Multimedia Tools and Applications (2020) 79:17551–17577
https://doi.org/10.1007/s11042-020-08694-z

A novel quantum steganography-Steganalysis system for audio signals

Javad Chaharlang, et al. ***[full author details at the end of the article]***

Received: 20 March 2019 / Revised: 3 January 2020 / Accepted: 28 January 2020 /
Published online: 20 February 2020

Abstract
As a substitute for classical solutions, quantum information hiding techniques have become an essential issue in the field of quantum communications by utilizing the inherent features of quantum mechanics and creating more secured communications for the more reliable exchange of digital media within the context of quantum communications networks. Quantum steganography has been considered as one of these approaches in recent years, but the importance of investigating and discovering these hidden communications within the context of quantum communication networks that require the use of quantum steganalysis methods has not been addressed so far. Therefore, in this paper, a novel quantum steganography-steganalysis system for digital audio signals is proposed, which can accurately detect audio steganography methods in the context of quantum communication networks. The proposed model consists of two separate sections: steganography and steganalysis; in the steganography part, to minimize the impacts of the embedding process and increasing the Signal to Noise Ratio (SNR), the embedding operation is carried out within the Least Significant Fractional Qubit (LSFQ) of the amplitude information of the audio signal samples. Then, a universal steganalyzer in the steganalysis part distinguishes the stego audio signals using the extracted statistical features from the audio signals. The universal steganalyzer consists of a mean feature extraction module to extract features from the audio signal frames and the quantum circuits for implementing the K-Nearest Neighbor (KNN) algorithm and the Hamming distance criterion. The simulation-based quantum circuits of the proposed system tested and evaluated using different audio files. Over 80% accuracy in detecting stego audio signals indicates high accuracy and efficiency of the proposed scheme and its applicability in quantum communication networks. Along with the higher efficiency and security of quantum steganography methods when compared with the classical one, the results show that the proposed quantum steganography-steganalysis scheme is also capable of competing with classical methods in terms of accurately detecting steganography methods.

Keywords Nano communication · Quantum computing · Quantum circuits · Quantum audio steganography · Quantum audio steganalysis

1 Introduction

Information security is one of the branches of science that has been fully affected by the era of digital computers. In this area, some fields, such as multimedia encryption systems [4, 18, 21], steganography [3, 5, 16, 24], steganalysis [31, 56], and watermarking [19, 24, 30, 32] have become more prominent. Digital steganography is a newer security technique than cryptography that can be defined as an art and science to hide hidden messages in various digital media files (image, audio, video, text, etc.) so that using it, a message can be received without increasing suspicion of observers and properly received by the recipient [6]. Steganalysis is the science of detecting hidden messages inside digital media that are embedded by steganography methods and can help to improve the security of existing steganography methods.

The prisoner problem scenario can be imagined to illustrate steganography and steganalysis [47]. In this scenario, Alice (sender) and Bob (receiver) are imprisoned and guarded by Wendy (steganalyzer). Alice and Bob want to talk about an escape plan, and they can only talk about their plan if they can hide and share their secret message in the normal messages using steganography methods. The steganalysis can be defined as a set of methods that can help Wendy to detect the existence of a hidden message in a cover media without the need for any knowledge of the secret key and even without knowing the embedding method [9]. Hence, Alice tries to exchange a secret message m with Bob, by inserting it into a cover object C, and by creating a stego object S that is similar to the cover object C. A secret key k, can also be used by the embedding process, after the embedding process, Alice sends S to the bob and hopes that Wendy will not notice the embedded message. Finally, Bob can extract the secret message m from the stego object S because he knows the embedding method and the key used. The overall schematic of a classical steganography-steganalysis system is shown in Fig. 1.

Recently, with the advent of quantum information theory and the advancement of related experiments, secure quantum communication has been an important area of research [17, 27, 29, 45]. The rapid development of quantum communication networks to achieve the secure and efficient transmission of quantum digital information over the quantum communication network and the use of the quantum states for storing and transmitting digital information such as audio and image led to the development of quantum information hiding methods. Similar to

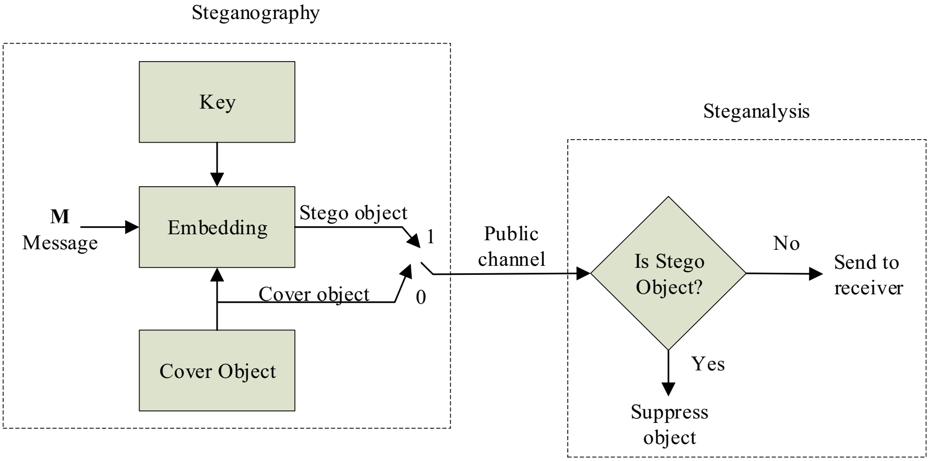


Fig. 1 The schematic scheme of a classical steganography-steganalysis system

classical information hiding, quantum methods are also classified into three main categories: quantum steganography, quantum covert channels, and quantum watermarking [46]. Quantum steganography is a promising branch of quantum information hiding methods that utilize quantum mechanical capabilities, including quantum communication and quantum computing. Quantum steganography methods are an alternative to the classic methods of privacy protection for achieving quantum or classical data hiding applications. Quantum steganography can create a much more secure communication when compared whit the classical one, relying on the inherent characteristics of quantum mechanics such as NO-cloning theorem [55] and Heisenberg uncertainty principle [12]. Due to the Heisenberg uncertainty principle, any attempt to measure a quantum system will disrupt it, alerting legal users to the presence of eavesdropping. Therefore, quantum steganography and other quantum cryptographic schemes can guarantee certain security without eavesdropping [46].

Until now, various researches have been carried out on the methods of quantum information hiding, such as quantum image steganography [20, 22, 23, 36, 42, 53, 59], quantum watermarking [10, 28, 33, 37, 59, 60], and quantum cryptography [15, 35, 44], but very few achievements have been made in quantum audio steganography and steganalysis. In the field of quantum audio steganography, the purpose is to hide a secret quantum message within a quantum audio signal to secret transmission. In 2017, two LSB-based steganography algorithms for quantum audio signal proposed by Chen et al. [11]. They used Flexible Representation for Quantum Audio (FRQA) method to store the amplitude and time information of quantum audio signals [57]. In these methods, a concept called the qubit layer in the LSQb (Least Significant Qubit)-based algorithm is used to represent the qubit position in the host quantum audio signal.

In the first method, the 1st qubit layer (Least significant qubit of the amplitude information sequence) of the host quantum audio is used. In this method, first, the host quantum audio signal and the secret quantum audio message are encoded as FRQA signals, then each qubit of the quantum audio message will be replaced with the LSQb (1st qubit layer) of a sample in the host quantum audio signal. This method has been called the conventional LSQb Quantum audio steganography protocol or, simply the cLSQ steganography protocol. The second method is called the pseudo-MSQb (Most Significant Qubit) or simply the pMSQ steganography protocol, in which the author to improve the robustness of the steganography protocol, modifies the position of the target qubit to the i^{th} qubit layer based on some predefined constraints. In this idea, increasing the value of i reduces the imperceptibility functionality and increases the robustness functionality of the steganography method. Therefore, in this case, there must be a trade-off between imperceptibility and robustness.

Research to date on quantum steganography in audio and image has been focused on particular steganography techniques, which uses methods based on the construction of quantum circuits for the embedding and extraction of the secret quantum message in the quantum host media. Indeed, quantum steganalysis has not been discussed in these researches, and only the operations of embedding and extracting secret data at the sender side and receiver side has been studied for quantum steganography. Steganalysis methods are based on machine learning techniques and feature extraction methods that attempt to identify the presence or absence of secret data in the host media with a high probability by extracting distinct features between the host media and the stego media.

Accordingly, in this paper, in conjunction with quantum information hiding systems, we proposed and simulated a scheme for a quantum steganography-steganalysis system that can be used in quantum communications and networks. This system has two distinct parts. In the first part, to provide quantum stego audio, we first propose a quantum audio steganography scheme based on the LSB method, which embeds the secret data into the least significant qubit of the fractional part of the audio signal amplitude information to minimize the effects of embedding operation in the host audio signal. In the next part, we propose a blind quantum steganalysis method using the quantum circuits network to detect the embedded data in the host quantum audio signals. The proposed steganalyzer uses a feature extraction module that extracts the mean value of the quantum audio signal frames. The classification process in this steganalyzer is based on the quantum KKN algorithm and the quantum hamming distance criterion, which makes the classification process done with the high precision.

The rest of this paper is organized as follows: In Section 2, the prerequisites for the representation of the digital audio signals and digital images into the quantum form are presented, then some of the quantum arithmetic modules required for this paper are introduced, and their operation is described. In Section 3, we proposed the scheme for a quantum steganography-steganalysis system then, the proposed quantum audio steganography method and the proposed quantum audio steganalysis method are explained by the implementation of quantum circuits and an applied example, In Section 4, simulation of proposed methods and analysis of results are presented. The article ends with the conclusion section.

2 Preliminaries

In this section, first, the quantum audio representation based on the QRDS (Quantum Representation of Digital Signals) method and the quantum image representation based on the NEQR (Novel Enhanced Quantum Representation) method are introduced; next, we introduced some basic quantum arithmetic modules.

2.1 Quantum representations for audio and image signals

Similar to FRQA quantum audio signal representation, quantum representation of digital signals (QRDS), was proposed by Li et al. in 2018 [51]. Indeed, the QRDS representation is used two entangled qubit sequences to store the amplitude and position (time) information of the samples of the audio signal. In the QRDS, the amplitude information is represented by an (n + 1)-qubit signed number in 2's complement notation, including on sign qubit A_t^m, m integer qubits $A_t^{m-1}\ldots A_t^0$, and m-n fractional qubits $A_t^{-1}\ldots A_t^{m-n}$. Also, time information sequence $|t\rangle$ represented by the l-qubit sequence in true binary form. The QRDS representation can be defined by Eqs. (1–4).

$$|A\rangle = \frac{1}{\sqrt{2^l}} \sum_{t=0}^{2^l-1} |A_t\rangle \otimes |t\rangle \tag{1}$$

$$|t\rangle = |t_0 t_1 \ldots t_{l-1}\rangle, t_i \in \{0,1\} \tag{2}$$

$$|A_t\rangle = |A_t^m A_t^{m-1} \ldots A_t^0 A_t^{-1} \ldots A_t^{m-n}\rangle, S_t^i \in \{0,1\} \tag{3}$$

$$l = \begin{cases} \lceil log_2 L \rceil, L > 1 \\ 1 \qquad\quad , L = 1 \end{cases} \tag{4}$$

QRDS employing $(l + n + 1)$ qubits for the quantum representation of an audio signal with a length 2^l in range $(-2^m + 1/2^{n-m}, 2^{m-1}/2^{n-m})$. It should be noted that in the QRDS representation if the number of signal samples is less than 2^l, the values of $2^i - L$ rest samples of the signal must be set to$|0\rangle$, in this case, the QRDS signal representation is defined by Eq. (5).

$$|A'\rangle = \frac{1}{\sqrt{2^l}}\left(\sum_{t=0}^{L-1}|A_t\rangle\otimes|t\rangle + \sum_{t=0}^{2^l-1}|0\rangle^{\otimes q}\otimes|t\rangle \tag{5}$$

In this paper, the embedded quantum secret message is a grayscale quantum image represented by NEQR [58]. In NEQR representation, a grayscale image with $2^n \times 2^n$pixels can be defined by Eqs. (6–8):

$$|I\rangle = \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1}|c_i\rangle\otimes|i\rangle, \tag{6}$$

$$|c_i\rangle = |c_i^{q-1}c_i^{q-2}\dots c_i^1 c_i^0\rangle, \tag{7}$$

$$c_i^k \in \{0,1\}, \quad k = q-1, q-2, \dots, 1, 0, \quad i = 0, 1, \dots, 2^{2n-1}. \tag{8}$$

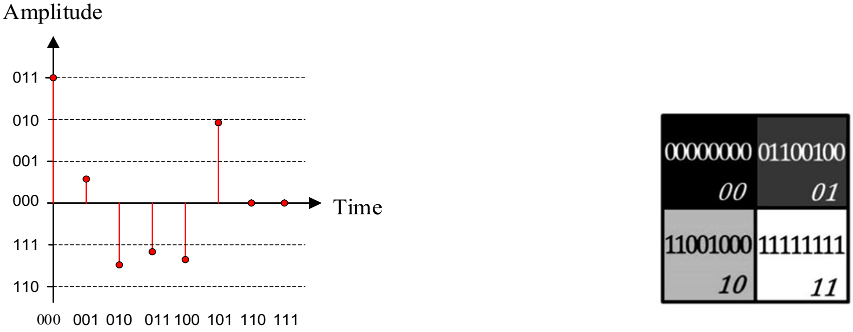
Where, $|I\rangle$ is the quantum representation of the digital image, the grayscale value and the position information of each pixel are encoded by $|c_i\rangle$ and $|i\rangle$, respectively. The pixel Position information includes the vertical and horizontal information, which $|y\rangle$ store the vertical information and $|x\rangle$ store the horizontal information. Figure 2 shows the quantum representation of digital audio signal A = {3,0.5,-1.5,-1.125,-1.25,2} in the QRDS representation and, a 2 × 2 quantum image based on NEQR representation. Further discussions regarding the preparation and retrieval of both the QRDS and NEQR methods could be obtained via [25, 58].

2.2 Realization of quantum arithmetic operations

In this subsection, we briefly introduced some of the fundamental quantum arithmetic modules and how they are operating, such as quantum adder, quantum multiplier, quantum divider, quantum sum, and the quantum comparator that some of them used in this research**.**

2.2.1 Quantum adder

Different implementations of adding two quantum numbers are proposed in [25, 50]. Because the values of samples of an audio signal in the QRDS method are signed numbers, the adder module (i.e., ADD) presented in [25] is used here for the addition of signal samples. As shown in Fig. 3. In this implementation, the modulus addition operation is used to add two signed numbers. The operation of this module can be defined as Eq. (9), in which a and b are $(n + 1)$-qubits signed numbers. Readers can see the complete details of these modules' circuits network in the relevant reference.



$$|A\rangle = \frac{1}{2\sqrt{2}}\begin{pmatrix} |0,0011.0000\rangle|000\rangle + |0,0000.1000\rangle|001\rangle + \\ |1,1110.1000\rangle|010\rangle + |1,1110.1110\rangle|011\rangle + \\ |1,1110.1100\rangle|100\rangle + |0,0010.0000\rangle|101\rangle + \\ |0,0000.0000\rangle|110\rangle + |0,0000.0000\rangle|110\rangle \end{pmatrix}$$

$$|I\rangle = \frac{1}{2}(|00000000\rangle \otimes |00\rangle + |01100100\rangle \otimes |01\rangle + |11001000\rangle \otimes |10\rangle + |11111111\rangle \otimes |11\rangle)$$

Fig. 2 The examples of a QRDS audio signal and a NEQR image (figures and descriptions adapted from [25, 58], respectively)

$$ADD|a\rangle|b\rangle = |a\rangle|a+b\rangle \tag{9}$$

2.2.2 Quantum sum

Quantum sum is an operation used to accumulate a series of quantum states (such as summing up some pixels values from a quantum image or summing up the amplitude values of some samples from a quantum audio signal). In [25], the implementation of a quantum sum module (i.e., SUM) was proposed based on the quantum ADD module to sum a series of QRDS audio samples, as shown in Fig. 4.

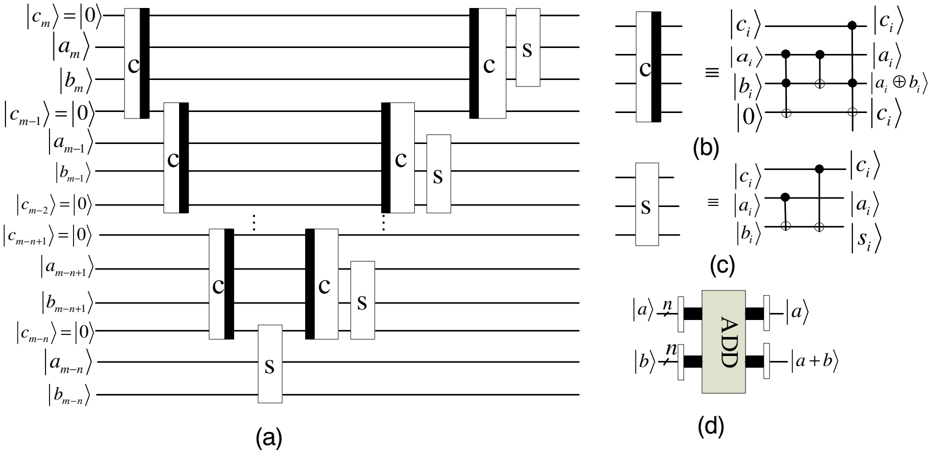


Fig. 3 The quantum circuits of modulus addition for two signed numbers (a) circuits for quantum adder (modulo 2 ^ *m*) b) circuits for the carry (c) circuits for sum (d) quantum ADD module, figures, and descriptions adapted from [25])

Where in, $|\ t\rangle\ =|\ t_{l-1}\ldots t_1t_0\rangle$ is l control qubits of the ADD modules, and $|\ A_t\rangle\ =|\ A_n\ldots t_1t_0\rangle$, denotes the amplitude of the audio signal samples with the length of l. The 2^l ADD modules are utilized to perform the summation of $|\ A_t\rangle$ in 2^lposition of $|\ t\rangle$. Therefore, $n+1$ ancillary qubits of $|\ 0\rangle$ are used to store the accumulation result of each ADD module. The final result will be the summation of the outputs of all ADD modules.

2.2.3 Quantum multiplier

Similar to the classic multiplication, quantum multiplication is an operation used to calculate the multiplication of two quantum numbers. In [25], an efficient implementation of the quantum multiplier (i.e., MUL) is presented based on the quantum ADD module for two signed numbers, which perform as Eq. (10).

$$MUL|a\rangle|b\rangle|0\rangle = |a\rangle|b\rangle|p\rangle \tag{10}$$

Where register $|\ 0\rangle$ (including 2n + 1 qubits) is used as input to store the product result of $|\ a\rangle\ =|\ a_n\ldots a_0\rangle$ and $|\ b\rangle\ =|\ b_n\ldots b_0\rangle$. After multiplication operation, the result will be stored in $|\ p\rangle\ =|\ p_{2n}\ldots p_0\rangle$.

2.2.4 Quantum divider

In [25], a quantum divider module (i.e., DIV) is presented to divide two quantum signed numbers. The DIV module computes the operation (11).

$$DIV|a\rangle|b\rangle|0\rangle|0\rangle 0\rangle = |a\rangle|r\rangle|q\rangle|p_a\rangle|p_b\rangle \tag{11}$$

Where $|\ a\rangle\ =|\ a_n\ldots a_0\rangle$ is as the dividend and $|\ b\rangle\ =|\ b_n\ldots b_0\rangle$ is as the divisor. In this operation four registers of $|\ 0\rangle$ (each contains $n+1$ qubits) are used to store the final result of divide operation, quotient and, the number of left shifts performed by a and b in the division process. After the divide operation, the quotient is stored in $|\ q\rangle$, the remainder in $|\ r\rangle$ also, the number of left shifts by a and b, stored in $|\ p_a\rangle$ and $|\ p_b\rangle$. The quantum circuits and module of multiplication and division of two signed numbers are shown in Fig. 5a and b, respectively. For details on the network circuits for these two modules, refer to the descriptions in the [25].

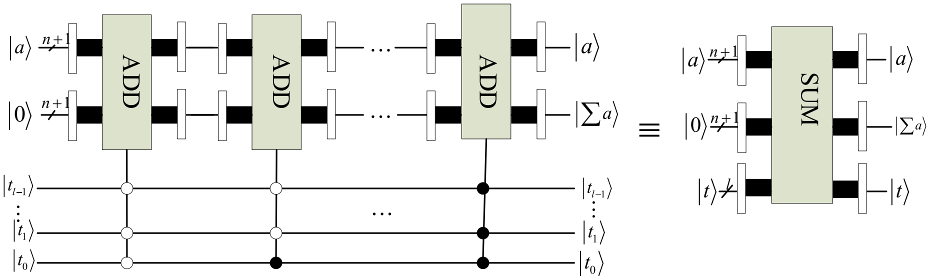


Fig. 4 The quantum circuits network and module of computing the sum of all amplitude values (figures adapted from [25])

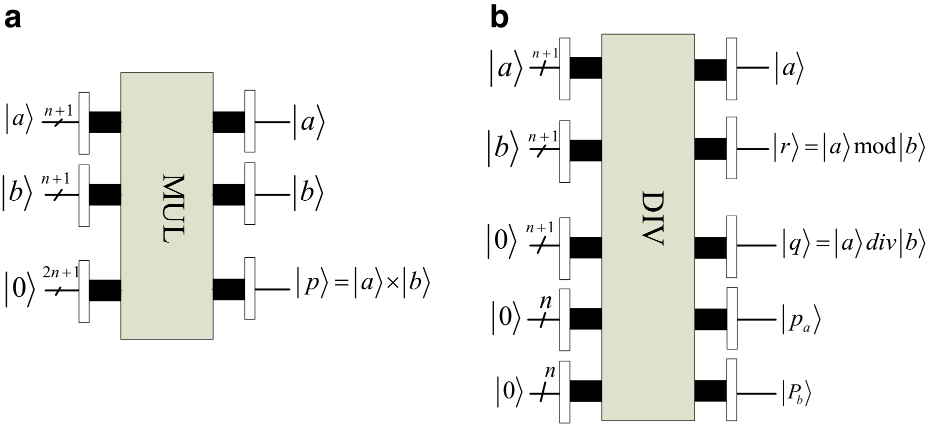


Fig. 5 **a** The quantum module of multiplication for two signed numbers (figure adapted from [25]) **b** The quantum module of division for two signed numbers (figure adapted from [25])

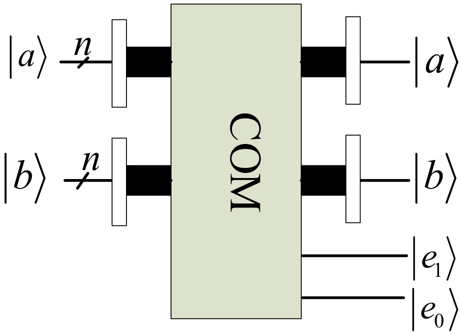
2.2.5 Quantum comparator

A quantum comparator (i.e., COM) is a module used to compare two quantum quantities. A quantum comparator, along with other modules, can be used to specify identical positions in the quantum signal. The proposed quantum comparator in [52] that its quantum circuit is shown in Fig. 6. The comparator compares $| a_{n-1}\dots a_0\rangle$ and $| b\rangle = | b_{n-1}\dots b_0\rangle$. Qubits e_0 and e_1 are the outputs of the comparator, if $a > b$ then $e_1e_0 = 10$, if $a < b$ then $e_1e_0 = 01$, and if $a = b$ then $e_1e_0 = 00$.

3 Proposed quantum audio steganography-steganalysis system

In this section, we proposed a scheme for the quantum steganography-steganalysis audio system. The general framework of this system is shown in Fig. 7, which consists of two distinct parts; the steganography section, which implements the embedding operation through quantum circuits and includes a host quantum audio, a secret quantum data, and a quantum embedding key. The output of the steganography section is a quantum stego audio, which may be sent to the receiver instead of the quantum host audio. The steganalysis section also includes a quantum steganalyzer that performs prediction and classification operations on

Fig. 6 The quantum module of the comparator (figure adapted from [52])



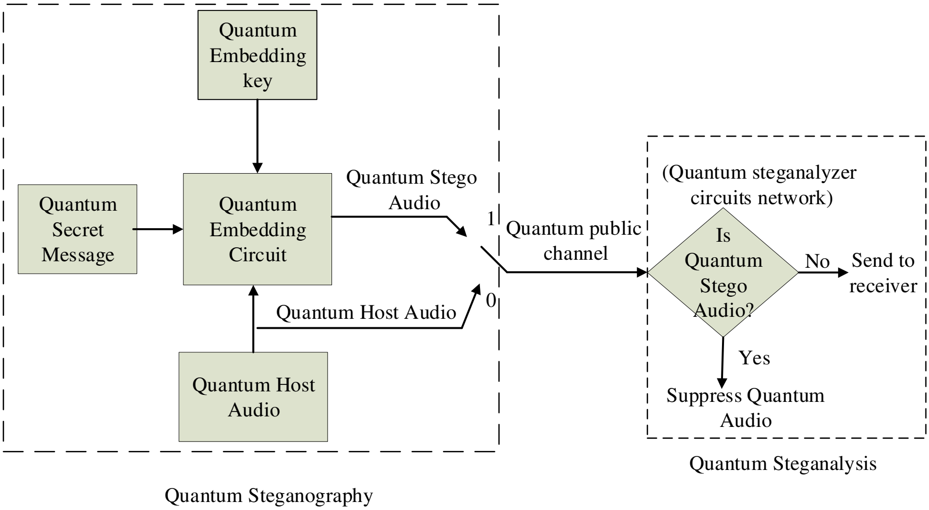


Fig. 7 The general framework of the proposed quantum audio steganography-steganalysis system

the received quantum audio signals from the quantum public channel to explore the probable steganography operations. In the following, details of both sections are described, along with the implementation of their quantum circuits and the presentation of an example.

3.1 Proposed quantum audio steganography method

The LSB steganography first proposed in [48] as a basic and simple data hiding method. Afterward, many improved versions of LSB algorithms have proposed by researchers. The principle of the LSB is to use message bits to substitute the least significant bit of the host media. The LSB-based steganography method has a simple concept and easy implementation. The stego media produced by the LSB algorithm is very similar to host media, in such a way that the two media are not distinguishable by visual perception.

In the quantum audio representation, each quantum audio signal is represented in the form of a qubits sequence, which indicates the information of the quantum signal samples. The least significant qubit in each quantum sequence is considered as LSQb. The quantum version of the LSB algorithm was first proposed in [53], that is widely used in the quantum steganography and quantum watermarking to hide a secret quantum message into a quantum host media such as quantum audio, quantum image, and quantum video; For this purpose, the quantum media must be represented in the form of a qubit sequence. In the following, we introduce some basic concepts in the quantum audio steganography used in this paper. LSQb in the quantum audio sequences is the least significant (the rightmost) qubit of the qubit sequence that is used to encode the amplitude information of each sample in the quantum audio signal. The host (carrier) quantum audio is the audio used to hide the secret quantum message within it, which transmitted on the public channel and towards the receiver. A quantum message is a secret message (such as quantum audio, a quantum image, or a quantum video) to be embedded in the host quantum audio and transmitted. After embedding the secret message inside the host quantum audio, the host quantum audio becomes a stego quantum audio signal which is publicly accessible and must be sent to the destination.

In this paper, a version of the LSQB-based embedding algorithm is proposed based on the QRDS representation for quantum audio signals. In this scheme, we call it Least Significant Fractional Qubit (i.e., LSFQ), the embedding of the secret data is performed in the least significant qubit of the fractional part of the amplitude information in the QRDS representation to improve the SNR of the proposed steganography method. The steganography algorithms based on LSFQ modification have significant capacity embedding and easy implementation. In this section, we first provided a high-level description of our methods to obtain the stego quantum audio. Then, the details of the method and the embedded circuit provided. The general framework of the proposed embedding method is shown in Fig. 6. The steps to hide a secret quantum binary image in a host quantum audio signal are as follows:

Step 1. Transforming a classical secret binary image I with the size of $2^n \times 2^n$ into the quantum image $|I\rangle$ by the NEQR representation and converting it into a sequence of $|0\rangle$ and $|1\rangle$.

Step 2. Selecting the host audio signal A with length L so that $L \geq 2^n \times 2^n$.

Step 3. Transforming the host audio signal A into the host quantum audio $|A\rangle$ by the QRDS representation.

Step 4. Executing the LSFQ embedding algorithm between $|A\rangle$ and $|I\rangle$ to obtain the stego quantum audio $|AI\rangle$.

The details of the embedding procedure to obtain the stego quantum audio are as follows:

1. Preparing the secret quantum image and host quantum audio

To realize the proposed embedding scheme, first, the secret binary image of size $2^n \times 2^n$ and, the color range of 2^1 (Black or White) is converted into a quantum binary image by the NEQR model, as Eq. (6). At the same time, the host audio signal with length L is prepared by the QRDS representation as Eq. (1). (it should be $L \geq n^2 \times n^2$, that is, the number of host audio signal samples must be at least equal to the total number of secret image pixels) (Fig. 8).

2. Embedding procedure

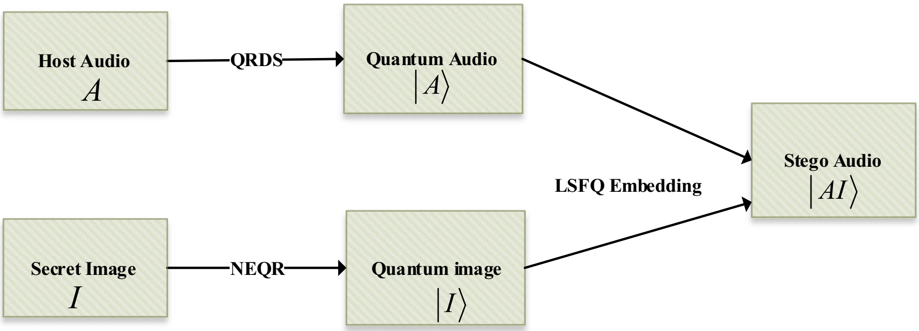


Fig. 8 The general framework of the proposed embedding method

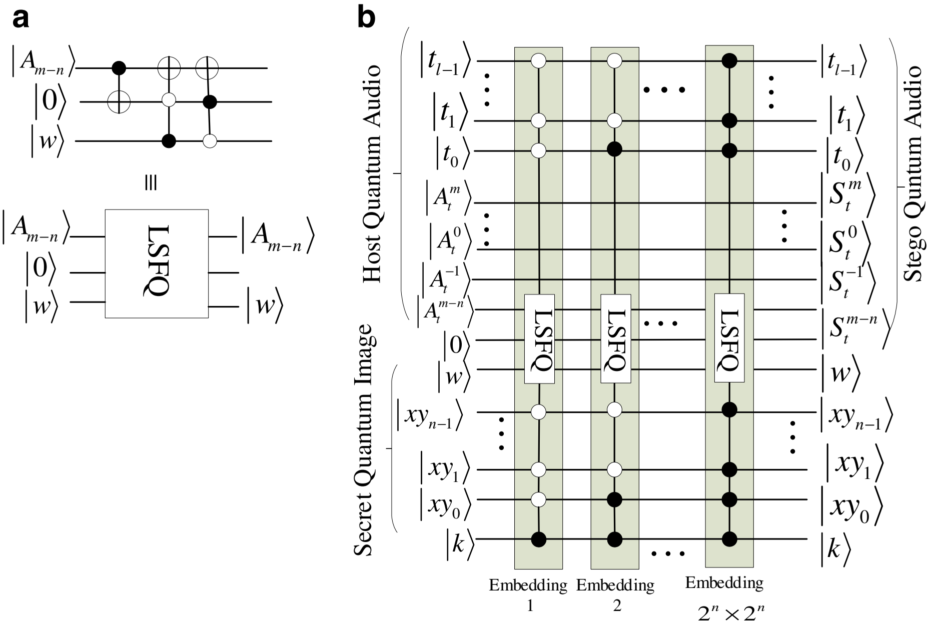


Fig. 9 **a** The proposed LSFQ embedding module **b** The circuits network for the implementation of the proposed embedding method

The secret quantum image $|I\rangle$ is embedded in the host quantum audio $|A\rangle$ through the LSFQ method. The circuit is shown in Fig. 9a performs the LSFQ embedding process. In this circuit, $|A_{m-n}\rangle$ is the least significant fractional qubit of the sample amplitude information in the QRDS representation and, $|w\rangle$ is the binary value of secret quantum image pixels. Also, $|0\rangle$ is an ancillary qubit which stores a copy of $|A_{m-n}\rangle$. In this circuit, if the two qubits $|A_{m-n}\rangle$ and $|w\rangle$ are not identical, qubit $|A_{m-n}\rangle$ will be reversed. The circuit network to obtain the quantum stego audio is shown in Fig. 9b, where $|A_t^m \ldots A_t^0 A_t^{-1} \ldots A_t^{m-n} t_{l-1} \ldots t_0\rangle$ represent the quantum host audio signal and $|w\, xy_{n-1} \ldots xy_0\rangle$ indicates the quantum stego audio. Also, $|w\rangle$ is utilized to store the binary information of secret quantum image pixels and $|xy_{n-1} \ldots xy_0\rangle$ is used to store the spatial information of each pixel. Furthermore, $|0\rangle$ is an ancillary qubit that used in the LSFQ module. In this method, the LSFQ module is used to substitute the least significant fractional qubit $|A_t^{m-n}\rangle$ ($|A_t^{m-n}\rangle$ is the least significant fractional qubit in the quantum sequence that represents the amplitude of the quantum signal samples) with the qubit w (w represents the pixel value of the secret quantum binary image) of the secret quantum image. In this structure, the insertion key $|k\rangle = |111\ldots1\rangle$ of length $2^n \times 2^n$ is used for embedding operations, if the host signal length is larger than the number of image pixels, for the rest of the host audio signal samples, the value of k must be set to $|0\rangle$. After embedding all $2^n \times 2^n$ pixels of the secret quantum image in the LSFQ of the host audio samples, the stego quantum audio signal is obtained as $|S_t^m \ldots S_t^0 S_t^{-1} \ldots S_t^{m-n} t_{l-1} \ldots t_0\rangle$. For example, five different wave audio files were selected first (i.e., quantum clean (host) audio files), then the downsampling operation was performed, and 16 samples of each audio file were selected and normalized to the interval [−1,1]. Next, these audio files were converted into the QRDA representation with values of $n = 5$, m = 2, t = 4 (one sign qubit, two integer qubits, and three

Table 1 The quantum host (clean) audio signals and the secret quantum binary image

Bagpipe.wav	Ballad.wav	Bartok.wav	Beat.wav	Beatles.wav	Secret image
| 0.375⟩	| −1⟩	| 1⟩	| −0.375⟩	| 0.125⟩	| 1⟩
| 0.250⟩	| −0.750⟩	| 0.750⟩	| −0.125⟩	| 0.625⟩	| 0⟩
| 0.125⟩	| −0.500⟩	| 0.625⟩	| −0.250⟩	| 1⟩	| 0⟩
| 0.500⟩	| −0.375⟩	| 0.500⟩	| −0.500⟩	| 0.875⟩	| 1⟩
| 0.875⟩	| −0.375⟩	| 0.500⟩	| −0.625⟩	| 0.500⟩	| 1⟩
| 1⟩	| −0.500⟩	| 0.625⟩	| −0.750⟩	| 0.125⟩	| 0⟩
| 0.750⟩	| −0.750⟩	| 0.625⟩	| −0.625⟩	| 0.125⟩	| 0⟩
| 0.500⟩	| −0.875⟩	| 0.625⟩	| −0.250⟩	| 0.125⟩	| 0⟩
| −0.250⟩	| −0.875⟩	| 0.500⟩	| −0.125⟩	| 0⟩	| 1⟩
| −1⟩	| −0.750⟩	| 0.250⟩	| −0.625⟩	| −0.125⟩	| 1⟩
| −0.750⟩	| −0.375⟩	| 0⟩	| −1⟩	| −0.500⟩	| 0⟩
| 0.250⟩	| 0⟩	| −0.250⟩	| 0⟩	| −0.875⟩	| 0⟩
| 0.875⟩	| 0.375⟩	| −0.625⟩	| 0.875⟩	| −1⟩	| 1⟩
| 0.625⟩	| 0.750⟩	| −0.750⟩	| 1⟩	| −0.750⟩	| 0⟩
| 0.250⟩	| 1⟩	|−1⟩	| 0.375⟩	| −0.625⟩	| 0⟩
| 0.125⟩	| 0.875⟩	| −0.875⟩	| −0.125⟩	| −0.375⟩	| 1⟩

fractional qubits for amplitude information and four qubits for time information). A 4 × 4 quantum binary image is also selected as the secret data and converted to a vector. The results of these operations are shown in Table 1. The circuits network proposed in Fig. 9b performed the process of embedding the secret image into the quantum audio signals, and the quantum steganography audio files (i.e., stego quantum audio) were obtained according to Table 2. In these Tables for ease of displaying samples value of the signal, classical numbers are used instead of the binary representation of qubits in the QRDS method.

3.2 Proposed quantum audio steganalysis method

Because the steganography methods manipulate and modify the content of the host signal, they leave the traces that can be distinguished by the steganalysis methods. Generally, steganalysis

Table 2 The quantum stego audio signals obtained by LSFQ embedding method

Bagpipe.wav	Ballad.wav	Bartok.wav	Beat.wav	Beatles.wav
| 0.375⟩	| −0.875⟩	| 1.125⟩	| −0.375⟩	| 0.125⟩
| 0.250⟩	| −0.750⟩	| 0.750⟩	| −0.205⟩	| 0.500⟩
| 0⟩	| −0.500⟩	| 0.500⟩	| −0.250⟩	| 1⟩
| 0.625⟩	| −0.375⟩	| 0.625⟩	| −0.375⟩	| 0.875⟩
| 0.875⟩	| −0.375⟩	| 0.625⟩	| −0.625⟩	| 0.625⟩
| 1⟩	| −0.500⟩	| 0.625⟩	| −0.750⟩	| 0⟩
| 0.675⟩	| −0.750⟩	| 0.500⟩	| −0.750⟩	| 0⟩
| 0.500⟩	| −1⟩	| 0.500⟩	| −0.250⟩	| 0⟩
| −0.125⟩	| −0.875⟩	| 0.500⟩	| −0.125⟩	| 0.125⟩
| −0.875⟩	| −0.625⟩	| 0.325⟩	| −0.625⟩	| −0.125⟩
| −0.750⟩	| −0.500⟩	| 0⟩	| −1⟩	| −0.500⟩
| 0.250⟩	| 0⟩	| −0.250⟩	| 0⟩	| −1⟩
| 0.875⟩	| 0.375⟩	| −0.625⟩	| 0.875⟩	| −0.875⟩
| 0.500⟩	| 0.750⟩	| −0.750⟩	| 1⟩	| −0.750⟩
| 0.250⟩	| 1⟩	| −1⟩	| 0.250⟩	| −0.750⟩
| 0.125⟩	| 0.875⟩	| −0.875⟩	| −0.125⟩	| −0.375⟩

is a decision problem, and if it solved for a specific method with a high probability, that method is considered broken [8]. If the embedding method and the statistical model of the host signal are known, an optimal steganalyzer can be created to identify the secret message within it. However, such information is usually not available from the host signal, and so the steganalysis systems are usually made based on the feature extracting techniques and machine learning algorithms. Detecting secret messages in digital media is usually considered as a classification problem. In other words, steganalysis algorithms receive digital media as inputs and classify them into two categories of "clean" or "stego." Therefore, some classification tools, such as pattern recognition and machine learning, are used for steganalysis. Steganalysis methods can be categorized into three main types: blind, semi-blind, and targeted (particular) [37]. If an observer had no prior information about the secret communication between the sides and only suspects the communication between them, he should use the blind steganalysis methods so that he can recognize all (or at least a wide range of) methods of steganography. Also, if an observer expects a secret communication between the sides and has an idea about their hidden steganography algorithms, he should use a semi-blind steganalysis algorithm that can detect a wide variety of steganography methods. A semi-blind steganalysis method can be used for a specific set of steganography methods. Moreover, when an observer is aware of the existence of secret communication between the sides and also of the steganography method they are using, he must construct a targeted steganalysis method that is capable of identifying hidden messages that are only hidden by that specific steganography method [37].

In recent years, the idea of using quantum computing has been considered as a new tool for accelerating classical computations. Using quantum computing has been beneficial in reducing the processing time in areas that require large amounts of information to be analyzed and processed, such as digital signal processing and big data analyzing. Recently, in the classical machine learning, the use of quantum algorithms has been considered and has led to the emergence of quantum machine learning [7, 13, 14]. The use of quantum algorithms in classification and pattern recognition systems can speed up the training phase of the algorithms and reduce computational complexity and improve the overall performance of the system [2, 26, 39].

So far, In the field of quantum steganalysis for the quantum signals (including quantum audio and quantum image), no research has been done, and the lack of research on this crucial topic has encouraged us to investigate this. In the following, we proposed a blind (universal) quantum steganalysis method for detecting quantum steganography methods in the quantum audio signals; wherein, we use the Quantum K Nearest Neighbors (QKNN) algorithm based on the Humming distance metric [43] to construct a quantum steganalyzer to check if a quantum audio signal is stego or clean. The structure of the QKNN algorithm is based on the quantum probabilistic memory [49], which has been used by researchers in the fields of quantum pattern recognition [54] and quantum classification [40, 41]. The idea of QKNN is to construct a superposition state of the training data set and write the Hamming distance to the input state into the amplitude of each vector in the superposition state, then measuring the class-qubit retrieves the desired class with the highest probability [43]. The purpose of our proposed quantum steganalyzer is to distinguish between a test quantum audio signal and a training quantum audio dataset to determine whether the test audio belongs to the training dataset. In this scheme First, the specific feature vectors extracted from the test audio files and training set audio files by using a proposed feature extraction module. Then a superposition state of training feature vectors is constructed by quantum circuits (the details of constructing a superposition state are described in [49] and are not mentioned here), next the Hamming distance between the test feature vector and

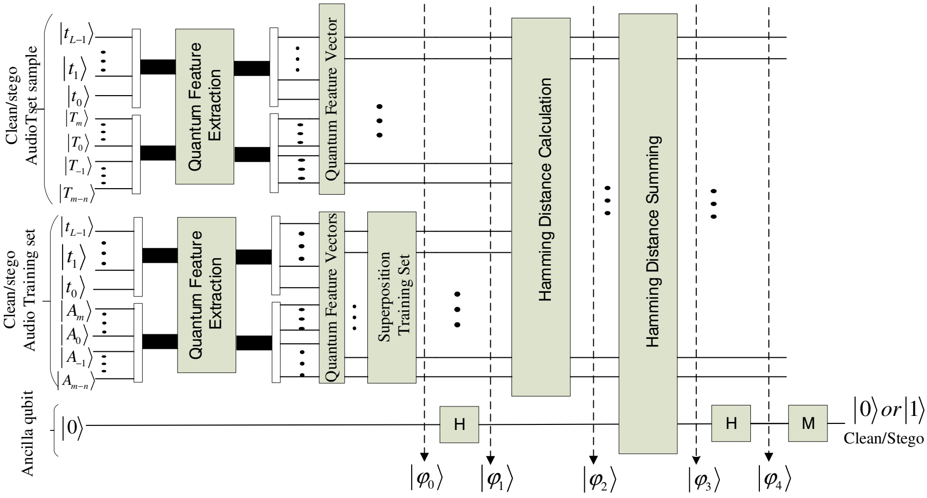


Fig. 10 The proposed quantum audio steganalyzer

superposition state of training feature vectors is calculated; eventually, the circuits generate a quantum state which indicates the proportion of the test feature vector to the training set feature vectors. The schematic scheme of the proposed quantum steganalyzer based on the QKNN algorithm and the Hamming distance is shown in Fig. 10.

In general, the operation details of the proposed quantum audio steganalyzer can be described in the following steps:

3.2.1 Preliminary steps

Step 1. Providing a clean (host) audio dataset and converting it to the quantum form using the QRDS representation for construction the clean quantum audio dataset.

Step 2. Embedding the secret quantum image into the quantum clean audio dataset to obtain the quantum stego audio dataset by using the proposed LSFQ algorithms in Section 3.1.

After these two steps, each sample of quantum clean/stego audio dataset is indicated by a normalized $(n + 1 + l)$−dimensional vector $|A_t^m\ldots A_t^0A_t^{-1}\ldots A_t^{m-n}t_{l-1}\ldots t_0\rangle$. Here, for ease of presentation, we assume $(n + 1 + l = N)$, and each vector is represented as $| A^1A^2\ldots A^{\mathrm{N}}\rangle$. The training set also is indicated by N vectors $|A_1^p\ldots A_N^p\rangle,\ p = 1, 2, \ldots, L$.

3.2.2 Main steps

Step 1. Inputting an unclassified quantum audio file as a test sample.

Step 2. Inputting the clean/stego quantum training dataset as the training dataset.

Step 3. Extracting feature vectors from the test sample and training dataset samples by the proposed feature extraction methods in 3.2.3. After this step, each quantum audio is expressed as a vector of its features called quantum feature vector (i.e., QFV).

Step 4. Constructing a superposition training set from clean/stego QFVs as Eq.)12(.

$$|T\rangle = \frac{1}{\sqrt{L}} \sum_{p=1}^{L} |A_1^p \ldots A_N^p\rangle \tag{12}$$

Step 5. Creating a quantum state with three registers. The first containing a test QFV | $T_1\ldots T_N\rangle$, the second containing the superposition of the training set *QFVs* | $T\rangle$, and the third containing an ancillary qubit set to | 0⟩ . The result can be defined by Eq. (13).

$$|\psi_0\rangle = |T_1 \ldots T_N\rangle \otimes \frac{1}{\sqrt{L}} \sum_{p=1}^{L} |A_1^p \ldots A_N^p\rangle \otimes |0\rangle \tag{13}$$

Step 6. The ancillary qubit | 0⟩ is put into the superposition state through a Hadamard gate, leading to the state | $\psi_1\rangle$ according to Eq. (14).

$$|\psi_1\rangle = |T_1 \ldots T_N\rangle \otimes \frac{1}{\sqrt{L}} \sum_{p=1}^{L} |A_1^p \ldots A_N^p\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \tag{14}$$

Step 7. Computing the Hamming distance between the test QFV | $T_1\ldots T_N\rangle$ and each QFV of the superposition training set | $T\rangle$ also, save the result $|d_1^p \ldots d_N^p\rangle$ in the second register. Hamming distance is a measure of the distance between two sequences and represents the number of differences between the bits having the same position in two sequences and in here can be calculated by performing the XOR operation on every couple qubits(T_i, A_i^p), i = 1,…, N.

After this operation, the next system state is defined by Eq. (15).

$$|\psi_2\rangle = |T_1 \ldots T_N\rangle \otimes \frac{1}{\sqrt{L}} \sum_{p=1}^{L} |d_1^p \ldots d_N^p\rangle \otimes \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \tag{15}$$

Step 8. Constructing the unitary operator U and apply it on | $\psi_2\rangle$ to sum the Hamming distances of all training samples and calculate the total Hamming distance between a test QFV vector and the QFVs of the training set superposition. These operations can be defined by Eqs. (16–18).

$$U = e^{-i\frac{\pi}{2N}H} \tag{16}$$

$$H = I_{N\times N} \otimes \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}^{\otimes N} \otimes \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix} \tag{17}$$

$$|\psi_3\rangle = U|\psi_2\rangle = \frac{1}{\sqrt{2L}} \sum_{p=1}^{L} \left(e^{i\frac{\pi}{2N}d(T,A^p)} \| T_1 \ldots T_N \Big\rangle \otimes |d_1^p \ldots d_N^p\rangle \otimes |0\rangle + e^{-i\frac{\pi}{2N}d(T,A^p)} |T_1 \ldots T_N\rangle \otimes |d_1^p \ldots d_N^p\rangle \otimes |1\rangle \right) \tag{18}$$

Step 9. Applying the Hadamard gate on the last register and obtain final state $|\psi_4\rangle$ by Eq. (19).

$$|\psi_4\rangle = \frac{1}{\sqrt{L}}\sum_{p=1}^{L}\left(\cos\frac{\pi}{2N}d(T,\mathrm{A}^p)\right)|T_1\ldots T_N\rangle\otimes|d_1^p\ldots d_N^p\rangle\otimes|0\rangle + \sin\left(\frac{\pi}{2N}d(T,A^p)\right)|T_1\ldots T_N\rangle\otimes|d_1^p\ldots d_N^p\rangle\otimes|1\rangle\Big) \tag{19}$$

Step 10. Measuring the last register (ancillary qubit). If the result is $|0\rangle$,which means the test audio sample is close to most training dataset samples and will take the training data class label. Also, if the result is $|1\rangle$,which means the test audio sample is far away from most training dataset samples and will take the opposite training data class label. The probabilities of being in the states $|0\rangle$ and $|1\rangle$ are defined by Eqs. (20–21).

$$p(|c\rangle = |0\rangle) = \frac{1}{\sqrt{L}}\sum_{p=1}^{L} cos^2\left[\left(\frac{\pi}{2N}\right)d(T,A^p)\right] \tag{20}$$

$$p(|c\rangle = |1\rangle) = \frac{1}{\sqrt{L}}\sum_{p=0}^{L} sin^2\left[\left(\frac{\pi}{2N}\right)d(T,A^p)\right] \tag{21}$$

3.2.3 Proposed feature extraction method

In this subsection, first, the extracting feature method used by the proposed quantum steganalyzer is introduced, and then the quantum circuits of the proposed feature extraction method are implemented and illustrated with an example.

In the signal processing, the mean M of a discrete-time signal x[n] in range $n1 \le x \le n2$ is defined by Eq. (22) [34].

$$M = \frac{1}{n2-n1+1}\sum_{n=n1}^{n2} x[n] \tag{22}$$

Accordingly, the quantum mean $|M\rangle$ of the quantum signal $|A\rangle$ in range $[l1\ l2]$ is given by Eq. (23).

$$|M\rangle = \frac{1}{l2-l1+1}\sum_{i=l1}^{l2}|A_i\rangle \tag{23}$$

In this paper, we extract the mean value of quantum audio frames as the QFVs. To this end, we proposed a quantum features extraction module (i.e., QFE module) using introduced quantum arithmetic modules in Section 2.2. The quantum implementation of the QFE module involves three steps to achieve an audio signal based on the mean feature of the initial audio signal frames; firstly, the sum of the samples of each quantum frame (i.e., Qframe) is computed. Secondly, the result is divided by the number of Qframe samples to calculate the mean of the Qframe samples. Finally, the mean value obtained for each Qframe is stored as a sample of an empty quantum mean signal.

To implement the quantum mean circuits network based on Eq. (23), in the first step, we divide the input quantum audio signal $| A\rangle$ $=|A_t^m \dots A_t^0 A_t^{-1} \dots A_t^{m-t} t_{l-1} \dots t_0\rangle$ obtained with the QRDS model and with the length of $=2^l \times 2^l$, into 2^l non-overlapping Qframes of length 2^l. Also, we create an initial quantum mean signal, wherein, the length of the signal is $| t\rangle$ $= | t_{l-1} \dots t_0\rangle$ and the amplitude of the samples is $| 0\rangle$ $= | 0_m \dots 0_0 0_{-1} \dots 0_{m-n}\rangle$; Then the sum value of the amplitudes of the 2^lsamples for each Qframe is computed by the 2^l ADD module (details of module operation are described in Section 2.2). In the second step, the result of the ADD modules (the sum of the amplitude of Qframe samples) is divided by the DIV module into 2^l (the length of each Qframe is 2^lsamples and represented by a sequence containing $n + 1$ qubit as $| 2^l\rangle$ $= | l_n \dots l_0\rangle$). In the final step, the output of the DIV module, which is the mean value of the Qframe samples, is copied into the initial (empty) quantum mean signal. This process is performed for 2^l Qframes so that the mean quantum signal is eventually obtained as $|M\rangle = |M_t^m \dots M_t^0 M_t^{-1} \dots M_t^{m-n} t_{l-1} \dots t_0\rangle$. Given that each Qframe of the input signal $| A\rangle$ (which contains 2^l sample) is converted to 1 sample of the mean signal $| M\rangle$, so in this structure, the length of the obtained mean audio signal $| M\rangle$ is $\frac{1}{2^l}$ of the input audio signal $| A\rangle$,also, the length of the resulting quantum feature vector will be less than the original audio signal. The quantum circuits network of this scheme and its module is shown in Figs. 11 and 12, respectively.

By applying the proposed mean feature extraction module, on the clean and stego quantum audio signals in Tables 1 and 2, the mean quantum signals associated with these two sets are obtained as Tables 3 and 4. Moreover, by applying the proposed steganalysis model by the steps outlined in Section 3.2 on these two sets of audio files, the predicted results will be as Tables 5 and 6. In these experiments, five test audio files examined by two learning datasets (clean and stego) and different test samples. In these tables, the actual test sample class and the

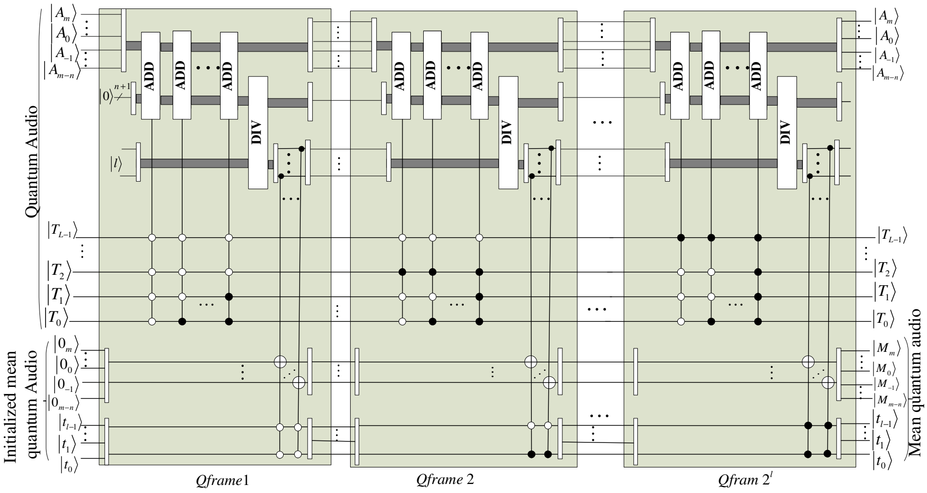


Fig. 11 The circuits network of implementation the proposed mean quantum feature extraction method

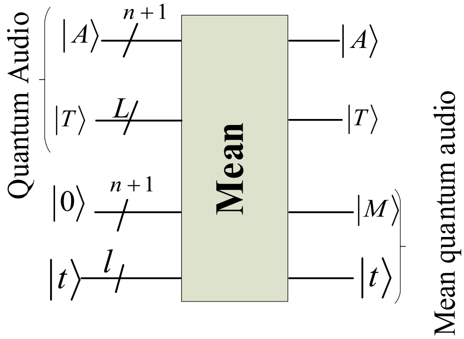


Fig. 12 The quantum module of the proposed mean feature extraction method

training dataset class (dataset to be compared by the steganalyzer with the test sample) are specified. In these tables, $p|\ 0\rangle$ expresses the probability of closeness the test sample to the learning dataset samples and $p|\ 1\rangle$ represents the probability that the test sample is far from the learning dataset samples. The predicted class also represents the prediction results of the proposed quantum steganalysis method. In these experiments, first, two learning sets of the clean dataset and stego dataset were created; Then, the degree of closeness or remoteness of each test sample is calculated from the training sets. The larger value of $p|\ 0\rangle$ for each test audio sample, it indicates that the test sample is closer to the learning set, and the class label of the learning set is considered as the predicted class label for the test sample by the steganalyzer. For each test sample, the conformity of the actual class with its predicted class proves the correct prediction and the accuracy of the proposed steganalysis method.

4 The simulation-based experiment results and performance analysis

Given that quantum hardware is not physically available for implementation of proposed schemes at present, the simulation of these quantum operations with MATLAB is done on the classic computer. In this section, Under the scheme proposed in Fig. 7, two sets of experiments are performed for the steganography and steganalysis parts. In general, the procedures for conducting these experiments can be summarized as follows:

1. Selecting 100 audio files in wave format as host media and performing preprocessing operations (downsampling and normalization).
2. Converting any audio file to a quantum audio file using the QRDS model.
3. Creating the clean quantum dataset using 100 quantum host audio files.

Table 3 The results of the proposed quantum mean feature extraction method on the quantum clean audio signals in Table 1

Bagpipe.wav	Ballad.wav	Bartok.wav	Beat.wav	Beatles.wav
clean	clean	clean	clean	clean
$\|0.375\rangle$	$\|0.625\rangle$	$\|0.750\rangle$	$\|-0.375\rangle$	$\|0.750\rangle$
$\|0.750\rangle$	$\|-0.625\rangle$	$\|0.625\rangle$	$\|-0.625\rangle$	$\|0.250\rangle$
$\|-0.500\rangle$	$\|-0.500\rangle$	$\|0.125\rangle$	$\|-0.500\rangle$	$\|-0.375\rangle$
$\|0.750\rangle$	$\|0.750\rangle$	$\|-0.875\rangle$	$\|0.625\rangle$	$\|-0.750\rangle$

Table 4 The results of the proposed quantum mean feature extraction method on the quantum stego audio signals in Table 2

Bagpipe.wav	Ballad.wav	Bartok.wav	Beat.wav	Beatles.wav
Stego	stego	stego	stego	stego
$\|0.375\rangle$	$\|-0.625\rangle$	$\|0.875\rangle$	$\|-0.375\rangle$	$\|0.625\rangle$
$\|0.750\rangle$	$\|-0.750\rangle$	$\|0.625\rangle$	$\|-0.625\rangle$	$\|0.250\rangle$
$\|-0.375\rangle$	$\|-0.500\rangle$	$\|0.250\rangle$	$\|-0.625\rangle$	$\|-0.500\rangle$
$\|0.500\rangle$	$\|0.875\rangle$	$\|-0.875\rangle$	$\|0.500\rangle$	$\|-0.750\rangle$

4. Selecting a binary image as secret data and perform the pre-processing operation (scaling).
5. Converting the classic binary image into the quantum binary image using the NEQR model.
6. embedding the secret quantum image into the clean quantum dataset audio files using the proposed embedding method in Section 3.1 and create the quantum stego dataset.
7. Calculate and analysis of steganography evaluation criteria according to the results of the proposed steganography method.
8. Use clean and stego quantum audio datasets obtained from the steganography process to apply the proposed quantum steganalysis model in Section 3.2 and obtain the classification results.
9. Calculate and analysis of classification evaluation criteria according to the results of the proposed steganalysis method.

The details of the quantum audio steganography and quantum audio steganalysis experiments are explained below.

4.1 Steganography experiments and analysis

The proposed quantum steganography method is simulated and tested on two sets of wave audio files (100 music audio files and 100 speech audio files). All files were sampled at 44.1 kHz with 16-bit precision. We down-sampled these wave files into audio files, which have 1024 samples in the range [−1 1]. In the first step, these files were selected as host audio signals dataset and converted to the quantum format using the QRDS method (with values, $n =$

Table 5 The results of proposed steganalyzer by construction the clean learning set from the mean audio signals in Table 3

Test audio sample	*Actual class*	*Learning dataset class*	*P*$\|0\rangle$	*P*$\|1\rangle$	*Predicted class*
Bagpipe.wav	clean	Clean	**0.9940**	0.0060	clean
	stego	Clean	0.9933	0.0067	
Ballad.wav	clean	Clean	**0.9936**	0.0064	
	stego	Clean	0.9934	0.0066	
Bartok.wav	clean	Clean	**0.9940**	0.0060	
	stego	Clean	0.9925	0.0075	
Beat.wav	clean	Clean	**0.9928**	0.0072	
	stego	Clean	0.9925	0.0075	
Beatles.wav	clean	Clean	**0.9928**	0.0072	
	stego	Clean	0.9922	0.0078	

the predicted class probability for each audio sample is indicated in bold.

Table 6 The results of proposed steganalyzer by construction the stego learning set from the mean audio signals in Table 4

Test audio sample	Actual class	Learning dataset class	P| 0〉	P| 1〉	Predicted class
Bagpipe.wav	clean	Stego	**0.9940**	0.0060	Stego
	stego	Stego	0.9933	0.0067	
Ballad.wav	clean	Stego	**0.9936**	0.0064	
	stego	Stego	0.9934	0.0066	
Bartok.wav	clean	Stego	**0.9940**	0.0060	
	stego	Stego	0.9925	0.0075	
Beat.wav	clean	Stego	**0.9928**	0.0072	
	stego	Stego	0.9925	0.0075	
Beatles.wav	clean	Stego	**0.9928**	0.0072	
	stego	Stego	0.9922	0.0078	

the predicted class probability for each audio sample is indicated in bold.

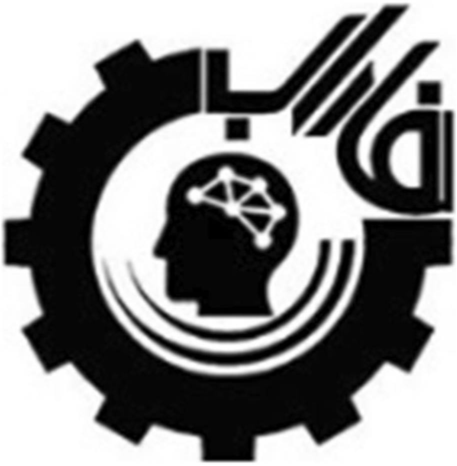
9, m = 4, t = 10) to produce the clean quantum dataset. Also, a 32 × 32 binary image as shown in Fig. 13 was selected as the secret data, which is converted into the quantum binary image by the NEQR method, then it has converted to a 1 × 1024 quantum binary vector consists of | 0〉 and | 1〉 . Then, using the proposed embedding scheme in Section 3.1, the secret quantum image is embedded within the 100 clean quantum audio signals to produce 100 quantum stego audio signals. The performance of our proposed quantum steganography method is measured by the steganography criteria such as quality, security, capacity, and embedding efficiency. In order to evaluate quantum signals using these parameters, quantum signal information must first be retrieved using quantum measurement operations [11].

4.1.1 Quality evaluation

There are various parameters for analyzing the stego audio quality, mean square error (MSE), signal to noise ratio (SNR) and peak signal to noise ratio (PSNR) values, which are the most important of them is used here.

MSE is used as an important parameter in evaluating the performance of the steganographic system, which defined as the mean square error between the cover audio signal and its

Fig. 13 The 32 × 32 secret binary image



corresponding stego audio signal. It calculated by Eq. (24) [16].

$$MSE(H_i, S_i) = \frac{1}{l}\sum_{i=0}^{l-1}(H_i - S_i)^2 \tag{24}$$

SNR calculates the ratio of signal power to the noise power in decibels (dB) and measures the distortion in the fidelity between two audio signals, host and stego; it computed by Eq. (25) [3].

$$SNR(dB) = 10\log_{10}\frac{\sum_{i=0}^{2^l-1} H_i^2}{\sum_{i=0}^{2^l-1}(H_i - S_i)^2} \tag{25}$$

where l is the number of signal samples, H_i is the value of the i^th^ sample in host audio signal H, and S_i is the value of the i^th^ sample in the stego audio signal S.

PSNR is the ratio of the maximum signal to noise in the stego audio signal in decibels, and it defined by Eq. (26) [16].

$$PSNR(dB) = 10\log_{10}\frac{R^2}{MSE(H_i, S_i)} \tag{26}$$

Where R is the maximum signal value that exists in the host audio signal.

In these experiments, 100 quantum host audio signal (100 wave files and 100 speech files) and their stego version (with the length of 1024 samples) were used. It is worth noting that the SNR, PSNR values between the two host signals and the stego signal in this method is highly dependent on the number of the fractional qubit in the QRDS signal representation. The average SNR, PSNR, and MSE values between the host audio and stego audio are shown in Tables 7. The results indicate acceptable values of these parameters for the proposed steganography method.

4.1.2 Security evaluation

During the embedding process, some parts of the host signal may be affected by external factors such as channel noise, filters, etc. Bit Error Rate (BER) is a measure that can be used to identify these changes. BER is a criterion used to evaluate security in quantum simulations and is defined as the ability of secret qubits to survive in attacks [36]. BER is defined by Eq. (27) [20, 36, 42].

Table 7 The average SNR, PSNR, MSE, BER, and EE for the proposed steganography method

Audio type	Number of fractional qubits	Number of audio samples	SNR(dB)	PSNR(dB)	MSE	BER	EE
Music	4	1024	30.2141	41.6391	0.2135	0.0240	2.11
Music	8	1024	49.3267	62.5426	0.0381	0.0159	2.54
Speech	4	1024	30.4872	41.7890	0.2030	0.0239	2.18
Speech	8	1024	49.7442	62.8189	0.0374	0.0159	2.59

$$BER = \frac{1}{PSNR} \tag{27}$$

It can be seen from Table 7 that the BER values obtained for the proposed steganography method are relatively small, indicating that external factors have little influence on the proposed method, and this method has relatively good security.

4.1.3 Embedding capacity evaluation

In the quantum steganography, the embedding capacity is defined as the ratio between the number of secret message qubits and the number of host signal's samples. Therefore, the embedding capacity of the proposed method is defined by Eq. (28).

$$Embedding\ capacity = \frac{the\ number\ of\ secret\ message\ qubits}{the\ number\ of\ host\ signal^{'}s\ samples} \tag{28}$$

In order to a secret image to be fully embedded within the carrier audio signal, and since the host signal length can be varied (according to the proposed steganography method), the number of host signal samples at the minimum length must be equal to the number of secret image pixels. So in this method, the maximum embedded capacity is 1 qubit/sample.

4.1.4 Embedding efficiency evaluation

Embedding efficiency (EE) is one of the criteria for evaluating steganographic systems, which is defined as the ratio between the number of embedded qubits and the probability of modifying to the host signal samples [38]. The embedding efficiency of an audio steganography scheme is defined by Eq. (29).

$$EE = \frac{1}{ratio\ of\ modified\ samples} \tag{29}$$

Higher EE values indicate a less detectable traces on stego audio, thus making the steganographic scheme more robust against steganalysis techniques.

The probability ratio of host signal samples that changes after embedding is proportional to the size of the embedded secret image and is calculated by Eq. (30) [1].

$$P = 1 - \left(R_0 \times R_0^{'}\right) + \left((1 - R_0) \times \left(1 - R_0^{'}\right)\right) \tag{30}$$

Where R_0 is the ratio of 0's in the secret bit-stream, and $R_0^{'}$ is the ratio of 0's in the LSB of the host signal samples. The average embedding efficiency for the proposed method when the number of signal samples is equal to the number of confidential image pixels is shown in Table 7. The results indicate acceptable values of embedded efficiency for the proposed steganography method. It should be noted that since the embedding efficiency is proportional to the size of the secret image, it can be improved by selecting a smaller secret image.

4.2 Steganalysis experiments and analysis

The quantum clean and stego audio datasets obtained from the steganography process are used to evaluate and test the proposed steganalysis scheme to perform proposed quantum steganalysis experiments. In these experiments, 30% of the clean and stego datasets were used to build learning datasets, and another 70% was used as test samples. The experiments are carried out based on the proposed QFE module and by the explanations in Section 3.2.3. In this section, each quantum signal with 1024 samples is divided into 32 Qframes, each containing 32 samples, and then the mean of each Qframe is computed. After using the proposed QFE module, the mean quantum signal parameters obtained with the QRDS model are n = 9, m = 4, t = 5.

The performance of our proposed quantum steganalyzer is measured by sensitivity (SE), specificity (SP), and accuracy (ACC). These criteria are described as follows:

- True negative (TN): the number of clean audio signals that are classified as the clean audio signals.
- True positive (TP): the number of stego audio signals that are classified as the stego audio signals.
- False negative (FN): the number of stego audio signals that are classified as the clean audio signals.
- False positive (FP): the number of clean audio signals that are classified as the stego audio signals.

Sensitivity (SE) is the probability of correct detection of stego audio signal and is defined by Eq. (31).

$$SE = \frac{TP}{TP + FN} \times 100\% \tag{31}$$

Specificity (SP) is the probability of correct detection of the clean audio signal and is defined by Eq. (32).

$$SP = \frac{TN}{TN + FP} \times 100\% \tag{32}$$

Accuracy (ACC) is the probability of correct classification and is defined by Eq. (33).

$$ACC = \frac{TN + TP}{TN + FP + TP + FN} \times 100\% \tag{33}$$

Table 8 The results of the proposed quantum steganalysis method on two types of quantum audio datasets

Audio type	Embedding Rate percentage	TN	TP	FN	FP	SE	SP	ACC
Music	100	67	66	4	5	94.29%	93.06%	93.66%
	50	61	62	9	11	87.32%	84.72%	86.01%
	25	55	57	13	14	81.43%	79.71%	80.58%
Speech	100	68	69	3	3	95.83%	95.77%	95.80%
	50	63	62	6	8	91.18%	88.73%	89.93%
	25	57	56	12	14	82.35%	80.28%	81.29%

In Table 8, the results of the proposed steganalysis method are presented on two types of audio signals, including music and speech. In these experiments, randomly, 30 audio files from each set were used to build the learning dataset, and 70 remaining audio files were also used as test samples. In these experiments, the image shown in Fig. 13 was used for embedding at rates of 100, 50, and 25% in the quantum host audio signal with the length of 1024 samples. The experiments for each set are repeated several times to get the best results. The results show the high accuracy of the proposed quantum audio steganalysis method. In addition to the capabilities and advantages of quantum steganalysis methods over classical methods, the results indicate that the proposed universal quantum steganalysis method is also competitive with classical methods in terms of accuracy of detection. The accuracy of the results can vary according to the length of the host signal and the amount of data embedding. The number of integer qubits and the number of fractional qubits used to represent the signal amplitude information in the QRDS representation also have an impact on the length of feature vectors and better prediction accuracy of the proposed method. Here, because of the limitations and ease of display, a limited number of audio signals with the low samples are used, as well as due to the computing power limitations of classical computers during simulation, the QRDS representation with the low number of qubits is used.

5 Conclusion

In this study, the structure of a steganography-steganalysis system for the quantum audio signal was explored, which is comprised of two parts of quantum steganography and quantum steganalysis. In this structure, the quantum representation for digital signals (QRDS) used to encode the host audio signal, and the hidden message is a binary image by the NEQR representation. The quantum audio steganography (QAS) method was proposed based on the least significant fractional qubit (LSFQ) to improve the traditional LSQB method. The proposed quantum audio steganalysis method is also made up of a universal quantum steganalyzer that includes a module for calculating the mean of quantum audio frames and performs prediction and classification operations based on the quantum KNN algorithm and the Hamming distance metric. The circuit networks required to implement the steganography part and steganalysis part were realized. Simulation-based experiments that were conducted indicate the effective simulation and high performance of the proposed quantum audio steganography-steganalysis system.

In the future works, we plan to provide the quantum circuits network that extracts quantum features from the quantum frequency domains, such as quantum Fourier transform and quantum wavelet transform. We will also try to provide a more robust and more efficient quantum steganalyzer, which can recognize and categorize with higher precision.

References

1. Abdulla AA, Sellahewa H, Jassim SA (2019) Improving embedding efficiency for digital steganography by exploiting similarities between secret and cover images. Multimed Tools Appl:1–25
2. Aïmeur E, Brassard G, Gambs S (2013) Quantum speed-up for unsupervised learning. Mach Learn 90(2): 261–287

3. Ali AH, George LE, Zaidan A, Mokhtar MR (2018) High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain. Multimed Tools Appl 77(23): 31487–31516
4. Aljawarneh S, Yassein MB (2017) A resource-efficient encryption algorithm for multimedia big data. Multimed Tools Appl 76(21):22703–22724
5. Atawneh S, Almomani A, Al Bazar H, Sumari P, Gupta B (2017) Secure and imperceptible digital image steganographic algorithm based on diamond encoding in DWT domain. Multimed Tools Appl 76(18): 18451–18472
6. Bailey K, Curran K, Condell J (2004) Evaluation of pixel-based steganography and stegodetection methods. Imaging Sci J 52(3):131–150
7. Biamonte J, Wittek P, Pancotti N, Rebentrost P, Wiebe N, Lloyd S (2017) Quantum machine learning. Nature 549(7671):195
8. Böhme R (2010) Advanced statistical steganalysis. Springer Science & Business Media
9. Chandramouli R, Kharrazi M, Memon N (2003) Image steganography and steganalysis: Concepts and practice. In: International Workshop on Digital Watermarking. Springer, pp 35–49
10. Chen K, Yan F, Iliyasu AM, Zhao J (2018) A quantum audio watermarking scheme. In: 2018 37th Chinese control conference (CCC). IEEE, pp 3180–3185
11. Chen K, Yan F, Iliyasu AM, Zhao J (2018) Exploring the implementation of steganography protocols on quantum audio signals. Int J Theor Phys 57(2):476–494
12. Deutsch D (1983) Uncertainty in quantum measurements. Phys Rev Lett 50(9):631
13. Dunjko V, Briegel HJ (2018) Machine learning & artificial intelligence in the quantum domain: a review of recent progress. Rep Prog Phys 81(7):074001
14. Dunjko V, Taylor JM, Briegel HJ (2016) Quantum-enhanced machine learning. Phys Rev Lett 117(13): 130501
15. Ekert A (2018) Quantum cryptography: the power of independence. Nat Phys 14:114–115
16. El-Khamy SE, Korany NO, El-Sherif MH (2017) A security enhanced robust audio steganography algorithm for image hiding using sample comparison in discrete wavelet transform domain and RSA encryption. Multimed Tools Appl 76(22):24091–24106
17. Gisin N, Thew R (2007) Quantum communication. Nat Photonics 1(3):165
18. Gupta B, Agrawal DP, Yamaguchi S (2016) Handbook of research on modern cryptographic solutions for computer and cyber security. IGI global
19. Hai H, Qing XD, Ke Q (2018) A watermarking-based authentication and image restoration in multimedia sensor networks. Int J High Perform Comput Networking 12(1):65–73
20. Heidari S, Pourarian MR, Gheibi R, Naseri M, Houshmand M (2017) Quantum red–green–blue image steganography. Int J Quantum Inf 15(05):1750039
21. Ibtihal M, Hassan N (2017) Homomorphic encryption as a service for outsourced images in mobile cloud computing environment. Int J Cloud Appl Comput (IJCAC) 7(2):27–40
22. Jiang N, Zhao N, Wang L (2016) LSB based quantum image steganography algorithm. Int J Theor Phys 55(1):107–123
23. Li P, Lu A (2018) LSB-based steganography using reflected gray code for color quantum images. Int J Theor Phys 57(5):1516–1548
24. Li J, Yu C, Gupta B, Ren X (2018) Color image watermarking scheme based on quaternion Hadamard transform and Schur decomposition. Multimed Tools Appl 77(4):4545–4561
25. Li P, Wang B, Xiao H, Liu X (2018) Quantum representation and basic operations of digital signals. Int J Theor Phys 57(10):3242–3270
26. Lloyd S, Mohseni M, Rebentrost P (2013) Quantum algorithms for supervised and unsupervised machine learning. arXiv preprint arXiv:02779
27. Long G-l, Deng F-g, Wang C, X-h L, Wen K, Wang W-y (2007) Quantum secure direct communication and deterministic secure quantum communication. Front Phys China 2(3):251–272
28. Luo G, Zhou R-G, Luo J, Hu W, Zhou Y, Ian H (2019) Adaptive LSB quantum watermarking method using tri-way pixel value differencing. Quantum Inf Process 18(2):49
29. Martin K (2007) Steganographic communication with quantum information. In: International Workshop on Information Hiding. Springer, pp 32–49
30. Mohsenfar SM, Mosleh M, Barati A (2015) Audio watermarking method using QR decomposition and genetic algorithm. Multimed Tools Appl 74(3):759–779
31. Mohtasham-Zadeh V, Mosleh M (2019) Audio Steganalysis based on collaboration of fractal dimensions and convolutional neural networks. Multimed Tools Appl 78(9):11369–11386
32. Mosleh M, Setayeshi S, Barekatain B, Mosleh M (2019) High-capacity, transparent and robust audio watermarking based on synergy between DCT transform and LU decomposition using genetic algorithm. Analog Integr Circ Sig Process 100(3):513–525

33. Nejad MY, Mosleh M, Heikalabad SR (2019) An LSB-Based Quantum Audio Watermarking Using MSB as Arbiter. Int J Theor Phys:1–24
34. Oppenheim AV (1999) Discrete-time signal processing. Pearson Education India
35. Pljonkin A (2019) Vulnerability of the synchronization process in the quantum key distribution system. Int J Cloud Appl Comput (IJCAC) 9(1):50–58
36. Qu Z, Cheng Z, Liu W, Wang X (2018) A novel quantum image steganography algorithm based on exploiting modification direction. Multimed Tools Appl:1–21
37. Qu Z-G, He H-X, Li T (2018) Novel quantum watermarking algorithm based on improved least significant qubit modification for quantum audio. Chin Phys B 27(1):010306
38. Qu Z, Cheng Z, Liu W, Wang X (2019) A novel quantum image steganography algorithm based on exploiting modification direction. Multimed Tools Appl 78(7):7981–8001
39. Rebentrost P, Mohseni M, Lloyd S (2014) Quantum support vector machine for big data classification. Phys Rev Lett 113(13):130503
40. Ruan Y, Chen H, Tan J, Li X (2016) Quantum computation for large-scale image classification. Quantum Inf Process 15(10):4049–4069
41. Ruan Y, Xue X, Liu H, Tan J, Li X (2017) Quantum algorithm for k-nearest neighbors classification based on the metric of hamming distance. Int J Theor Phys 56(11):3496–3507
42. Şahin E, Yilmaz İ (2018) A novel quantum steganography algorithm based on LSBq for multi-wavelength quantum images. Quantum Inf Process 17(11):319
43. Schuld M, Sinayskiy I, Petruccione F (2014) Quantum computing for pattern classification. In: Pacific Rim International Conference on Artificial Intelligence. Springer, pp 208–220
44. Sergienko AV (2018) Quantum communications and cryptography. CRC press
45. Shu-Jiang X, Xiu-Bo C, Xin-Xin N, Yi-Xian Y (2013) A novel quantum covert channel protocol based on any quantum secure direct communication scheme. Commun Theor Phys 59(5):547
46. Shu-Jiang X, Xiu-Bo C, Xin-Xin N, Yi-Xian Y (2013) Steganalysis and improvement of a quantum steganography protocol via a GHZ4 state. Chin Phys B 22(6):060307
47. Simmons GJ (1984) The prisoners' problem and the subliminal channel. In: Advances in Cryptology. Springer, pp 51–67
48. Tirkel AZ, Rankin G, Van Schyndel R, Ho W, Mee N, Osborne CF (1993) Electronic watermark. Digit Image ComputTechnol Appl 666–673
49. Trugenberger CA (2001) Probabilistic quantum memories. Phys Rev Lett 87(6):067901
50. Vedral V, Barenco A, Ekert A (1996) Quantum networks for elementary arithmetic operations. Phys Rev A 54(1):147
51. Wang J (2016) QRDA: quantum representation of digital audio. Int J Theor Phys 55(3):1622–1641
52. Wang D, Liu Z-H, Zhu W-N, Li S-Z (2012) Design of quantum comparator based on extended general Toffoli gates with multiple targets. Comput Therm Sci 39(9):302–306
53. Wang S, Sang J, Song X, Niu X (2015) Least significant qubit (LSQb) information hiding algorithm for quantum image. Measurement 73:352–359
54. Wiśniewska J, Sawerwain M (2018) Recognizing the pattern of binary Hermitian matrices by quantum kNN and SVM methods. Vietnam J Comput Sci:1–8
55. Wootters WK, Zurek WH (1982) A single quantum cannot be cloned. Nature 299(5886):802
56. Xia Z, Wang X, Sun X, Liu Q, Xiong N (2016) Steganalysis of LSB matching using differences between nonadjacent pixels. Multimed Tools Appl 75(4):1947–1962
57. Yan F, Iliyasu AM, Guo Y, Yang H (2018) Flexible representation and manipulation of audio signals on quantum computers. Theor Comput Sci 752:71–85
58. Zhang Y, Lu K, Gao Y, Wang M (2013) NEQR: a novel enhanced quantum representation of digital images. Quantum Inf Process 12(8):2833–2860
59. Zhou R-G, Luo J, Liu X, Zhu C, Wei L, Zhang X (2018) A novel quantum image steganography scheme based on LSB. Int J Theor Phys 57(6):1848–1863
60. Zhou Y, Zhou R-G, Liu X, Luo G (2019) A quantum image watermarking scheme based on two-bit superposition. Int J Theor Phys 58(3):950–968

Affiliations

Javad Chaharlang[1] • **Mohammad Mosleh**[1] • **Saeed Rasouli-Heikalabad**[2]

✉ Mohammad Mosleh
Mosleh@iaud.ac.ir

[1] Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran

[2] Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran