Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

A High-Capacity Quantum Image Steganography Scheme Based on a Double-Layer Tortoise Shell Matrix

Jia-Hao Huang
Shandong University of Science and Technology
Hong-Mei Yang
yanghongmei@sdust.edu.cn
Shandong University of Science and Technology
Bin Yan
Shandong University of Science and Technology
Dong-Huan Jiang
Shandong University of Science and Technology
Hao-Ming Dang
Shandong University of Science and Technology
Xuan Lu
Shandong University of Science and Technology

Research Article

Keywords: Quantum image steganography, Double-layer turtle shell,YCbCr color space, Grover search algorithm

Posted Date: March 30th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-8787950/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

A High-Capacity Quantum Image Steganography Scheme Based on a Double-Layer Tortoise Shell Matrix

Jia-Hao Huang[1], Hong-Mei Yang[1*], Bin Yan[2], Dong-Huan Jiang[3], Hao-Ming Dang[1], Xuan Lu[1]

[1*]College of Computer Science and Engineering, Shandong University of Science and Technology, Qingdao, 266590, Shandong, P. R. China.
[2]College of Electronic and Information Engineering, Shandong University of Science and Technology, Qingdao, 266590, Shandong, P. R. China.
[3]College of Mathematics and Systems Science, Shandong University of Science and Technology, Qingdao, 266590, Shandong, P. R. China.

*Corresponding author(s). E-mail(s): yanghongmei@sdust.edu.cn;
Contributing authors: 18970018566@163.com; yanbinhit@sdust.edu.cn;
donghuan_jiang@163.com; 15953152266@163.com; 1352477930@qq.com;

Abstract

In recent years, quantum image steganography has attracted considerable attention; however, achieving high embedding capacity while preserving imperceptibility and security remains challenging. To address this issue, a quantum color image steganography scheme based on a double-layer turtle shell matrix is proposed.The scheme transforms RGB into the YCbCr color space to separate luminance and chrominance components according to the human visual system (HVS), and embeds secret information mainly into chrominance channels in combination with a check-digit mechanism to reduce visual distortion and enhance security. Meanwhile, the double-layer turtle shell matrix allows each coordinate to store more secret information. By jointly combining the YCbCr-based perceptual embedding strategy with the double-layer turtle shell matrix, the proposed scheme achieves **5** bpp embedding capacity while maintaining a PSNR above **50 dB**.Moreover, the Grover search algorithm is incorporated to exploit quantum parallelism, significantly reducing the time complexity of searching embedding coordinates. A corresponding quantum circuit diagram is provided as a fundamental component for realizing the embedding and extraction processes. Experimental comparisons demonstrate that the proposed scheme outperforms

existing methods in imperceptibility and embedding capacity, with a particularly notable improvement in payload.

Keywords: Quantum image steganography, Double-layer turtle shell,YCbCr color space, Grover search algorithm

1 Introduction

In the era of big data, information has permeated all aspects of human social production and daily life and plays a pivotal role in modern society. With the rapid development of information technologies, the transmission, sharing, and processing of data have become increasingly convenient. However, without effective protection mechanisms during transmission, data are highly vulnerable to theft, destruction, or malicious tampering [1–3]. Consequently, ensuring the security of information transmission has become a critical issue. As an important approach to information security, information hiding technology has attracted extensive attention and is generally classified into two categories: digital watermarking and steganography.

The primary objective of digital watermarking is to verify data integrity or protect intellectual property rights by embedding carrier-related features, such as trademarks or serial numbers, into digital content. Even when the carrier is subjected to tampering or attacks, the embedded watermark can still be detected, thereby enabling copyright protection or integrity verification. In contrast, steganography aims to conceal secret information that is independent of the carrier within digital media, making the very existence of the hidden information imperceptible to potential attackers.

Quantum computing introduces principles of quantum mechanics into conventional computing systems [4], exploiting quantum superposition and entanglement to achieve parallel processing capabilities that surpass those of classical computers [5]. With the advancement of quantum computing, Quantum Image Processing (QIP), which integrates quantum computing with traditional image processing, has gradually emerged as a prominent interdisciplinary research field [6]. Research in QIP primarily focuses on transplanting classical image processing algorithms onto quantum platforms, as well as developing novel quantum-native image processing algorithms. A fundamental task in QIP is the efficient representation and storage of image data in quantum systems. To address this challenge, various quantum image representation models have been proposed, including the qubit array model and the Realket model [7, 8].

At present, the most widely adopted quantum image representation schemes for grayscale images are the Flexible Representation of Quantum Images (FRQI) and the Novel Enhanced Quantum Representation (NEQR) [9]. Both models encode pixel position and color information using quantum states, where FRQI employs a single qubit to represent color information, while NEQR uses multiple qubits for precise grayscale description. For color images, extensions such as the NEQR-based Quantum Color Image representation (NCQI) and the FRQI-based Multi-Channel Quantum Image representation (MCQI) have been proposed [10]. Building upon these representations,

a variety of QIP algorithms have been developed, including quantum image filtering [11], compression [12], scaling [13], and quantum image watermarking [14, 15].

With the continuous progress of QIP, Quantum Image Steganography has gradually become a new research hotspot. Based on the NEQR and FRQI models, numerous quantum steganography schemes with inherent parallelism have been proposed. In 2014, Jiang et al. introduced a quantum steganography scheme based on moiré patterns using the NEQR model, enabling the embedding of a binary secret image of the same size into a grayscale carrier image of size $2^n \times 2^n$ [16]. Subsequently, in 2015, Jiang et al. proposed two LSB-based quantum steganography algorithms: a direct substitution method and a block-based LSB switching scheme [17].

In 2017, Heidari et al. presented three LSB-based quantum color image steganography methods by embedding secret information into the red (R), green (G), and blue (B) channels. These approaches mainly quantize classical steganographic concepts; however, their security is relatively weak, rendering the hidden information susceptible to detection [18]. To enhance security, Heidari and Farzadnia proposed a quantum steganography scheme based on a Gray-code reference matrix in the same year, significantly improving resistance to detection [19]. In 2018, Zhou et al. introduced an LSB-based quantum steganography method incorporating bit-plane decomposition and scrambling techniques, which made the extracted secret information difficult to reconstruct even if intercepted. Nevertheless, the embedding capacity of these schemes remains limited [20].

In 2019, Qu et al. proposed a quantum steganography algorithm that combines the NEQR model with the Exploiting Modification Direction (EMD) technique [21]. Experimental results demonstrated favorable performance in terms of visual quality and embedding capacity. However, Hu et al. later identified certain limitations in this approach and, in 2020, proposed an improved scheme based on the NCQI model, which embeds two binary key images of size $2^n \times 2^n$ into a color carrier image, thereby significantly enhancing both capacity and security [22].

In addition to these studies, various quantum color image steganography algorithms have been proposed. For instance, Pan Chi and Liu Xiande developed an LSB-based quantum color steganography method in 2018, capable of embedding 3 bits per pixel (bpp) [23]. In the same year, Li et al. introduced an improved scheme based on image segmentation and grayscale difference, achieving an embedding rate of 4 bpp [24]. In 2020, Li et al. further combined LSB substitution with reflective Gray codes to propose a new quantum steganography algorithm with enhanced embedding capacity [25].

Despite these advancements, most existing quantum image steganography algorithms still struggle to achieve an optimal trade-off between visual quality and embedding capacity, and relatively few studies focus on using color images as carriers. Inspired by classical steganography, Chang et al. proposed a data hiding method based on a turtle shell reference matrix in 2014, which achieved high embedding capacity while maintaining good visual quality [26]. Building upon this work, Meng et al. introduced quantization improvements to the turtle shell algorithm and proposed a quantum color steganography scheme combined with an LSB mechanism in 2022, significantly enhancing visual performance and security [27].

Motivated by these studies, this paper proposes a quantum color image steganography algorithm based on a double-layer turtle shell structure. The proposed method incorporates the YCbCr color space to model human visual system (HVS) characteristics and integrates a parity-bit strategy to further enhance embedding capacity while preserving visual quality. The maximum embedding rate of the proposed scheme can reach 5 bpp. Experimental results demonstrate that the proposed algorithm outperforms existing methods in terms of imperceptibility, embedding capacity, robustness, and security.

The remainder of this paper is organized as follows. Section 2 introduces the fundamental concepts employed in this work, including quantum image representation models, the double-layer turtle shell structure, the YCbCr color space, Grover's search algorithm, and quantum circuits for comparison, assignment, addition, and subtraction. Section 3 details the proposed steganography scheme and the corresponding quantum circuits. Circuit complexity analysis is presented in Section 4. Section 5 reports simulation results and performance evaluations in terms of imperceptibility, structural similarity, embedding capacity, and robustness. Finally, conclusions are drawn in Section 6.

2 Preliminaries

2.1 Quantum image representation model

2.1.1 NCQI

NCQI was proposed by Sang et al. [11] as an extension of the NEQR model. Unlike NEQR, in which image channels are represented independently, the red (R), green (G), and blue (B) channels of a color image in NCQI are encoded as quantum entangled states. Consider a color image of size $2^n \times 2^n$, where the grayscale value of each channel lies in the range $[0, 2^q - 1]$, as illustrated below.

$$|I\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |c_i\rangle \otimes |i\rangle, \tag{1}$$

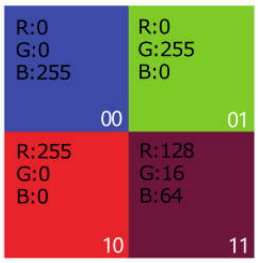
where $|i\rangle = |YX\rangle = |Y\rangle|X\rangle = |Y_{n-1}Y_{n-2}\cdots Y_0\rangle|X_{n-1}X_{n-2}\cdots X_0\rangle$ indicates the pixel positions. $|c_i\rangle = |R_i\rangle|G_i\rangle|B_i\rangle = |R_i^{q-1}R_i^{q-2}\cdots R_i^0\rangle|G_i^{q-1}G_i^{q-2}\cdots G_i^0\rangle |B_i^{q-1}B_i^{q-2}\cdots B_i^0\rangle$, and $P_i^{q-1}, P_i^{q-2}, \ldots, P_i^0 \in \{0,1\}$, $P = \{R, G, B\}$. $R_i, G_i, B_i \in \{0, 2^{q-1}\}$, which represents the grayscale values of color pixels in the R, G, and B channels, respectively.

Figure 1 shows a 2×2 sized color image and its NCQI representation.

2.2 Data hiding method based on turtle shell

In 2014, Chang et al. first proposed a data hiding method based on turtle shells[26]. Each shell is a hexagon containing the octal numbers 0-7 ("000" to "111" in binary). The figure below shows the reference matrix T of 256×256 size based on turtle shells.

The construction rules are as follows:



$$|I\rangle = \frac{1}{2}(|00000000\rangle|00000000\rangle|11111111\rangle \otimes |00\rangle + |00000000\rangle|11111111\rangle|00000000\rangle \otimes |01\rangle + |11111111\rangle|00000000\rangle|00000000\rangle \otimes |10\rangle + |10000000\rangle|00010000\rangle|01000000\rangle \otimes |11\rangle)$$

Fig. 1 A NCQI-based color image of size 2×2

Step 1: For pixels in the same row, the pixel value of column k is denoted as m_k, defined as

$$m_k = (m_{k-1} + 1) \bmod 7.$$

Step 2: For pixels in the same column, the pixel value of row k is denoted as n_k, defined as

$$n_k = \begin{cases} (n_{k-1} + 3) \bmod 7, & \text{if row } k \text{ is odd,} \\ (n_{k-1} + 2) \bmod 7, & \text{if row } k \text{ is even.} \end{cases}$$

The initial value of the first row and first column is

$$m_1 = n_1 = 0.$$

The turtle shell after construction is completed is shown in Fig. 2

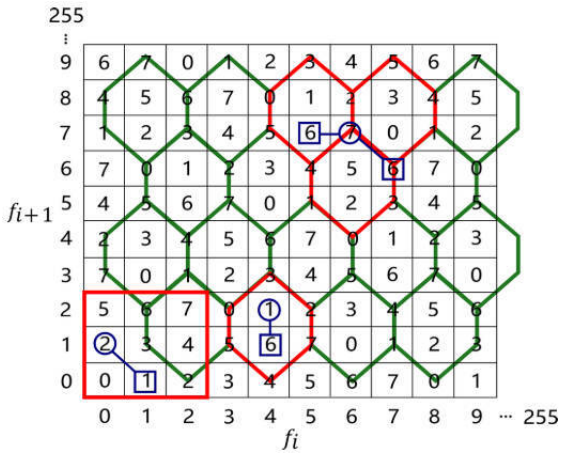


Fig. 2 Monolayer tortoise shell

2.3 Double-layer tortoise shell

On the basis of the single-layer turtle shell, in 2018, the double-layer turtle shell algorithm was first proposed in the classic field[28]. The reference matrix is transformed into a two-dimensional matrix. The reference matrix can store more secret information, so the embedding capacity will be greatly increased.

The construction process of the double-layer turtle shell matrix is as follows:

- **Step 1:** Number each shell (shells in the same layer share the same number). For turtle shells in the same row, the shell in column i is assigned the number m_i, where

$$m_i = (m_{i-1} + 1) \bmod 3.$$

- **Step 2:** For turtle shells in the same column, the shell in row j is assigned the number n_j. When $j > 2$,

$$n_j = (n_{j-2} - 1) \bmod 3.$$

  Turtle shells in odd-numbered rows are initially assigned the number 3, whereas shells in even-numbered rows are initially assigned the number 1. The resulting numbering pattern is illustrated in Fig. 3 .
- **Step 3:** Traverse each pixel to determine how many turtle shells it belongs to:
  - **Case 1:** If the pixel does not belong to any turtle shell (e.g., $(1, 1)$), set the value of *type* to 4.
  - **Case 2:** If the pixel belongs to exactly one turtle shell, set the value of *type* to the number of that turtle shell.
  - **Case 3:** If the pixel belongs to two turtle shells, set the value of *type* to the XOR of the two corresponding shell numbers.
  - **Case 4:** If the pixel belongs to three turtle shells, set the value of *type* to the XOR of the three corresponding shell numbers.

Combining all the above operations, the resulting double-layer turtle shell structure is shown in Fig. 4

2.4 YCbCr color space

The YCbCr color space is a widely used color representation model in image and video processing [29]. It decomposes image color information into one luminance component (Y) and two chrominance components (Cb and Cr). The Y component describes the brightness information of the image, i.e., luminance intensity, whereas the Cb and Cr components correspond to the blue-difference and red-difference chrominance signals, respectively. Compared with the conventional RGB color space, a key characteristic of YCbCr lies in its separation of luminance and chrominance information, which is more consistent with the perceptual mechanism of the human visual system.

In image processing, the human visual system is significantly more sensitive to variations in luminance than to changes in chrominance. Consequently, the YCbCr model allows chrominance components to be compressed or modified while preserving high visual quality. This property makes YCbCr particularly suitable for applications such as image compression, encoding, and steganography. For instance, widely adopted

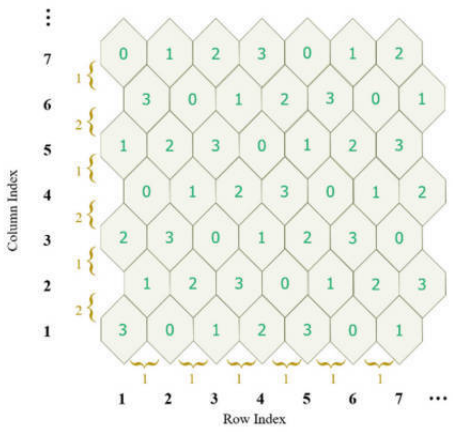


Fig. 3 Double-layer turtle shell numbering

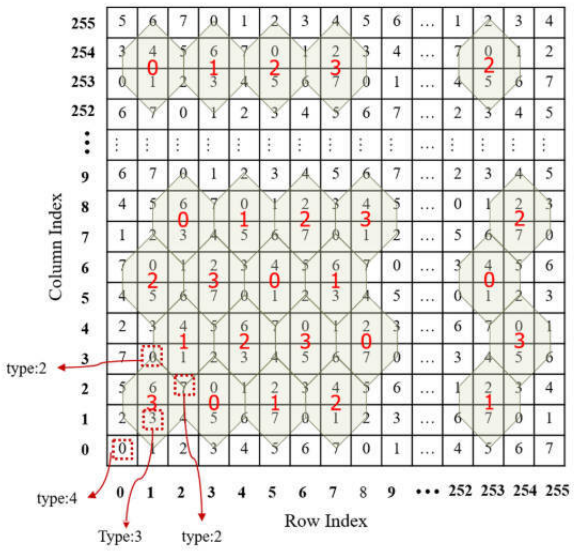


Fig. 4 Double-layer tortoise shell

international image and video standards, including JPEG and MPEG, employ YCbCr as the fundamental color model to improve compression efficiency and reduce data redundancy.

From a mathematical perspective, RGB and YCbCr color spaces can be converted into each other via linear transformations. For 8-bit images, the conversion from RGB to YCbCr is typically expressed as follows:

$$\begin{bmatrix} Y \\ Cb \\ Cr \end{bmatrix} = \begin{bmatrix} 0.299 & 0.587 & 0.114 \\ -0.168736 & -0.331264 & 0.5 \\ 0.5 & -0.418688 & -0.081312 \end{bmatrix} \begin{bmatrix} R \\ G \\ B \end{bmatrix} + \begin{bmatrix} 0 \\ 128 \\ 128 \end{bmatrix} \tag{2}$$

This transformation not only guarantees a one-to-one correspondence with the RGB color space, but also adjusts the ranges of the Cb and Cr components to be suitable for digital storage and transmission by introducing appropriate offsets.

In the context of information hiding and image steganography, the YCbCr color space plays a crucial role. Since the luminance component Y conveys the primary visual information, direct modification of this channel is likely to introduce perceptible distortion. In contrast, the Cb and Cr components have a relatively lower impact on human visual perception and are therefore more suitable as carriers for embedded steganographic information. Consequently, embedding watermarks or secret data into the chrominance components of the YCbCr space enables higher embedding capacity while maintaining high image fidelity. This property has been extensively exploited in image watermarking, image compression, and steganography algorithms.

In summary, the YCbCr color space not only occupies a central position in conventional image and video coding standards, but also provides a solid theoretical foundation and practical support for information hiding and image steganography, owing to its effective separation of luminance and chrominance information.

2.5 Grover search algorithm

Grover's search algorithm was proposed by Lov Grover in 1996 and is one of the most representative algorithms in quantum computing [30]. Compared with classical algorithms, it achieves a quadratic speedup for searching in an unordered database and is widely regarded as a landmark breakthrough in the field of quantum computation, particularly for data search problems.

In the classical computing paradigm, if only a single target element satisfies a given condition in an unordered database containing N elements, the optimal classical algorithm requires, on average, $O(N)$ queries to locate the target. By exploiting the principles of quantum superposition and quantum interference, Grover's algorithm can identify the target element using approximately $\sqrt{N}$ queries. This acceleration arises from the mechanism of quantum amplitude amplification.

The Grover algorithm mainly consists of the following steps:

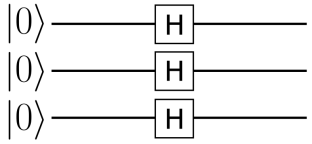


Fig. 5 * Initial

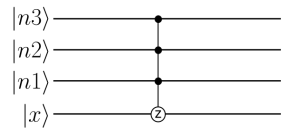


Fig. 6 * Oracle

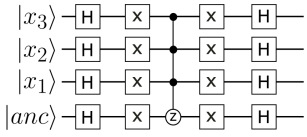


Fig. 7 * diffusion

Fig. 8 Quantum Circuit Diagram of Three Modules of Grover Algorithm

1. **Quantum state initialization:** Initialize the system to a uniform superposition of N ground states:
$$|\psi_0\rangle = \frac{1}{\sqrt{N}} \sum_{x=0}^{N-1} |x\rangle \tag{3}$$
2. **Oracle phase marking:** Construct a quantum Oracle operator O_f. When the input target element is x_0, the corresponding quantum state is flipped. This can be realized using multi-controlled NOT gates:
$$O_f|x\rangle = \begin{cases} -|x\rangle & \text{if } x = x_0 \\ |x\rangle & \text{otherwise} \end{cases} \tag{4}$$
3. **Diffusion amplification:** Quantum states are iterated multiple times by the Grover iteration operator
$$G = D \cdot O_f \tag{5}$$
where D is the Diffusion Operator that reflects the amplitudes of all states around the average. Each iteration increases the probability amplitude of the target state, thus amplifying the probability of obtaining the target state upon measurement.
4. **Measurement:** After
$$r \approx \frac{\pi}{4}\sqrt{N} \tag{6}$$
iterations, the quantum state is measured, and the result obtained is x_0 with very high probability.

The advantage of this algorithm lies in its exploitation of quantum parallelism. All pixels can be evaluated simultaneously, rather than being processed sequentially through iterative loops. The logical circuit diagrams corresponding to the three main stages of Grover's algorithm—initialization, oracle marking, and diffusion amplification—are clearly presented in the classical textbook by Michael A. Nielsen and Isaac L. Chuang [31]. Figure 8 illustrates a simple example of the corresponding quantum circuit.

2.6 Quantum circuit

2.6.1 Adder and subtractor

The adder is a fundamental quantum logic circuit, as illustrated in Fig. 9.

Due to the unitary nature of quantum circuits, reversing the order of the logic gates results in an inverse operation. Consequently, the circuit implements the inverse function of addition, effectively acting as a subtractor. The corresponding subtractor circuit is illustrated in Fig. 10.

2.6.2 Quantum comparator

From the most significant bit to the least significant bit, each qubit in $|b\rangle$ is associated with an auxiliary qubit that records the intermediate comparison result. First, we determine whether a_1 and b_1 are equal. If they are not equal, the output qubits o_1

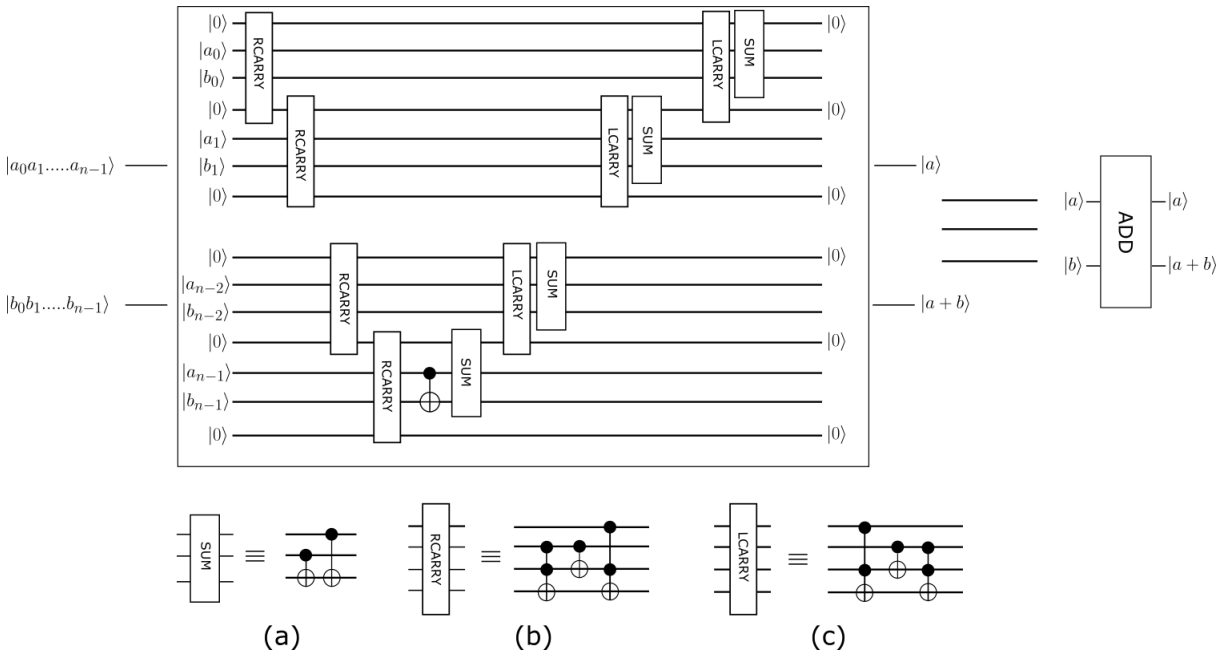


Fig. 9 Adder

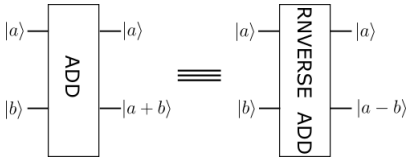


Fig. 10 subtractor

and o_0 are directly assigned according to the magnitude of a_1 and b_1. Otherwise, the same comparison procedure is recursively applied to the lower-order bits. After the comparison, the auxiliary qubits are used to restore the original value of $|b\rangle$.

If the output state $|o\rangle$ is $|10\rangle$, then $|a\rangle$ is greater than $|b\rangle$; if $|o\rangle = |01\rangle$, then $|a\rangle$ is less than $|b\rangle$; otherwise, the two values are equal. The corresponding quantum circuit diagram is shown in Fig. 11

2.6.3 Quantum Equality (QE)

The quantum equivalence model is a quantum comparator designed by Zhou et al. It is used to compare whether two n-qubit sequences $|A\rangle$ and $|B\rangle$ are equal. The sequences are represented as $|A\rangle = |a_{n-1}a_{n-2}\cdots a_0\rangle$ and $|B\rangle = |b_{n-1}b_{n-2}\cdots b_0\rangle$, where $a_i, b_i \in \{0, 1\}$. The comparison result is determined by the output qubit $|r\rangle$. If $|r\rangle = |0\rangle$, then $|A\rangle \neq |B\rangle$. If $|r\rangle = |1\rangle$, then $|A\rangle = |B\rangle$. Figure 12 shows the quantum circuit and the simplified circuit diagram of the QE module.

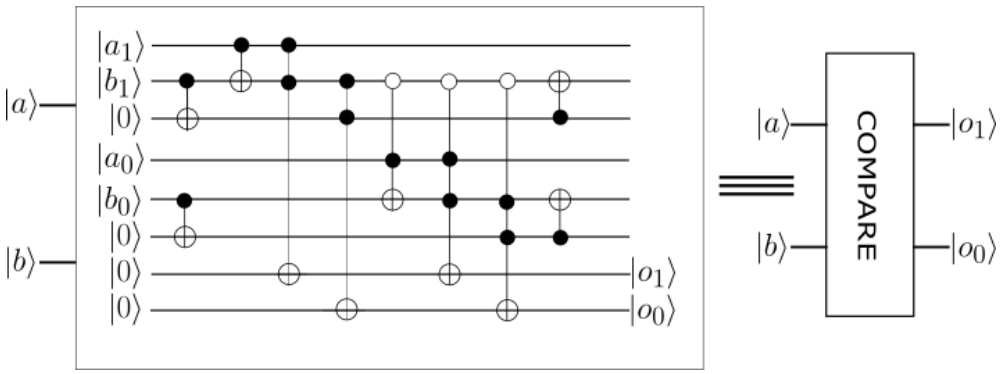


Fig. 11 Quantum comparator

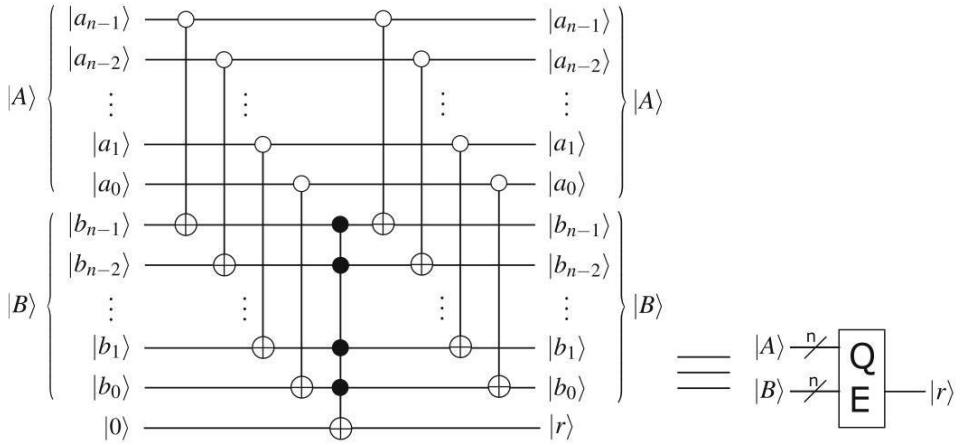


Fig. 12 Quantum equality circuit

2.6.4 Quantum Assignment (QA)

The quantum assignment model is used to assign an n-qubit binary sequence $|A\rangle$ to another n-qubit binary sequence $|B\rangle$. The two sequences are represented as $|A\rangle = |a_{n-1}a_{n-2}\cdots a_0\rangle$ and $|B\rangle = |b_{n-1}b_{n-2}\cdots b_0\rangle$, where $a_i, b_i \in \{0, 1\}$.

First, the value of $|A\rangle$ is stored in a set of n auxiliary qubits initially prepared in the state $|0\rangle$ by applying controlled-NOT (CNOT) gates. Then, the values of $|B\rangle$ are exchanged with those of the auxiliary qubits using SWAP gates. After the operation, the output state of $|B\rangle$ becomes identical to $|A\rangle$, i.e., $|B\rangle = |A\rangle$.Figure 13 shows the quantum circuit and simplified circuit diagram of the QA module.

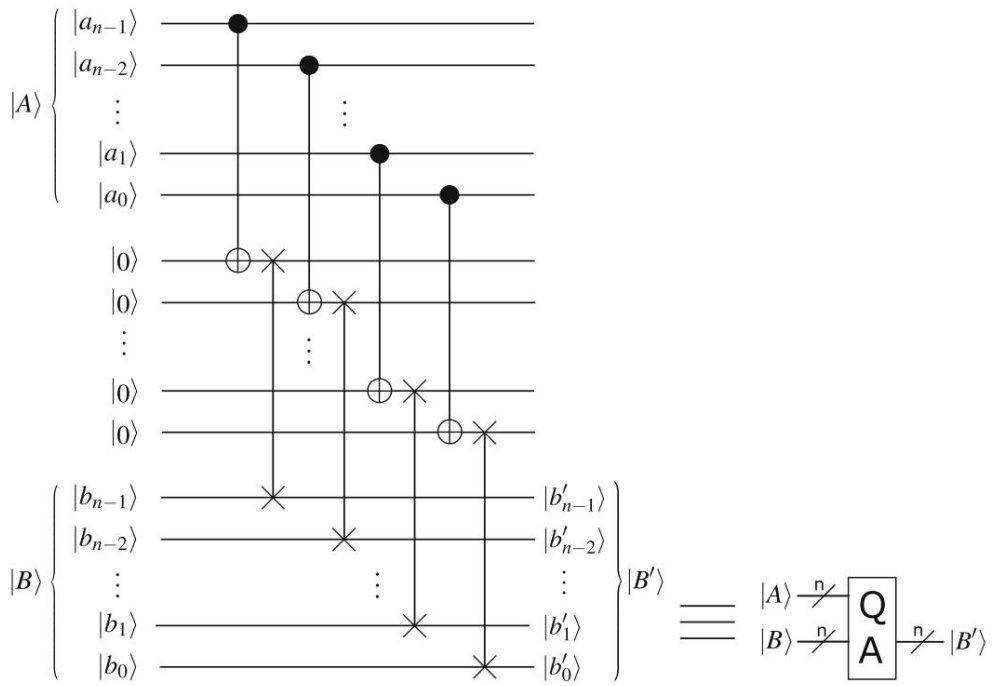


Fig. 13 Quantum assignment circuit

2.6.5 distance calculating circuit (dist)

To calculate the distance between two coordinates, Fig. 14 illustrates the quantum circuit of the QA module along with its corresponding simplified circuit diagram.

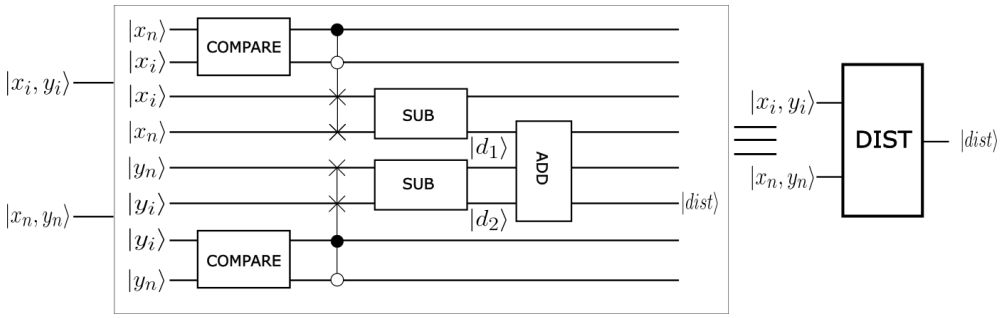


Fig. 14 distance calculating circuit

3 The proposed scheme and the realization of quantum circuit

Based on the double-layer turtle shell algorithm combined with the NCQI model, the proposed scheme is applied to a color carrier image. By incorporating the YCbCr color space introduced in Section 2.4, the method preserves excellent visual quality while significantly enhancing the embedding capacity. In this work, a $2^n \times 2^{n-1}$ grayscale secret image is embedded into a $2^n \times 2^n$ carrier image. The scheme employs key information, namely the reference matrix introduced in Section 2.3. A total of 5 bits (3 bits in the first layer and 2 bits in the second layer) are embedded into the carrier image through the mapping defined by the reference matrix. The flowcharts of the embedding and extraction processes are shown in Figs. 15 and 16.

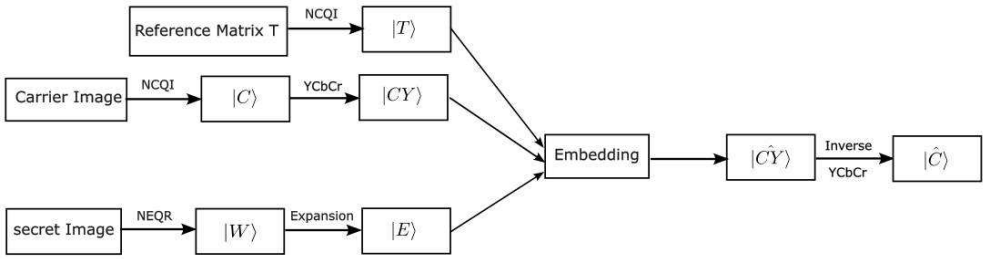


Fig. 15 Embed flow chart

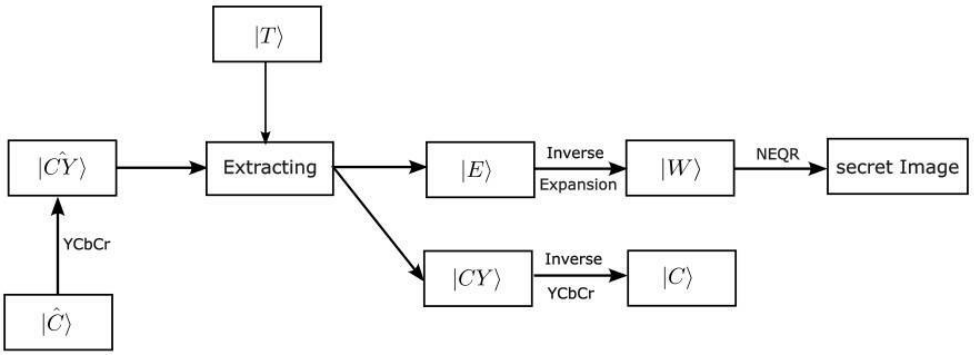


Fig. 16 Extract flow chart

3.1 Preparation

A grayscale image of size $2^n \times 2^{n-1}$, with pixel values ranging from 0 to 255, is used as the secret image, while a grayscale image of size $2^n \times 2^n$ serves as the carrier

image. The carrier image and the double-layer turtle shell matrix are subsequently transformed into quantum images $|C\rangle$ and $|T\rangle$, respectively, using the NCQI model, where the pixel values of the first and second layers are encoded in the B and R channels. The secret image and the reference matrix are converted into a quantum image $|W\rangle$ via the NEQR model.

$$|C\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |R_{YX}\, G_{YX}\, B_{YX}\rangle \otimes |YX\rangle_C, \tag{7}$$

where $R_{YX} = R_{YX}^7 R_{YX}^6 \cdots R_{YX}^0$, $G_{YX} = G_{YX}^7 G_{YX}^6 \cdots G_{YX}^0$, $B_{YX} = B_{YX}^7 B_{YX}^6 \cdots B_{YX}^0$, and $R_{YX}^i, G_{YX}^i, B_{YX}^i \in \{0, 1\}$.

$$|T\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^n-1} |T_{YX}^R\, T_{YX}^G\, T_{YX}^B\rangle \otimes |YX\rangle_T, \tag{8}$$

where $T_{YX}^\alpha = T_{YX}^{\alpha,7} T_{YX}^{\alpha,6} \cdots T_{YX}^{\alpha,0}$ for $\alpha \in \{R, G, B\}$, and $T_{YX}^{\alpha,i} \in \{0, 1\}$.

$$|W\rangle = \frac{1}{2^n} \sum_{Y=0}^{2^n-1} \sum_{X=0}^{2^{n-1}-1} |w_{YX}^7 w_{YX}^6 \cdots w_{YX}^0\rangle \otimes |YX\rangle, \tag{9}$$

where the secret image (and reference matrix) is of size $2^n \times 2^{n-1}$, each pixel $w_{YX} = (w_{YX}^7 \cdots w_{YX}^0)$ is an 8-bit gray value, and $w_{YX}^i \in \{0, 1\}$.

3.2 Embedding process

The specific embedding steps are as follows.

Step 1: The pixel values of the secret image are mapped to the coordinates of the reference matrix via the double-layer turtle shell mechanism. All pixels of the secret image are traversed, and the image is expanded from $2^n \times 2^{n-1}$ to $2^n \times 2^n$. The expanded secret image is denoted as $|E\rangle$.

Step 2: A double-layer turtle shell matrix is generated using the algorithm described in Section 2.3 and subsequently converted into a reference matrix $|T\rangle$ using the NCQI model. Meanwhile, the RGB channels of the carrier image $|C\rangle$ are transformed into the Y, Cb, and Cr channels according to the YCbCr conversion formula.

Step 3: Both the carrier image $|C\rangle$ and the expanded secret image $|E\rangle$ are traversed. The Cb and Cr values of the carrier image are extracted to form the coordinate pair (Cb, Cr). If the pixel value at this coordinate in $|T\rangle$ matches the corresponding pixel value in $|E\rangle$, the embedding is completed directly. Otherwise, the Grover search algorithm is employed to locate the coordinate (X_0, Y_0) of the secret pixel value in $|T\rangle$, and the identified coordinates are embedded into the Cb and Cr channels of the carrier image.

3.2.1 Expanding secret imagery

To enable information embedding into the carrier image, the secret image must first be expanded. In the proposed method, a secret image of size $2^n \times 2^{n-1}$ is expanded

to $2^n \times 2^n$. Two parity bits are appended to each pixel to improve robustness and enhance resistance against malicious attacks.

Each pixel of the original secret image contains 8 bits. After expansion, the first 5 bits are stored in the first pixel, while the remaining 3 bits are combined with two parity bits and stored in the second pixel. A practical example illustrating this expansion process is shown in Fig. 18. To implement this operation, the logic circuit depicted in Fig. 17 is designed.

Following this procedure, a digital watermark image with a final size of $2^n \times 2^n$ and 5 bits per pixel is obtained.

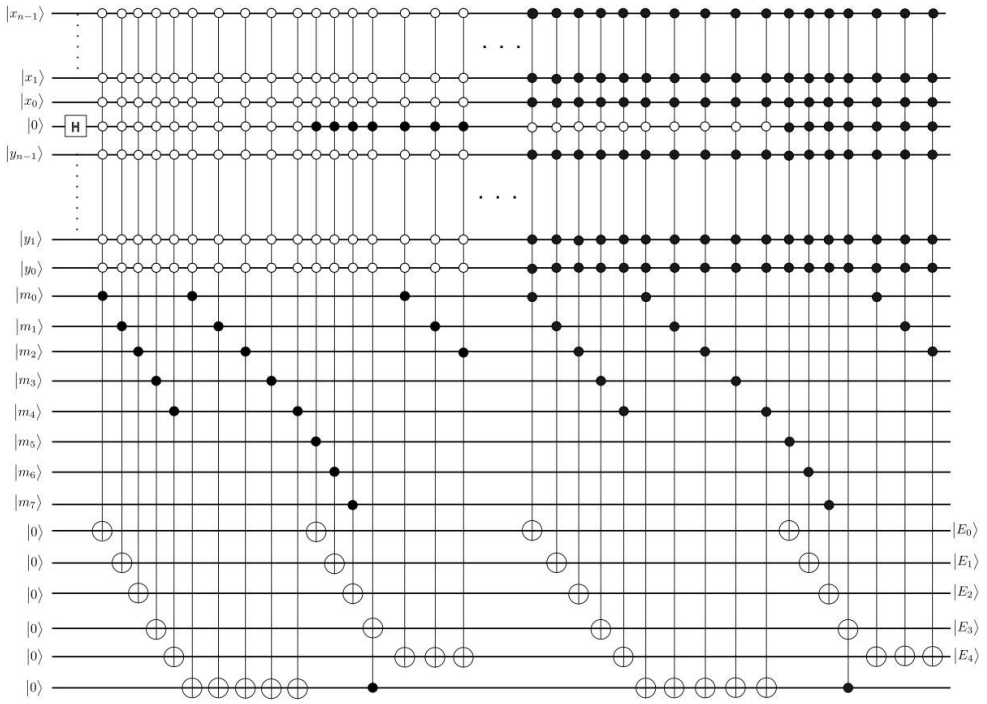


Fig. 17 Extended circuit

3.2.2 Embedding of information

Step 1: Input of Carrier and Secret Images. The system receives the quantum state C of the carrier image and the quantum state E of the secret image after extended merging. The carrier image is a $2^n \times 2^n$ color quantum image, and each pixel value is encoded by several qubits.

Step 2: Conversion to YCbCr Color Space. The RGB channels of C are converted to the YCbCr space using the formulas given in Chapter 2. Since the YCbCr model is mathematically bijective, embedding information in this space does not affect later extraction.

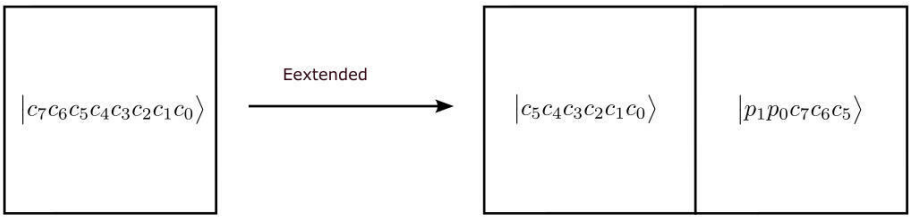


Fig. 18 Extended example

Step 3: Double-Layer Tortoise-Shell Mapping. For each pixel, the Cb and Cr channel values are taken as coordinates to query the double-layer tortoise-shell matrix T. Because the Y channel is highly sensitive to the human visual system, no information is embedded in the Y channel.

Step 4: Quantum Coordinate Processing and Oracle Marking. A 16×16 coordinate matrix centered on the current coordinate is defined. Each coordinate is represented as

$$|XY\rangle = |X_3X_2X_1X_0\, Y_3Y_2Y_1Y_0\rangle,$$

where both X and Y occupy 4 qubits. A Hadamard transform is applied to generate an equal-probability superposition of all coordinate states. An improved Oracle is then applied: the 5-bit secret information is divided into 3 bits for the first-layer shell and 2 bits for the second layer. Traditional multi-controlled Z gates cannot adapt to dynamically changing bit values, so a QE (Quantum Equality) module is used instead. When the coordinate matches the embedded secret bits exactly, a phase flip is performed. Finally, a Diffusion operator is applied. After iterating the Oracle and Diffusion operations approximately N times, the target coordinate obtains a significantly amplified measurement probability.

Step 5: Minimum-Distance Screening and Embedding. Due to the 16×16 texture structure, at most two candidate coordinates exist. These candidates and the input coordinate are processed by an adder circuit to obtain the real coordinate. A distance-calculation circuit selects the minimum-distance coordinate. The resulting X and Y coordinate values are then written into the Cb and Cr channels, requiring modification of at most the last three bits.

Result. Using this procedure, 5 bits of secret information can be embedded while only 1–3 bits of the pixel coordinates are modified. This approach achieves a high embedding capacity with a PSNR exceeding 50 dB, and further improves visual quality and security due to the use of the YCbCr color representation. The circuit diagrams of the complete embedding process are shown in Figs. 19, 20, 21, 22, and 23. Figure 21 illustrates the complete workflow of the Grover search algorithm, while Figs. 19 and 20 present the corresponding oracle and diffusion modules. Figure 22 shows the circuit for shortest-distance comparison, and Fig. 23 depicts the complete embedding process.

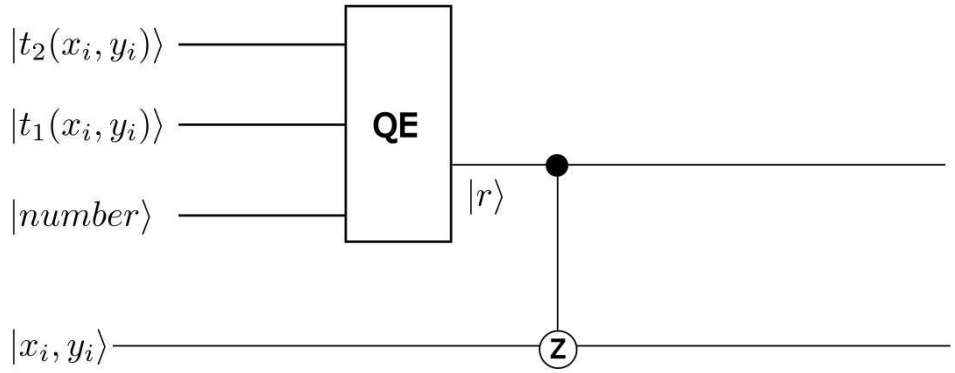


Fig. 19 Oracle Module Circuit Diagram

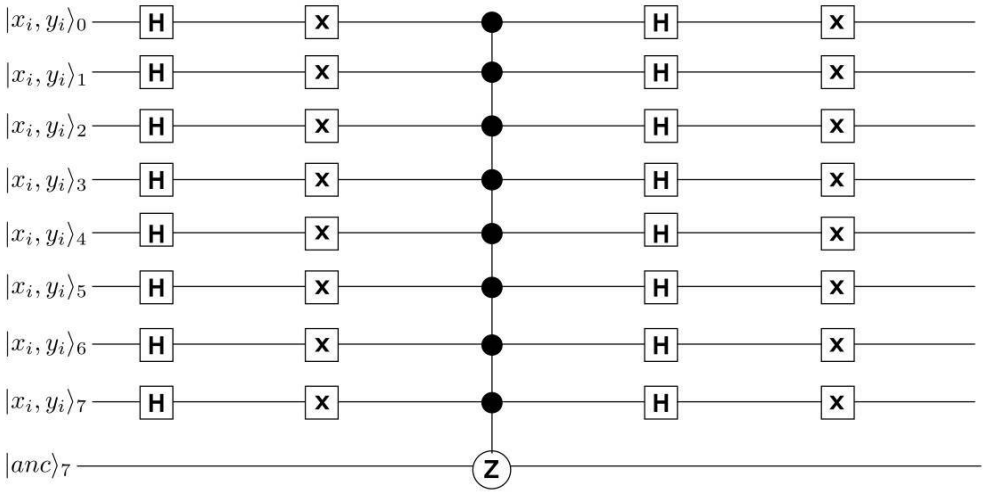


Fig. 20 Diffusion Module Circuit Diagram

3.3 Extraction process

The quantum circuit used to extract the expanded secret pixel $|E\rangle$ is shown in Fig. 24, and the extraction procedure is described in detail below. The stego image is traversed, and the pixel values are read from the Cb and Cr channels as the X and Y coordinates, respectively. The pixel values of the stego image are compared with the corresponding coordinate positions in the reference matrix $|T\rangle$ through the comparison module QE, and five auxiliary qubits are allocated to store the extracted secret information. If $r = 1$, the pixel values of the first-layer matrix $|T\rangle$ are stored in the lower three qubits, denoted as E_0, E_1, E_2, while the pixel values of the second-layer matrix $|T\rangle$ are stored

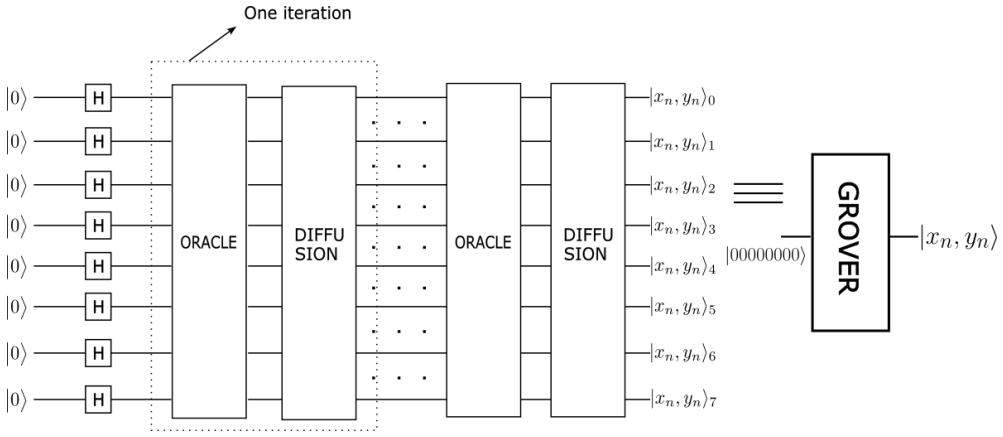


Fig. 21 Grover Search Algorithm Circuit Diagram

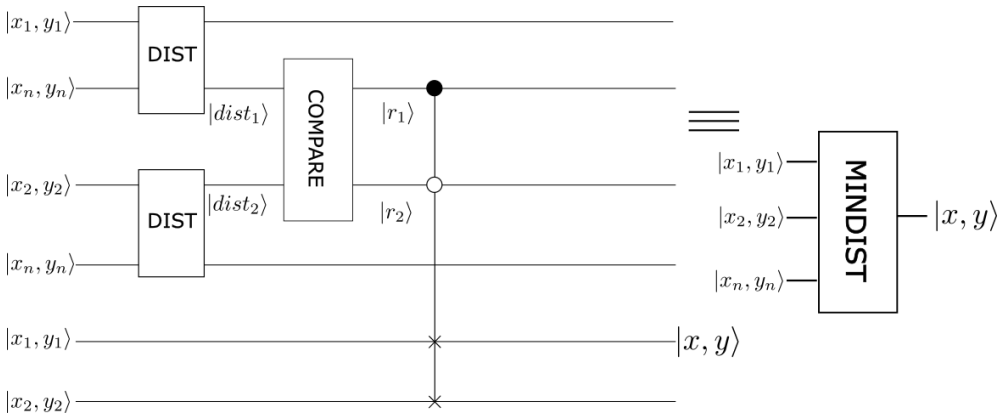


Fig. 22 Shortest distance coordinate circuit

in the higher two qubits, denoted as E_3, E_4. After the inverse expansion, the secret information and the corresponding parity bits of the secret image $|W\rangle$ are obtained.

The inverse expansion circuit is employed to reduce the expanded secret image $|E\rangle$ of size $2^n \times 2^n$ to the original secret image $|W\rangle$ of size $2^n \times 2^{n-1}$ and to separate the secret information from the parity bits, as illustrated in Fig. 25.

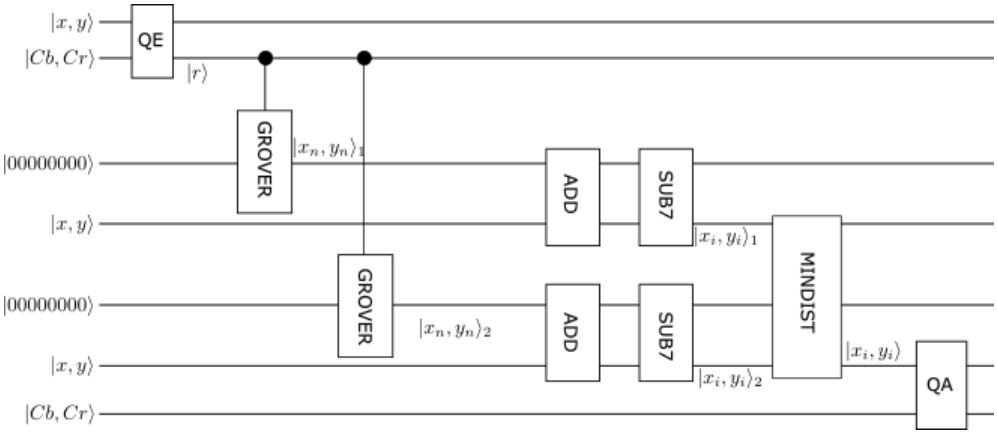


Fig. 23 Complete embedded circuit

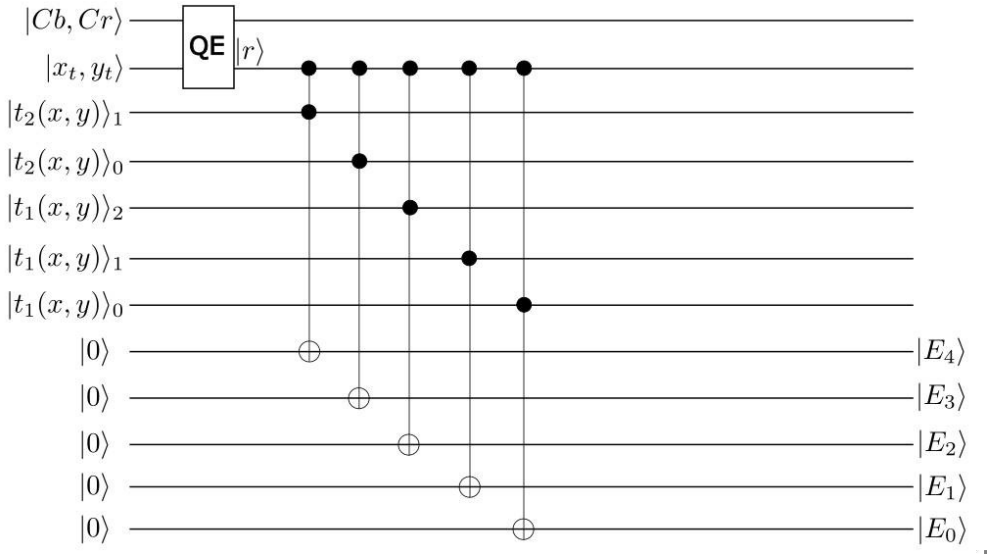


Fig. 24 extraction circuit

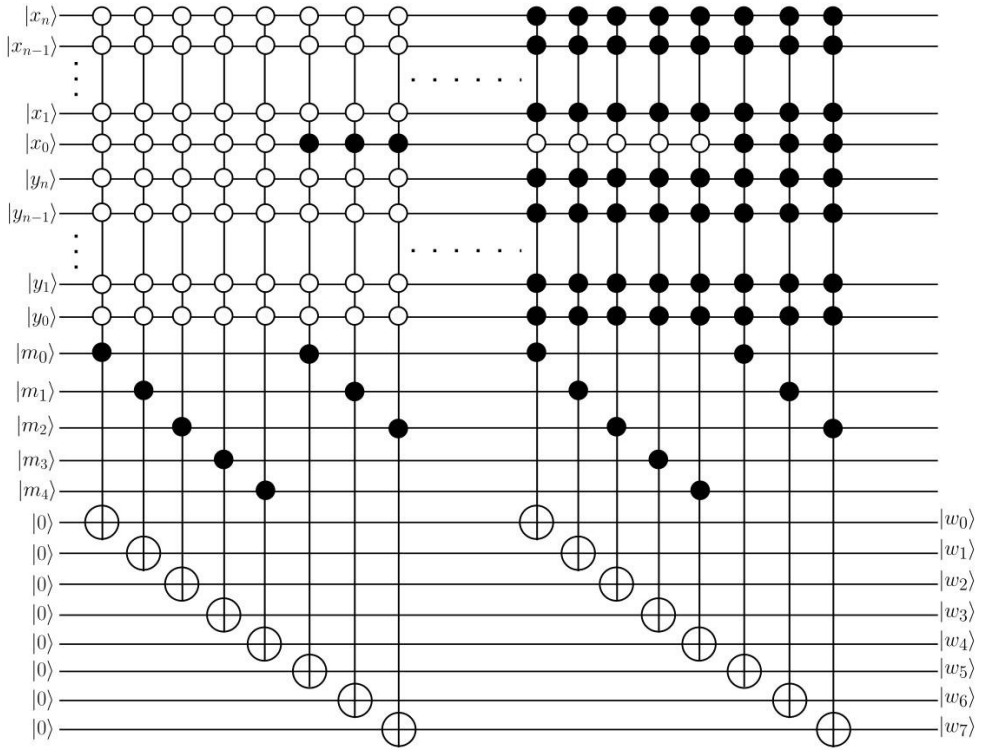


Fig. 25 Inverse expansion circuit

4 Circuit complexity

This section analyzes the circuit complexity of the proposed algorithm. The complexity of a quantum circuit is generally evaluated in terms of the number of elementary quantum gates it contains. As pointed out in the literature [32], any complex quantum logic gate can be decomposed into a sequence of single-qubit and two-qubit gates. Accordingly, in this paper, single-qubit gates (such as the Hadamard gate and the NOT gate) and two-qubit gates (such as the CNOT gate) are regarded as the basic gate set.

Let $C^n(X)$ denote an $(n+1)$-qubit controlled-NOT gate (i.e., an n-controlled NOT gate), where the first n qubits serve as control qubits and X represents the NOT operation. For $n \geq 3$, a $C^n(X)$ gate can be decomposed into $2(n-1)$ Toffoli gates, together with one CNOT gate, with the assistance of auxiliary qubits [33]. Since a single Toffoli gate is equivalent to six CNOT gates, the complexity of multi-controlled CNOT gates can be derived as shown in Eq. (10).

$$2(n-1) \times 6 + 1 = 12n - 11 \tag{10}$$

4.1 Complexity Analysis of Embedding Process

The embedding process consists of four main stages: secret image expansion, Grover search, minimum-distance coordinate selection, and secret information embedding. The extended circuit contains $8 \times 2^{2n-1}$ $2n$-controlled CNOT gates and $6 \times 2^{2n-1}$ CNOT gates. The complexity of the multi-controlled CNOT gates can be calculated as shown in Eq. (11).

$$8 \times 2^{2n-1} \times (12 \times 2n - 11) + 6 \times 2^{2n-1} = \mathcal{O}\left(n \cdot 2^{2n}\right) \tag{11}$$

The Grover search algorithm consists of eight Hadamard (H) gates, an oracle module, and a diffusion module. The oracle module includes a 5-qubit quantum equality (QE) module and a single-qubit Z gate. The diffusion module is composed of eight H gates, eight X gates, and an 8-controlled Z gate. After approximately 11 Grover iterations, the overall gate composition can be expressed as $11 \times (8H + 8X +$ 5-qubit QE module $+ Z) + 8H$. Each QE module compares two n-qubit registers and contains $2n$ CNOT gates and one n-controlled CNOT gate. In Grover's algorithm, all components except the QE comparison circuit have constant circuit depth. Since the QE module has a circuit complexity of $O(n)$, the overall circuit complexity of the Grover search algorithm is also $O(n)$.

The MinDist module and the information embedding process are composed of two Compare modules, two 2-qubit SWAP gates (each equivalent to three two-qubit CNOT gates), two Sub modules, one Add module, and a QA assignment circuit. The Sub and Add modules share identical circuit complexity and are therefore analyzed together. Each Add module consists of $2n-1$ carry circuits, n addition circuits, and one CNOT gate. Each carry circuit contains two two-qubit CNOT gates and one single-qubit CNOT gate, while each addition circuit includes two CNOT gates. Consequently, each Add module requires $4n - 2$ two-qubit CNOT gates and $4n$ single-qubit CNOT gates.

In a Compare module, comparing two n-qubit registers requires $2n$ single-qubit CNOT gates and $2n$ two-qubit CNOT gates, resulting in a circuit complexity of $O(n)$. Therefore, the overall circuit complexity of the MinDist and information embedding modules is $O(n)$. In summary, the circuit complexity of the entire embedding process is $O(n)$, and when the extended circuit is taken into account, the total complexity becomes $O(n \cdot 2^{2n})$. Otherwise, the circuit complexity remains $O(n)$.

4.2 Complexity Analysis of Extraction Process

The extraction process consists of two main stages: secret information extraction and inverse expansion. The extraction stage comprises one QE comparison module and five two-qubit CNOT gates, whereas the inverse expansion stage contains $8 \cdot 2^{2n-1}$ $(2n+1)$-qubit CNOT gates.

Based on the preceding analysis, the circuit complexity of the extraction stage is $O(n)$, while that of the inverse expansion stage is $O(n \cdot 2^{2n})$. Accordingly, the overall circuit complexity of the complete extraction process is

$$O(n) + O(n \cdot 2^{2n}) = O(n \cdot 2^{2n}).$$

Table 1 compares the circuit complexity of existing quantum steganography schemes based on image expansion with that of the proposed scheme. The experimental results indicate that, when the circuit complexity of the expansion circuit is taken into account, the proposed scheme achieves a comparable level of complexity to other related schemes. Moreover, when the circuit complexity of the expansion circuit is excluded, the proposed scheme exhibits lower circuit complexity than the existing schemes.

Table 1 Comparison of complexity results.

Algorithm	Time Complexity
Proposed scheme	$O(n * 2^{2n})$
Scheme in [20]	$O(624n * 2^{2n-4})$
Scheme in [24]	$O(n * 2^{2n+3} + n^2)$
Scheme in [25]	$O(n * 2^{2n+3} + n^2)$
Scheme in [23]	$O(n * 2^{2n+2} + n^2)$

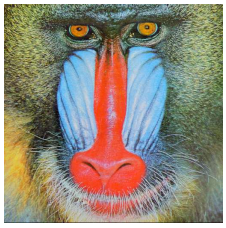
5 Simulation and Analysis

In this part, the invisibility, embedding ability, robustness and security of the proposed algorithm are evaluated through theoretical and experimental analysis. Due to

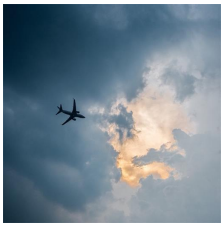
the lack of hardware support, there is currently no quantum computer capable of conducting experiments. The proposed quantum steganography algorithm is simulated on a classical computer in MatLab environment. Figure 26 shows the digital images used in the simulation experiment



(a) c1:Sailboat



(b) c2:Baboon



(c) c3:Air



(d) w1:Plane



(e) w2:Leopard



(f) w3:Women



(g) w4:Town

Fig. 26 Test images used in the simulation experiments. (a)–(c) are 512 × 512 cover images, namely Sailboat, Baboon, and Air. (d)–(g) are 256 × 256 secret images, including Plane, Leopard, Women, and Town.

5.1 Visual quality

The imperceptibility of the proposed scheme is systematically investigated, since visual quality is a critical criterion for evaluating steganographic performance. In general, the closer the stego-image appears to the original carrier image from the perspective of human vision, the higher the imperceptibility achieved by the algorithm. In this subsection, the visual performance of the proposed method is quantitatively assessed using two widely adopted metrics: peak signal-to-noise ratio (PSNR) and histogram analysis.

It is well known that the human visual system (HVS) exhibits significantly higher sensitivity to luminance information than to chrominance components. Consequently, the conventional average PSNR, which assigns equal importance to all color channels, does not adequately reflect the perceived visual quality of color images. To address this limitation, a weighted peak signal-to-noise ratio (WPSNR) metric is employed in this work, where channel-dependent perceptual weights are introduced to better model human visual sensitivity[34].

For each channel $C \in \{Y, Cb, Cr\}$, the mean squared error (MSE) is defined as

$$\mathrm{MSE}_C = \frac{1}{2^{2n}} \sum_{i=1}^{2^n} \sum_{j=1}^{2^n} \left| I_C(i,j) - K_C(i,j) \right|^2 . \tag{12}$$

The weighted mean squared error is computed as

$$\mathrm{MSE}_w = w_Y \cdot \mathrm{MSE}_Y + w_{Cb} \cdot \mathrm{MSE}_{Cb} + w_{Cr} \cdot \mathrm{MSE}_{Cr}. \tag{13}$$

Accordingly, the weighted peak signal-to-noise ratio (WPSNR) is defined as

$$\mathrm{PSNR}_w = 10 \cdot \log_{10} \left(\frac{\mathrm{MAX}_Y^2}{\mathrm{MSE}_w} \right). \tag{14}$$

When data embedding is performed only in the Cb and Cr channels, the WPSNR is given by

$$\mathrm{PSNR}_w^{CbCr} = 10 \cdot \log_{10} \left(\frac{\mathrm{MAX}_Y^2}{w_{Cb} \cdot \mathrm{MSE}_{Cb} + w_{Cr} \cdot \mathrm{MSE}_{Cr}} \right). \tag{15}$$

Unlike the traditional RGB color space, in which the perceptual sensitivities to the R, G, and B channels are relatively similar, the proposed scheme adopts the YCbCr color model. In this representation, the luminance component (Y) plays a dominant role in visual perception, while the chrominance components (Cb and Cr) are considerably less perceptually significant. By restricting data embedding to selected channels, the proposed method effectively preserves visual fidelity. Experimental results demonstrate that the average PSNR of the stego-images consistently exceeds 50 dB, Table 2 presents the PSNR values of various secret images embedded into different carrier images, illustrating the fidelity of the proposed quantum-based information embedding scheme.

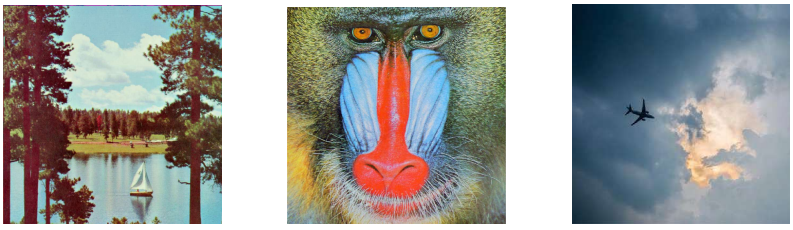
5.2 Histogram analysis

The image histogram shows the frequency of each pixel value in the image. It illustrates the brightness distribution of the image. The horizontal axis of the histogram represents the pixel values, and the vertical axis represents the number of pixels. For grayscale images, the horizontal coordinate range of the histogram is [0, 255]. By comparing the histogram similarity of the carrier image and the histogram of the steganography image, the visual quality of the steganography algorithm can be evaluated.

Figure 28 illustrates the histograms of the R, G, and B channels of the color carrier images shown in Fig. 26, together with those of their corresponding steganographic images presented in Fig. 27. The red, green, and blue curves represent the histogram distributions of the R, G, and B channels, respectively. The left column shows the histograms of the carrier images *Sailboat*, *Air*, and *Baboon*, whereas the right column displays the histograms of the corresponding steganographic images. As observed

Table 2 The PSNR values of the carrier images after embedding the information images in each group of experiments.

Carrier image	Information image	PSNR (dB)
C1	C1-W1	50.07
C1	C1-W2	50.02
C1	C1-W3	50.06
C1	C1-W4	50.03
C2	C2-W1	50.04
C2	C2-W2	50.06
C2	C2-W3	50.05
C2	C2-W4	50.05
C3	C3-W1	50.23
C3	C3-W2	49.87
C3	C3-W3	49.88
C3	C3-W4	50.05



(a) a-d **(b)** b-e **(c)** c-f



(d) d-a **(e)** e-b **(f)** f-c

Fig. 27 **a**–**c** represent the steganographic images obtained by embedding the secret images into the carrier images. **d**–**f** correspond to the secret images extracted from **a**–**c**, respectively.

from the comparison, the differences between each pair of histograms are negligible, and the overall luminance distributions exhibit highly similar trends. These results indicate that the proposed embedding scheme effectively preserves the statistical characteristics of the original images, thereby achieving strong visual imperceptibility.

5.3 Analysis of SSIM, NCC and other indicators

In addition to the widely adopted peak signal-to-noise ratio (PSNR) for image quality assessment, the structural similarity index measure (SSIM) and normalized cross-correlation (NCC) are also commonly employed to evaluate image matching performance and structural resemblance. Among them, SSIM provides a perceptually

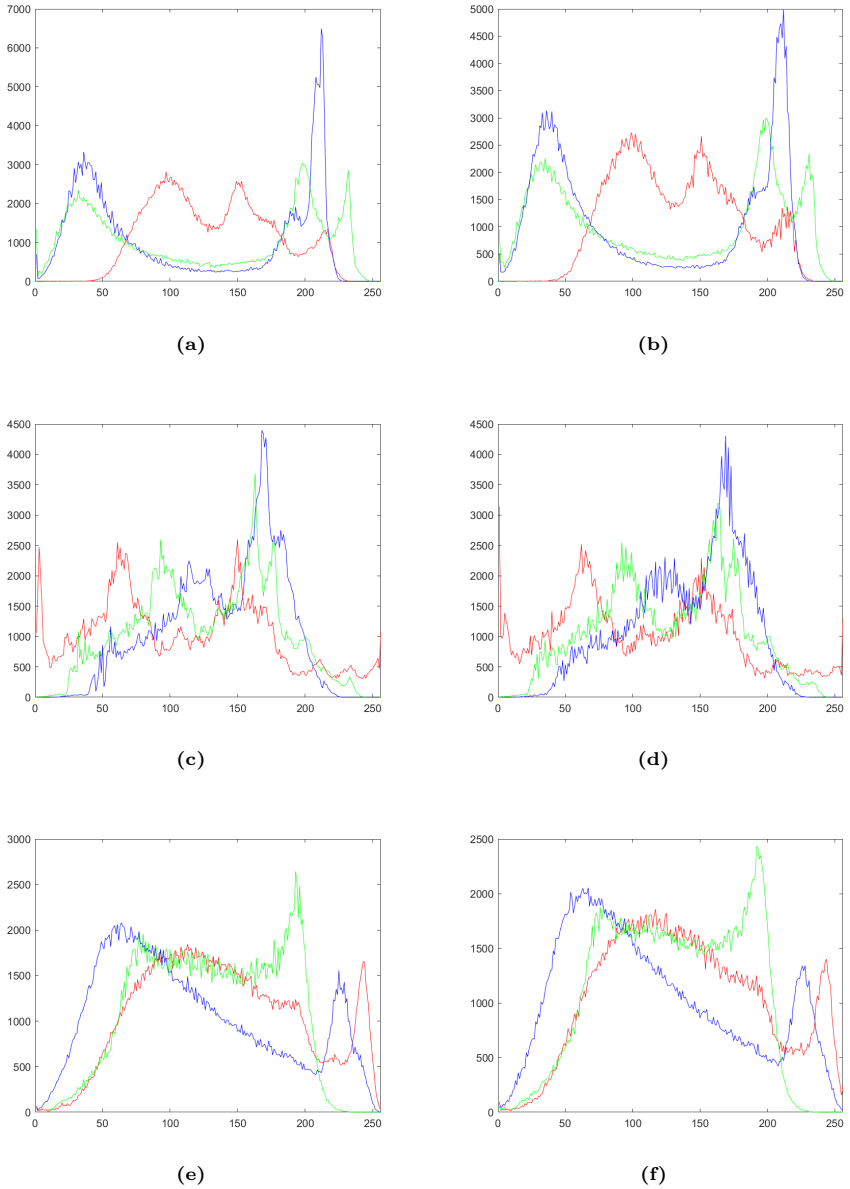


Fig. 28 The first column presents the histograms of the original carrier images (Sailboat, Air, and Baboon), while the second column illustrates the corresponding histograms of the steganographic images.

motivated metric that better aligns with the human visual system compared with PSNR. It comprehensively evaluates image similarity by jointly considering three components: luminance, contrast, and structural information. An SSIM value approaching unity indicates a high degree of structural similarity and superior visual quality, whereas a value significantly lower than one suggests severe degradation of image quality. The basic formula for SSIM is shown in Eq. (16):

$$\mathrm{SSIM}(x,y) = \frac{(2\mu_x\mu_y + C_1)(2\sigma_{xy} + C_2)}{(\mu_x^2 + \mu_y^2 + C_1)(\sigma_x^2 + \sigma_y^2 + C_2)}, \tag{16}$$

where μ_x and μ_y represent the mean luminance of images x and y, σ_x and σ_y denote the corresponding contrast information, σ_{xy} is the covariance between the two images, and C_1 and C_2 are small positive constants introduced to ensure numerical stability. The normalized cross-correlation (NCC) is employed to quantify the overall correlation between two images and is widely used for image matching and image quality evaluation.The closer the NCC is to 1, the higher the correlation between the two images, while the NCC is close to 0 or 1, and the NCC is close to 0. The closer the NCC is to 1, the higher the correlation between the two images, and the closer the NCC is to 0 or negative, the lower the correlation between the two images. The basic formula for SSIM is shown in Eq. (17):

$$\mathrm{NCC} = \frac{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} c(i,j)\,\hat{c}(i,j)}{\sqrt{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1} c(i,j)^2 \sum_{i=0}^{n-1}\sum_{j=0}^{n-1} \hat{c}(i,j)^2}}, \tag{17}$$

where $c(i,j)$ and $\hat{c}(i,j)$ denote the pixel values of the original image and the corresponding hidden image at position (i,j), respectively. As reported in Table 3, both the SSIM and NCC values obtained by the proposed scheme are close to 0.99, demonstrating that the modified image maintains high visual quality and exhibits strong similarity to the original image.

Table 3 SSIM and NCC values of the carrier images after embedding the information images in each group of experiments.

Carrier image	Information image	SSIM	NCC
C1	C1-W1	0.991	0.993
C1	C1-W2	0.988	0.995
C1	C1-W3	0.991	0.997
C2	C2-W1	0.992	0.999
C2	C2-W2	0.992	0.997
C2	C2-W3	0.992	0.997

Image error analysis and fidelity measurement are also important indicators for evaluating experimental results. The normalized absolute error measures the pixel error between two images. The smaller the normalized absolute error, the smaller the

error, and the higher the similarity of the image. The larger the NAE, the greater the deviation of the modified image from the original image. Therefore, NAE is often used as an indicator of error evaluation. The basic formula for NAE is shown in Eq. (18):

where $c(i,j)$ and $\mathrm{arcc}(i,j)$ denote the pixel values of the original image and the hidden image at coordinates (i,j), respectively. The Normalized Absolute Error (NAE) ranges from 0 to 1, where 0 indicates that the two images are identical. The closer the NAE value is to 0, the more similar the images are, whereas values approaching 1 indicate greater differences between the images.

$$\mathrm{NAE} = \frac{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}|c(i,j)-\hat{c}(i,j)|}{\sum_{i=0}^{n-1}\sum_{j=0}^{n-1}|c(i,j)|} \tag{18}$$

Image Fidelity (IF) quantifies the overall similarity between the modified image and the original image. Higher IF values, approaching 1, indicate better preservation of image quality, while lower IF values suggest more significant image distortion. The basic formula for IF is shown in Eq. (19):

$$IF = -\sum_{i} P(i)\log_2 P(i) \tag{19}$$

where $P(I)$ denotes the probability of pixels with gray value I occurring in the image. As shown in Table 4, the average value of NAE is approximately 0.003, and values below 0.005 indicate that the experimental results are excellent with negligible information loss. With an average Image Fidelity (IF) of about 0.995, the modified image preserves most of the original information, ensuring that the image details and overall quality remain well maintained.

Table 4 NET and IF values of the carrier images after embedding the information images in each group of experiments.

Carrier image	Information image	NET	IF
C1	C1-W1	0.0014	0.998
C1	C1-W2	0.0076	0.992
C1	C1-W3	0.0051	0.994
C2	C2-W1	0.0012	0.998
C2	C2-W2	0.0006	0.994
C2	C2-W3	0.0043	0.995

5.4 Steganography capacity

Steganographic capacity refers to the average number of bits that can be embedded in each carrier pixel and is one of the key metrics for evaluating the performance of a steganographic scheme. The steganographic capacity, denoted by C, is defined as follows.

$$C\ (\text{bits/pixel}) = \frac{\text{the number of embedded secret bits}}{\text{the number of carrier pixels}}. \tag{20}$$

In the proposed scheme, $2^{n-1} \times 2^n$ grayscale images together with 2^{2n} parity bits are embedded into a $2^n \times 2^n$ carrier image. Accordingly,The calculation method of equation Eq. (20) is parameterized, and the calculation process of this scheme is shown in Eq. (21)

$$\frac{2^n \times 2^{n-1} \times 8 + 2^{2n}}{2^n \times 2^n} = \frac{5 \times 2^{2n}}{2^{2n}} = 5 \text{ bits/pixel} \tag{21}$$

Table 5 compares the performance of the proposed scheme with several existing steganographic methods. As shown in Table 5, in recent years, few schemes have been able to maintain a PSNR higher than 50 dB while achieving an embedding capacity of 5 bits per pixel. Compared with other similar methods, the proposed scheme exhibits a clear advantage in terms of embedding capacity.

Specifically, the PSNR of the scheme in [35] is comparable to that of the proposed scheme; however, its embedding capacity is slightly lower. Although the method in [27, 36] achieves a higher PSNR, its embedding capacity is significantly inferior to that of the proposed method.Overall, the proposed scheme successfully achieves excellent visual quality while maintaining an ultra-high embedding capacity

Table 5 Comparison of steganography schemes in terms of PSNR and capacity.

Steganography scheme	PSNR (dB)	Capacity (bits/pixel)
Proposed scheme	50.05	**5**
Scheme in [35]	50.2	4
Scheme in [37]	48	3
Scheme in [38]	43	4
Scheme in [27]	54.5	3
Scheme in [36]	52	2
Scheme in [39]	38–43	1.04–2.28

5.5 Robustness in Noisy Environments

Under ideal conditions, the proposed scheme enables the complete extraction of the embedded secret information. Nevertheless, according to Shannon's information theory, classical information is inevitably affected by noise during transmission. Likewise, in practical quantum communication systems, a perfectly secure transmission environment cannot always be guaranteed. Consequently, robustness constitutes an essential criterion for evaluating the performance of quantum steganography schemes.

Pepper noise attack is a commonly adopted image noise model, in which the pixel values of randomly selected positions in grayscale images are modified to either black or white. In the case of color images, pixels are randomly chosen for attack, and one channel among the R, G, and B channels of each selected pixel is randomly selected.

The value of the chosen channel is then set to 0 or 255, corresponding to black or white, respectively, with equal probability. The intensity of pepper noise is defined as the ratio of the number of attacked pixels to the total number of pixels in the image.

To assess the robustness and security of the proposed scheme, stego-images subjected to pepper noise attacks with different intensities are first scrambled, and the secret images are subsequently extracted from the scrambled stego-images. The robustness of the scheme is evaluated by analyzing the amount of effective information retained in the extracted images.

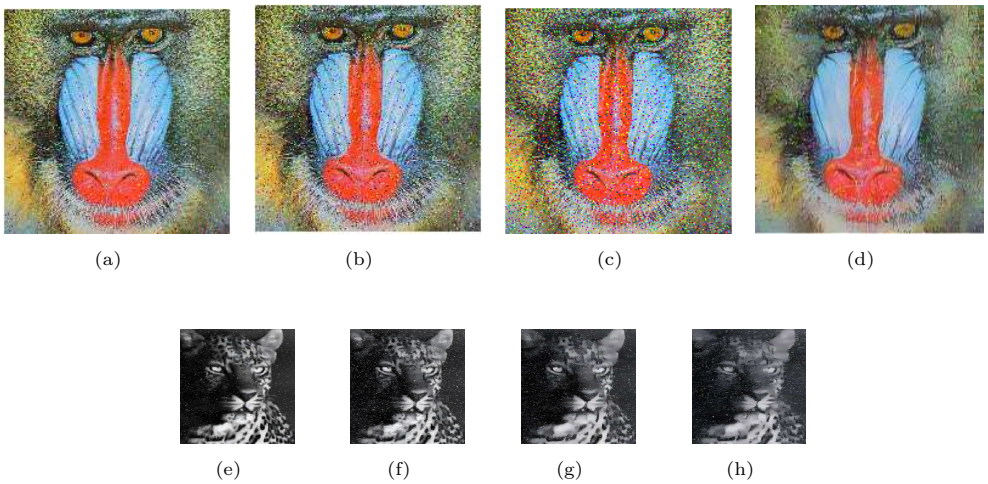


Fig. 29 Experimental performance under pepper noise attacks. The first row shows the color stego-images, while the second row presents the corresponding grayscale recovered images.

Table 6 PSNR values (dB) of stego-images under different pepper noise intensities.

Carrier image	Image pair	0.02	0.05	0.10	0.15
C1	C1–W1	36.9892	33.4150	30.8549	29.4948
C1	C1–W2	39.6774	36.2622	33.8155	32.5318
C2	C2–W1	37.1640	33.5798	30.9969	29.5432
C2	C2–W2	39.8313	36.3421	33.8765	32.6278
C3	C3–W1	36.7025	33.3579	30.8465	29.5039
C3	C3–W2	39.3186	36.1066	33.8179	32.5724

Figs. 29(a)–(d) present the stego-images subjected to pepper noise attacks with noise intensities of 0.02, 0.05, 0.10, and 0.15, corresponding to cases in which 2%, 5%, 10%, and 15% of the pixels in the stego-images are randomly corrupted, respectively. The secret images extracted from the attacked stego-images are illustrated in Figs. 29(e)–(h). As observed from Figs. 29(e)–(h), the extracted secret images remain

visually recognizable even under noise attacks, indicating that the proposed scheme exhibits satisfactory robustness against pepper noise.

The visual quality of the extracted secret images is further evaluated in terms of PSNR, as reported in Table 6. In addition, Table 7 presents a comparison of the PSNR values of the extracted images obtained by the proposed algorithm and several existing methods.

Table 7 PSNR values (dB) of stego-images under different pepper noise intensities.

Scheme	**0.05**	**0.10**	**0.15**
Proposed scheme	36.26	33.82	32.53
Scheme in [16]	15.03	12.15	10.2
Scheme in [40]	19.30	16.34	14.37
Scheme in [41]	–	31.3001	30.1445
Scheme in [42]	37.1933	34.3333	32.7966

6 Conclusion

Quantum computing and quantum information have attracted extensive attention from researchers across various disciplines and have achieved remarkable progress in recent years. Due to the high computational efficiency of quantum computing, many existing classical cryptographic systems are no longer considered secure. Consequently, the integration of quantum computing with classical computing has become an inevitable development trend.

In this paper, a double-layer tortoise shell quantum color image steganography algorithm is proposed, which exhibits the following advantages. First, a $(2^n \times 2^{n-1})$ grayscale image together with 2×2^n parity bits is embedded as secret information into a $(2^n \times 2^n)$ color carrier image. The embedding capacity of the proposed scheme reaches 5 bpp, which outperforms most existing quantum image steganography algorithms. Second, the YCbCr color space is adopted to exploit the lower sensitivity of the human visual system to the chrominance components Cb and Cr. By embedding secret information into the Cb and Cr channels, the visual quality of the stego-image is significantly improved from the perspective of human perception. Third, parity bits are introduced during image expansion to enable integrity verification. When the stego-image is subjected to malicious attacks, the parity bits can be used to detect tampering, and there exists a certain probability of restoring the attacked image. Fourth, the Grover search algorithm from quantum computing is employed to locate target coordinates efficiently. By leveraging quantum parallelism, the proposed scheme can find the required embedding positions significantly faster than classical search methods, enhancing the overall efficiency of the embedding process.

Both theoretical analysis and experimental results demonstrate that the proposed algorithm achieves excellent visual quality and security while maintaining a high embedding capacity, and exhibits superior performance compared with other state-of-the-art quantum steganography methods.

Declarations

- **Author Contributions**: All authors contributed to the study conception and design. Material preparation, data collection, and analysis were performed by [Jia-Hao Huang], [Hong-Mei Yang], [Bin Yan], [Dong-Huan Jiang],[Hao-Ming Dang] and [Xuan Lu]. The first draft of the manuscript was written by [Jia-Hao Huang], and all authors commented on previous versions of the manuscript. All authors read and approved the final manuscript.
- **Funding**: This work was supported by the Natural Science Foundation of Shandong Province, China (Grant No. ZR202102220198).
- **Availability of data and materials**: The datasets analysed during the current study are available from the corresponding author on reasonable request.
- **Competing interests**: All authors certify that they have no affiliations with or involvement in any organization or entity with any financial interest or non-financial interest in the subject matter or materials discussed in this manuscript.

References

[1] Huang, H.-C., Chu, S.-C., Pan, J.-S., Huang, C.-Y., Liao, B.-Y.: Tabu search based multi-watermarks embedding algorithm with multiple description coding. Information Sciences **181**(16), 3379–3396 (2011)

[2] Tao, J., Li, S., Zhang, X., Wang, Z.: Towards robust image steganography. IEEE Transactions on Circuits and Systems for Video Technology **29**(2), 594–600 (2018)

[3] Pan, J.-S., Sun, X.-X., Chu, S.-C., Abraham, A., Yan, B.: Digital watermarking with improved sms applied for qr code. Engineering Applications of Artificial Intelligence **97**, 104049 (2021)

[4] Bennett, C.H., DiVincenzo, D.P.: Quantum information and computation. Nature **404**(6775), 247–255 (2000)

[5] Xu, G.-B., Jiang, D.-H.: Novel methods to construct nonlocal sets of orthogonal product states in an arbitrary bipartite high-dimensional system. Quantum Information Processing **20**(4), 1–38 (2021)

[6] Beach, G., Lomont, C., Cohen, C.: Quantum image processing (quip). In: Proc. 32nd Applied Imagery Pattern Recognition Workshop (AIPR), pp. 39–44 (2003). IEEE

[7] Venegas-Andraca, S.E., Bose, S.: Storing, processing, and retrieving an image using quantum mechanics. In: Proceedings of SPIE Conference on Quantum Information and Computation, vol. 5105, pp. 137–147 (2003)

[8] Latorre, J.I.: Image compression and entanglement. arXiv preprint arXiv:quant-ph/0510031 (2005)

[9] Le, P.Q., Dong, F., Hirota, K.: A flexible representation of quantum images for polynomial preparation, image compression, and processing operations. Quantum Information Processing **10**(1), 63–84 (2011)

[10] Sun, B., Iliyasu, A., Yan, F., Dong, F., Hirota, K.: An rgb multi-channel representation for images on quantum computers. Journal of Advanced Computational Intelligence and Intelligent Informatics **17**(3) (2013)

[11] Yuan, S., Mao, X., Zhou, J., Wang, X.: Quantum image filtering in the spatial domain. International Journal of Theoretical Physics **56**(8), 2495–2511 (2017)

[12] Jiang, N., Lu, X., Hu, H., Dang, Y., Cai, Y.: A novel quantum image compression method based on jpeg. International Journal of Theoretical Physics **57**(3), 611–636 (2018)

[13] Jiang, N., Wang, L.: Quantum image scaling using nearest neighbor interpolation. Quantum Information Processing **14**(5), 1559–1571 (2015)

[14] Zhou, R.-G., Hu, W., Fan, P., Luo, G.: Quantum color image watermarking based on arnold transformation and lsb steganography. International Journal of Quantum Information **16**(3), 1850021 (2018)

[15] Hu, W., Zhou, R.-G., Luo, J., Liu, B.: Lsbs-based quantum color images watermarking algorithm in edge region. Quantum Information Processing **18**(1), 1–27 (2019)

[16] Jiang, N., Wang, L.: A novel strategy for quantum image steganography based on moiré pattern. International Journal of Theoretical Physics **54**(3), 1021–1032 (2015)

[17] Jiang, N., Zhao, N., Wang, L.: Lsb based quantum image steganography algorithm. International Journal of Theoretical Physics **55**(1), 107–123 (2016)

[18] Heidari, S., Pourarian, M.R., Gheibi, R., Naseri, M., Houshmand, M.: Quantum red-green-blue image steganography. International Journal of Quantum Information **15**(05), 1750039 (2017)

[19] Heidari, S., Farzadnia, E.: A novel quantum lsb-based steganography method using the gray code for colored quantum images. Quantum Information Processing **16**(10), 1–28 (2017)

[20] Zhou, R.-G., Luo, J., Liu, X., Zhu, C., Wei, L., Zhang, X.: A novel quantum image steganography scheme based on lsb. International Journal of Theoretical Physics **57**(6), 1848–1863 (2018)

[21] Qu, Z., Cheng, Z., Liu, W., Wang, X.: A novel quantum image steganography algorithm based on exploiting modification direction. Multimedia Tools and

Applications **78**(7), 7981–8001 (2019)

[22] Hu, W.-W., Zhou, R.-G., Liu, X.-A., Luo, J., Luo, G.-F.: Quantum image steganography algorithm based on modified exploiting modification direction embedding. Quantum Information Processing **19**(5) (2019)

[23] Li, P., Liu, X.: A novel quantum steganography scheme for color images. International Journal of Quantum Information **16**(02), 1850020 (2018)

[24] Li, P., Lu, A.: Lsb-based steganography using reflected gray code for color quantum images. International Journal of Theoretical Physics **57**(5), 1516–1548 (2018)

[25] Xiao, H., Li, P.: Quantum steganography based on reflected gray code for color images. Intelligent Decision Technologies, 1–22 (2020)

[26] Chang, C.-C., Liu, Y., Nguyen, T.S.: A novel turtle shell based scheme for data hiding. 2014 Tenth International Conference on Intelligent Information Hiding and Multimedia Signal Processing, 89–93 (2014)

[27] Wang, M.-X., Yang, H.-M., Jiang, D.-H., Yan, B., Pan, J.-S., Liu, T.: A novel quantum color image steganography algorithm based on turtle shell and lsb. Quantum Information Processing **21**(4), 148 (2022)

[28] Xie, X.-Z., Lin, C.-C., Chang, C.-C.: Data hiding based on a two-layer turtle shell matrix. Applied Sciences **8**, 246 (2018)

[29] Sharma, G., Trussell, H.J.: Digital color imaging. IEEE Transactions on Image Processing (1992)

[30] Grover, L.K.: A fast quantum mechanical algorithm for database search. Proceedings of the 28th Annual ACM Symposium on Theory of Computing (STOC) (1996)

[31] Nielsen, M.A., Chuang, I.L.: Quantum circuit description of grover's algorithm. Quantum Computation and Quantum Information (2004)

[32] Barenco, A., Bennett, C.H., Cleve, R., DiVincenzo, D.P., Margolus, N., Shor, P., Sleator, T., Smolin, J.A., Weinfurter, H.: Elementary gates for quantum computation. Physical Review A **52**(5), 3457–3467 (1995)

[33] Nielsen, M.A., Chuang, I.L.: Quantum computation and quantum information. Cambridge University Press **1**, 676 (2002). 1st edition, ISBN 978-0521635035

[34] Shang, X., Li, G., Wang, G.: Color-sensitivity-based combined psnr for objective video quality assessment. Journal of Visual Communication and Image Representation **48**, 380–392 (2017)

[35] Luo, G., Shi, L., Oad, A., Zong, L.: Steganography of quantum color images based on blocking and gray level difference. Quantum Information Processing **19**(3), 1–20 (2020)

[36] Dang, H.-M., Yang, H.-M., Jiang, D.-H., Yan, B., Huang, J.-H., Sun, X.-T., Yang, X.-H.: A lsb quantum steganography algorithm based on hash encryption. Quantum Information Processing (2025). Published online 7 July 2025

[37] Luo, G., Zhou, R.-G., Mao, Y.: Two-level information hiding for quantum images using optimal lsb. Quantum Information Processing **18**(9), 1–22 (2019)

[38] Xie, H.-w., Gao, Y.-j., Liu, X.-l., Zhang, J., Zhang, H.: A novel exploiting modification direction scheme and its application in quantum color image steganography. Quantum Information Processing **21**(8), 1–25 (2022)

[39] Qu, Z., Sun, H., Zheng, M.: An efficient quantum image steganography protocol based on improved emd algorithm. Quantum Information Processing (2021). Published online 5 February 2021

[40] Miyake, S., Nakamae, K.: A quantum watermarking scheme using simple and small-scale quantum circuits. Quantum Information Processing **15**(5), 1849–1864 (2016)

[41] Naseri, M., Heidari, S., Baghfalaki, M., Gheibi, R., Batle, J., Farouk, A., Habibi, A., *et al.*: A new secure quantum watermarking scheme. Optik **139**, 77–86 (2017)

[42] Luo, G., Zhou, R.-G., Luo, J., Hu, W., Zhou, Y., Ian, H.: Adaptive LSB quantum watermarking method using tri-way pixel value differencing. Quantum Information Processing **18**(2), 1–20 (2019)