Optik 126 (2015) 3221–3226

Contents lists available at ScienceDirect

Optik

journal homepage: www.elsevier.de/ijleo

Quantum-assisted encryption for digital audio signals

Yu-Guang Yang[a,b,c,d,*], Ju Tian[a], Si-Jia Sun[a], Peng Xu[a]

[a] College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China
[b] State Key Laboratory of Information Security (Institute of Information Engineering, Chinese Academy of Sciences, Beijing 100093, China
[c] Beijing Key Laboratory of Trusted Computing, Beijing 100124, China
[d] National Engineering Laboratory for Critical Technologies of Information Security Classified Protection, Beijing 100124, China

ARTICLE INFO

Article history:
Received 19 June 2014
Accepted 19 July 2015

PACS:
03.67.Dd
03.67.Hk

Keywords:
Audio encryption
Quantum Fourier transform
Double random phase encoding

ABSTRACT

A novel quantum encryption method for audio signals is proposed. We introduce a novel quantum representation model for audio. The encryption principle is based on two secret random-phase encoding operations performed in both the input and quantum Fourier transform (QFT) planes of the proposed quantum representation model for audio respectively. Due to the reversibility of the quantum computation, the decryption process is the inverse of the encryption process. Simulation results and theoretical analyses show that the proposed approach offers a significant gain in terms of robustness, computational complexity and advantages over its classical counterparts. It opens the way for introducing audio encryption into quantum scenarios.

1. Introduction

With the fast development of Internet and the underlying applications, the secure transmission of multimedia data (such as audio, video and images) over the public channels has been more and more important over the last decades. The open nature of these channels makes data transfer over them vulnerable to various attacks and hence, multimedia content protection has become an essential requirement. Various techniques have been developed for content protection for different purposes, including watermarking, steganography and encryption technique and so on.

These remarks apply particularly to multimedia data encryption. Various physical-optics based methods for high dimensional data encryption have been proposed in past few years to increase the security level [1–4]. Although optical systems may be useful for security applications owing to their operation with parallelism and high speed, most optical encryption systems are far from satisfactory [5–8].

With the development of quantum computation, classical information processing is naturally extended to the quantum scenario. As a novel computing model, quantum computation can store, process and transport information using the peculiar properties of quantum mechanics [9] such as the superposition and entanglement. Quantum algorithms have been developed to demonstrate their proven efficiency over the classical versions [10,11]. Although a physical quantum computer has not been realized yet, it seems necessary to perform different information processing tasks involving various types of data on a quantum computer once realized physically.

Quantum information processing is focused on information whose physical representation is confined within the realm of quantum mechanics. Research on quantum information processing started with proposals on quantum representation for images and video [12–19]. Then various quantum information processing tasks were shown to be more efficient than their classical counterparts [9,20–48].

Audio, one of the most important information representation models, has been extensively used in modern society. In some cases such as secret commercial talks and audio evidence in court, digital audio must be hidden as secret information. In particular, more and more awareness of individual privacy protection stimulates the rapid development of audio encryption techniques. Therefore, audio encryption has drawn a great deal of attention from researchers and various schemes have been proposed for this purpose [49–51].

In contrast to quantum image processing, unfortunately, the discussion about audio encryption on a quantum computer has not been found yet. To solve the problem of audio encryption on a quantum computer, we propose a novel audio encryption method, following the idea of the double random phase encoding (DRPE)

* Corresponding author at: College of Computer Science and Technology, Beijing University of Technology, Beijing 100124, China. Tel.: +86 01067396818.
E-mail address: yangyang7357@bjut.edu.cn (Y.-G. Yang).

http://dx.doi.org/10.1016/j.ijleo.2015.07.082
0030-4026/

technique first proposed by Refregier and Javidi [1]. Combining the idea of the DRPE method and the merit of quantum computation, the proposed quantum encryption scheme for audio can make the audio completely confused. Thanks to the characters of quantum computation, the proposed method will improve the efficiency and security of audio encryption greatly.

The rest of this paper is organized as follows. The next section introduces a novel quantum representation model of audio. In Section 3, we describe our quantum encryption strategy for audio in detail. Section 4 is devoted to classical simulation and performance comparison. A brief conclusion is drawn in Section 5.

2. Quantum representation of audio

As we know, amplitude and frequency are two important parameters in describing audio. Amplitude and frequency denotes the magnitude and tone of audio respectively. The acquisition of digital audio begins by sampling the audio input in regular and discrete intervals of time and quantizing the sampled values into a discrete number of evenly spaced levels. Typical sampling rates range from 8 to 48 kHz [52]. Typical bit number per sample used for digital audio ranges from 8 to 16 bits. Digital audio displays as a digital data stream, it can be taken as 1-D data matrix. In classical scenario, several audio codecs (such as PCM, WMA, ADPCM, LPC, CELP, MP3, MPEG2 AAC, MPEG4 AAC, TwinVQ and Dolby AC3) have widely been used for digital audio encoding. By contrast, in quantum scenario, the information about audio can be extracted from the audio to generate a quantum representation of audio as follows:

$$|I(\theta)\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|c_j\rangle \otimes |j\rangle, \tag{1}$$

$$|c_j\rangle = (|0\rangle + e^{i\theta_j}|1\rangle) \tag{2}$$

where N denotes the number of samples in each audio data block. $|c_j\rangle$ represent the amplitude at the jth sample point. $\theta_j \in \left[0, \frac{\pi}{2}\right], j = 0, 1, \cdots, N-1$ encode the information about amplitude information. $|0\rangle$ and $|1\rangle$ are two dimensional computational basis quantum states. For $j = 0, 1, \cdots, N-1$, $|j\rangle$ are N-dimensional computational basis quantum states and represent the position information of the jth sample point. There are two parts in the quantum audio representation: $|c_j\rangle$ and $|j\rangle$ which encode the amplitude and position information of the jth sample point, respectively. To perform operation on the amplitude information, a phase gate $U = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\psi_j} \end{bmatrix}$ can be performed on $|c_j\rangle$.

3. Digital audio encryption and decryption process

To solve the problem of audio encryption on a quantum computer, a novel audio encryption method is proposed, which utilizes QFT and DRPE [1].

3.1. Digital audio encryption

As shown in Section 2, a quantum audio is written as $|I(\theta)\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|c_j\rangle \otimes |j\rangle$, where $|c_j\rangle$ represent the amplitude information. Assume the original quantum audio is $|O\rangle = \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|c_j\rangle \otimes |j\rangle$, the keys for spatial and QFT domain are phase operations $U_{K_1} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\psi_j} \end{bmatrix}$ and $U_{K_2} = \begin{bmatrix} 1 & 0 \\ 0 & e^{i\upsilon_j} \end{bmatrix}$, respectively. Here ψ_j, υ_j are real numbers and distributed uniformly between 0 and 2π. In the following, E_{Ki} and $E_{K_i}^{-1}$, $i = 1, 2$ denote the encryption and decryption functions, respectively.

Step 1. Encode the original audio in spatial domain to get $|M\rangle$ using the key K_1.

$$\begin{aligned} |M\rangle &= E_{K_1}|O\rangle = U_{K_1} \otimes I_N|O\rangle \\ &= U_{K_1} \otimes I_N \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|c_j\rangle \otimes |j\rangle \\ &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}U_{K_1}|c_j\rangle \otimes |j\rangle \\ &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|d_j\rangle \otimes |j\rangle. \end{aligned} \tag{3}$$

Here,

$$|d_j\rangle = (|0\rangle + e^{i(\theta_j+\psi_j)}|1\rangle). \tag{4}$$

Step 2. Execute QFT on $|M\rangle$ to get its QFT form, $QFT(|M\rangle)$, shown as follows.

$$QFT(|M\rangle) = QFT\left(\frac{1}{2\sqrt{N}}\sum_{j=0}^{N-1}|d_j\rangle \otimes |j\rangle\right). \tag{5}$$

Here, the QFT on an orthonormal basis $|0\rangle, \cdots, |N-1\rangle$ is defined to be a linear operator with the following action on the basis states,

$$QFT : |j\rangle \to \frac{1}{\sqrt{N}}\sum_{k=0}^{N-1}e^{2\pi ijk/N}|k\rangle. \tag{6}$$

Step 3. Encrypt $QFT(|M\rangle)$ using the key K_2, and get $|M_1\rangle$.

$$\begin{aligned} |M_1\rangle &= E_{K_2}QFT(|M\rangle) \\ &= U_{K_2} \otimes I_N QFT(|M\rangle) \\ &= U_{K_2} \otimes I_N QFT\left(\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}|d_j\rangle \otimes |j\rangle\right) \\ &= \frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}U_{K_2}QFT\left(|d_j\rangle \otimes |j\rangle\right). \end{aligned} \tag{7}$$

Step 4. Execute the inverse QFT to get the quantum cipher audio $|C\rangle$ expect as follows.

$$\begin{aligned} |C\rangle &= inQFT(|M_1\rangle) \\ &= inQFT\left(\frac{1}{\sqrt{N}}\sum_{j=0}^{N-1}U_{K_2}QFT\left(|d_j\rangle \otimes |j\rangle\right)\right). \end{aligned} \tag{8}$$

Here the inverse QFT is the implementation of the quantum circuit of QFT in the reverse order.

3.2. Digital audio decryption

In this phase, only two keys are needed to decrypt the cipher audio, i.e. the phase operations U_{K_1} and U_{K_2}. Because all the quantum operations are unitary, the decryption procedure is just the inverse with the encryption procedure. Our decrypting procedure is as follows.