ISSN 1674-1056
http://cpb.iphy.ac.cn
http://iopscience.iop.org/cpb
中国物理 B
Chinese Physics
中国物理
Chinese Physics B

Novel quantum watermarking algorithm based on improved least significant qubit modification for quantum audio

Zhi-Guo Qu(瞿治国), Huang-Xing He(何煌兴), Tao Li(李涛)
Citation: Chin. Phys. B . 2018, 27(1): 010306. **doi:** 10.1088/1674-1056/27/1/010306

Journal homepage: http://cpb.iphy.ac.cn; http://iopscience.iop.org/cpb

What follows is a list of articles you may be interested in

Decoy-state reference-frame-independent quantum key distribution with both source errors and statistical fluctuations

Kang Liu(刘康), Jian Li(李剑), Jian-Rong Zhu(朱建荣), Chun-Mei Zhang(张春梅), Qin Wang(王琴)
Chin. Phys. B . 2017, 26(12): 120302. **doi:** 10.1088/1674-1056/26/12/120302

Improving continuous-variable quantum key distribution under local oscillator intensity attack using entanglement in the middle

Fang-Li Yang(杨芳丽), Ying Guo(郭迎), Jin-Jing Shi(石金晶), Huan-Li Wang(王焕礼), Jin-Jin Pan(潘矜矜)
Chin. Phys. B . 2017, 26(10): 100303. **doi:** 10.1088/1674-1056/26/10/100303

Time-energy high-dimensional one-side device-independent quantum key distribution

Hai-Ze Bao(包海泽), Wan-Su Bao(鲍皖苏), Yang Wang(汪洋), Rui-Ke Chen(陈瑞柯), Hong-Xin Ma(马鸿鑫), Chun Zhou(周淳), Hong-Wei Li(李宏伟)
Chin. Phys. B . 2017, 26(5): 050302. **doi:** 10.1088/1674-1056/26/5/050302

Continuous variable quantum key distribution

Yong-Min Li(李永民), Xu-Yang Wang(王旭阳), Zeng-Liang Bai(白增亮), Wen-Yuan Liu(刘文元), Shen-Shen Yang(杨申申), Kun-Chi Peng(彭堃墀)
Chin. Phys. B . 2017, 26(4): 040303. **doi:** 10.1088/1674-1056/26/4/040303

Spherical reconciliation for a continuous-variable quantum key distribution

Zhao Lu(卢钊), Jian-Hong Shi(史建红), Feng-Guang Li(李风光)
Chin. Phys. B . 2017, 26(4): 040304. **doi:** 10.1088/1674-1056/26/4/040304

Novel quantum watermarking algorithm based on improved least significant qubit modification for quantum audio*

Zhi-Guo Qu(瞿治国)[1,†] Huang-Xing He(何煌兴)[2], and Tao Li(李涛)[2]

[1] *Jiangsu Engineering Center of Network Monitoring, Nanjing University of Information Science and Technology, Nanjing* 210044, *China*
[2] *School of Electronic & Information Engineering, Nanjing University of Information Science and Technology, Nanjing* 210044, *China*

(Received 9 July 2017; revised manuscript received 9 September 2017; published online 22 December 2017)

As one of essential multimedia in quantum networks, the copyright protection of quantum audio has gradually become an important issue in the domain of quantum information hiding in the decades. In this paper, an improved quantum watermarking algorithm based on quantum audio by using least significant qubit (LSQb) modification is proposed. Compared with the previous achievements, it can effectively improve the robustness and security of watermark for copyright protection of quantum audio. In the new algorithm, the least significant bites and the peripheral least significant bits of the amplitudes are modified in terms of their logical consistency and correlation to enhance watermark robustness of resisting various illegal attacks. Furthermore, the new algorithm can avoid the weak robustness defect of many previous algorithms that directly embedded the watermark into the least significant bits. In order to implement the new algorithm, some specific quantum circuits are designed to obtain better applicability and scalability for embedding and extracting watermark. Finally, the simulation results including the values of audio waveforms and signal to noise ratios (SNR) prove that the new algorithm has good transparency, robustness, and security.

Keywords: quantum audio watermarking, least significant qubit, logical consistency and correlation, quantum circuits

PACS: 03.67.Dd, 03.67.Hk, 03.67.Ac **DOI:** 10.1088/1674-1056/27/1/010306

1. Introduction

Information security[1,2] is a significant issue in the field of information and communication technology.[3] With the rapid development of computer network[4,5] in the decades, information security becomes more and more important. Quantum key distribution protocol[6] is an ingenious application of quantum mechanics in information security. It was firstly proposed by Bennett and Brassard in 1984. On this basis, quantum secure communication technology in quantum networks witnessed the considerable development, such as quantum key distribution (QKD),[7–9] quantum secret sharing (QSS),[10–12] and quantum secure direct communication (QSDC).[13–17] In recent years, quantum multimedia is rapidly becoming the important carrier with the development of quantum networks. More and more classical digital multimedia, including text, image, video, and audio, are extended to quantum communication networks with various quantum multimedia representations. As a result, information security of digital multimedia in quantum channel becomes a significant issue that can not be ignored and need to be urgently solved, as being consistent with the classical digital multimedia technology. Consequently, various information protection technologies emerged in the last decades. As one of important quantum information security technologies, quantum watermarking is the technique for copyright protection, which is fulfilled by embedding invisible signal carrying identity information into a variety of quantum multimedia carriers. In 2011, based on a flexible representation of quantum image (FRQI),[18] Abdullah *et al.* proposed a watermarking and authentication algorithm for quantum images by means of restricted geometric transformations.[19] The algorithm can excellently authenticate the identity of the owner. In 2012, Negin *et al.* proposed a quantum watermarking algorithm using entanglement swapping.[20] It enables to make secret information secure and reliable. Subsequently, Zhang *et al.* proposed a quantum watermarking protocol[21] and a watermark algorithm for quantum images based on quantum Fourier transform.[22] In 2014, Song *et al.* proposed a dynamic watermarking scheme for quantum images based on Hadamard transforming.[23] The proposed scheme has better visual quality, higher embedding capacity, and lower complexity. In 2015, Wang *et al.* proposed a watermarking scheme for quantum images based on least significant bit (LSB).[24] In this scheme, only the copyright owner who held the private key could extract the watermark information by quantum circuits of embedding and extracting algorithms. Jiang *et al.* presented two blind LSB steganography algorithms based on quantum images in 2016.[25] The algorithms are absolutely blind and the whole extracting procedure can be accomplished in quantum computer without the help of

*Project supported by the National Natural Science Foundation of China (Grant Nos. 61373131, 61303039, 61232016, and 61501247), Sichuan Youth Science and Technique Foundation, China (Grant No. 2017JQ0048), NUIST Research Foundation for Talented Scholars of China (Grant No. 2015r014), and PAPD and CICAEET Funds of China.

†Corresponding author. E-mail: qzghhh@126.com

© 2018 Chinese Physical Society and IOP Publishing Ltd

classical channel. In addition, a watermarking scheme is proposed by using simple and small-scale quantum circuits.[26] Although its computational complexity is reduced, however, the embedding capacity is only 1/4 of the image carrier. After reviewing the existing achievements, it can be known that most of the previous achievements focus on quantum image for copyright protection. As another important multimedia in quantum networks, so far, the copyright protection of quantum audio is seldom involved.

In 2015, a least significant qubit (LSQb) modification algorithm[27] based on a novel enhanced quantum representation (NEQR) of digital images was put forward. The algorithm substituted the least significant bit of the carrier image with the secret information for covert communication. It has the merits of large capacity and easy to calculate. However, its security is vulnerable to be attacked or tempered by illegal third parties, due to that it embeds the secret information into the least significant bit of carrier image. On this account, a novel LSB watermarking algorithm for quantum audio based on logical consistency and correlation is proposed in this paper. It changes the embedding position of watermark bit sequence by means of connecting the least significant bit and that of sub-low bits, which improves the robustness, security, and transparency. The good performances make it harder to be detected and attacked by illegal third parties. Besides that, to make embedding and extracting processes of watermark based on QLSb more applicable, the quantum embedding and extracting circuits are designed in this paper to obtain better applicability and scalability for copyright protection.

In addition, compared with classical watermarking algorithms for audio, the proposed quantum watermarking algorithm has the following advantages.

(i) Due to the quantum no-cloning theorem and eavesdropping detection, as carrier, quantum audio transmitted in quantum channel is generally difficult to be imperceptibly intercepted for attackers. Even if some copies of quantum audio were imperceptibly intercepted by attackers, due to the quantum uncertainty theorem, it is still impossible to obtain the whole information of carrier audio for attackers, not mention that of embedded watermark in carrier audio. Therefore, the proposed algorithm can achieve better security.

(ii) For classical audio watermarking algorithms, there are various audio processing methods available to remove embedded watermark for attackers after obtaining carrier audio in classical channel by eavesdropping. However, it is impossible for attackers to get all the copies of quantum carrier audio without being detected as mentioned above. Besides that, even if attackers have obtained all the information of carrier audio and embedded watermark, because quantum state is very easily collapsed by external disturbances, it is still impossible for them to remove embedded watermark by multiple attacks on it, in case carrier audio remains intact or still available. From this point of view, the proposed algorithm also can achieve better robustness.

(iii) Moreover, based on basic quantum gates, the corresponding quantum circuits are designed in the new algorithm. Compare to classical watermarking algorithms, the new algorithm theoretically can be implemented at a much higher speed through quantum computer with the power of concurrent computation. From this perspective, the new algorithm can also have better applicability and scalability for its high processing efficiency.

2. Preliminaries

2.1. Quantum representation of digital audio (QRDA)

In 2016, Wang proposed the first quantum representation for digital audio.[28] In this new audio model, the amplitude of classical audio is represented by the amplitude of quantum audio. Based on the model, a QRDA can be denoted as

$$\begin{aligned}|\psi\rangle &= |A\rangle + |B\rangle \\ &= \frac{1}{\sqrt{2^l}}\sum_{T=0}^{L-1}|D_T\rangle\otimes|T\rangle + \frac{1}{\sqrt{2^l}}\sum_{T=L}^{2^l-1}\bigotimes_{i=0}^{q-1}|0\rangle|T\rangle \\ &= \frac{1}{\sqrt{2^l}}\sum_{T=0}^{L-1}\left|D_T^{q-1}\ D_T^{q-2}\ \cdots\ D_T^{0}\right\rangle|T\rangle \\ &\quad + \frac{1}{\sqrt{2^l}}\sum_{T=L}^{2^l-1}\bigotimes_{i=0}^{q-1}|0\rangle|T\rangle, \\ |T\rangle &= |t_{l-1}\ t_{l-2}\ \cdots\ t_1\ t_0\rangle, \qquad (1) \\ l &= \begin{cases}\log_2 L, & L>1,\\ 1, & L=1.\end{cases} \qquad (2)\end{aligned}$$

Here, $|\psi\rangle$ is the quantum representation of digital audio, $|D_T\rangle$ represents a binary sequence for encoding the amplitude value, and $|T\rangle$ denotes the corresponding time point in quantum audio. In addition, $|A\rangle$ denotes the amplitudes with the length of L corresponding to the effective time points, and the last 2^l-L time points are redundancies, denoted by $|B\rangle$. QRDA sets the amplitude values of all the redundancies as $|0\rangle$. For clarity, its representative expression in QRDA with length $2^l=16$ is given by

$$\begin{aligned}|\psi\rangle &= \frac{1}{\sqrt{2^4}}(|0101\rangle\otimes|0000\rangle + |1010\rangle\otimes|0001\rangle \\ &\quad + |1110\rangle\otimes|0010\rangle + |1110\rangle\otimes|0011\rangle \\ &\quad + |1010\rangle\otimes|0100\rangle + |0101\rangle\otimes|0101\rangle \\ &\quad + |0010\rangle\otimes|0110\rangle + |0010\rangle\otimes|0111\rangle + |0101\rangle\otimes|1000\rangle \\ &\quad + |0110\rangle\otimes|1001\rangle + |0110\rangle\otimes|1010\rangle + |0101\rangle\otimes|1011\rangle \\ &\quad + |0010\rangle\otimes|1100\rangle + |0000\rangle\otimes|1101\rangle \\ &\quad + |0000\rangle\otimes|1110\rangle + |0000\rangle\otimes|1111\rangle) \qquad (3)\end{aligned}$$

and by Fig. 1.

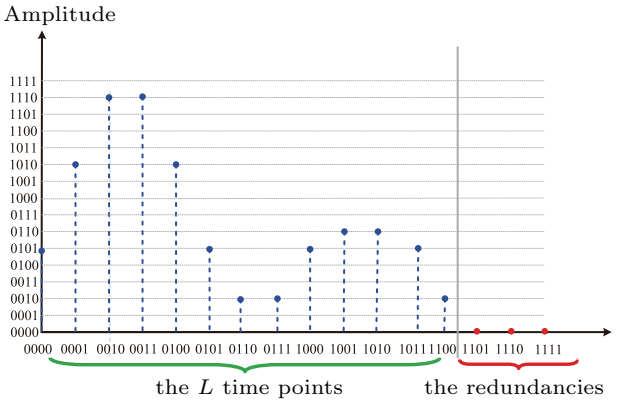


Fig. 1. (color online) An example audio and its representative expression in QRDA.

2.2. NEQR of digital images

In this paper, the embedded quantum watermark is represented by NEQR.[29] For NEQR, the gray-scale image with $2^n \times 2^n$ pixels can be denoted by

$$\begin{aligned} |I\rangle &= \frac{1}{2^n}\sum_{i=0}^{2^{2n}-1} |c_i\rangle \otimes |i\rangle, \\ |c_i\rangle &= \left|c_i^{q-1} c_i^{q-2} \ldots c_i^1 c_i^0\right\rangle, \\ & c_i^k \in \{0,1\}, \quad k = q-1, q-2, \ldots, 1, 0, \\ & i = 0, 1, \ldots, 2^{2n}-1. \end{aligned} \tag{4}$$

Here, $|I\rangle$ is the quantum representation of digital image. The gray-scale value and the position information are encoded by $|c_i\rangle$ and $|i\rangle$, respectively. Position information includes the vertical information and the horizontal information, while $|y\rangle$ encodes the vertical information and $|x\rangle$ encodes the horizontal information.

$$\begin{aligned} |i\rangle &= |y\rangle|x\rangle = |y_{n-1}\, y_{n-2}\, \cdots\, y_0\rangle |x_{n-1}\, x_{n-2}\, \cdots\, x_0\rangle, \\ & |y_j\rangle |x_j\rangle \in \{0,1\}. \end{aligned}$$

Taking an image with 2×2 pixels as an example, figure 2 shows its NEQR. Since the range of gray scale is from 0 to 255, the gray values of pixels are stored with 8 qubits, and the subsidiary two particles are used to denote the coordinates of pixels,

$$\begin{aligned} |I\rangle = \frac{1}{2}(&|10011001\rangle \otimes |00\rangle + |01100110\rangle \otimes |01\rangle \\ &+ |00110011\rangle \otimes |10\rangle + |11001100\rangle \otimes |11\rangle). \end{aligned} \tag{5}$$

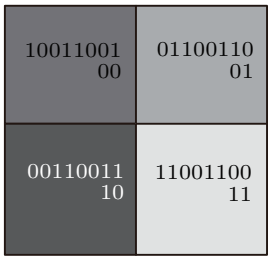


Fig. 2. An example image and its representative expression of NEQR.

2.3. A watermark-scrambling method based on quantum circuits

In the new algorithm, in order to enhance the robustness to resist invalid attack and increase the security perfectly, compared with previous embedding methods, a watermark-scrambling method is adopted[22] to transform a meaningful image into a meaningless or disorder image. For example, figure 3 shows an original watermark and scrambled watermark with 4×4 pixels, and the quantum circuit corresponding to the watermark image's scrambling is also given in Fig. 4.

	00	01	10	11
00	1	2	3	4
01	5	6	7	8
10	9	10	11	12
11	13	14	15	16

	01	00	11	10
11	9	12	11	10
01	13	16	15	14
10	1	4	3	2
00	5	8	7	6

Fig. 3. Watermark-scrambling method on a quantum image sized 4×4. The left is the original watermark and the right is the corresponding scrambled watermark.

For a image with $2^n \times 2^n$ pixels, two random permutations K and R are generated by the owner, denoted by the sequences of binary value respectively. Here, $K = \{K(1), K(2), \ldots, K(2^n)\}$ and $R = \{R(1), R(2), \ldots, R(2^n)\}$. The secret key K is corresponding to the vertical information, and the other secret key R is corresponding to the horizontal information. Specifically, assuming that $K(i)$ and $R(j)$ are the i-th and j-th binary values of K and R, respectively, the (i, j) pixel value of the original watermark will be interchanged with the pixel value at position $(K(i), R(j))$ in the new watermark. By executing watermark scrambling on the watermark, the watermark can be scrambled to be meaningless or disordered.

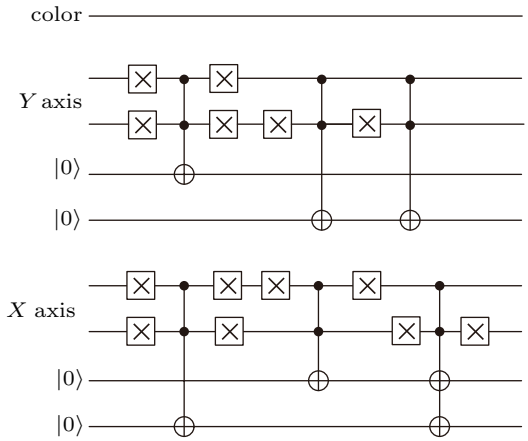


Fig. 4. The image-scrambling quantum circuit on the quantum image sized 4×4 of Fig. 3.

Assuming $K = \{1,0,3,2\}$ and $R = \{3,1,2,0\}$, the original position values are rearranged as {9, 12, 11, 10, 13, 16, 15, 14, 1, 4, 3, 2, 5, 8, 7, 6} by using the watermark-scrambling quantum circuit shown as Fig. 4. The first two qubits of the output x and y coordinates are the original watermark's coordinates, while the last two qubits of the output x and y coordinates are the scrambled watermark's coordinates.

The inverse watermark-scrambling process is similar to the scrambling process. The pixel $(K(i),R(j))$ value of the scrambled watermark replaced the pixel value at the position (i,j) of the new watermark. Thus the image obtained is the original watermark. The corresponding inverse watermark-scrambling circuit is similar to that of watermark-scrambling.

3. New quantum watermarking algorithm based on LSQb

Most of information hiding algorithms based on LSQb modification have the characteristics of large capacity and easy to operate. In this section, an improved quantum audio watermarking algorithm based on LSQb modification and QRDA is proposed. The steps of the algorithm are presented in details as follows.

3.1. The embedding process of watermark

The classical algorithm based on LSB modification substitutes the least significant bit of carrier's pixel values with the bit sequence of secret information. Thus the changes happening on the original carrier are ± 1. The method has little effect on the quantized audio by modifying the least significant qubits, which nearly is impossible to be perceived just by the ear. The outline of the embedding process in our algorithm is given in Fig. 5.

Due to that two bits can denote four binary numbers $\{00,01,10,11\}$, the decimal value of the last two bits (x_1,x_0) can denote the position of lowest four bit planes of each pixel. Adjusting the decimal value denoted by (x_1,x_0) can make values of bit plane denoted by it consistent with the pixels of binary watermark. Assuming that the amplitude of quantum audio corresponding to time points are expressed as $D = \{D_0,D_1,D_2,D_3,\ldots,D_{n-1}\}$, the scrambled watermark can be denoted as $W = \{w_0,w_1,w_2,w_3,\ldots,w_{n-1}\}$.

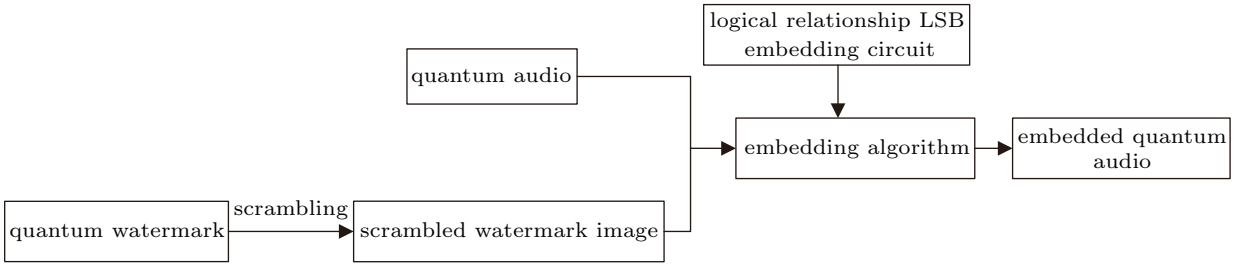


Fig. 5. The LSQb embedding process of watermark based on logical relationship (LR-LSQb).

The process of embedding watermark is presented in details as follows.

Step 1 The copyright owner firstly determines the embedding positions for watermark in quantum audio. The determined positions are required to be sufficient to embed all the watermark pixels with binary values.

Step 2 Assuming that an amplitude of quantum audio corresponding to time-point is D_i, the binary values of D_i are denoted as $D_i = D_i^7 D_i^6 D_i^5 D_i^4 D_i^3 D_i^2 D_i^1 D_i^0$, whose binary values of the low four bit planes will be $(D_i^3,D_i^2,D_i^1,D_i^0)$.

Step 3 Get the binary value of the pixel w_i in the scrambled watermark. Then, the binary value of the pixel w_i will be compared with the binary values of the low bit planes of the carrier audio's amplitude selected successively according to the order of $D_i^2 \rightarrow D_i^3$.

Step 4 Compare the binary value of the pixel w_i with the binary value of the bit plane denoted by $D_i^1 D_i^0$. If the two values are equal, nothing will happen on $D_i^1 D_i^0$. For example, when the binary value of w_i is 0 and the value of $(D_i^3,D_i^2,D_i^1,D_i^0)$ is (1010), the binary value of the bit plane denoted by $D_i^1 D_i^0(10)$ is 0, which means that it is marked as D_i^2. Since the binary value of the bit plane D_i^2 is consistent with that of the pixel w_i, there is no modification to be done on $D_i^1 D_i^0$.

Step 5 Otherwise, the binary value of $D_i^1 D_i^0$ is needed to be modified correspondingly. If the binary value of w_i is consistent with D_i^2 or D_i^3, it needs to modify $D_i^1 D_i^0$ by getting the binary value of w_i and comparing it with the binary value of the low bit planes of the corresponding amplitude. For example, if the binary value of w_i is 0, the value of $(D_i^3,D_i^2,D_i^1,D_i^0)$ is (0110). The bit plane D_i^2 is denoted by $D_i^1 D_i^0(10)$. We can see that the value of bit plane D_i^2 is 1 and it is not consistent with the binary value of w_i. However, due to the binary value of bit plane D_i^3 is equal to that of w_i, the copyright owner will change the binary value of $D_i^1 D_i^0$ to 11. Herein, it means that the binary value of the low four bit planes of amplitude will be changed to 0111. Thus the pixel of binary watermark can be embedded into the amplitude in quantum audio carrier without

modifying the value of D_i^3.

Step 6 For other special cases, the unique agreements are presented in details as follows.

Case 1: If the binary value of w_i is 0 and the binary value of $(D_i^3, D_i^2, D_i^1, D_i^0)$ is (0000), the binary value of $D_i^1 D_i^0$ will be modified to 01.

Case 2: If the binary value of w_i is 0 and the binary value of $(D_i^3, D_i^2, D_i^1, D_i^0)$ is (1100), (1101), or (1110), the binary value of $D_i^1 D_i^0$ will be modified to 00.

Case 3: If the binary value of w_i is 0 and the binary value of $(D_i^3, D_i^2, D_i^1, D_i^0)$ is (1111), the binary value of $D_i^1 D_i^0$ will remain unchanged. In this case, the algorithm makes an agreement that the extracted binary value is unified as 1100.

Case 4: If the binary value of w_i is 1 and the binary value of $(D_i^3, D_i^2, D_i^1, D_i^0)$ is (0000), the binary value of $D_i^1 D_i^0$ will remain unchanged. In this case, the algorithm makes an agreement that the extracted binary value is unified as 0001.

Case 5: If the binary value of w_i is 1 and the binary value of $(D_i^3, D_i^2, D_i^1, D_i^0)$ is (1111), modify the binary value of $D_i^1 D_i^0$ to 10.

Case 6: Otherwise the binary value of w_i is 1 and the binary value of $(D_i^3, D_i^2, D_i^1, D_i^0)$ is (0001), (0010), or (0011), modify the binary value of $D_i^1 D_i^0$ to 01.

In specific, Table 1 shows the logical relationship (LR) between bit information of watermark and binary values of the low four bit planes of amplitude for LSQb modification of embedding watermark. Meanwhile, in order to make the embedding process more practical and obtain better usability and scalability for copyright protection, an effective quantum embedding circuit is designed in Fig. 6. The LR-LSQb embedding circuit contains two parts. One is quantum comparator and the other is modification circuit based on the logical relationship in Table 1 (the special cases are excepted). Here, four ancillary states used as the input are prepared in the standard states $|0\rangle$, while the states $|a\rangle$, $|b\rangle$, $|c\rangle$, and $|d\rangle$ are the outputs.

If $|a\rangle|b\rangle|c\rangle|d\rangle = |0\rangle|0\rangle|0\rangle|0\rangle$, the binary value of D_i^2 is consistent with that of w_i. If the binary value of the bit plane denoted by $D_i^1 D_i^0$ is consistent with the binary value of D_i^2, the binary value of $D_i^1 D_i^0$ is remained unchanged. Otherwise, the binary value of $D_i^1 D_i^0$ will be modified correspondingly.

If $|a\rangle|b\rangle|c\rangle|d\rangle = |0\rangle|1\rangle|0\rangle|0\rangle$ or $|a\rangle|b\rangle|c\rangle|d\rangle = |1\rangle|0\rangle|0\rangle|0\rangle$, the binary value of D_i^3 is consistent with that of w_i. If the binary value of the bit plane denoted by $D_i^1 D_i^0$ is consistent with the binary value of D_i^3, the binary value of $D_i^1 D_i^0$ is remained unchanged. Otherwise, the binary value of $D_i^1 D_i^0$ will be modified correspondingly.

If $|a\rangle|b\rangle|c\rangle|d\rangle = |0\rangle|1\rangle|0\rangle|1\rangle$ or $|a\rangle|b\rangle|c\rangle|d\rangle = |0\rangle|1\rangle|1\rangle|0\rangle$ or $|a\rangle|b\rangle|c\rangle|d\rangle = |1\rangle|0\rangle|0\rangle|1\rangle$ or $|a\rangle|b\rangle|c\rangle|d\rangle = |1\rangle|0\rangle|1\rangle|0\rangle$, the corresponding modification on the binary value of $D_i^1 D_i^0$ will be implemented in term of the logical relationship shown in Table 1.

Table 1-1. The relationship between bit information of watermark and the binary values of the low four bit plane of amplitude.

The binary values of low four bit planes of carrier	The binary values of watermark image	The modified binary values of low four bit planes of carrier
$D_i^3 D_i^2 D_i^1 D_i^0$	w_i	$D'^3_i D'^2_i D'^1_i D'^0_i$
0 0 0 0	0	0 0 **1 0**
0 0 0 1	0	0 0 **1 0**
0 0 1 0	0	0 0 **1 0**
0 0 1 1	0	0 0 **1 0**
0 1 0 0	0	0 1 **1 1**
0 1 0 1	0	0 1 **1 1**
0 1 1 0	0	0 1 **1 1**
0 1 1 1	0	0 1 **1 1**
1 0 0 0	0	1 0 **1 0**
1 0 0 1	0	1 0 **1 0**
1 0 1 0	0	1 0 **1 0**
1 0 1 1	0	1 0 **1 0**
1 1 0 0	0	1 1 **0 0**
1 1 0 1	0	1 1 **0 0**
1 1 1 0	0	1 1 **0 0**
1 1 1 1	0	1 1 **0 0**

Table 1-2. The relationship between bit information of watermark and the binary values of the low four bit plane of amplitude.

The binary values of low four bit planes of carrier	The binary values of watermark image	The modified binary values of low four bit planes of carrier
$D_i^3 D_i^2 D_i^1 D_i^0$	w_i	$D'^3_i D'^2_i D'^1_i D'^0_i$
0 0 0 0	1	0 0 **0 1**
0 0 0 1	1	0 0 **0 1**
0 0 1 0	1	0 0 **0 1**
0 0 1 1	1	0 0 **0 1**
0 1 0 0	1	0 1 **1 0**
0 1 0 1	1	0 1 **1 0**
0 1 1 0	1	0 1 **1 0**
0 1 1 1	1	0 1 **1 0**
1 0 0 0	1	1 0 **1 1**
1 0 0 1	1	1 0 **1 1**
1 0 1 0	1	1 0 **1 1**
1 0 1 1	1	1 0 **1 1**
1 1 0 0	1	1 1 **1 0**
1 1 0 1	1	1 1 **1 0**
1 1 1 0	1	1 1 **1 0**
1 1 1 1	1	1 1 **1 0**

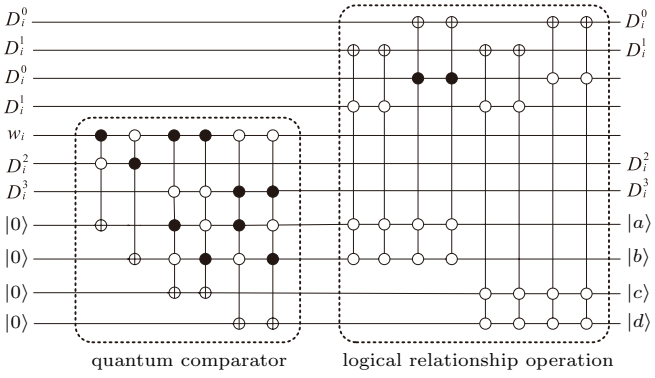


Fig. 6. The LSQb modification circuit of embedding watermark based on logical relationship.

Note The copyright owner firstly obtains the binary sequence W after zigzag sorting the watermark. If the length of the bit sequence W is less than that of quantum audio as the carrier, the binary sequence W needs to be filled so that its length can be consistent with that of quantum audio. In other words, if there are no enough pixels of watermark to

be embedded into all the carrier amplitudes, the amplitudes of redundancy in quantum audio will be filled with copies of some amplitudes based on corresponding parts of time-points in quantum audio. Hence, the length of watermark can be consistence with that of quantum audio carrier.

3.2. Watermark image's extracting process

In the new algorithm, the embedding process is based on the logical relationship of bit values of different lowest bit planes. By comparison, the extracting process of quantum watermark basically is an inverse process of embedding. The crucial factors of extracting process for copyright owner also is the logical relationship shown as Table 1. The outline of the extracting process in the new algorithm is given in Fig. 7.

It is noteworthy that the watermark was embedded into the superimposed components of quantum carrier audio. Thus, if any one attempts to obtain the embedded watermark, it is necessary for him to perform measurement on the quantum state of carrier audio. However, each of superimposed component of quantum state only contain a small part of audio information. Due to the quantum uncertainty theorem, many enough copies of quantum carrier audio shall be prepared to transmit or measure all the information of audio for communicators. Similarly, the same rule applies to the embedded watermark. On this account, many enough copies of the watermarked quantum audio is needed to extract the whole information of embedded watermark.

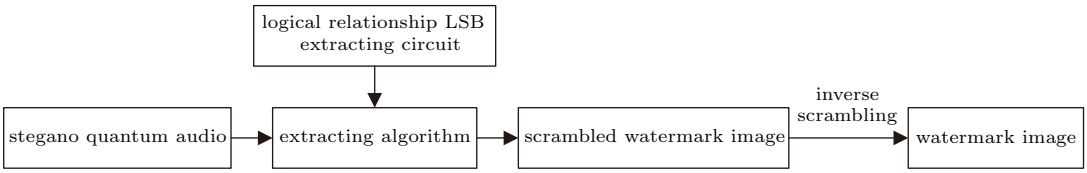


Fig. 7. The LSQb extracting process of watermark based on the logical relationship (LR-LSQb).

Since that LSQb watermarked quantum audio can be regarded as a complex vector in Hilbert space with the size of 2^{q+l}, it can be decomposed as a vector direct product of amplitudes and the corresponding time-points.

For the cast that the length of time-points is 16 in Fig. 2 (the length of effective time-points $L = 13$), the stegano audio vector is denoted as $\boldsymbol{D}$, which can be disintegrated as

$$\boldsymbol{D} = D_1 \otimes \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + D_2 \otimes \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + D_3 \otimes \begin{pmatrix} 0 \\ 0 \\ 1 \\ \vdots \\ 0 \\ 0 \end{pmatrix} + \cdots + D_{13} \otimes \begin{pmatrix} 0 \\ \vdots \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix}. \tag{6}$$

The vector $\boldsymbol{D}$ and time-points encoded by binary values are known for the copyright owner. He can covert the first part of every direct product (amplitude information) to a binary data, and the number of binary values exactly equals to that of quantum audio carrier's amplitudes encoded. Based on Table 1, the binary values of watermark can be extracted by getting the binary values of lowest two bit planes, successively. The extracting process can be described in details as follows.

Step 1 The copyright owner firstly confirms the positions of watermark embedded in quantum audio carrier. The corresponding amplitudes can be extracted in term of Eq. (6).

Step 2 Get the binary value of the lowest two bit planes $D_i^1 D_i^0$ of each amplitudes successively. The bits denoted by $D_i^1 D_i^0$ can be extracted according to the Eq. (6) and the logical relationship in Table 1. Then the binary sequence of scrambled watermark W can be extracted from quantum audio carrier.

Step 3 The correct binary sequence of watermark can be recovered according to the scrambling key K and R.

The LSQb extracting module based on the logical relationship is given by Fig. 8. An image with 2×2 pixels as scrambled watermark can be denoted as $w_i = \{0,0,1,1\}$, where $i \in \{0,1,2,3\}$. Taking the quantum audio in Fig. 1 as example, the quantum extracting circuit of watermark is shown in Fig. 9.

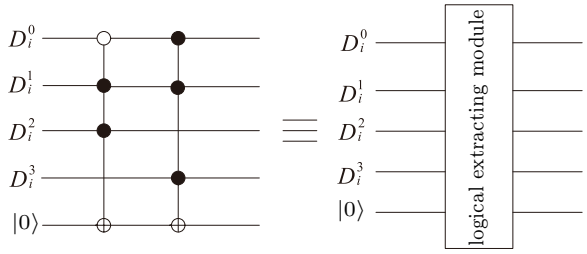


Fig. 8. The extracting module based on the logical relationship in Table 1.

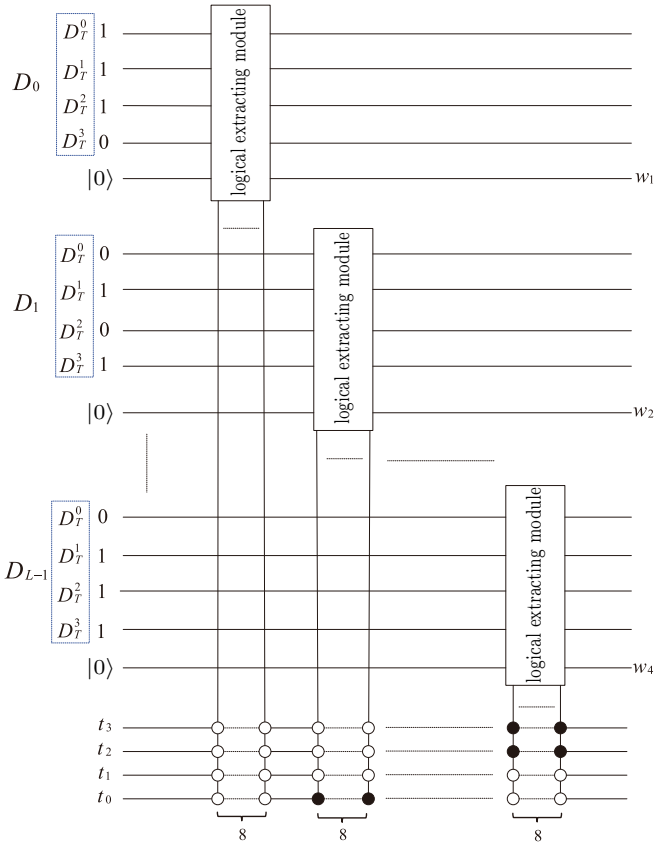


Fig. 9. A concrete example for extracting the watermark image with the size of 2×2.

4. Simulation-based experiments and analysis

4.1. The evaluation criteria of audio quality

Because that the signal to noise ratio (SNR) is generally used to evaluate the quality of stegano audio, in this paper, we also adopt this evaluation criteria to evaluate transparency of our new watermarking algorithm. If the quality of an audio does not change obviously after embedding watermark, it indicates that the algorithm has good transparency.

SNR is also widely used for the objective evaluation of the audio quality. The definition of SNR is the ratio of signal to noise in an electronic system. The noise is regarded as an additional signal that produced by the electronic system, which does not exist in the original signal. Due to that watermark can be regarded as a kind of noise, the transparency of the watermark can be effectively evaluated by SNR. The calculation formula of SNR is defined as

$$\mathrm{SNR} = 10\lg\left(\frac{P_\mathrm{s}}{P_\mathrm{N}}\right), \tag{7}$$

where its unit is dB, and P_s and P_N represent the effective power of the signal and noise, respectively.

4.2. Experimental simulation and results

The transparency and robustness of the new algorithm can be demonstrated by simulation experiments on MATLAB

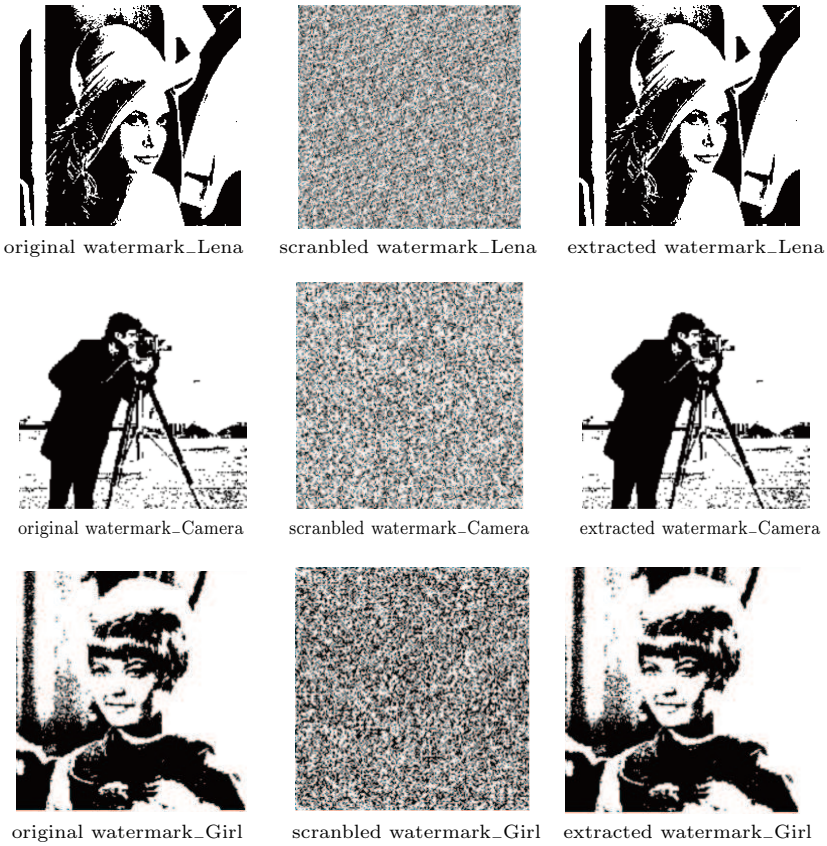


Fig. 10. Three binary watermark images. The left images are original watermarks, the medium images are scrambled watermarks, and the right image are extracted watermarks.

R2014a. The audios used in the simulation experiments are based on WAV format, and provided by Microsoft Windows itself without any compression. For digital audio, some changes to the least significant bits will not affect the audio auditory effect apparently. The experimental audios used are labeled as WAV1 and WAV2. Besides that, in order to facilitate the simulation, we choose three binary images as watermarks to be embedded into the audio, as shown in Fig. 10. The corresponding scrambled watermarked images are named as Watermark_Lena, Watermark_Camera, and Watermark_Girl.

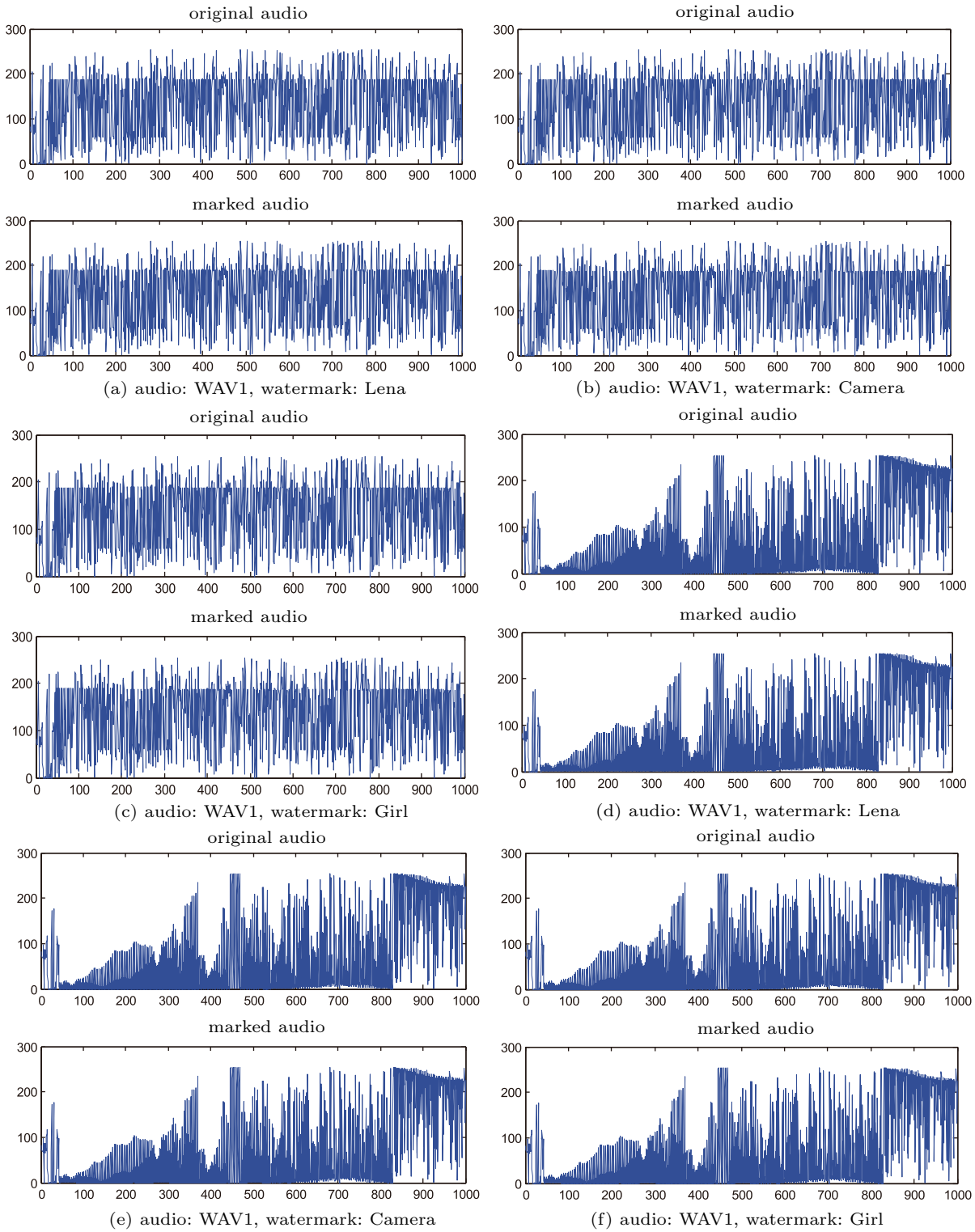


Fig. 11. (color online) Simulation waveforms of the original and marked quantum audio for embedding different binary images. (a) The audio carrier is WAV1 and the watermark image is Lena, (b) the audio carrier is WAV1 and the watermark image is Camera, (c) the audio carrier is WAV1 and the watermark image is Girl, (d) the audio carrier is WAV2 and the watermark image is Lena, (e) the audio carrier is WAV2 and the watermark image is Camera, and (f) the audio carrier is WAV2 and the watermark image is Girl.

4.2.1. Transparency experiment

The simulations are demonstrated on a computer with Intel(R) Core(TM) i5-2400 CPU3.10 GHZ 4GB RAM, and 64-bit operating system. Based on the logical relationship in Table 1, the experimental results are shown in Fig. 11. The SNR values of the three embedded binary images are presented in Table 2.

Table 2. SNR values of three examples used in the simulation.

Audio	Binary watermark image	SNR/dB
WAV1	Lena	59.4628
WAV1	Camera	59.3266
WAV1	Girl	58.9347
WAV2	Lena	57.2553
WAV2	Camera	56.8298
WAV2	Girl	56.6542

From the simulation waveforms given in Fig. 11, it can be seen that no matter what the embedded watermark is, the waveforms of the original audio and the stegano audio are virtually identical. This means that it is nearly impossible for a third party to detect the watermark embedded in the audio by ears. So transparency of the watermark is good. Besides, from Table 2, it can be seen that the SNR values are high enough for all the stegano quantum audios after combining different carriers and watermarks. It further proves that our new algorithm has very good transparency.

4.2.2. Robustness experiment under noise channel

In an open quantum channel interacted with external environment, the transmitted qubits are susceptible to the noise. To demonstrate the robustness of the proposed watermarking algorithm under noise attacks, the related simulation and analysis on four Pauli noise attacks are presented in this section.

In general, there are four common quantum noises including $\boldsymbol{\sigma}_{\mathrm{I}}$, $\boldsymbol{\sigma}_x$, $\boldsymbol{\sigma}_y$, and $\boldsymbol{\sigma}_z$. Since they belong to Pauli matrix, they are also called as four Pauli matrix noises. The specific definitions are given as

$$\boldsymbol{\sigma}_{\mathrm{I}} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \quad \boldsymbol{\sigma}_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix},$$
$$\boldsymbol{\sigma}_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad \boldsymbol{\sigma}_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}. \tag{8}$$

Herein, $\boldsymbol{\sigma}_{\mathrm{I}}$ is unitary matrix and it means that there is no noise effect on qubit. $\boldsymbol{\sigma}_x$ is the bit-flip and $\boldsymbol{\sigma}_z$ is the phase-flip. $\boldsymbol{\sigma}_y = \mathrm{i}\boldsymbol{\sigma}_x\boldsymbol{\sigma}_z$ is the superposition of $\boldsymbol{\sigma}_x$ and $\boldsymbol{\sigma}_z$ excepting a global phase of $\pi/2$. Obviously, the types of noise that really need to be discussed are only $\boldsymbol{\sigma}_x$, $\boldsymbol{\sigma}_y$, and $\boldsymbol{\sigma}_z$.

(i) The bit-flip noise $\boldsymbol{\sigma}_x$. Simply speaking, the effect of this noise is to cause $|0\rangle \to |1\rangle$ and $|1\rangle \to |0\rangle$. No matter for quantum carrier audio represented by QRDA, or quantum image watermark represented by NEQR, the amplitude values or pixel values are all encoded by binary qubit sequences. It is easy to know that bit-flip noise $\boldsymbol{\sigma}_x$ can cause direct influence on quantum carrier audio and quantum watermark.

Due to quantum computer is not yet available for us, it is impossible to simulate the bit-flip $\boldsymbol{\sigma}_x$ noise on a quantum computer directly. Because the Gauss–White noise in classical channel can perform bit-flip on any position of classical binary bit sequences, in this paper, the simulation experiment of Gauss–White noise attack on classical computer is carried out effectively to evaluate the influence of bit-flip noise on the proposed algorithm and prove the robustness of watermark in the new algorithm. The experimental results are shown in Fig. 12. The SNR values of three embedded binary image watermarks are presented in Table 3.



Fig. 12. Three extracted watermarks under Gauss–White noise attack.

Table 3. SNR values of three examples under Gauss–White noise attack.

Audio	Binary watermark image	SNR/dB
WAV1	Lena	50.4038
WAV1	Camera	49.6576
WAV1	Girl	47.8630
WAV2	Lena	49.3523
WAV2	Camera	48.2176
WAV2	Girl	47.4805

From the simulation results given in Fig. 12 and Table 3, although the SNR values of watermarks are slightly reduced compared with the original watermarks, their visual qualities have no obvious changes and the watermarks still have high fidelity. It proved that the new algorithm has good robustness and can effectively resist on bit-flip noise attack.

(ii) The phase-flip noise $\boldsymbol{\sigma}_z$. The effect of this noise is to

cause $|0\rangle \rightarrow |0\rangle$ and $|1\rangle \rightarrow -|1\rangle$. As mentioned above, due to quantum audio amplitude and quantum image pixels are all encoded by binary qubit sequences, the phase-flip noise will not have substantial effect on the quantum carrier audio and quantum image watermark. As a result, the new algorithm can effectively resist phase-flip noise attack to obtain good robustness.

(iii) The bit and phase-flip noise $\boldsymbol{\sigma}_y$. It is a superposition of the noises of $\boldsymbol{\sigma}_x$ and $\boldsymbol{\sigma}_z$ excepting a global phase of $\pi/2$. As mentioned above, phase-flip noise $\boldsymbol{\sigma}_z$ has no substantial effect on quantum carrier audio and quantum image watermark, while only bit-flip noise $\boldsymbol{\sigma}_x$ has effect. Therefore, the influence on robustness of the new algorithm caused by the noise $\boldsymbol{\sigma}_y$ can be simplified to be that of the bit-flip noise $\boldsymbol{\sigma}_x$. Consequently, the relevant simulation and analysis of the bit-flip noise also can prove that the proposed algorithm has good robustness to resist on the bit and phase-flip noise $\boldsymbol{\sigma}_y$.

In conclusion, the new algorithm can achieve good robustness to resist on the four quantum Pauli noises.

5. Performance analysis

5.1. Transparency

In the new algorithm, the embedding positions (third or fourth bit plane) of watermark based on logical relationship can be adjusted by modifying $D_i^1 D_i^0$. The embedding of watermark does not modify the binary values in high-level bit planes of amplitudes. So it avoids obvious distortion to audio carrier caused by substituting corresponding bit values of amplitudes with the binary values of watermark's pixels. In addition, the simulation waveforms and SNR values show that it is nearly impossible to detect the embedded watermark in stegano quantum audio by ears for any third parties. It proves that the new algorithm has good transparency.

5.2. Security

In this paper, the embedding positions of watermark are indirectly selected by using the four low bit planes of amplitudes based on logical relationship, which enhances the link between bit values of watermark pixels and binary values of amplitudes in quantum audio carrier. Besides, embedding positions (in third or fourth bit plane) of watermark based on logical relationship can be dynamically adjusted by modifying $D_i^1 D_i^0$. As a result, compared with previous quantum watermarking algorithms, embedding positions of watermark are dynamic rather than fixed. It means that, for illegal third parties, it is more difficult to find out the correct positions of embedding watermark. Thus, the new algorithm can greatly enhance watermark's security.

5.3. Robustness

In the new algorithm, embedding positions of watermark are determined by the logical relationship between binary values of four lowest bit planes of amplitudes in quantum audio carrier. By virtue of this logical relationship, the inner connection between four low bit planes of amplitudes can be used to effectively improve the robustness of watermark embedded into quantum audio carrier. At least, it is easy to know that its robustness will be better than that of previous algorithms in which LSQb modification is simply adopted to embed watermark. Furthermore, in a open network environment, the new proposed algorithm can effectively resist illegal attacks. The reason is that, for the illegal third parties, it is very hard or even impossible to know the correct embedding positions of watermark. Under this circumstance, illegal attacks will focus on LSQb values of amplitudes in quantum audio carrier to remove watermark. Consequently, the bits of watermark embedded into the third bit plane or the fourth bit plane will not be affected. In summary, the new algorithm can improve the robustness of watermark.

6. Conclusion

In this paper, an improved watermarking algorithm based on LSQb modification for quantum audio is proposed. Compared with previous algorithms, it substitutes the least significant bits of corresponding amplitudes of quantum audio carrier with the binary values of watermark pixels by utilizing the logical relationship between the sub-low bit planes and lowest bit plane of quantum audio amplitudes, for achieving better transparency, security, and robustness. The new algorithm can enhance the connection between watermark's bits and binary values of amplitudes, and realize dynamically embedding and extracting of watermark image. In order to implement the new watermarking algorithm, the unique quantum circuits are designed to realize embedding and extracting processes of watermark. In addition, these quantum circuits make it possible for the new algorithm to obtain better usability and scalability. The SNR values and simulation waveforms in the experimental results prove that the watermarking algorithm proposed achieves good transparency, good security, and strong robustness.

References

[1] Xia Z H, Wang X H, Zhang L G, Qin Z, Sun X M and Ren K 2016 *IEEE T. Inf. Foren. Sec.* **11** 2594

[2] Fu Z J, Sun X M and Xi J 2015 *J. Commun. Netw.* **17** 525

[3] Fu Z J, Ren K, Shu J G, Sun X M and Huang F X 2016 *IEEE T. Parall. Distr.* **27** 2546

[4] Qu Z G, Keeney J, Robitzsch S, Zaman F and Wang X J 2016 *China Commun.* **13** 108

[5] Liu Q, Cai W D, Shen J, Fu Z J, Liu X D and Linge N 2016 *Secur. Commun. Netw.* **9** 4002

[6] Bennett C H and Brassard G 2012 *IEEE. Int. Conf. Comput. Syst. Sig. Process.* **2012** 175
[7] Xu P, Wang Y, Bao H Z, Wang Y and Bao H Z 2017 *Chin. Phys. Lett.* **34** 20302
[8] Jiang M S, Zhou C and Wang Y 2017 *Chin. Phys. B* **26** 020303
[9] Kulik S P, Molotkov S N and Radchenko I V 2012 *JETP Lett.* **96** 336
[10] Yang Y G, Cao W F and Wen Q Y 2010 *Chin. Phys. B* **19** 050306
[11] Zhu Z C, Zhang Y Q and Fu A M 2012 *Chin. Phys. B* **21** 010307
[12] Guo Y, Shi J J and Liang J W 2016 *Acta Phys. Sin.* **65** 160301 (in Chinese)
[13] Bostrom K and Felbinger T 2012 *Phys. Rev. Lett* **89** 187902
[14] Zhao G, Cao Z W, Feng X Y and Peng J Y 2016 *Acta Phys. Sin.* **65** 230301 (in Chinese)
[15] Liu Z H, Chen H W and Liu W J 2016 *Chin. Phys. Lett.* **33** 070305
[16] Wang M M, Chen X B and Yang Y X 2013 *Sci. China Phys. Mech.* **56** 1636
[17] Xu S J, Chen X B, Niu X X and Yang Y X 2013 *Sci. China Phys. Mech.* **56** 1745
[18] Le P Q, Dong F and Hirota K 2010 *Quantum Inf. Process.* **10** 63
[19] Abdullah M I, Phuc Q L, Dong F Y and Hirota K 2012 *Inform. Sciences* **186** 126
[20] Negin F and Mosayeb N 2012 *Int. J. Theor. Phys.* **51** 2094.
[21] Zhang W W, Gao F, Liu B, Jia H Y, Wen Q Y and Chen H 2013 *Int. J. Theor. Phys.* **52** 504
[22] Zhang W W, Gao F, Liu B, Wen Q Y and Chen H 2012 *Quantum Inf. Process.* **12** 793
[23] Song X H, Wang S, Ahmed A A E and Niu X M 2014 *Multimedia Syst.* **20** 379
[24] Wang N and Lin S 2015 *Chin. J. Quantum Electron.* **32** 263
[25] Jiang N, Zhao N and Wang L 2016 *Int. J. Theor. Phys.* **55** 107
[26] Miyake S and Nakamae K 2016 *Quantum Inf. Process.* **15** 1849
[27] Wang S, Sang J Z, Song X H and Niu X M 2015 *Measurement* **73** 352
[28] Wang J 2016 *Int. J. Theor. Phys.* **55** 1622
[29] Zhang Y, Lu K, Gao Y H and Wang M 2013 *Quantum Inf. Process.* **12** 2833