

We are IntechOpen, the world's leading publisher of Open Access books Built by scientists, for scientists

4,800

Open access books available

122,000

International authors and editors

135M

Downloads

Our authors are among the

154

Countries delivered to

TOP 1%

most cited scientists

12.2%

Contributors from top 500 universities



WEB OF SCIENCE™

Selection of our books indexed in the Book Citation Index
in Web of Science™ Core Collection (BKCI)

Interested in publishing with us?
Contact book.department@intechopen.com

Numbers displayed above are based on latest data collected.
For more information visit www.intechopen.com



A Novel Quantum Steganography Scheme Based on ASCII

Ri-Gui Zhou and Jia Luo

Abstract

Based on the novel enhanced quantum representation for quantum image (NEQR), a new blind quantum steganography scheme is proposed. In this scheme, an improved quantum representation of text utilizing ASCII is provided that uses two qubit sequences to store the same quantum text message. The general embedding process of the scheme is as follows: firstly, the cover image of sized $2^n \times 2^n$ will be divided into eight blocks of sized $2^{n-2} \times 2^{n-1}$, and the secret quantum text of sized $2^{n-2} \times 2^{n-1}$ is scrambled by Gray code transform method. Then, the disorder quantum text is embedded into the eight blocks of cover image employing the Gray code as a judgment condition. Meanwhile, the corresponding quantum circuits are drawn. Through the analysis of all quantum circuits, it can be concluded that the scheme has a lower complexity, that is, $O(n)$. And the performance of the proposed scheme is analyzing in terms of simulation results of three items: visual quality, circuit complexity, and robustness.

Keywords: quantum steganography, quantum text, ASCII, Gray code, quantum circuit

1. Introduction

With the advantage of quantum physics, quantum computer has demonstrated a bright prospect over than the classic computer, especially in Grover's database searching algorithm [1] and Shor's prime factor decomposition algorithm [2].

Over the past few decades, teams of researchers have been noticed by quantum image processing that is a young emerging cross-discipline of image processing and quantum mechanics. The investigation in this direction is how to construct the quantum representations to represent images on quantum computer at first. So various quantum representations have been proposed, such as, Qubit Lattice [3], entangled image [4], real ket [5], flexible representation of quantum images (FRQI) [6], a novel enhanced quantum representation of digital images (NEQR) [7], multi-channel representation for quantum images (MCRQI) [8], a normal arbitrary quantum superposition state (NAQSS) [9], and a novel quantum representation for color digital images (NCQI) [10]. Secondly, many kinds of quantum image processing algorithms were developed, such as geometric transformations [11, 12], image translation [13–15], image scaling [16–18], image scrambling [19–21], image segmentation [22], feature extraction [23], edge detection [24], and image matching [25, 26].

It is worth pointing out that the protection of network information, especially the increasing number of multimedia information on the network, has attracted researcher's attention. Thus information hiding was came into being a hot issue, which utilizes the sensory redundancy of the human sense organ to the digital signal, hiding a message in another ordinary message without changing the essential characteristics and use value of the ordinary message.

Similarly, quantum information hiding also includes steganography and watermarking, which have been gradually studied as the two main branches of quantum information hiding technology. In 2012, Iliyasa et al. proposed a quantum image watermarking algorithm based on restricted geometric transformations [27]. Zhang et al. introduced a protocol in 2013, that the watermark image was embedded into the Fourier coefficients of the quantum carrier image [28]. Later on, a dynamic watermarking scheme for quantum images based on Hadamard transform was proposed by Song et al. [29]. Two blind steganography algorithms based on LSB were proposed by Jiang et al. [30]. Miyake proposed a quantum watermarking scheme using simple and small-scale quantum circuits [31]. In this algorithm, the gray scale image was first used as a secret image. A watermarking scheme through Arnold scrambling and LSB was proposed by Zhou et al. [32], in which the quantum equal circuit was demonstrated. In 2017, Abd-El-Atty et al. proposed a new steganography scheme with Hadamard transformation [33]. In this scheme, the quantum text message was hidid into the cover image. In addition, some algorithms that adopt color image as cover image have also been reported [34–37]. Wherein, a quantum copyright protection method based on a new quantum representation of text was presented by Heidari et al. [34].

In order to reduce the qubits of the representation of text in literature [34], we introduce an improved quantum representation of text. Then, the quantum text will be embedded in cover image through utilizing Gray code and quantum gates. Furthermore, the extracting procedure is absolutely blind and without any other help from classical computer.

The physical implementation of qubits and gates is difficult, for the same reasons that quantum phenomena are hard to observe in everyday life. One approach is to implement the quantum computers in superconductors, where the quantum effects become macroscopic, though at a price of extremely low operation temperatures.

In a superconductor, the basic charge carriers are pairs of electrons (known as Cooper pairs), rather than the single electrons in a normal conductor. At every point of a superconducting electronic circuit (that is a network of electrical elements), the condensate wave function describing the charge flow is well-defined by a specific complex probability amplitude. In a normal conductor electrical circuit, the same quantum description is true for individual charge carriers, however the various wave functions are averaged in the macroscopic analysis, making it impossible to observe quantum effects. The condensate wave function allows designing and measuring macroscopic quantum effects. And successive generations of IBM Q processors have demonstrated the potential of superconducting transmon qubits as the basis for electrically controlled solid-state quantum computers. But in this chapter, we focus on the theoretical design of quantum steganography scheme and describe it in the remaining sections.

The rest of the chapter is organized as follows. Section 2 gives fundamental knowledge of NEQR, Gray code and quantum equal circuit. The improved quantum representation of text is provided in Section 3. The proposed embedding and extracting procedures are depicted in Section 4. In Section 5, simulations and analysis that include visual quality, capacity, robustness, and computational complexity are provided. Finally, the conclusion is drawn in Section 6.

2. Preliminaries

2.1 NEQR

For a gray scale image, a novel enhanced quantum representation of digital images (NEQR) was proposed in 2013 [7]. A quantum image can be described by the NEQR model as follows:

$$|I\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |C_{YX}\rangle |Y\rangle |X\rangle = \frac{1}{2^n} \sum_{YX=0}^{2^{2n}-1} \bigotimes_{i=0}^{q-1} C_{YX}^i \otimes |YX\rangle \quad (1)$$

where, $|YX\rangle$ represents the position information and $|C_{YX}^i\rangle$ encodes the color information.

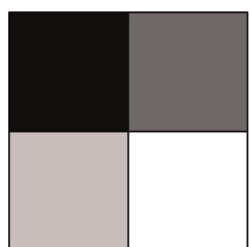
$$\begin{aligned} |YX\rangle &= |Y\rangle |X\rangle = |y_{n-1}y_{n-2}\dots y_0\rangle |x_{n-1}x_{n-2}\dots x_0\rangle, y_i, x_i \in \{0, 1\}, i = 0, 1, \dots, n-1 \\ |C_{YX}\rangle &= |C_{YX}^{q-1} C_{YX}^{q-2} \dots C_{YX}^0\rangle, C_{YX}^i \in \{0, 1\}, i = 0, 1, \dots, q-1 \end{aligned} \quad (2)$$

Thus, there are $q + 2n$ qubits being employed to store image information into a NEQR state for an $2^n \times 2^n$ image with gray range $[0, 2^q]$. An example of a 2×2 image with ranged $[0, 2^8 - 1]$, i.e., $n = 2, q = 8$ is demonstrated in **Figure 1**, in which the equation indicates that NEQR model stores the whole image in the superposition of the two entangled qubit sequences, encoding the color and position information, respectively.

Replace the entirety of this text with the main body of your chapter. The main body is where the author explains experiments, presents and interprets data of one's research. Authors are free to decide how the main body will be structured. However, you are required to have at least one heading. Please ensure that either British or American English is used consistently in your chapter.

2.2 Gray code

The typical binary Gray Code, called the Gray Code, was originally proposed by Frank Gray in 1953 for communication purposes and is now commonly used in analog-to-digital and position-to-digital conversion. In a group of Gray codes, there is only one different binary number between any two adjacent codes, as well as in the maximum and minimum numbers. By Gray code transform, the binary code can be converted into Gray code [21]. Denote $n(q) = n_{q-1}n_{q-2}\dots n_1n_0$ as a q -bit binary code, where n_i is a binary bit, the definition of Gray code transform is as follows:



$$\begin{aligned} |I\rangle &= \frac{1}{2} (|0\rangle \otimes |00\rangle + |100\rangle \otimes |01\rangle + |200\rangle \otimes |10\rangle + |255\rangle \otimes |11\rangle) \\ &= \frac{1}{2} \left(|00000000\rangle \otimes |00\rangle + |01100100\rangle \otimes |01\rangle \right. \\ &\quad \left. + |11001000\rangle \otimes |10\rangle + |11111111\rangle \otimes |11\rangle \right) \end{aligned}$$

Figure 1.
 A 2×2 example image and its representative expression in NEQR.

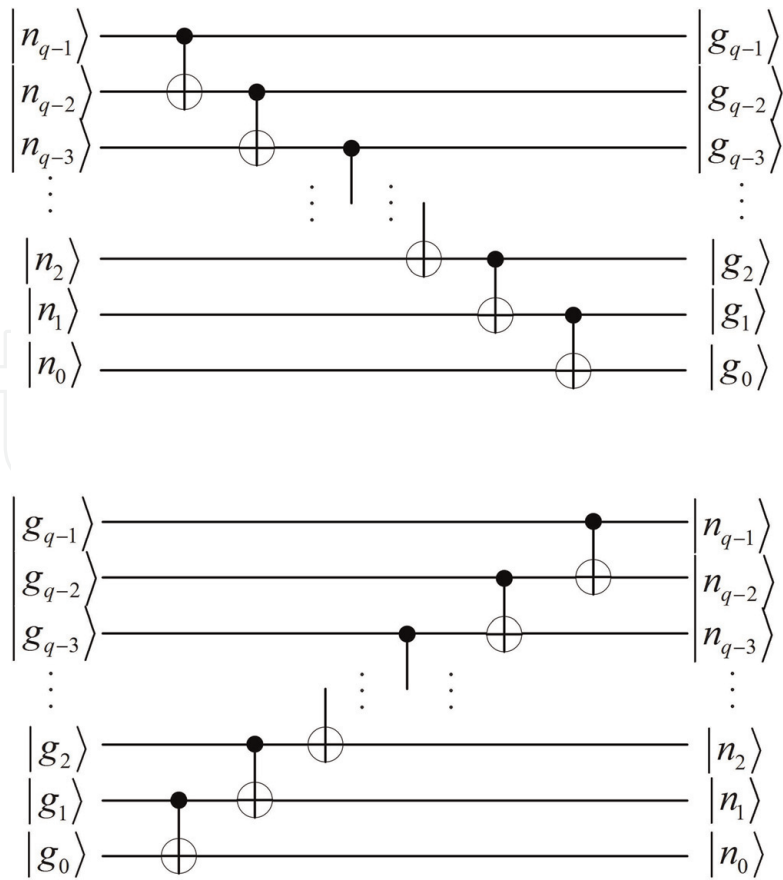


Figure 2. Quantum circuits of (a) Gray code transform and (b) inverse Gray code transform.

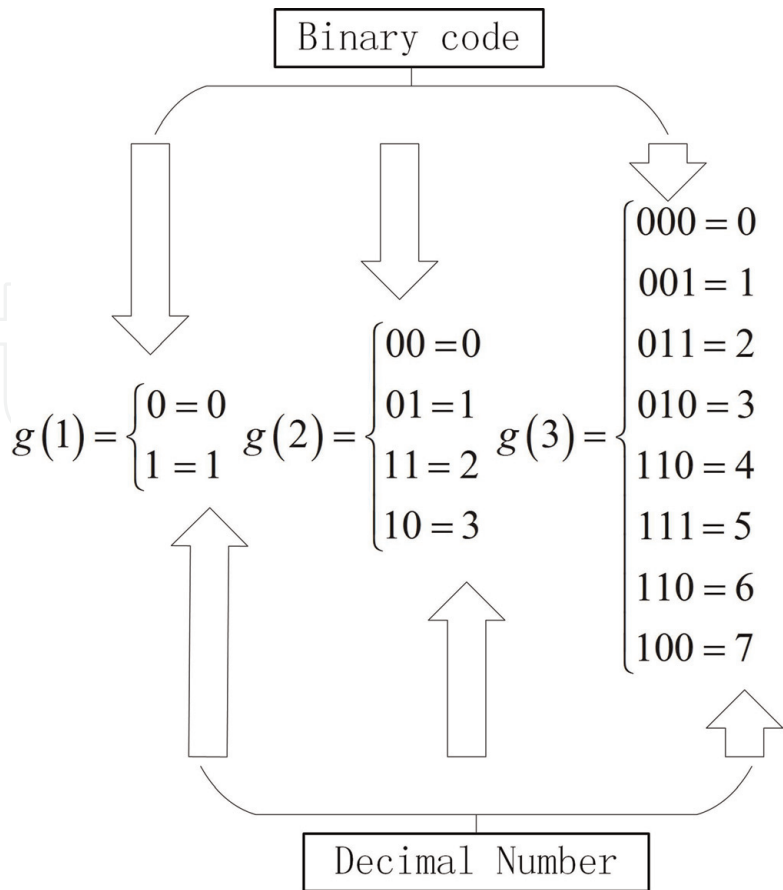


Figure 3. 1-bit, 2-bit and 3-bit Gray codes.

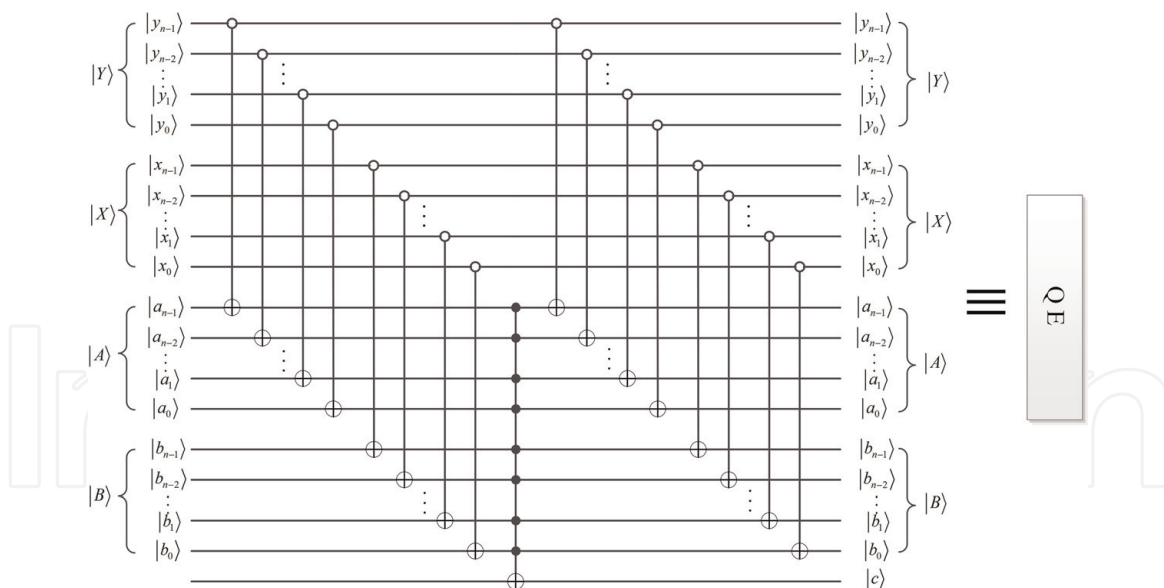


Figure 4.
 Quantum equal circuit.

$$g_{q-1} = n_{q-1}$$

$$g_i = n_i \oplus n_{i+1}, \quad i = 0, 1, \dots, q-2 \quad (3)$$

and its inverse transform is:

$$n_i = g_{i+1} \oplus g_i, \quad i = 0, 1, \dots, q-2$$

$$n_{q-1} = g_{q-1} \quad (4)$$

their corresponding quantum circuits are illustrated in **Figure 2a** and **b**.

The transformed binary code $g(q) = g_{q-1}g_{q-2}\dots g_1g_0$ is defined as the q -bit Gray code of $n(q)$. An example of Gray code where the bit number $q = 1, 2, 3$ is shown in **Figure 3**.

2.3 Quantum equal circuit

In literature [32], Zhou et al. provided a quantum equal circuit to determine whether two qubit sequences are equal or not. The quantum circuit is shown in **Figure 4**, which compares $|YX\rangle$ and $|AB\rangle$, where $|YX\rangle = |Y\rangle|X\rangle = |y_{n-1}\dots y_0\rangle|x_{n-1}\dots x_0\rangle$ and $|AB\rangle = |A\rangle|B\rangle = |a_{n-1}\dots a_0\rangle|b_{n-1}\dots b_0\rangle$, $y_i, x_i, a_i, b_i \in \{0, 1\}$, $i = n-1, \dots, 0$. Qubit $|c\rangle$ is output. If $|c\rangle = |1\rangle$, $|YX\rangle = |AB\rangle$, otherwise, $|YX\rangle \neq |AB\rangle$.

3. The improved representation of quantum text

ASCII (American Standard Code for Information Interchange) is a Latin alphabet-based computerized coding system that is the most versatile single-byte coding system available today [38]. The ASCII code uses the specified combination of 7-bit or 8-bit binary sequence to represent 128 or 256 possible characters. A standard ASCII code that uses 7-bit binary sequence (a total 8-bit sequence and the remaining 1-bit is 0) to represent all uppercase and lowercase letters, Arabic numerals, punctuation marks, and special control characters used in American

English. Zero to thirty one and 127 (33 in total) are special characters for control or communication, and the rest are displayable characters. **Figure 5** shows a table of characters that can be displayed.

Through analysis of the quantum text representation model proposed in literature [34], it is known that the model uses a seven-qubit sequence to store one character in the text message. In our proposed scheme, an improved quantum representation of text based on ASCII is proposed. Like NEQR model, the model including text message and position information. The text message $f(Y, X)$ on the corresponding coordinates (Y, X) is encoded using ASCII of 8-bit binary sequence $T_{YX}^7 T_{YX}^6 \dots T_{YX}^2 T_{YX}^1 T_{YX}^0$, $T_{YX}^i \in \{0, 1\}$, $i = 0, 1, \dots, 7$, this quantum text-representation model can be expressed as in Eq. (5) for a $2^n \times 2^m$ text.

ASCII	symbol	ASCII	symbol	ASCII	symbol
00100000	(space)	01000000	@	01100000	`
00100001	!	01000001	A	01100001	a
00100010	"	01000010	B	01100010	b
00100011	#	01000011	C	01100011	c
00100100	\$	01000100	D	01100100	d
00100101	%	01000101	E	01100101	e
00100110	&	01000110	F	01100110	f
00100111	'	01000111	G	01100111	g
00101000	(01001000	H	01101000	h
00101001)	01001001	I	01101001	i
00101010	*	01001010	J	01101010	j
00101011	+	01001011	K	01101011	k
00101100	,	01001100	L	01101100	l
00101101	-	01001101	M	01101101	m
00101110	.	01001110	N	01101110	n
00101111	/	01001111	O	01101111	o
00110000	0	01010000	P	01110000	p
00110001	1	01010001	Q	01110001	q
00110010	2	01010010	R	01110010	r
00110011	3	01010011	S	01110011	s
00110100	4	01010100	T	01110100	t
00110101	5	01010101	U	01110101	u
00110110	6	01010110	V	01110110	v
00110111	7	01010111	W	01110111	w
00111000	8	01011000	X	01111000	x
00111001	9	01011001	Y	01111001	y
00111010	:	01011010	Z	01111010	z
00111011	;	01011011	[01111011	{
00111100	<	01011100	\	01111100	
00111101	=	01011101]	01111101	}
00111110	>	01011110	^	01111110	~
00111111	?	01011111	_		

Figure 5.
ASCII of displayable characters.

$$|T\rangle = \frac{1}{2^{n+m/2}} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^m-1} |f(Y,X)\rangle |Y\rangle |X\rangle = \frac{1}{2^{n+m/2}} \sum_{YX=0}^{2^{n+m}-1} \bigotimes_{i=0}^7 T_{YX}^i \otimes |YX\rangle \quad (5)$$

Figure 6 illustrates an example of a 2×4 text and its representative expression, where eight qubits are desired to store the text message and three qubits to store the position information. Therefore, this model just needs $8 + n + m$ qubits to represent a $2^n \times 2^m$ text, namely there are 2^{n+m} symbols be stored. It is can be captured according to [34] which fifty-six qubits and $7 \times 2^{n+m}$ qubits are required to represent the text in this example and a text of 2^{n+m} symbols, respectively.

In order to embed the text information into quantum image, firstly, the text information needs to be transformed into a quantum state. The preparation procedure will now be described.

Step 1: this step is to prepare $8 + n + m$ qubits that all are with state $|0\rangle$. The initial state $|\psi\rangle_0$ can be expressed as in Eq. (6):

$$|\psi\rangle_0 = |0\rangle^{\otimes n+m+8} \quad (6)$$

Step 2: two single-qubit gates, I and H (shown in Eq. (7)), are used to transform $|\psi\rangle_0$ to the intermediate state $|\psi\rangle_1$, which is the superposition of all the characters of an empty text. The unitary operation U_1 can be written in Eq. (8):

$$I = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad H = 1/\sqrt{2} \begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix} \quad (7)$$

$$U_1 = I^{\otimes 8} \otimes H^{\otimes (n+m)} \quad (8)$$

The operation U_1 is setting on the $|\psi\rangle_0$ as shown in Eq. (9), and the position information is prepared in $|\psi\rangle_1$.

$$\begin{aligned} U_1(|\psi\rangle_0) &= (I|0\rangle)^{\otimes 8} \otimes (H|0\rangle)^{\otimes (n+m)} \\ &= \frac{1}{2^{n+m/2}} |0\rangle^{\otimes 8} \otimes \sum_{i=0}^{2^{n+m}-1} |i\rangle \\ &= \frac{1}{2^{n+m/2}} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^m-1} |0\rangle^{\otimes 8} |YX\rangle \\ &= |\psi\rangle_1 \end{aligned} \quad (9)$$

Step 3: In this step, 2^{n+m} sub-operations used to store the text message value for every position. In position (Y, X) , the unitary operation U_{YX} is shown below:

$$U_{YX} = \left(I \otimes \sum_{j=0}^{2^n-1} \sum_{i=0}^{2^m-1} |ji\rangle \langle ji| \right) + \Omega_{YX} \otimes |YX\rangle \langle YX| \quad (10)$$

$$\begin{aligned} |T\rangle &= \frac{1}{2^3} \left(|G\rangle|000\rangle + |R\rangle|001\rangle + |A\rangle|010\rangle + |Y\rangle|011\rangle \right) \begin{array}{|c|c|c|c|} \hline G & R & A & Y \\ \hline c & o & d & e \\ \hline \end{array} \\ &= \frac{1}{2^3} \left(|01000111\rangle|000\rangle + |01010010\rangle|001\rangle + |01000001\rangle|010\rangle + |01011001\rangle|011\rangle \right) \\ &\quad \left(|01100011\rangle|100\rangle + |01101111\rangle|101\rangle + |01100100\rangle|110\rangle + |01100101\rangle|111\rangle \right) \end{aligned}$$

Figure 6.
 A 2×4 text and its representative expression.

where, Ω_{YX} is a unitary operation as shown in Eq. (11), which is manipulating on $|\psi\rangle_1$ for altering digital representation of characters to the quantum state.

$$\begin{aligned}\Omega_{YX} &= \bigotimes_{i=0}^7 \Omega_{YX}^i \\ \Omega_{YX}^i : |0\rangle &\rightarrow |0 \oplus T_{YX}^i\rangle\end{aligned}\quad (11)$$

And if $T_{YX}^i = 1$, Ω_{YX}^i is a $(n + m)$ -CNOT gate, otherwise if $T_{YX}^i = 0$ then Ω_{YX}^i is a quantum identity gate. Therefore, the text message value in position (Y, X) is preparing by employing unitary operation Ω_{YX} :

$$\Omega_{YX}|0\rangle^{\otimes 8} = \bigotimes_{i=0}^7 (\Omega_{YX}^i|0\rangle) = \bigotimes_{i=0}^7 |0 \oplus T_{YX}^i\rangle = \bigotimes_{i=0}^7 |T_{YX}^i\rangle = |f(Y, X)\rangle \quad (12)$$

Applying U_{YX} on intermediate state $|\psi\rangle_1$, the transformation is shown in Eq. (13).

$$\begin{aligned}U_{YX}(|\psi\rangle_1) &= U_{YX} \left(\frac{1}{2^n} \sum_{j=0}^{2^n-1} \sum_{i=0}^{2^m-1} |0\rangle^{\otimes 8} |ji\rangle \right) \\ &= \frac{1}{2^n} U_{YX} \left(\sum_{j=0, i=0, ji \neq YX}^{2^n-1, 2^m-1} |0\rangle^{\otimes 8} |ji\rangle + |0\rangle^{\otimes 8} |YX\rangle \right) \\ &= \frac{1}{2^n} \left(\sum_{j=0, i=0, ji \neq YX}^{2^n-1, 2^m-1} |0\rangle^{\otimes 8} |ji\rangle + \Omega_{YX}|0\rangle^{\otimes 8} |YX\rangle \right) \\ &= \frac{1}{2^n} \left(\sum_{j=0, i=0, ji \neq YX}^{2^n-1, 2^m-1} |0\rangle^{\otimes 8} |ji\rangle + |f(Y, X)\rangle |YX\rangle \right)\end{aligned}\quad (13)$$

To store all the values to the quantum state, the whole operation U that consists of 2^{n+m} sub-operations and shown in Eq. (14) is necessary. The final state $|\psi\rangle_2$ that is transformed from $|\psi\rangle_1$ is the improved representation of quantum text.

$$\begin{aligned}U &= \prod_{Y=0}^{2^n-1} \prod_{X=0}^{2^m-1} U_{YX} \\ U(|\psi\rangle_1) &= U \left(\frac{1}{2^n} \sum_{j=0}^{2^n-1} \sum_{i=0}^{2^m-1} |0\rangle^{\otimes 8} |YX\rangle \right) \\ &= \frac{1}{2^n} \sum_{j=0}^{2^n-1} \sum_{i=0}^{2^m-1} \Omega_{YX} |0\rangle^{\otimes 8} |YX\rangle \\ &= \frac{1}{2^n} \sum_{j=0}^{2^n-1} \sum_{i=0}^{2^m-1} |f(Y, X)\rangle |YX\rangle = (|\psi\rangle_2)\end{aligned}\quad (14)$$

4. Proposed scheme

This section will discuss the particulars of embedding and extracting procedures about the proposed steganography scheme that hides a secret text into a cover grayscale image. Assume that the sizes for cover image and secret text are $2^n \times 2^n$ and $2^{n-2} \times 2^{n-1}$, respectively, the quantum representation can be formulated in Eqs. (15) and (16).

$$|C\rangle = \frac{1}{2^n} \sum_{YX=0}^{2^{2n}-1} \otimes_{i=0}^7 C_{YX}^i \otimes |YX\rangle, \quad C_{YX}^i \in \{0, 1\} \quad (15)$$

$$|T\rangle = \frac{1}{2^{2^{n-3}/2}} \sum_{YX=0}^{2^{2^{n-3}}-1} \otimes_{i=0}^7 T_{YX}^i \otimes |YX\rangle, \quad T_{YX}^i \in \{0, 1\} \quad (16)$$

The general framework for the proposed scheme is shown in **Figure 7**, from which we can see that it is delineated into the classical and quantum domains. The preparation interface can transform classic image data into quantum states, which realizes the function of preparing the quantum image [7]. After the quantum image is stored in quantum states, our proposed quantum image steganography scheme can be implemented to transform the original quantum states to the desired states through the designed embedding circuits. Then, the quantum measurement operation is utilized to retrieve the processed image information. And once identified, the stego image is sent to the receiver by the public channel. The extraction operations are similarly for the receiver.

4.1 Embedding procedure

The embedding procedure in the proposed scheme is as follows.

1. Transform a classical cover image with $2^n \times 2^n$ size and eight bits gray scale into a quantum image $|C\rangle$ by NEQR, and transform a secret text with size $2^{n-2} \times 2^{n-1}$ into a quantum text $|T\rangle$ by ASCII expression.
2. Scramble the secret text $|T\rangle$ to be a meaningless text $|\hat{T}\rangle$ by Gray code transforming method.
3. The cover image will be divided into eight blocks of the same size and the secret text will be divided into eight bit-planes.
4. The divided eight bit-planes are embedded into eight blocks one by one.

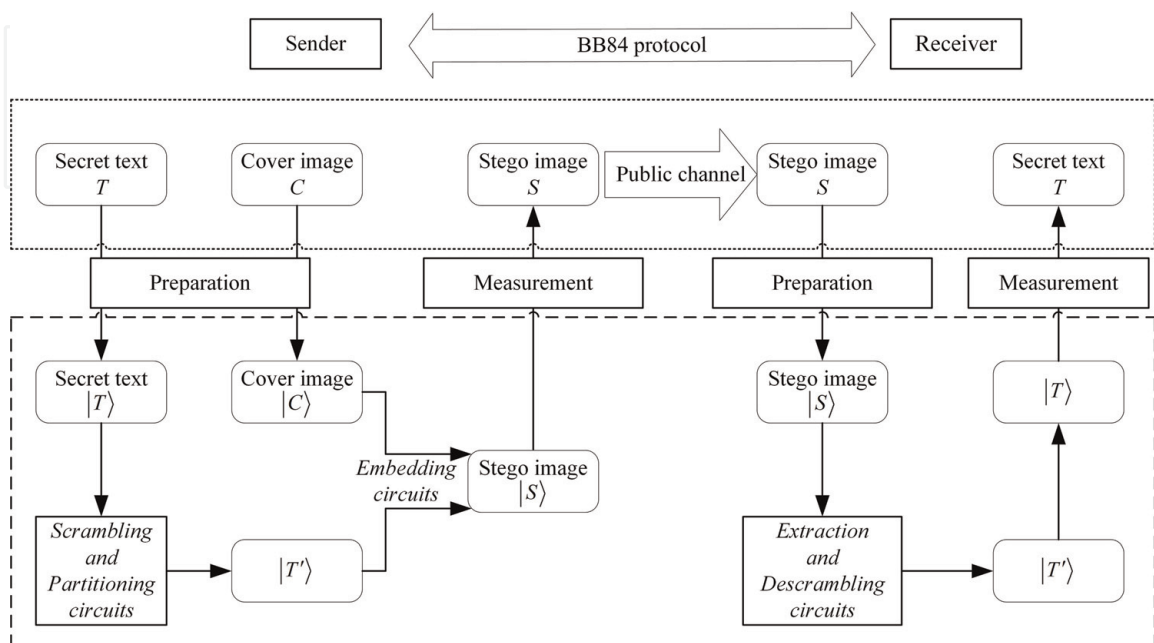


Figure 7.
 The general framework of the proposed scheme.

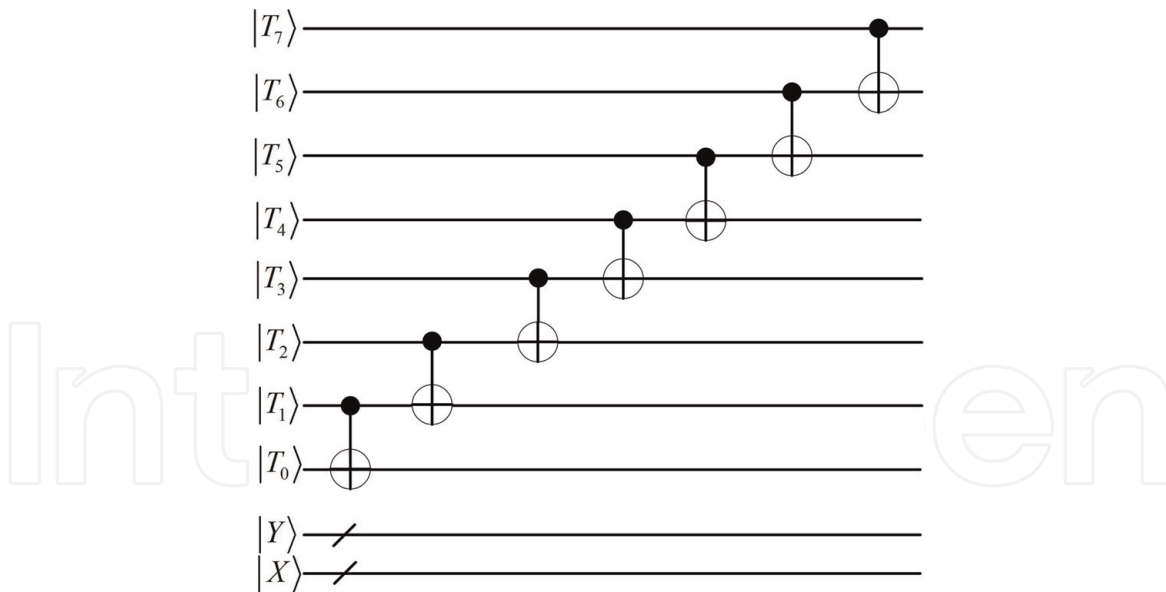


Figure 8.
Scrambling by Gray code transform.

4.1.1 Scrambling

For purpose of improving the security of secret text, the text message of $|T\rangle$ will be scrambled by Gray code transform before the embedding procedure. As mentioned in Subsection 2.2, in the eight qubits which store the text message, seven CNOT gates are used according to Gray code transform method, while the qubits representing for position information are not changed by quantum gates, the corresponding circuit is demonstrated in **Figure 8**.

4.1.2 Partitioning

In the proposed scheme, the $2^n \times 2^n$ cover image is divided into 4×2 blocks sized $2^{n-2} \times 2^{n-1}$. We define these blocks as B_{ij} , where $|i\rangle = |y_n y_{n-1}\rangle$ and $|j\rangle = |x_n\rangle$ are called control coordinates because if they are restricted as a specific value, then one of blocks will be selected. For example, if their values are equal to $|00\rangle$ and $|0\rangle$,

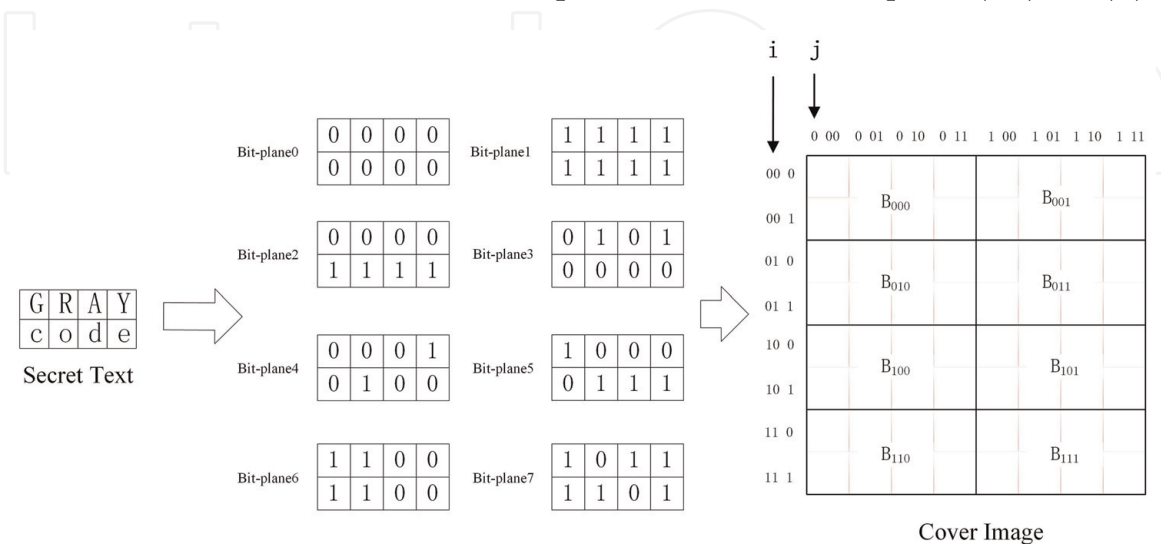


Figure 9.
An example of partition.

then $2^{n-2} \times 2^{n-1}$ pixels in the top-left corner, that is, the first block B_{000} is designated. For quantum text, the binary length of text message is eight, i.e., the text can be separated into eight bit-planes. Assume that the highest bit is embedded in B_{000} , the second highest bit is embedded in B_{001} , and so on. An example of partition with cover image size of $2^3 \times 2^3$ and secret text size of $2^1 \times 2^2$ is illustrated in **Figure 9**.

4.1.3 Embedding

After dividing the cover image, the quantum equal (QE) circuit is used to compare the coordinates of a block and quantum text. Then, the stego image $|S\rangle$ is obtained after embedding process. More specifically, taking one of the blocks as an illustration, if the coordinates $|y_{n-3}y_{n-4}\dots y_0\rangle|x_{n-2}x_{n-3}\dots x_0\rangle$ of $|C\rangle$ is equal to the coordinates of $|\hat{T}^i\rangle$, $|\hat{T}^i\rangle$ is embedded in $|C^0\rangle$ by the following pseudo-code.

```

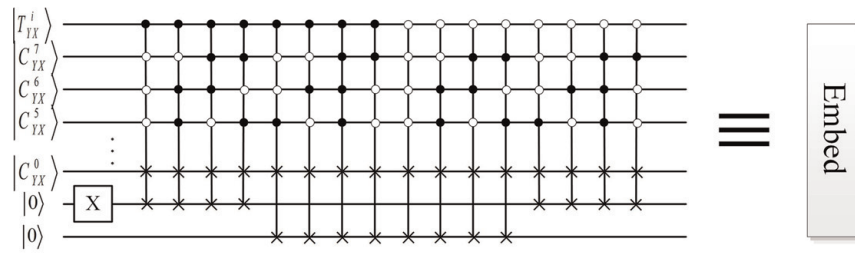
If  $|\hat{T}^i\rangle = |1\rangle$ 
  If  $GRAY(C_{YX}^7 C_{YX}^6 C_{YX}^5)$  is even
     $SWAP(C_{YX}^0, 1)$ 
  Else if  $GRAY(C_{YX}^7 C_{YX}^6 C_{YX}^5)$  is odd
     $SWAP(C_{YX}^0, 0)$ 
  End
If  $|\hat{T}^i\rangle = |0\rangle$ 
  If  $GRAY(C_{YX}^7 C_{YX}^6 C_{YX}^5)$  is even
     $SWAP(C_{YX}^0, 0)$ 
  Else if  $GRAY(C_{YX}^7 C_{YX}^6 C_{YX}^5)$  is odd
     $SWAP(C_{YX}^0, 1)$ 
  End
    
```

where the function $GRAY(i)$ is the Gray code value of i , and the function $SWAP(i, j)$ is to swap the value of i and j . The corresponding embed block circuit is shown in **Figure 10a** and **b** presents the integrated embedding circuit that contains the selection of the block of cover image, the comparison of the coordinates, and the embedding process of the bit-planes of secret text into the LSB of cover image.

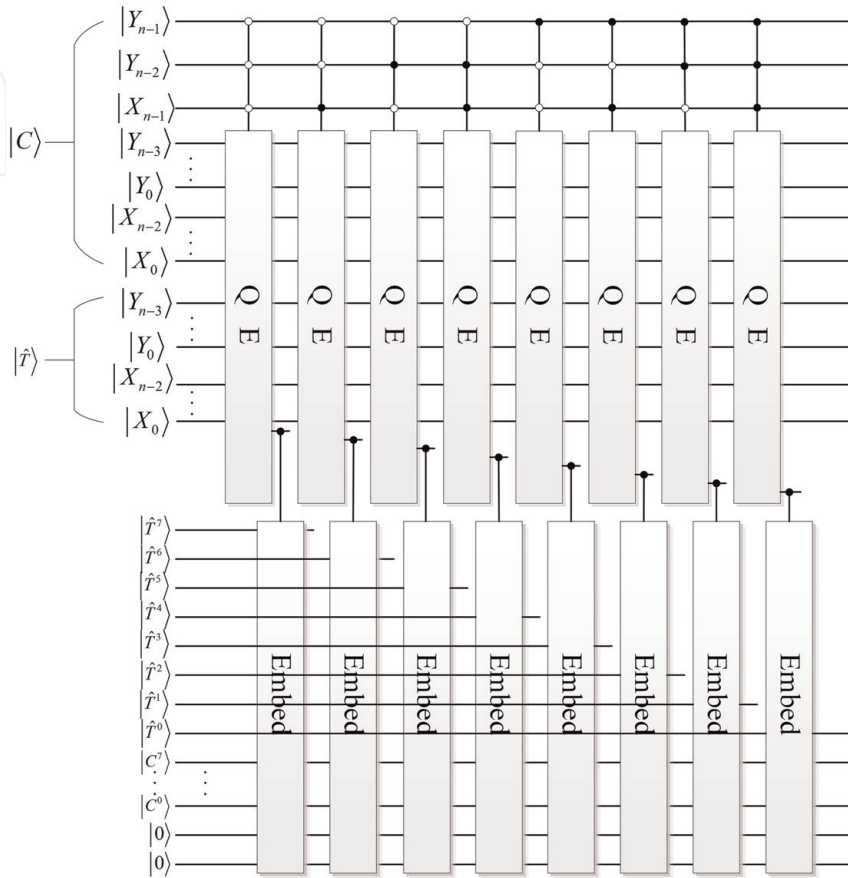
4.2 Extraction procedure

Like all the information hiding papers, only the receiver can extract the message. But it is worth pointing out the receiver only uses the stego image to extract the secret text in our scheme that means it is a blind scheme. The extracting procedure can be described as follows.

1. Extract and reorganize the bit plane from the stego image to obtain the disordered text $|\hat{T}\rangle$.
2. Descramble $|\hat{T}\rangle$ by using inverse Gray code transform in order to obtain original secret text $|T\rangle$.



a



b

Figure 10. Embedding circuit: (a) specific embedding block circuit and (b) the whole circuit.

4.2.1 Extraction

As can be seen from the above, the eight bit-planes of the secret text can be extracted from the eight blocks of the stego image. Accordingly, we can consider one block as an example. If the position of the stego image and the auxiliary blank quantum text are equal, and $GRAY(S_{YX}^7 S_{YX}^6 S_{YX}^5)$ is even and $C_{YX}^0 = 1$ or $GRAY(S_{YX}^7 S_{YX}^6 S_{YX}^5)$ is odd and $C_{YX}^0 = 0$, then $|\hat{T}^i\rangle = |1\rangle$. The corresponding circuit is shown in **Figure 11a**, and a whole extracting circuit that combines the extraction of all eight blocks together is exposed in **Figure 11b**.

4.2.2 Descrambling

Due to the operators used in embedding process are unitary, for this step of extracting process, we can use the inverse transpose of operators used in the embedding process. **Figure 12** affords the quantum circuit to extract the secret image $|T\rangle$ from $|\hat{T}\rangle$.

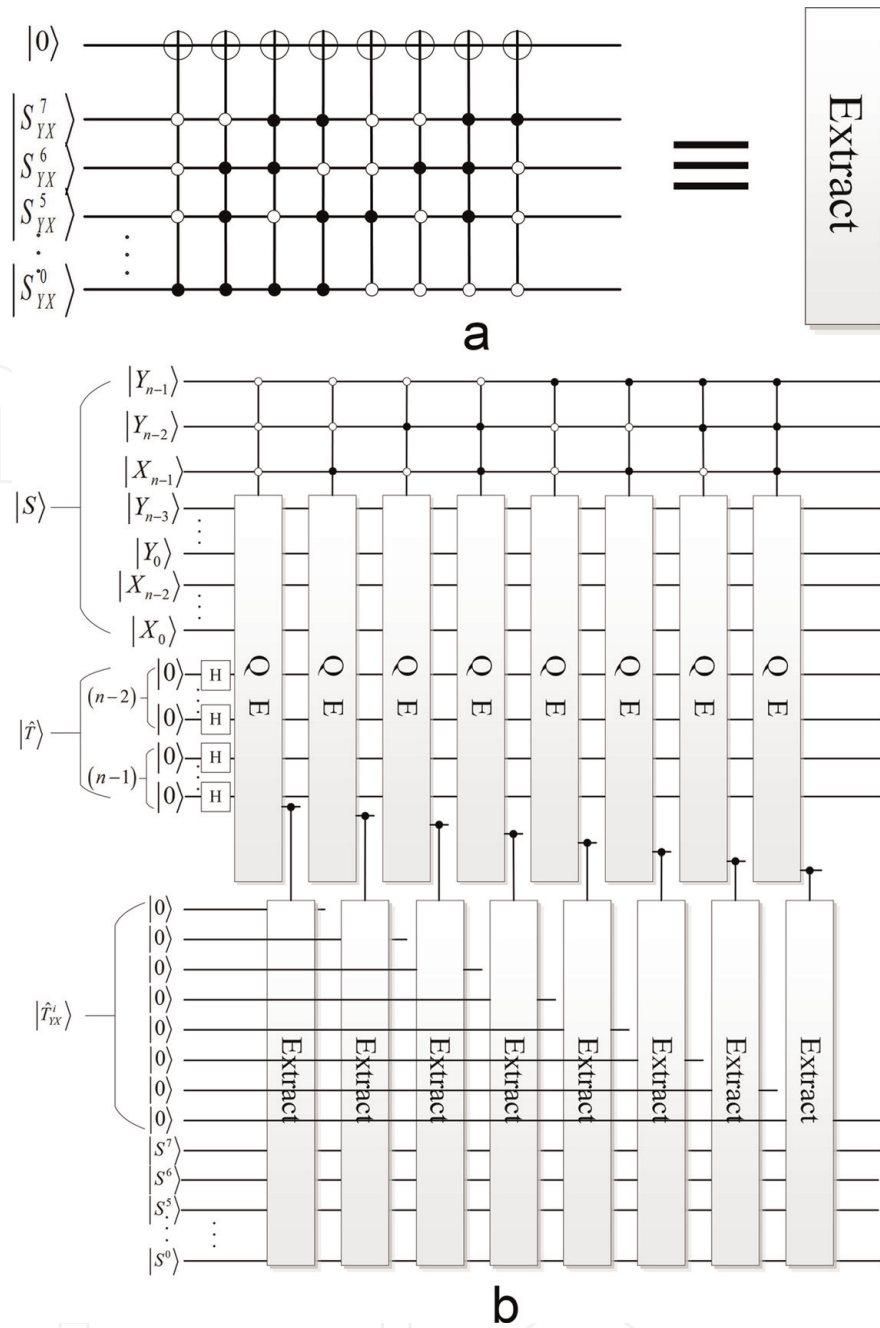


Figure 11. Extracting circuit: (a) specific extracting block circuit and (b) the whole circuit.

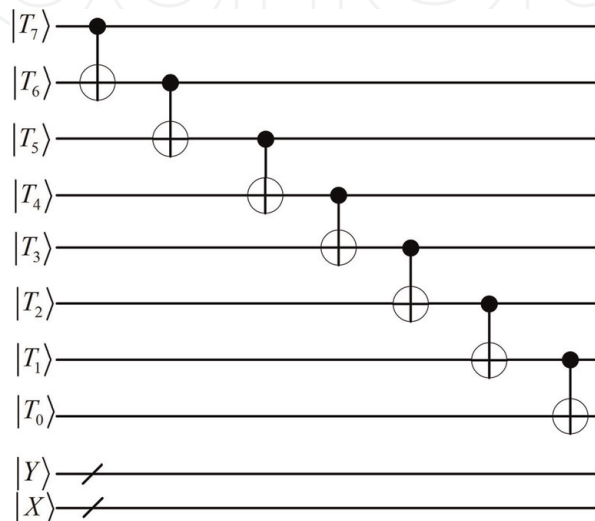


Figure 12. Inverse transform.

5. Simulations and analysis

In this section, some simulations and analysis of the results and properties of the proposed scheme are demonstrated. All the simulations are based on a classical computer equipped with software Matlab R2014b. The secret text of size 64×128 used in our proposed scheme is full of “Quantum Text and Quantum Image.” And all the cover images are with size of 256×256 , and shown in **Figure 13**.

In general quantum image steganography scheme, the peak-signal-to-noise ratio (PSNR) is one of the most employed techniques to compare the fidelity of the stego image and the cover image. However, Iliyasu et al. explained that these available classical metrics are insufficient and/or ill-suited to effectively quantify the fidelity between two or more quantum images [39]. And in Refs. [39, 40], a wholly quantum-based metric to assess fidelity between quantum images (QIFM) is proposed. By using a statistical analysis they established that the proposed QIFM metric had a better correlation with digital image quality assessments of congruity than the other quantum image quality measures. And the formulation of the QIFM metric is the important in ensuring that applications sensitive to the peculiarities of quantum computation are formulated for effective quantum image processing (QIP). Before this, inspired to Ref. [41] that proposed a method to analyze the similarity between two quantum images of the same size based on the flexible representation of quantum images, a quantum image matching algorithm was introduced in [26], which sums up all the grayscale differences between two quantum images. In this chapter, we use the above two algorithms to assess the similarity of two images.

5.1 Visual quality

To verify the visual quality of the proposed scheme, we use the algorithm introduced in [26] to compare the congruity of the stego image and the cover image. Here, we briefly describe the algorithm as follows and the details can be acquired in [26].

Quantum stego image is directly mapped with quantum cover image, i.e., the quantum register representing each corresponding pixel of the quantum template image is subtracted from that of the quantum reference image by running a quantum subtractor. According to the quantum measurement results, all the grayscale difference can be summed. The smaller the sum, the higher the similarity between two quantum images, that is, the better visual quality of the stego image.

Table 1 shows the sum of all the grayscale differences between the stego image and the cover image, in which the secret text 1 is embedded.

Compared with the value 5,189,090 of Lena with watermark in Ref. [26], we can see that the values of the sum all the grayscale differences between cover image and stego image in our proposed scheme are smaller.



Figure 13.
Cover images used in the proposed scheme.

Cover image	Stego image	Sum of differences
Lena	Stego-Lena	4,026,525
Airplane	Stego-airplane	4,260,325
Cameraman	Stego-cameraman	4,455,338
Pepper	Stego-pepper	4,461,076

Table 1.
 Sum of all the grayscale differences between cover image and stego image.

5.2 Robustness

In a noise-free environment, the proposed scheme can extract an intact secret text. However, the text extracting procedure is not always performed in a noiseless environment. The fidelity of the extracted text from the stego image under noise (simulate with salt and pepper noise) is verified, that is, using the QIFM metric. In this chapter, we give an outline of the steps of QIFM metric. For more details of the concepts and principles of QIFM, the reader can referred to [40].

Based on a pixel threshold (p) that assigns a value of zero or one to the pixel when $0 \leq p < 127$ or $128 \leq p < 255$, respectively. The content of both the cover and stego image is converted into their binary versions. Then the binary detail between cover image I_c and stego image I_s is evaluated using the following equation:

$$\Gamma = I_{Dc} - I_{Ds} \quad (17)$$

where the $I_{D(c\ or\ s)}$ for an $N = n \times n$ pixel image is defined in:

$$I_{D(c\ or\ s)} = \begin{cases} \frac{\sum (n_{(c\ or\ s)}^b - n_{(c\ or\ s)}^w)}{N}; & \text{if } n_{(c\ or\ s)}^b \neq n_{(c\ or\ s)}^w \\ \frac{\sum (n_{(c\ or\ s)}^b - n_{(c\ or\ s)}^w)}{N} + 1; & \text{otherwise} \end{cases} \quad (18)$$

Here, the notations n_c^b and n_c^w for the cover image and n_s^b and n_s^w for the stego image, which are referred to the number of white (0) and black (1) pixels in the cover and stego images.

Next, we count the number of pixel correspondences, D , which is defined as the number of pixels in cover image corresponding with pixels in stego image. And then, the total pixel-wise variation B is computed by the equation:

$$B = \frac{\sum BER}{8N} \quad (19)$$

where BER denotes the bit error rate.

Finally, the fidelity of two images expressed in the form of a percentage is quantified by equation:

$$F = \frac{D + (1 - B) \times \Gamma}{N} \times 100 \quad (20)$$

As can be found from **Table 2**, four frequently-used cover images are used here as examples, when the value of the noise densities is set to 0.1. The average value of

Stego image	QIFM values of two texts
Stego-Lena	91.0899
Stego-airplane	91.5049
Stego-cameraman	91.6392
Stego-pepper	91.1998

Table 2.
QIFM values of the extracted text and their original secret text.

QIFM values is around 91, which is considered that the extracted text have a good fidelity.

5.3 Circuit complexity

The circuit complexity depends on the number of the elementary quantum gates. Thus, we take C -NOT gate as the basic unit. For our proposed scheme, the circuit complexity consists of two parts: embedding and extracting. In embedding part, the scrambling circuit complexity is 7. The embedding circuit is composed of eight QE circuits with three control qubits and eight embedding blocks with one control qubit. As the literature [42] pointed out, only $(4k - 8)$ 2 - C -NOT gates are needed to construct one k - C -NOT gate. Again, one SWAP gate is equivalent to three C -NOT gates. The complexity of embedding circuit is:

$$\begin{aligned} & 8 \times [4n \times (4 \times 4 - 8) + (4 \times 2n - 8)] + 8 \times [16 \times 3 \times (4 \times 5 - 8)] \\ & = 320n - 64 + 4608 = 320n + 4544 \end{aligned} \quad (21)$$

In extracting part, the complexity of descrambling circuit is 7, and the extracting circuit is consist of eight QE circuits with three control qubits and eight extracting blocks with one control qubit. The complexity of extracting circuit is:

$$\begin{aligned} & 8 \times [4n \times (4 \times 4 - 8) + (4 \times 2n - 8)] + 8 \times [8 \times (4 \times 5 - 8)] \\ & = 320n - 64 + 768 = 320n + 704 \end{aligned} \quad (22)$$

Therefore, the circuit complexity of the proposed scheme is $(640n + 5262)$, i.e., $O(n)$.

6. Conclusion

This chapter proposes a new grayscale image steganography scheme which using NEQR representation to represent a $2^n \times 2^n$ cover image and presenting an improved representation of quantum text to store secret text with $2^{n-1+n-2}$ symbols. The Gray code of the highest three qubits of the gray value of the cover image is used as a judgment condition in embedded procedure. The acquisition of secret text is a process of extracting and reorganizing and inversely scrambling eight bit-planes, and it is worth mentioning that the process is absolutely blind. In addition, simulation results about the visibility quality and robustness of the proposed scheme are provided. And the circuit complexity is analyzed at last.

Acknowledgements

This work is supported by the National Key R&D Plan under Grant No. 2018YFC1200200 and 2018YFC1200205, National Natural Science Foundation of China under Grant No. 61463016 and “Science and technology innovation action plan” of Shanghai in 2017 under Grant No. 17510740300.

Conflict of interest

The authors declare no conflict of interest.

Author details


Ri-Gui Zhou^{1,2} and Jia Luo^{1,2*}

1 College of Information Engineering, Shanghai Maritime University, Shanghai, China

2 The Research Center of Intelligent Information Processing and Quantum Intelligent Computing, Shanghai, China

*Address all correspondence to: luojia@stu.shmtu.edu.cn

IntechOpen

© 2019 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution License (<http://creativecommons.org/licenses/by/3.0>), which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited. 

References

- [1] Grover LK, Labs B, Avenue M, Nj MH. A fast quantum mechanical algorithm for database search. In: Twenty-Eighth ACM Symposium on Theory of Computing. 1996. pp. 212-219
- [2] Peter W, Labs AB, Ave M, Hill M. Algorithms for quantum computation: Discrete logarithms and factoring. In: Proceedings of 35th Annual Symposium on Foundations of Computer Science. 1994. pp. 124-134
- [3] Venegas-Andraca SE, Bose S. Storing, processing and retrieving an image using quantum mechanics. In: Proceedings of SPIE—The International Society for Optical Engineering. 2003
- [4] Venegas-Andraca SE, Ball JL. Processing images in entangled quantum systems. *Quantum Information Processing*. 2010;**9**(1):1-11
- [5] Latorre JI. Image compression and entanglement. *Quantum Physics*. 2005; **3**:3-6
- [6] Le PQ, Dong F, Hirota K. A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. *Quantum Information Processing*. 2011; **10**(1):63-84
- [7] Zhang Y, Lu K, Gao Y, Wang M. NEQR: A novel enhanced quantum representation of digital images. *Quantum Information Processing*. 2013; **12**(8):2833-2860
- [8] Sun B, Le PQ, Iliyasu AM, Yan F, Garcia JA, Dong F, et al. A multi-channel representation for images on quantum computers using the RGB D color space. In: 2011 IEEE International Symposium on Intelligent Signal Processing (WISP). 2011
- [9] Qingxin HL, Zhou ZR, Yang LSX. Multi-dimensional color image storage and retrieval for a normal arbitrary quantum superposition state. *Quantum Information Processing*. 2014;**13**: 991-1011
- [10] Sang J, Wang S, Li Q. A novel quantum representation of color digital images. *Quantum Information Processing*. 2017;**16**(2):42
- [11] Le PQ, Iliyasu AM, Dong F, Hirota K. Fast geometric transformations on quantum images. *International Journal of Applied Mathematics*. 2010;**40**(3): 113-123
- [12] Fan P, Zhou R, Jing N, Li H. Geometric transformations of multidimensional color images based on NASS. *Information Sciences*. 2016; **340-341**:191-208
- [13] Fan P, Zhou R. Quantum Gray-scale image translation transform the representation of quantum Gray-scale image. *Quantum Information Processing*. 2015;**23**:8763-8770
- [14] Zhou R, Tan C, Ian H. Global and local translation designs of quantum image based FRQI. *International Journal of Theoretical Physics*. 2017;**56**(4): 1382-1398
- [15] Wang J, Jiang N, Wang L. Quantum image translation. *Quantum Information Processing*. 2015;**14**: 1589-1604
- [16] Zhou R, Hu W, Fan P, Ian H. Quantum realization of the bilinear interpolation method for NEQR. *Scientific Reports*. 2017;**7**(1): 2511
- [17] Sang J, Wang S, Niu X. Quantum realization of the nearest-neighbor interpolation method for FRQI and NEQR. *Quantum Information Processing*. 2016;**15**(1):37-64

- [18] Jiang N, Wang L. Quantum image scaling using nearest neighbor interpolation. *Quantum Information Processing*. 2015;**14**(5):1559-1571
- [19] Heidari S, Vafaei M, Houshmand M, Tabatabaey-Mashadi N. A dual quantum image scrambling method. *Quantum Information Processing*. 2019;**2**:1-23
- [20] Jiang N, Luo WW. The quantum realization of Arnold and Fibonacci image scrambling. 2014;**13**:1223-1236
- [21] Sun RZY, Fan P. Quantum image Gray-code and bit-plane scrambling. *Quantum Information Processing*. 2015; **14**:1717-1734
- [22] Caraiman S, Manta VI. Image segmentation on a quantum computer. *Quantum Information Processing*. 2015; **14**(5):1693-1715
- [23] Zhang Y, Lu K, Xu K, Gao Y, Wilson R. Local feature point extraction for quantum images. *Quantum Information Processing*. 2015;**14**:1573-1588
- [24] Yi Z, Kai LU, Yinghui GAO. QSobel: A novel quantum image edge extraction algorithm. *Science China Information Sciences*. 2015;**58**(1):1-13
- [25] Zhou RG, Liu XA, Zhu C, Wei L, Zhang X, Ian H. Similarity analysis between quantum images. *Quantum Information Processing*. 2018;**17**(6):1-12
- [26] Yang YG, Zhao QQ, Sun SJ. Novel quantum gray-scale image matching. *Optik*. 2015;**126**(22):3340-3343
- [27] Iliyasa AM, Le PQ, Dong F, Hirota K. Watermarking and authentication of quantum images based on restricted geometric transformations. *Information Sciences*. 2012;**186**(1):126-149
- [28] Zhang W-W, Gao F, Liu B, Wen Q-Y, Chen H. A watermark strategy for quantum images based on quantum fourier transform. *Quantum Information Processing*. 2013;**12**(2): 793-803
- [29] Song X, Wang S, Abd AA. Dynamic watermarking scheme for quantum images based on Hadamard transform. *Multimedia Systems*. 2014;**20**(4): 379-388
- [30] Jiang N, Zhao N, Wang L. LSB based quantum image steganography algorithm. *International Journal of Theoretical Physics*. 2016;**55**:107-123
- [31] Miyake S, Nakamae K. A quantum watermarking scheme using simple and small-scale quantum circuits. *Quantum Information Processing*. 2016;**15**(5): 1849-1864
- [32] Wenwen RZ, Ping H. Quantum watermarking scheme through Arnold scrambling and LSB steganography. *Quantum Information Processing*. 2017; **16**(9):212-242
- [33] Sang J, Wang S, Li Q. Least significant qubit algorithm for quantum images. *Quantum Information Processing*. 2016;**15**(11):4441-4460
- [34] Heidari S, Gheibi R, Houshmand M, Nagata KA. Robust blind quantum copyright protection method for colored images based on owner's signature. *International Journal of Theoretical Physics*. 2017;**56**(8):2562-2578
- [35] Li P, Zhao Y, Xiao H, Cao M. An improved quantum watermarking scheme using small-scale quantum circuits and color scrambling. *Quantum Information Processing*. 2017;**16**(5):127
- [36] Qu Z, He H, Li T, Liu K, Li J, Zhu J, et al. Novel quantum watermarking algorithm based on improved least significant qubit modification for quantum audio. *Chinese Physics B*. 2018;**27**(1):010306
- [37] Heidari S, Farzadnia E. A novel quantum LSB-based steganography

method using the Gray code for colored quantum images. *Quantum Information Processing*. 2017;**16**(10):1-28

[38] Gorn S. Proposed revised american standard code for information interchange. *Communications of the ACM*. 1965;**8**(4):207-214

[39] Iliyasu AM, Abuhasel KA. A quantum-based image fidelity metric. In: *2015 Science and Information Conference (SAI)*; IEEE. 2015. pp. 664-671

[40] Iliyasu AM, Yan F. Metric for estimating congruity between quantum images. *Entropy*. 2016;**18**(10):360

[41] Yan F, Le PQ, Iliyasu AM, Sun B, Garcia JA, Dong F, et al. Assessing the similarity of quantum images based on probability measurements. In: *2012 IEEE Congress on Evolutionary Computation*. 2012. pp. 10-15

[42] Barenco A, Bennett CH, Cleve R, Divincenzo DP, Margolus N, Shor P, et al. Elementary gates for quantum computation. *Physical Review A*. 1995; **52**(5):3457-3467