the gray level differences of the pixel G channel in the block, namely, $|f_G(Y, X) - f_G(Y + 1, X)|$, and $|f_G(Y, X) - f_G(Y + 1, X + 1)|$, were in the interval [0, 7], the highest bit plane of the secret image was embedded into the least significant qubit (LSQb) plane of the R channel of the carrier image, namely, $r_{ys} = s_{ys}^3$. Other bit planes of the secret image were embedded in the lower three LSQb of the B channel of the carrier image, namely, $b_{ys}^2 = s_{ys}^2$, $b_{ys}^1 = s_{ys}^1$, and $b_{ys}^0 = s_{ys}^0$. Similarly, when the gray level difference values of the three directions of the pixel G channel in the carrier image block were in the interval [8, 15], the secret image bit plane was embedded into the lowest 2 LSQb of the R and B channels of the carrier image, namely, $r_{ys}^3 = s_{ys}^3$, $r_{ys}^2 = s_{ys}^2$, $r_{ys}^1 = s_{ys}^1$, $b_{ys}^3 = s_{ys}^3$, $b_{ys}^2 = s_{ys}^2$, and $b_{ys}^1 = s_{ys}^1$. As the gray value difference in the three directions of the pixel G channel in the carrier image block was in the interval [16, 255], the secret image bit plane was embedded into the lower 3 LSQb of the R channel of the carrier image, namely, $r_{ys}^3 = s_{ys}^3$, $r_{ys}^2 = s_{ys}^2$, and $r_{ys}^1 = s_{ys}^1$, and the least significant qubit plane of the B channel, namely, $b_{ys}^0 = s_{ys}^0$. The gray level difference judgment and the embedded circuits are shown in Fig. 8.

Through the above-mentioned embedded quantum circuits, all pixels of the secret image were embedded in the R and B channels of the carrier image to complete the steganography of the image information. At the receiving end, authorized users must extract secret messages through the embedded carrier image (steganography image). In this algorithm, the qubit plane is unchanged because the G channel is only used to determine the area. Therefore, when extracting secret image information, only the gray-scale value of the G channel of the steganographic image is calculated to determine the area. The corresponding qubit plane was extracted according to the embedding methods in different areas to reconstruct the original secret image qubit plane. The steganography algorithm is completely blind, that is, the secret message extraction does not require the auxiliary and key of the original carrier.
4. Result analysis and discussion

Common quantum computers have not yet entered the stage of practicality. Hence, the simulation of the proposed scheme and the quantum circuits was completed using classic computers. The computer hardware configuration is Intel (R) Core (TM) i5-7200U CPU 2.70-GHz 8.00-GB RAM, and the software is MATLAB 2014b. In the simulation experiment, three color images with the size of 256×256 (“Lena,” “Baboon,” and “Airplane”) and the gray level of 255 were used as quantum carrier images and the gray image (Rice) with the size of 256×128 as the secret image to be embedded. All test images are shown in Fig. 9. The secret images to be embedded were extended to 256×256 and scrambled. In the experiment, the extended and scrambled images were embedded into three quantum color images. The visual effects after the embedding are shown in Fig. 10, where (d) is the effect after expansion and scrambling.

4.1 Visual quality

Peak signal-to-noise ratio (PSNR) is one of the important indicators for judging the similarity of two images (such as the embedded carrier image and the original carrier image). High values indicate high degrees of similarity among images. For two carrier images $I$ with the size of $m \times n$ and the corresponding carrier image $J$ after embedding the secret image, PSNR is defined as follows:

$$PSNR=10\log_{10} \frac{MAX^2}{MSE} = 20\log \frac{MAX_I}{\sqrt{MSE}}$$ (11)

where $MAX_I$ represents the maximum gray value of the image color, and $MSE$ is mean squared error, which is defined as follows:

$$MSE = \frac{1}{mn} \sum_{i=1}^{m} \sum_{j=1}^{n} [I(i, j) - J(i, j)]^2$$ (12)

To calculate the PSNR of (a), (b), and (c) in Figs. 9 and 10, the total PSNR value is about 50dB. With RGB image Lena as an example and under different steganographic capacities, PSNR values are compared with algorithms in similar literature, as shown in Table 1, where bpp represents bit per pixel. Obviously, the proposed scheme has great advantages in terms of visual quality.

<table>
<thead>
<tr>
<th>Scheme</th>
<th>PSNR(dB)</th>
<th>Capacity</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ref. [14]</td>
<td>55.9260</td>
<td>1 bpp</td>
</tr>
<tr>
<td>Ref. [14]</td>
<td>52.8852</td>
<td>2 bpp</td>
</tr>
<tr>
<td>Ref. [16]</td>
<td>48.2660</td>
<td>3 bpp</td>
</tr>
<tr>
<td>Ref. [17]</td>
<td>47.3168</td>
<td>4 bpp</td>
</tr>
<tr>
<td>Proposed</td>
<td>50.2653</td>
<td>4 bpp</td>
</tr>
</tbody>
</table>
4.2 Steganographic capacity

Embedding capacity is defined as the maximum amount of secret data hidden in the carrier image without influencing obvious distortion of the carrier image. In general, the embedding capacity is the ratio of the number of embedded secret bits to the total pixels of the carrier image, which is defined as follows:

\[ C = \frac{\text{Number of secret bits}}{\text{Number of cover pixels}} \]  \hspace{1cm} (13)

In this scheme, the steganographic capacity is calculated as follows:

\[ C = \frac{2^n \times 2^{-1} \times 8}{2^n \times 2^2} = 4 \text{ bits / pixel} \]  \hspace{1cm} (14)

Similarly, Table 1 indicates that the embedding capacity of the scheme is up to 4 bits per pixel, and the visible steganographic capacity also has obvious advantages.

4.3 Circuit complexity

According to the theories of quantum computing [1], the complex unitary operation for multiple qubits can be decomposed into a single-qubit logic gate and a two-qubit CNOT gate. Therefore, the complexity of the quantum circuit depends on the number of basic quantum logic gates. The CNOT gate is selected as the basic logical calculation unit. The complexity of the quantum circuit of the proposed method is analyzed as follows.

First, the complexity of the quantum circuit of the absolute value calculation module was 

\[ 4n^2 - 2 \]  . In the pre-processing operation before embedding, three absolute-value-calculation (CAV) modules were used, and the complexity was 

\[ 3 \times (4n^2 - 2) \]  . Second, two 2n qubit coordinate sequences were compared using a quantum equivalent circuit before embedding. The quantum equivalent circuit module consists of 4n-CNOT gates and a 2n-CNOT gate. The complexity of n-CNOT (n is the number of control qubits) is 

\[ 12n^2 - 9 \] . Therefore, the complexity of the quantum equivalence judgment module in the circuit is 

\[ 4n + 12 \times 2n - 9(n \geq 3) \] . Finally, the embedded circuit contains 12 qubit switching gates. The switching gate can be decomposed into 3 CNOT gates. Hence, the complexity of the quantum circuit is 36.

Based on the above analysis, the complexity of the steganographic embedded circuit of the quantum image is as follows:

\[ 3 \times (4n^2 - 2) + 4n + 12 \times 2n - 9 + 36 = O(n^3) \]  \hspace{1cm} (15)

Ignoring the complexity of links in quantum image steganography, such as quantum image preparation and image expansion, the complexity of the embedded circuit of the proposed method is only 

\[ O(n^3) \] .

5. Conclusion

To enhance the steganographic embedding capacity of quantum images and ensure the steganographic visual quality, this study selected the quantum RGB image expression. On the basis of dividing the quantum image into blocks, the embedded quantum bit plane was determined according to the gray level difference of the pixel pairs in three directions in the block. The embedded quantum circuit was designed, and the steganographic capacity and visual quality were analyzed. Finally, the following conclusions could be drawn:

1. Different qubit planes embedded in each block can significantly improve the embedding concealment, thereby enhancing robustness.
2. Human visual system is sensitive to color. The gray level difference of the G channel is only used to determine the block area, whereas R and B channels are used to hide the embedded data. The steganographic images have high fidelity while increasing the steganography capacity.
3. The embedding algorithm is simple, and the complete blind extraction is realized. The quantum circuit has low complexity.

Combined with the basic theory of quantum computing and the quantum RGB image representation model, this study proposed a steganography method based on quantum image block and gray-scale difference. The corresponding quantum was designed, and it can be used as reference for studying steganography methods based on quantum color image block. Due to the differences in edge characteristics of images, future studies will consider to adjust the block size of images to further improve steganographic visual quality.

Acknowledgements

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

8. S. Miyake and K. Nakame, “A quantum watermarking scheme using simple and small-scale quantum circuits”. Quantum