Journal of Information Hiding and Privacy Protection
DOI:10.32604/jihpp.2021.025602
Article

Quantum Steganography Application in the Electrical Network for Quantum Image and Watermark with Self-Adaptive

Jie Shen[1,3,*,#], Wenqi Dong[2,#], Jing Wang[1,2,3,#], Yang Wang[1] and Haiyan Li[4]

[1]State Grid Jibei Zhangjiakou Wind and Solar Energy Storage and Transportation New Energy Co., Zhangjiakou, China
[2]Hebei Province Wind and Solar Energy Storage Combined Power Generation Technology Innovation Center, Zhangjiakou, China
[3]Beijing University of Posts & Telecom, Beijing, China
[4]Heibei Gaoji Auto Parts Technology Co., Shijiazhuang, China
[*]Corresponding Author: Jie Shen. Email: shenjie74@163.com
[#]These authors contributed equally to this work and should be considered co-first authors
Received: 29 November 2021; Accepted: 12 December 2021

Abstract: With the development of Globe Energy Internet, quantum steganography has been used for information hiding to improve copyright protection. Based on secure quantum communication protocol, and flexible steganography, secret information is embedded in quantum images in covert communication. Under the premise of guaranteeing the quality of the quantum image, the secret information is transmitted safely with virtue of good imperceptibility. A novel quantum watermark algorithm is proposed in the paper, based on the shared group key value of the communication parties and the transmission of the selected carrier map pixel gray higher than 8 bits. According to the shared group key value of the communication parties, the two effective Bell state qubits of the carried quantum streak image are replaced with secret information. Compared with the existing algorithms, the new algorithm improves the robustness of the secret information itself and the execution efficiency of its embedding and extraction. Experimental simulation and performance analysis also show that the novel algorithm has an excellent performance in transparency, robustness and embedded capacity.

Keywords: Quantum steganography; FSQb; quantum image; secret information; quantum watermark

1 Introduction

One of the quantum image information security process research area is steganography. The secret information is hidden in the text, sound, images and video and other multimedia by steganography, through being transmitted on public network media, to achieve a covert in communication. When communicating over a common channel, the unauthorized party can neither know the contents nor the fact of hiding the communication. With recently the progress of quantum computers and its network has made quantum steganography a new field of research, attracting a large number of researchers all over the world. The algorithm's performance parameters are evaluated by: imperceptibility, the capacity of secret information and its security. The secret information capacity refers to the maximum capacity of each secret transfer of security information. Imperceptibility, also called covert or conceal information that is impossible or difficult to detect. Security mainly refers to the secret information cannot be obtained even if found.

Quantum steganography generally contains three categories, the first Bell state-based quantum data hiding protocol [1] was proposed by Terhal, etc., in 2001, used for hiding quantum information, through establishing the covert channel in the conventional quantum channel, which completes the secret

information transmission. In 2002, Eggeling et al. extended the Terhal protocol by implementing LOCC on the multi-particle state [2]. Hayden et al. proposed the threshold access protocol applied for quantum access hiding in 2005 [3], which provides the basis for large-capacity data hiding. The second was proposed by Gea-Banacloche in 2002 concerning the narrow sense of quantum steganography, in 2002, the use of QECC secret information as the error amount hidden in the information carrier as any quantum bit [4]. In this protocol, a secret message can be used as a watermark to protect the authenticity or integrity of the data. Shaw proposed a steganography protocol in 2011, that would conceal the noise mask being disguised as a quantum error correction code for information hiding [5]. In 2015, Liao et al. [6] improved the basis of Shaw's protocol, making more efficiently depolarization the noise-free channels. The third class is a quantum secret channel (QCC) that establishes a covert channel by establishing these quantum secure communication schemes such as QKD, QSDC, and QSS. In 2007, a quantum steganalysis protocol that based on BB84 was proposed by Martin et al. [7], which analyzes the security and concealment of the protocol in detail, calculates the steganographic channel's capacity accurately. In 2010, a higher capacity quantum implicit algorithm based on the χ-state QSDC protocol was proposed [8], which has eight-fold increases in the capacity, by adopting χ-state code with entanglement and super density.

Quantum image as a digital medium in the role of quantum steganography becomes increasingly important. In 2013, some presentation methods for the quantum image process were proposed by Zhang et al., which based on different algorithm NEQR [9] and FRQI [10], respectively. In 2015, a Flexible Significant Bit (FSQb) algorithm was proposed by Wang, which used for information hiding, and based on NEQR [11] algorithm for quantum representation. Through this way, both chroma and position information are entangled in NEQR, Information embedding and extraction. This is of great significance for further study of quantum steganography by using images as carriers.

2 Quantum Implicit Algorithm

2.1 Pre-Prepared

2.1.1 Representation of NEAR Images

In 2015, Wang et al. [11] proposed a novel algorithm (NEQR) to enhance the quantum image representation. Let the gray value of the image range is 2^q, and the scope of $f(i)$ is $f(i) \in [0, 2^q - 1]$, where $f(i)$ stands for the gray value of image information. The gray value information $f(i)$ of the corresponding pixel is encoded by a series of binary sequences $M_{q-1}^i M_{q-2}^i \cdots M_0^i$, $C_m^i \in [0,1]\,(m = 0, 1, \cdots, q-1)$, according to NEQR, an image with the size of $2^n \times 2^n$ is represented as follows:

$$|I\rangle = \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} |f(i)\rangle |i\rangle = \frac{1}{2^n} \sum_{i=0}^{2^{2n}-1} |M_{q-1}^i M_{q-2}^i \cdots M_0^i\rangle |i\rangle \tag{1}$$

where $|I\rangle$ stores the gray value of the entire quantum state image, and $|i\rangle$ is the position information, including vertical and horizontal information.

$$|i\rangle = |y\rangle |x\rangle = |y_{n-1} y_{n-2} \cdots y_0\rangle |x_{n-1} x_{n-2} \cdots x_0\rangle \tag{2}$$

where $|y\rangle$ encodes vertical information, and $|x\rangle$ encodes vertical information. An image example with the size of $2^n \times 2^n$ and its NEQR is represented in Fig. 1. In the example, since the range of gray value is within $0 \sim 255$. Meanwhile, in the NEQR algorithm 8-qubit contain the gray value information of the watermark quantum carrier image, and the following two particles are used to represent the coordinate location of the pixel.

$$|I\rangle = \frac{1}{2}(|10011001\rangle \otimes |00\rangle + |01100110\rangle \otimes |01\rangle + |00110011\rangle \otimes |10\rangle + |11001100\rangle \otimes |11\rangle) \tag{3}$$

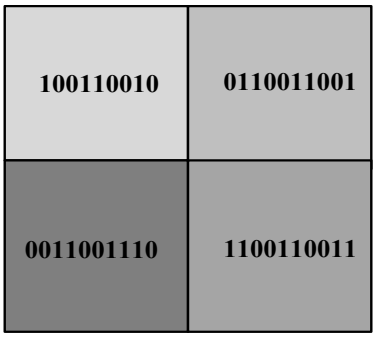

Figure 1: An image with the size of $2^n \times 2^n$ and its NEQR

2.1.2 Classic LSB Steganography

The classic LSB steganography technique is the simplest and widest used, which replaces the value of the Flexible Significant Bit of each pixel of the image with the secret information which should be embedded. When extracting the embedded secret information, it is only necessary to operate the secret image. It is easy to operate features. Meanwhile, there is no disparity between the visual image and the original image, and the difference cannot be perceived by the naked eye alone.

2.1.3 Quantum Comparator

Wang et al. [11] have defined a quantum comparator that determines the two qubits are the same or not. Let $|a\rangle$,$|b\rangle$ be the input qubit and $|c\rangle$,$|d\rangle$ be the corresponding output, as shown in Fig. 2:

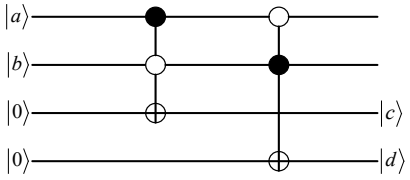

Figure 2: Quantum watermark embedded comparator circuit

(1) If $|c\rangle\,|d\rangle = |1\rangle\,|0\rangle$ or $|c\rangle\,|d\rangle = |0\rangle\,|1\rangle$, then $|a\rangle$ and $|b\rangle$ are not the same;

(2) If $|c\rangle\,|d\rangle = |0\rangle\,|0\rangle$, then $|a\rangle$ and $|b\rangle$ are the same.

Therefore, by comparing the quantum comparators, it can be judged whether the last qubit on the carrier of the original image is consistent with the quantum secret information, and then provide the basis for judging the unitary operation on the quantum image.

2.1.4 The Selection of the Embedding Location of Two Parts Secret Information

There are two parts composed of embedded secret information, they are the image carriers and the image watermarks of the quantum respectively. Considering that the two parts of the embedded secret information are overlapped after the watermark embedding, we use ZigZag sorting and Key location method to avoid the overlapping coverage problem.

Firstly, the ZigZag is used to get the quantum vector, image pixel sequence C_1, and then the ZigZag of the watermark image is sorted and the sequence W_1 of the watermark image is obtained. After the ZigZag sorting, the embedder secretly embeds information within the quantum image carrier and watermark

through the shared the secret key K_s, which consists of k_{s1} and k_{s2} (k_{s1} is the embedding secret key shared by the quantum image carrier , k_{s2} is the embedding secret key shared by the quantum image watermark). The embedder and receiver can embed and extract the precise secret quantum image carrier's information from the quantum image watermark through the key k_{s1} and k_{s2}, respectively. This situation means when the "1" appears in the key sequence, the flexible significant bit is used to embed the secret information, and extract the secret while "0" appears. Here it is worth noting that although the secret keys k_{s1} and k_{s2} are random sequences, in order to make the secret information not overlap when embedding, it is necessary to avoid putting the secret information in the same position as those of the carrier image and the watermark image when setting the keys k_{s1} and k_{s2}. To illustrate this problem, suppose the quantum image carrier with the size of $2^3 \times 2^3$ and quantum image watermark with the size of $2^2 \times 2^2$. The light gray area in Fig. 3 is the secret information embedded in the quantum carrier image, and the dark gray area is the secret information that being embedded in the quantum watermark. The partitioning makes the embedding of the secret information non-overlapping.

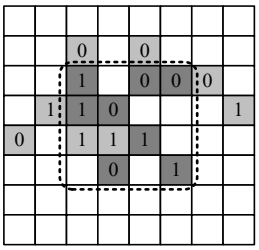

Figure 3: The division of the secret information in the embedded area

2.2 Quantum Watermark Embedding

According to Wang et al. [12], the embedding of the quantum watermark can be performed by designing a quantum line to replace the quantum image carrier with a certain qubit of gray scale value.

First, a string of keys K_r is shared between the embedder and the receiver, and the key K_r consists of sequences of 0 or 1 at the length of N. Assuming that i-th position of the quantum image carrier corresponds to "1" in the key K_r, the first position is subjected to quantum watermark embedding. The bit value of the quantum image watermark to be embedded is w_i, and the embedder uses the bit of quantum image watermark with value w_i to replace the Flexible Significant Bit's gray value, which corresponding carrier image pixel.

As shown in Fig. 4, assuming that the quantum image carrier with the size of $2^2 \times 2^2$ and the quantum image watermark with the size of 2×2, so as to embedding the gray value at $m_2 = 1$ in $|01\rangle$ to $|C_9\rangle$ of $|0110\rangle$ locate in the quantum image, hence after the combination, the gray value becomes $|C_9^{'}\rangle = |10110010\rangle$, the corresponding quantum watermark embedded the quantum circuit diagram shown as in Fig. 4.

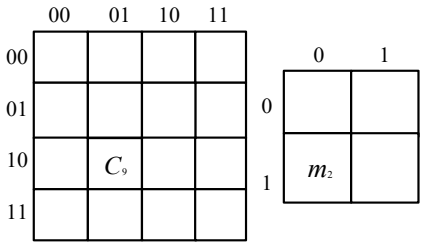

Figure 4: The quantum image carrier (left); Quantum image watermark (right)

2.3 Quantum Watermark Extraction

The embedder and receiver share the key k_r, by it the receiver can extract the quantum watermark from the quantum image carrier. E.g, the image watermark with the gray value 1 is extracted from $|C_9^{'}\rangle = |10110010\rangle$ at the location $|0110\rangle$ in the quantum image carrier. The extraction process is shown as b in Fig. 5, where a $|0\rangle$-state is the additional particle, and the output of the $|0\rangle$-state is the gray value of the extracted quantum image's watermark.

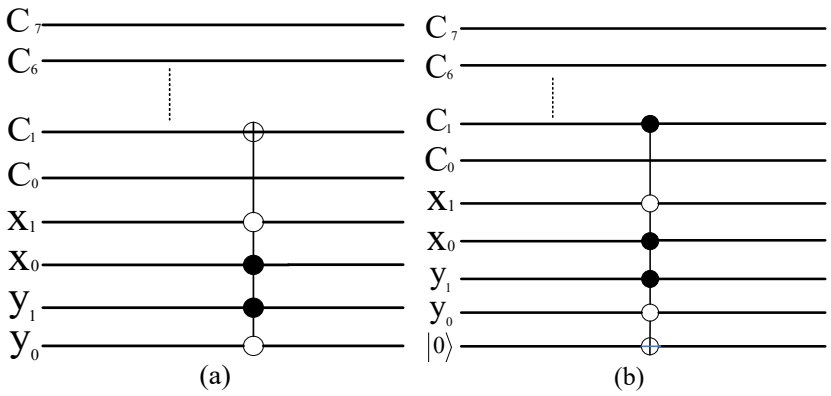

Figure 5: Quantum watermark embedding: (a) Quantum watermark embedding circuit diagram; (b) Quantum watermark extraction circuit diagram

2.4 The Quantum Image Carrier FSQb Embedding of Secret Information

The embedder prepares a quantum image carrier of the size $2^n \times 2^n$, and the corresponding quantum image carrier can be expressed as:

$$|Q\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|f(i)\rangle\,|i\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|C_{q-1}^i\,C_{q-2}^i\cdots C_0^i\rangle\,|i\rangle \tag{4}$$

The secret information S_N that needs to be embedded for the input, where the information string's length is presented as N. Based on the secret key, the secret information which should be embedded in the corresponding position of the quantum image carrier is embedded by embedder. Proceeded being embedded, the secret information $|S_0^n\rangle$ (where the superscript n indicates the n-th secret information that the information string S_N embeds it, the subscript 0 represents the Flexible Significant Bit' embedding location) and the flexible significant qubit $|C_0^i\rangle$ of the image carrier (the superscript i and the subscript 0 respectively represent the i-th quantum image carrier's pixel and the Flexible Significant Bit) are compared, hence determines which operation should be adopted on the watermark quantum carrier image, that based on the return value.

(1) When $|S_0^n\rangle = |C_0^i\rangle$, the implementation of the following operations:

$$U_j = I^{\otimes q} \otimes \left(\sum_{j=0}^{2^{2n}-1} |j\rangle \langle j| \right) \tag{5}$$

(2) When $|S_0^n\rangle \neq |C_0^i\rangle$, the following unitary transformation operation is implemented:

$$U_i = I^{\otimes q-1} \otimes U \otimes |i\rangle \langle i| + I^{\otimes q} \otimes \left(\sum_{j=0, j\neq i}^{2^{2n}-1} |j\rangle \langle j| \right) \tag{6}$$

Here $U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Then, the algorithm adopts the following procedures to create the embedding secret information.

(1) If the returned comparing value is same, which means: $|S_0^n\rangle = |C_0^i\rangle$, the secret information $|S_0^n\rangle$ to be embedded; and flexible significant bits $|C_0^i\rangle$ of quantum image carriers are equal. In such situation, nothing should be done.

(2) If the value returned by the comparator is different, that means $|S_0^n\rangle \neq |C_0^i\rangle$, the quantum image carrier $|S_0^n\rangle \neq |C_0^i\rangle$ performs the following operations:

$$\begin{aligned} U_i(|Q\rangle) &= \left(I^{\otimes q} \otimes U \otimes |i\rangle \langle i| + I^{\otimes q} \otimes \left(\sum_{j=0, j\neq i}^{2^{2n}-1} |j\rangle \langle j| \right) \right) \cdot \left(\frac{1}{2^n} \sum_{i=1}^{2^{2n}-1} |C_{q-1}^i C_{q-2}^i \cdots C_0^i\rangle |i\rangle \right) \\ &= \frac{1}{2^n} |C_{q-1}^i C_{q-2}^i \cdots C_1^i\rangle U |C_0^i\rangle |i\rangle| + \frac{1}{2^n} \sum_{j=0, j\neq i}^{2^{2n}} |C_{q-1}^j C_{q-2}^j \cdots C_0^j\rangle |j\rangle \\ &= \frac{1}{2^n} |C_{q-1}^i C_{q-2}^i \cdots C_1^i\rangle |S_0^n\rangle |i\rangle + \frac{1}{2^n} \sum_{j=0, j\neq i}^{2^{2n}} |C_{q-1}^j C_{q-2}^j \cdots C_0^j\rangle |j\rangle \end{aligned} \tag{7}$$

Here $|S_0^n\rangle = \begin{cases} |1\rangle, |C_0^i\rangle = |0\rangle \\ |0\rangle, |C_0^i\rangle = |1\rangle \end{cases}$.

Assuming that the length of the secret string to be embedded is $N = 2^4 \times 2^4$, the embedder only needs to specify $\prod_{i=0}^{2^8-1} U_i$ on the location of the quantum image carrier $|Q\rangle$ with respecting to k_1. The quantum image carrier following the entire secret information string S_N is presented in the Eq. (8).

$$|Q'\rangle = \frac{1}{2^n} \sum_{i=0}^{2^8-1} |C_{q-1}^i C_{q-2}^i \cdots C_1^i\rangle |S_0^n\rangle |i\rangle \tag{8}$$

2.5 The Embedding of the Quantum Watermarking Image's FSQb Secret Information

The embedder prepares a quantum image watermark with the size $2^m \times 2^m$, and the corresponding quantum image watermark $|R\rangle$ is expressed as the Eq. (9).

$$|R\rangle = \frac{1}{2^m} \sum_{h=0}^{2^{2m}-1} |f(h)\rangle |h\rangle = \frac{1}{2^m} \sum_{h=0}^{2^{2m}-1} \left| W_{q-1}^h W_{q-2}^h \cdots W_0^h \right\rangle |h\rangle \tag{9}$$

where $|R\rangle$ are the superposed quantum states of the quantum image watermark, $W_m^i, m \in [0, q-1]$ are the quantum image watermark's gray levels, and $|h\rangle$ is the position information of the quantum image

watermark, including the vertical, and the horizontal information. Hence the quantum image watermark has smaller size than that of the quantum image carrier ($m < n$).

Here T_M denotes the embedded secret information string within the quantum image watermark, and M denotes the length of information string. The embedder embeds the secret information which should be embedded in the corresponding location of the quantum image watermark, which generated by the secret key k_{s2}. Before embedding the secret information, at first embedding $|T_0^m\rangle$ through the quantum comparator (The superscript m indicates the first qubit to be embedded in the secret information string, and the subscript 0 indicates the embedding location of flexible and effective bits), and the quantum image carrier. While the lowest significant bit $|W_0^h\rangle$ (superscript h indicates the h-th pixel of the quantum image watermark, and the subscript 0 represents the flexible significant bit). The quantum comparator plays a role in determining that of unitary transformation.

(1) When $|T_0^m\rangle = |W_0^h\rangle$, the implementation of the following operations:

$$U_l = I^{\otimes q} \otimes \left(\sum_{l=0}^{2^{2m}-1} |l\rangle \langle l| \right) \tag{10}$$

(2) When $|T_0^m\rangle \neq |W_0^h\rangle$, the following unitary transformation operation is implemented

$$U_h = I^{\otimes q-1} \otimes U \otimes |h\rangle \langle h| + I^{\otimes q} \otimes \left(\sum_{l=0, l\neq h}^{2^{2m}-1} |l\rangle \langle l| \right) \tag{11}$$

Here $U = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

The next step in the embedding of the secret information can implement $\Pi_{h=0}^{N} U_h$ on the watermark quantum carrier $|R\rangle$ based the shared key. For the quantum image carrier, where only the difference in the value returned by the comparator is described, that is $|T_0^m\rangle \neq |W_0^h\rangle$.

$$\begin{aligned} U_h(|R\rangle) &= \left(I^{\otimes q-1} \otimes U \otimes |h\rangle \langle h| + I^{\otimes q} \otimes \left(\sum_{l=0, l\neq h}^{2^{2m}-1} |l\rangle \langle l| \right) \right) \cdot \left(\frac{1}{2^m} \sum_{h=0}^{2^{2m}-1} \left| W_{q-1}^h W_{q-2}^h \cdots W_0^h \right\rangle |h\rangle \right) \\ &= \frac{1}{2^m} \left| W_{q-1}^h W_{q-2}^h \cdots W_1^h \right\rangle U \left| W_0^h \right\rangle |h\rangle + \frac{1}{2^m} \sum_{l=0, l\neq h}^{2^{2m}-1} \left| W_{q-1}^l W_{q-2}^l \cdots W_0^l \right\rangle |l\rangle \\ &= \frac{1}{2^m} \left| W_{q-1}^h W_{q-2}^h \cdots W_1^h \right\rangle |T_0^m\rangle |h\rangle + \frac{1}{2^m} \sum_{l=0, l\neq h}^{2^{2m}-1} \left| W_{q-1}^l W_{q-2}^l \cdots W_0^l \right\rangle |l\rangle \end{aligned} \tag{12}$$

Here $|T_0^m\rangle = \begin{cases} |1\rangle, \left|W_0^h\right\rangle = |0\rangle \\ |0\rangle, \left|W_0^h\right\rangle = |1\rangle \end{cases}$

The secret information string to be embedded in the quantum image watermark has the length of $M = 2^4 \times 2^4$ and the embedder only needs to perform $\prod_{h=0}^{2^8-1} U_h$ on the basis of the key k_2 at the position designated by the quantum image carrier $|R\rangle$. After the entire secret information string T_M being embedded, and the quantum image watermark is represented by the Eq. (13).

$$\left|R'\right\rangle = \frac{1}{2^m} \sum_{h=0}^{2^8-1} \left| W_{q-1}^h W_{q-2}^h \cdots W_1^h \right\rangle |T_0^m\rangle |h\rangle \tag{13}$$

2.6 The Extraction of the Quantum Image Carrier and the Image's FSQb Watermark for Secret Information

The process of extracting the least significant qubit from the secret information has two respective sides, the first is based on the secret key K_{s1} to extract the exact qubit from the color vector of the quantum image carrier, while the second is based on K_{s2} to extract the qubit from quantum image watermark.

The size of the Hilbert space of the quantum image is 2^{q+2n}, hence the vector for the quantum image could be decomposed into color information and position information. Considering a quantum carrier image of size $2^2\times 2^2$ as an example, the vector of the FSQb quantum image carrier is X, which decomposes X into a form as shown in the Eq. (14).

$$X = C_1 \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + C_2 \otimes \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \cdots C_{16} \otimes \begin{pmatrix} 0 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} \tag{14}$$

The color information embedded in the secret information location is converted into a classic code according to the secret key K_{s1}. In the above example, if C_2, C_7 and C_{12} is color information after embedding secret information, it means that as long as C_2, C_7 and C_{12} are converted into C_{2b}, C_{7b} and C_{12b}, and then the flexible bit of each classic value is extracted. The last bit of each binary value is then extracted to extract the secret information embedded in the quantum carrier image.

The situation is same for quantum image watermark, its vector can be directly decomposed into the color information and the corresponding position information. For example, FSQb watermark image vector is a 2×2 matrix Y, to break down Y into the following form.

$$Y = W_1 \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} + W_2 \otimes \begin{pmatrix} 0 \\ 1 \\ 0 \\ 0 \end{pmatrix} + W_3 \otimes \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} + W_4 \otimes \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} \tag{15}$$

The color information embedded in the secret information location is converted into a binary code according to the secret key K_{s2}. In the example of the Eq. (14), if W_1, W_3, W_4 is the color information after embedding the secret information, it is only necessary to convert W_1, W_3, W_4 to W_{1b}, W_{3b}, W_{4b}, and then extracting the last bit of each binary value, the embedded secret information can be extracted from the quantum watermark.

2.7 Recovery of Mutual Secret Information and Location of Tampering Location

Even if an illegal eavesdropper does not easily detect the secret information during transmission, the third party can easily tamper with or ruin the image inadvertently or maliciously, resulting in the loss of secret information hidden in the flexible and important bit image. Therefore, in order to enable the secret information embedded in the quantum carrier image, or the quantum watermark image to be recovered after being destroyed, the communication parties present a string of keys K_t in advance, and it is composed of a series of U_I and U_X operations in advance, the secret information recovery relationship is as follows:

$$K_t \cdot WS = CS \tag{16}$$

where WS presents secret information extracted from quantum watermarks, and CS presents secret information extracted from a quantum carrier image.

An example of a secret information recovery relationship is given in the Table 1. Assuming a secret

string embedded in the quantum watermark sequence WS; secret information string CS embedded in a quantum carrier image, and the corresponding recovery key is K_t. For the embedded person, by means of this relationship, you can also know that the image is attacked, tampered with the location of the image of the secret information on the centralized destruction or tampering.

Table 1: The correspondence table of the secret information recovery

s	|	$\|0\rangle$	$\|0\rangle$		$\|0\rangle$
	I	I	I	X	X
s	|	$\|0\rangle$	$\|1\rangle$		$\|1\rangle$

Note: For the embedding person, it is also known that the image is attacked, and the tamper performs centralized destruction or tampering of the secret information being embedded in the image.

2.8 The Re-Combination of Two Parts Secret Information

Based on the shared essential key K_{s1}, the secret information can be extracted from the quantum image carrier and the watermark color coding's flexible significant bits in predetermined order to be recombined to form complete secret information. It is assumed that the recipient extracts the embedded secret information from the determined location in the vector image to 00101011 based on the secret key K_{s1}; and extracts the secret information 10010101 embedded therein from the determined position in the image watermark according to the secret key K_{s2}. The final recipient of the final secret message sequence is 01 00 10 01 10 01 10 11.

3 Simulation and Performance Analysis

3.1 Simulation

For the purpose of effectively evaluate the imperceptibility of the novel algorithm, the hidden effective of secret information is evaluated by peak signal to the noise ratio (PSNR) parameter. At the same time, we will also use the parameter to assess the visual effects of the image.

We demonstrate this quantum concealment scheme by simulating at MatlabR2016a. The peak signal to noise ratio is defined through the mean square error (MSE), and the latter is expressed by the Eq. (17). Suppose there are two images I and J (I is the original image carrier, J is the watermark image carrier), and $I(i,j)$ and $K(i,j)$ represents the pixel value corresponding to (i,j).

$$MSE = \frac{1}{mn}\sum_{i=1}^{2^m-1}\sum_{j=1}^{2^n-1}[(I(i,j)-K(i,j))^2] \tag{17}$$

$$PSNR = 20\times\log_{10}\left(\frac{MAX_I}{\sqrt{MSE}}\right) \tag{18}$$

The maximum pixel value of the image denotes as MAX_I. Fig. 6 demonstrates the simulation effect of the steganography scheme, where the image carrier uses a grayscale image of the size 512 × 512, and the watermark image uses a binary image of size 256 × 256. Table 2 shows the peak signal-to-noise ratio of the water-printed carrier image after embedding the secret information.

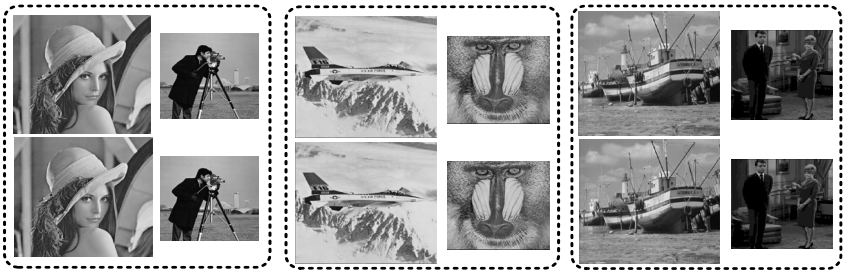

Figure 6: In three sets of examples, Ex. 1 is a carrier image; Ex. 2 is a watermark; Ex. 3 is an image of a watermark after embedding information.

Table 2: The simulation results of the PSNR

Intensive vector image	Dense image watermark	PSNR/dB
Lena	Camera	53.3746
Flighting boat	HIT	55.4965
Airplane	NUIST	52.3429

3.2 Performance Analysis

3.2.1 Concealment of Secret Information

The new algorithm uses a watermark quantum carrier image for secret information transmission. Transparency requires that it is difficult to perceive the quantum watermark embedded in the quantum carrier, and does not affect the normal use of the quantum carrier, and enhances the concealment of secret information through two layers of embedded operations. The simulation experiment results of the above scheme show that an illegal third party cannot distinguish the watermark image embedded therein by the naked eye region, and the secret information embedded therein is more difficult to be found, so the secret information to be transmitted is concealed. Concealment has been greatly improved. From Table 2, PSNR values are both 38 dB above the image quality standard, indicating that the carrier image of the watermark is less distorted. Therefore, the new algorithm has good transparency.

3.2.2 The Robustness of Secret Information

Robustness is the key to evaluating quantum watermark algorithms. The quantum watermark embedded in the quantum carrier not only makes it difficult for the illegal third party to detect, but also makes the quantum watermark less affected by the illegal third party attacking the watermark quantum carrier. Attacks by illegal third parties are classified into malicious attacks and unintentional attacks. Malicious attacks (such as data tampering and lossy compression) have a great chance of deleting or even destroying the quantum watermark embedded in the quantum carrier, making it impossible for both communication parties and illegal third parties to obtain the quantum watermark. Therefore, the quantum watermark algorithm usually focuses on analyzing the influence of unintentional attacks by illegal third parties on the quantum watermark. Common unintentional attacks include attacks such as scanning and copying, geometric transformations, and noise pollution.

According to another commonly used bit error rate (BER) in classical digital image processing, the impact of noise pollution attacks on the new algorithm is analyzed. When a watermark carrier image is transmitted in a communication network, the output image is misinterpreted due to the noise in the

channel, which is somewhat different from the original watermark carrier image. The human eye cannot distinguish the difference between the two images. Therefore, the bit error rate is used to measure the influence of noise pollution in the image transmission process. The BER is defined as the reciprocal of PSNR. The BER of the new algorithm is relatively small, indicating that noise pollution has less impact on the new algorithm. By analyzing the unintentional attacks of illegal third parties, it shows that the new algorithm has good robustness.

3.2.3 The Secret Information Embedding Rate

The embedding capacity of a quantum watermark algorithm can be measured by the embedding rate and the modification rate. According to the definition of the embedding rate (embedded rate = number of bits embedded in the watermark/the number of carrier image pixels), the embedding rate of the new algorithm is 1. In addition, according to the definition of the modification rate (the modification rate = the bit number of the carrier image unit pixel modified/the number of bits embedded in the watermark), assuming that the bit with a value equal to "0" and the watermark binary image with a value equal to "1" are evenly distributed, the carrier image unit pixel The least significant bit or the second least significant bit has a 50% probability of being modified, and the new algorithm has a modification rate of 0.5.

4 Conclusion

The quantum image representation model using log polar coordinates has the invariance characteristics of rotation and scaling, and key-based controlled least significant bit modification technology has the advantage of easy operation. This paper proposes a novel robust quantum watermark algorithm. While being compared with the previous quantum watermark algorithm, this algorithm utilizes the characteristics of the model quantum image. When the watermark quantum carrier image is attacked by geometric transformation such as rotation, flipping and scaling, but the image can still extract the embedded quantum image watermark. In addition, to ensure the robustness of the water-imprinted quantum carrier image, the embedding method of key-based controlled variable significant bit modification technology enables an illegal third party to recover from the watermark quantum carrier image, even if the key information cannot be obtained. The quantum image watermark further protects the copyright of the quantum image.

Based on the experimental simulation, combined with the peak signal-to-noise ratio and bit error rate in classical digital image processing, the transparency and robustness of the new algorithm are analyzed. Simulation results and experimental data also show that the new algorithm has good transparency and robustness. According to the analysis of the embedding capacity of the new algorithm, the embedding rate of the new algorithm is 1, which is a considerable embedding rate.

Another innovation of this paper is to design a quantum circuit based on the key-based controlled least significant bit modification technology and the key-based controlled least significant bit extraction technology to ensure that the new algorithm strictly follows the implementation process. The principle of quantum mechanics is feasible under the current physical experimental conditions; on the other hand, the new algorithm has excellent practicability.

Funding Statement: This project is funded by the State Grid Key Project "Key Technology of Scale Engineering Application of Power Battery for Echelon Utilization", the Project No. 52010119002F.

Conflicts of Interest: We declare that we have no financial and personal relationships with other people or organizations that can inappropriately influence our work, there is no professional or other personal interest of any nature or kind in any product, service and/or company that could be construed as influencing the position presented in, or the review of, the manuscript entitled.

References

[1] B. M. Terhal, D. P. DiVincenzo and D. W. Leung, "Hiding bits in Bell states," *Physical Review Letters*, vol. 86, no. 25, 5807, 2001.

[2] T, Eggeling and R. F. Werner, "Hiding classical data in multipartite quantum states," *Physical Review Letters*, vol. 89, no. 9, 097905, 2002.

[3] P. Hayden, D. Leung and G. Smith, "Multiparty data hiding of quantum information," *Physical Review A*, vol. 71, no. 6, pp. 362–368, 2005.

[4] J. Gea-Banacloche, "Hiding messages in quantum data," *Journal of Mathematical Physics*, vol. 43, no. 9, pp. 4531–4536, 2002.

[5] B. A. Shaw and T. A. Brun, "Quantum steganography with noisy quantum channels," *Physical Review A*, vol. 83, no. 2, 022310, 2011.

[6] X. Liao, Q. Wen, T. Song and J. Zhang, "Quantum steganography with high efficiency with noisy depolarizing channels," *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, vol. 96, no. 10, pp. 2039–2044, 2013.

[7] K. Martin, "Steganographic communication with quantum information," in *Int. Workshop on Information Hiding*, pp. 32–49, 2007.

[8] Z. G. Qu, X. B. Chen and M. X. Luo, "Quantum steganography with large payload based on entanglement swapping of χ-type entangled states," *Optics Communications*, vol. 96, no. 7, pp. 2075–2082, 2011.

[9] Y. Zhang, K. Lu, Y. H. Gao and M. Wang, "NEQR: A novel enhanced quantum representation of digital images," *Quantum Information Processing*, vol. 12, no. 8, pp. 2833–2860, 2013.

[10] P. Q. Le, F. Dong and K. Hirota, "A flexible representation of quantum images for polynomial preparation, image compression and processing operations," *Quantum Information Processing*, vol. 10, no. 1, pp. 63–84, 2011.

[11] S. Wang, J. Z. Sang, X. Song and X. M. Niu, "Least significant qubit (FSQb) information hiding algorithm for quantum image," *Measurement*, vol. 73, 352–359, 2015.

[12] N. Wang and S. Lin, "Watermarking scheme for quantum images based on Flexible Significant Bit," *Chinese Journal of Quantum Electronics*, vol. 32, no. 3, pp. 263–269, 2015.