信息与控制　2021 年　第 50 卷　第 5 期：513 ~ 521

DOI：10.13976/j.cnki.xk.2021.0471　　文章编号：1002 - 0411(2021) - 05 - 0513 - 09

基于量子信息处理的量子零水印算法

张景波，张云琦

长春电子科技学院，吉林 长春　130114

通信作者：张云琦，bozhangjing123@163.com　收稿/录用/修回：2020 - 10 - 13/2020 - 12 - 15/2020 - 12 - 28

摘要

基于量子信息处理提出了一种量子音频的零水印算法. 首先利用量子离散余弦变换在宿主量子音频频域内的低频区域提取一组量子序列，然后利用 Henon 映射对该序列执行加密算法，从而生成量子零水印. 通过将 Henon 映射的量子线路作为零水印的量子秘钥，有效地提高了量子零水印算法的安全性. 本文设计了量子 Henon 映射置乱和量子零水印生成及提取算法的线路图，对零水印算法的可行性进行了验证. 仿真实验表明，与现有的量子音频水印算法相比，本文提出的量子零水印算法具有更好的不可感知性及鲁棒性.

关键词

量子信息处理

量子离散余弦变换

量子 Henon 映射加密

量子零水印

中图法分类号：TP391

文献标识码：A

Quantum Zero-watermark Algorithm Based on Quantum Information Processing

ZHANG Jingbo, ZHANG Yunqi

Changchun College of Electronil Technology, *Changchun* 130114, *China*

Abstract

Based on quantum information processing, a zero watermarking algorithm for quantum audio is proposed. Firstly, a set of quantum sequences are extracted in the low frequency region of the host quantum audio frequency domain by quantum discrete cosine transform, and then the sequence is encrypted by Henon mapping to generate quantum zero watermark. By using the quantum circuit of Henon mapping as the quantum secret key of zero watermark, the security of quantum zero watermark algorithm is effectively improved. This paper designs the circuit diagram of quantum Henon map scrambling and quantum zero watermark generation and extraction algorithm, and verifies the feasibility of the zero watermark algorithm. Simulation results show that compared with the existing quantum audio watermarking algorithms, the quantum zero watermarking algorithm proposed in this paper has better imperceptibility and robustness.

Keywords

quantum information processing;

quantum discrete cosine transform;

quantum Henon map encryption;

quantum zero-watermark

0　引言

量子计算和量子信息处理在并行计算、多任务处理及高效存储等方面展现出了巨大潜力，可以解决或改进传统领域中难以处理或计算的难题. 1982 年，来自美国的物理学家 Feynman 首次提出了量子计算的概念[1]. 他指出直接利用经典计算机来模拟指数级增长的量子力学系统存在本质的困难，以此为基础创建的量子计算机对某些问题的处理能力将远远超过经典计算机. 这一理论的提出奠定了量子计算的基础. 1985 年，Deutsch 提出是否可以利用量子力学这一物理学的最终规律，根据经典图灵机的构造，创造出一种能够有效模拟任意物理系统的计算装置[2]. 特别地，他指出利用量子态的相干叠加性可以实现并行的量子计算，而且可以更加高效地解决在经典领域中存在的问题. 1994 年，Shor 提出大数因子分解问题和离散对数问题在量子计算领域范围内可以得到有效的解决[3]. 由于这两个问题在传统领域内没有有效的解决方法，使得以它们的计算安全为理论基础的经典保密通讯技术如 RSA(Ron Rivest、Adi Shamir、Leonard Adleman)公钥密码体制[4]，受到了严峻的挑战. 同时，量子信息处理作为一种计算工具越来越多地应用于计算机科学领域，如量子机器学习[5]和量子图像处理[6]等. 量子计算基于量子力学的理论体系，完全超脱于经典计算模式及宏观概念.

量子计算机在计算速度和信息存储能力方面相比于经

典计算机有着本质的超越，这种内在的计算优势使得很多学者相信经典计算机与量子计算机之间在计算能力上的差距是无法逾越的. 因此，在不久的将来，经典计算机在传统领域中的统治地位定会被一种更加成熟的计算模型所取代. 无论在存储效率及计算能力上传统计算机都将被全面超越. 此外，量子信息技术不仅仅局限于量子计算方面，在量子通讯(quantum information)[7]、量子密码学(quantum cryptography)[8]、量子隐形传态(quantum teleportation)[9-10]及量子密集编码(quantum dense coding)[11]等领域的发展也颇有成效. 最近，如何利用量子计算解决数字音频处理领域中的问题引起了中外学者的广泛关注[12-17].

2017 年，Yan 等[18]提出了一种可以双极表示数字音频振幅信息的量子表达式(flexible representation of quantum audio，FRQA)，这种表达式在直观上更加接近传统领域对数字音频的表示方法和真实的数字音频波形. 更重要地是，FRQA 可以更加方便而有效地执行量子音频的基础操作. 另外，水印技术利用特殊的信息嵌入方法，把要传递的信息隐藏在宿主信息中. 基于 FRQA 表达式，Chen 等提出了两种基于量子离散余弦变换(quantum discrete cosine transform，qDCT)的量子音频水印算法[19]. 利用 qDCT 很强的“能量集中”特性，即大多数的自然信号(如声音和图像)的能量都集中在离散余弦变换后的低频部分，提出了量子音频水印算法和分段量子音频水印算法，最后利用仿真实验对两种算法的不可感知性和鲁棒性进行了对比和分析.

本文针对算法的不可感知性和鲁棒性，提出了一种量子音频零水印算法. 利用量子离散余弦变换作用于宿主量子音频，基于加密后的频域内低频分量的序列特点生成该宿主量子音频的水印信息. 本文提出的算法与现有量子音频水印方法的最大区别是已有量子音频水印算法的水印信息可以是一幅量子图像或一段量子音频，再将量子水印信息嵌入到宿主量子音频中，而量子音频零水印的水印信息是通过宿主量子音频自身的结构特点提取出的一串不规则的二进制数列. 因此，本文提出的算法具有更好的不可感知性和更强的鲁棒性.

1 FRQA 及量子操作单元

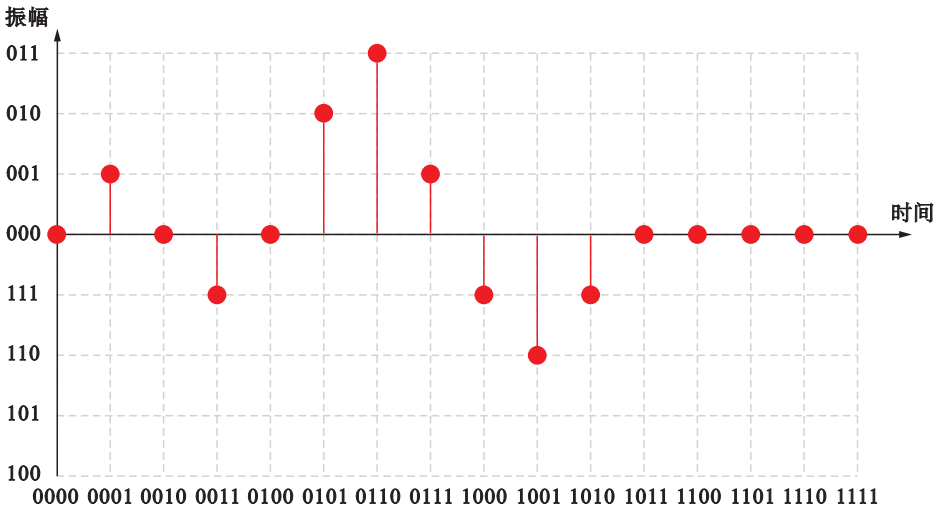
1.1 FRQA 表达式

对于一个长度为 2^l 的数字音频，其对应的 FRQA 表达式为

$$|Q_A\rangle=\frac{1}{2^{2^l}}\sum_{t=0}^{2^l-1}|Q_t\rangle\otimes|t\rangle \tag{1}$$

其中，$|A_t\rangle=|A_t^{q-1}\cdots A_t^1A_t^0\rangle$ 对每一个振幅利用二进制补码的方式进行编码，$|t\rangle=|t_{l-1}\cdots t_1t_0\rangle$，$t_i\in\{0,1\}$ 记录了与振幅对应的时间信息. 量子态 $|Q_A\rangle$ 是归一化的，满足 $\||Q_A\rangle\|=1$. 从式(1)可以看出，FRQA 需要 $q+l$ 个量子位表示具有 2^l 个采样点的量子音频信号.

在图 1 中展示了一段音频信号及如何用 FRQA 表达式对其进行表示. 在这个例子中，振幅的取值都是在 -2 到 3 之间，因此仅仅需要 3 个量子比特编码音频的振幅信息. 音频的长度是 13，故 $l=\lceil \mathrm{lb}13\rceil=4$，因此，共需要 7 个量子位对这个 FRQA 量子音频进行表示.



$$|Q_A\rangle=\frac{1}{\sqrt{2}^4}(|000\rangle\otimes|0000\rangle+|001\rangle\otimes|0001\rangle+|000\rangle\otimes|0010\rangle+|111\rangle\otimes|0011\rangle+|000\rangle\otimes|0100\rangle+|010\rangle\otimes|0101\rangle+$$
$$|011\rangle\otimes|0110\rangle+|001\rangle\otimes|0111\rangle+|111\rangle\otimes|1000\rangle+|100\rangle\otimes|1001\rangle+|111\rangle\otimes|1010\rangle+|000\rangle\otimes|1011\rangle+$$
$$|000\rangle\otimes|1100\rangle+|000\rangle\otimes|1101\rangle+|000\rangle\otimes|1100\rangle+|000\rangle\otimes|1111\rangle)$$

图 1 音频示例及对应的 FRQA 表达式量子态

Fig.1 A segment of audio and its corresponding FRQA representation quantum state

1.2 量子逻辑门

在量子算法中，常常需要对输入的量子态进行一系列的变换操作以完成特定的逻辑功能. 量子逻辑门可以在一定的时间间隔内完成不同量子态之间的逻辑转换[20-21]，从而实现简单的逻辑运算. 表 1 中的非门可以对一个量子位的态取反，用符号 X 表示. Hadamard 门(H 门)通常可以

对一系列量子基本态执行初始化操作，对应计算过程如式(2)所示：

$$(\underbrace{\boldsymbol{H}\otimes\boldsymbol{H}\otimes\boldsymbol{H}\otimes\cdots\otimes\boldsymbol{H}}_{n})\underbrace{|00\cdots0\rangle}_{n}=\frac{1}{\sqrt{2^n}}\sum_{x=0}^{2^n-1}|x\rangle \quad (2)$$

表 1　量子逻辑门

Tab.1　Quantum logic gates

量子门	公式	转换	符号
非门	$X=\|0\rangle\langle1\|+\|1\rangle\langle0\|$	$X\|0\rangle=\|1\rangle$ $X\|1\rangle=\|0\rangle$	
H 门	$H=\frac{\|0\rangle+\|1\rangle}{\sqrt{2}}\langle0\|+\frac{\|0\rangle-\|1\rangle}{\sqrt{2}}\langle1\|$	$H\|0\rangle=\frac{1}{\sqrt{2}}(\|0\rangle+\|1\rangle)$	
控非门	$\mathrm{CNOT}=\|0\rangle\langle0\|\otimes I+\|1\rangle\langle1\|\otimes X$	$\mathrm{CNOT}\|00\rangle=\|00\rangle$ $\mathrm{CNOT}\|01\rangle=\|01\rangle$ $\mathrm{CNOT}\|10\rangle=\|11\rangle$ $\mathrm{CNOT}\|11\rangle=\|10\rangle$	

当量子寄存器中的 n 个量子位的量子态都为$|0\rangle$时，H 变换分别作用于 n 个量子位会生成 2^n 个基本态的线性叠加，也可理解为经过 H 变换的作用后，量子态$|00\cdots0\rangle$转换为从 0 到 2^n-1 所有二进制数的线性叠加，它们存在的概率均为 $1/2^n$.

受控非门作用于两个量子位，对于量子态$|xy\rangle$，当$|x\rangle$为$|0\rangle$时，$|y\rangle$保持原有的量子态不变；当$|x\rangle$为$|1\rangle$时，$|y\rangle$执行取反操作，具体执行过程可以表述为

$$\mathrm{CNOT}|x,y\rangle=|x,x\oplus y\rangle \quad (3)$$

该变换实现了异或功能，故亦称 CNOT 门为量子异或门.

1.3　量子加法器

在文[20]中最先介绍了利用量子信息处理框架解决量子加法的计算问题，其目的是进行如下量子态之间的转换：

$$|x,y\rangle\rightarrow|x,x+y\rangle \quad (4)$$

其中，$|x\rangle$和$|y\rangle$是两个量子态的输入，而输出为$|x\rangle$和$|x+y\rangle$. 如图 2 所示，量子加法器由 $2n-1$ 个进位模块(图中的“Carry”)和 $2n$ 个求和模块(图中的“Sum”)组成. 此外，进位模块由 2 个 Toffoli 门和 1 个 CNOT 门组成，求和模块由 2 个 CNOT 门组成，如图 2 中(b)和(c)所示.

图 2　量子加法器

Fig.2　Quantum adder

2　量子离散余弦变换

离散余弦变换(discrete cosine transform，DCT)在信号和图像处理领域的应用非常广泛，特别是对于有损压缩，例如 MP3 格式的数字音频压缩和 JPEG 格式的数字图像压缩[22]. 这些应用都利用了 DCT 很强的“能量集中”特性. 信号的 DCT 运算可以将其从时域变换到频域. DCT 作用于音频或图像后，大部分信号信息往往集中在少量的低频分量中. 基于量子计算的 DCT 实现是一个非常复杂的过程，可以利用式(5)来实现量子 DCT[23]，表示为 qDCT：

$$\mathrm{qDCT}(|x\rangle)=g(x)\sum_{c=0}^{2^m-1}\cos\left[\frac{\pi}{N}\left(c+\frac{1}{2}\right)x\right]|c\rangle \quad (5)$$

其中，用 m 个量子位编码的$|x\rangle$可以记录信号中一系列采样振幅的叠加态. 在执行 qDCT 的变换操作后，$|x\rangle$被转化为$|c\rangle$，而$|c\rangle$用来记录在频域内采样点的振幅信息. 计算 qDCT 的方程为

$$\boldsymbol{U}_N^{\dagger}\cdot\boldsymbol{F}_{2N}\cdot\boldsymbol{V}_N=\boldsymbol{C}_N\oplus(-i)\boldsymbol{S}_N \quad (6)$$

其中，

$$\boldsymbol{V}_N=\frac{1}{\sqrt{2}}\begin{pmatrix}1 & & & 1 & & \\ & \ddots & & & \ddots & \\ & & 1 & & & 1\\ & & 1 & & & -1\\ & \iddots & & & \iddots & \\ 1 & & & -1 & & \end{pmatrix} \quad (7)$$

同时，$\omega=\exp(2\pi i/4N)$，其中，$i^2=-1$.

从式(7)中可以得出 $\boldsymbol{V}_N=\boldsymbol{\pi}_1(\boldsymbol{H}\otimes\boldsymbol{1}_{N\times N})$，其中，$\boldsymbol{\pi}_1$ 是常量，$\boldsymbol{1}_{N\times N}$是含有 N 行 N 列的单位矩阵. $\otimes$表示张量积，$\boldsymbol{H}$ 指广泛应用于量子计算中的 Hadamard 矩阵. 此外，需要定义一个函数操作 $\boldsymbol{\pi}_1$：在$0\leqslant x<2^n$ 的条件下，$\boldsymbol{\pi}_1|0x\rangle=|0x\rangle$且 $\boldsymbol{\pi}_1|1x\rangle=|1\bar{x}\rangle$. $\bar{x}$ 表示对 x 中的量子比特取反的操作，其线路图包含 1 个量子控制比特和 n 个 NOT 门.

实现 $\boldsymbol{U}_N$ 对于量子态的计算包括如下 4 种情况：

$$\begin{aligned}&\boldsymbol{U}_N|0\boldsymbol{0}\rangle=|0\boldsymbol{0}\rangle,\ \boldsymbol{U}_N|0\boldsymbol{1}\rangle=(-1)|1\boldsymbol{0}\rangle\\&\boldsymbol{U}_N|0x\rangle=\frac{\bar{\omega}^x}{\sqrt{2}}|0x\rangle+\frac{\omega^x}{\sqrt{2}}|1x'\rangle\\&\boldsymbol{U}_N|1y\rangle=-\frac{i\bar{\omega}^{y+1}}{\sqrt{2}}|0(y+1\bmod 2^n)\rangle+\frac{i\omega^{y+1}}{\sqrt{2}}|1\bar{y}\rangle\end{aligned}\tag{8}$$

其中，x 的取值范围为 $1\leqslant x<2^n$，而 y 的取值范围为 $0\leqslant y<2^n-1$，$\boldsymbol{0}$ 和 $\boldsymbol{1}$ 分别表示含有 n 个量子位的$|0\cdots0\rangle$态和$|1\cdots1\rangle$态. 同时，对 $\boldsymbol{D}_1$ 和 $\boldsymbol{T}_N$ 进行定义：

$$\boldsymbol{D}_1=\mathrm{diag}(1,\omega,\cdots,\omega^{N-1},\bar{\omega}^N,\cdots,\bar{\omega}^2,\bar{\omega})\tag{9}$$

另外，

$$\boldsymbol{T}_N=\begin{pmatrix}1&&&&&&&&\\&\frac{1}{\sqrt{2}}&&&&&\frac{i}{\sqrt{2}}&&\\&&\ddots&&&\iddots&&&\\&&&\frac{1}{\sqrt{2}}&&\frac{i}{\sqrt{2}}&&&\\&&&&1&&&&\\&&&\frac{1}{\sqrt{2}}&&-\frac{i}{\sqrt{2}}&&&\\&&\iddots&&&\ddots&&&\\&\frac{1}{\sqrt{2}}&&&&&-\frac{i}{\sqrt{2}}&&\\&&&&&&&&1\end{pmatrix}\tag{10}$$

其中，$\boldsymbol{D}_1$ 是一个对角矩阵，$\boldsymbol{T}_N$ 可以执行如下的操作：

$$\begin{aligned}&\boldsymbol{T}_N|0\boldsymbol{0}\rangle=|0\boldsymbol{0}\rangle,\ \boldsymbol{T}_N|0x\rangle=\frac{1}{\sqrt{2}}|0x\rangle+\frac{1}{\sqrt{2}}|1x'\rangle\\&\boldsymbol{T}_N|1\boldsymbol{0}\rangle=|10\rangle,\ \boldsymbol{T}_N|1x\rangle=\frac{i}{\sqrt{2}}|0x\rangle-\frac{i}{\sqrt{2}}|1x'\rangle\end{aligned}\tag{11}$$

其中，x 的取值范围为 $1\leqslant x<2^n$，$i^2=-1$，此外，公式中 $x'=2^n-x$. 为了完成 $\boldsymbol{T}_N$ 的运算，有如下的操作单元 $\boldsymbol{D}$(如果忽略 $\boldsymbol{T}_N$ 中二进制补码的情况)：

$$\begin{aligned}&\boldsymbol{D}|0\boldsymbol{0}\rangle=|0\boldsymbol{0}\rangle,\ \boldsymbol{D}|0x\rangle=\frac{1}{\sqrt{2}}|0x\rangle+\frac{1}{\sqrt{2}}|1x\rangle\\&\boldsymbol{D}|1\boldsymbol{0}\rangle=|1\boldsymbol{0}\rangle,\ \boldsymbol{D}|1x\rangle=\frac{i}{\sqrt{2}}|0x\rangle-\frac{i}{\sqrt{2}}|1x\rangle\end{aligned}\tag{12}$$

为了实现式(12)中的操作，需要量子算符 $\boldsymbol{B}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&i\\1&-i\end{pmatrix}$. 然后，设计另外一种量子操作把量子态转换为其二进制补码的形式，即 $\boldsymbol{\pi}_2|0x\rangle=|0x\rangle$和 $\boldsymbol{\pi}_2|1x\rangle=|1x'\rangle$. 实现这两种操作的量子线路图如图 3 中(a)和(b)所示.

从式(12)中可以计算出 $\boldsymbol{T}_N=\boldsymbol{\pi}_2\boldsymbol{D}$. 这里图 3(b)所表示的 $\boldsymbol{P}_n$ 可以完成一种映射操作：$|x\rangle\rightarrow|x+1\bmod 2^n\rangle$. 为了计算式(9)中的 $\boldsymbol{D}_1$，需要定义式(13)中 $\boldsymbol{\Delta}_1$、$\boldsymbol{\Delta}_2$ 和 $\boldsymbol{C}$ 的 3 个操作算符：

$$\begin{aligned}&\boldsymbol{\Delta}_1=\mathrm{diag}(1,\omega,\cdots,\omega^{N-1})=\boldsymbol{L}_n\otimes\cdots\otimes\boldsymbol{L}_2\otimes\boldsymbol{L}_1\\&\boldsymbol{\Delta}_2=\mathrm{diag}(\bar{\omega}^{N-1},\cdots,\bar{\omega},1)=\boldsymbol{K}_n\otimes\cdots\otimes\boldsymbol{K}_2\otimes\boldsymbol{K}_1\\&\boldsymbol{C}=\mathrm{diag}(1,\bar{\omega})\end{aligned}\tag{13}$$

其中，$\boldsymbol{L}_j=\mathrm{diag}(1,\omega^{2^{j-1}})$且 $\boldsymbol{K}_j=\mathrm{diag}(\bar{\omega}^{2^{j-1}},1)$. 因此，$\boldsymbol{D}_1=(\boldsymbol{C}\otimes\boldsymbol{1}_N)\cdot(\boldsymbol{\Delta}_1\oplus\boldsymbol{\Delta}_2)$. 此外，利用 $\boldsymbol{D}_0$ 可以完成如下的操作 $\boldsymbol{D}_0|1\boldsymbol{0}\rangle=i|1\boldsymbol{0}\rangle$或 $\boldsymbol{D}_0|x\rangle=|x\rangle$. 基于此，定义一个 $\boldsymbol{\pi}_3$ 的操作，$\boldsymbol{\pi}_3|0x\rangle=|0x\rangle$或 $\boldsymbol{\pi}_3|1x\rangle=|1(x+1\bmod 2^n)\rangle$.

考虑一个关键公式：$\boldsymbol{U}_N=\boldsymbol{D}_1^{\dagger}\bar{\boldsymbol{T}}_N\boldsymbol{D}_0\boldsymbol{\pi}_3$，基于对 $\boldsymbol{D}_1$ 和 $\boldsymbol{T}_N$ 的计算，可以计算出如下公式：

$$\begin{aligned}&\boldsymbol{D}_1^{\dagger}\bar{\boldsymbol{T}}_N|0x\rangle=\frac{\bar{\omega}^x}{\sqrt{2}}|0x\rangle+\frac{\omega^x}{\sqrt{2}}|1x'\rangle\\&\boldsymbol{D}_1^{\dagger}\bar{\boldsymbol{T}}_N|1x\rangle=-\frac{i\bar{\omega}^x}{\sqrt{2}}|0x\rangle+\frac{i\omega^x}{\sqrt{2}}|1x'\rangle\end{aligned}\tag{14}$$

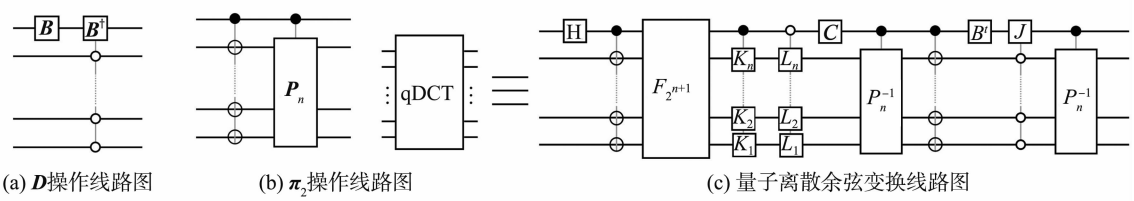
通过定义 $\boldsymbol{D}_0$ 和 $\boldsymbol{\pi}_3$，可以获得如下计算结果 $\boldsymbol{D}_0\boldsymbol{\pi}_3|0x\rangle=|0x\rangle$和 $\boldsymbol{D}_0\boldsymbol{\pi}_3|1x\rangle=|1(x+1\bmod 2^n)\rangle$，进而通过计算得到 $\boldsymbol{D}_0\boldsymbol{\pi}_3|11\rangle=i|1\boldsymbol{0}\rangle$. 此外，可以建立如下公式 $(x+1\bmod 2^n)'=\bar{x}$. 通过结合 $\boldsymbol{D}_1\bar{\boldsymbol{T}}_N$、$\boldsymbol{D}_0\boldsymbol{\pi}_3$ 和式(10)中提出的 $\boldsymbol{T}_N=\boldsymbol{\pi}_2\boldsymbol{D}$，可以获得 $\boldsymbol{U}_N^{\dagger}$ 的计算方法：

$$\boldsymbol{U}_N^{\dagger}=\boldsymbol{\pi}_3^{-1}(\bar{\boldsymbol{D}}_0\boldsymbol{D}^t)\boldsymbol{\pi}_2^{-1}\boldsymbol{D}_1\tag{15}$$

根据式(16)可以计算出 $\bar{\boldsymbol{D}}_0\boldsymbol{D}^t$：

$$\begin{aligned}&\bar{\boldsymbol{D}}_0\boldsymbol{D}^t|0\boldsymbol{0}\rangle=|0\boldsymbol{0}\rangle,\ \bar{\boldsymbol{D}}_0\boldsymbol{D}^t|0x\rangle=\frac{1}{\sqrt{2}}|0x\rangle+\frac{i}{\sqrt{2}}|1x\rangle\\&\bar{\boldsymbol{D}}_0\boldsymbol{D}^t|1\boldsymbol{0}\rangle=-i|1\boldsymbol{0}\rangle,\ \bar{\boldsymbol{D}}_0\boldsymbol{D}^t|1x\rangle=\frac{1}{\sqrt{2}}|0x\rangle-\frac{i}{\sqrt{2}}|1x\rangle\end{aligned}\tag{16}$$

利用算符 $\boldsymbol{B}^t$ 和 $\boldsymbol{J}$ 可以实现提出的 qDCT 的计算过程，$\boldsymbol{J}=\frac{1}{\sqrt{2}}\begin{pmatrix}1&-i\\-i&1\end{pmatrix}$. 图 3(c)给出了完整的 qDCT 量子线路图[24]，“$F_{2^{n+1}}$”表示对 $n+1$ 个量子比特序列进行量子傅里叶变换的操作.



(a) $\boldsymbol{D}$操作线路图　(b) $\boldsymbol{\pi}_2$操作线路图　(c) 量子离散余弦变换线路图

图 3　qDCT 中 3 种量子计算的线路图

Fig.3　Three quantum computing circuits of qDCT

3　量子 Henon 映射加密

在量子零水印算法中需要添加一种量子加密算法对零水印信息进行加密，本节的 Henon 映射可以利用密钥生成一组随机序列. Henon 映射的数学表达式为[24]

$$\begin{cases} x_{n+1} = 1 + y_n - ax_n^2 \\ y_{n+1} = bx_n \end{cases} \tag{17}$$

Henon 映射的参数 a 与 b 不同的选值会使序列 x 与 y 产生不同的效果：1）若干次迭代后 x_n 与 y_n 的值会趋向于无穷大；2）若干次迭代后 x_n 与 y_n 的值只取 m 个固定的数值，称此时的映射处于周期 m 的状态；3）x_n 与 y_n 的取值是一组随机序列，此时称映射处于混沌状态. 因此，为了获取随机序列所选取的 a 与 b 的值，应该保证 Henon 映射处于混沌状态：

$$a \geqslant -\frac{1}{4}(1-b)^2 \tag{18}$$

由式(17)可知，如果 b 的取值范围为 $|b|>1$，经过多次计算迭代后，x 与 y 序列的值趋向于无穷. 当 b 的值满足 $|b| \leqslant 1$ 的同时，a 应满足式(18)才可令序列的取值控制在有限的范围内. 最后利用图 4 中的 Henon 映射分叉图来确定当为 b 赋值后 a 值的取值范围. 如图 4 所示，当 $b=0.2$时，a 从 -0.16 开始进入周期 1 状态，随着 a 值的不断增加 Henon 映射出现了倍周期的分叉现象，当 $a>1.178$ 后开始出现混沌现象且取值范围逐渐增大，直到 1.613 为止. 因此，当 $b=0.2$ 时，a 的取值应控制在 $1.178<a<1.613$ 范围内. 同时应注意，当 $1.431 \leqslant a \leqslant 1.468$ 时，Henon 映射序列出现了周期窗口，在对参数 a 的值进行选取时也要同样避免这些窗口，这样的加密效果会相对更加理想.

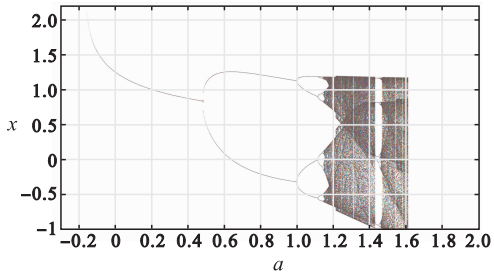


图 4　当 $b=0.2$ 时 Henon 映射的分插图

Fig.4　The Henon map feigenbaum chart when $b=0.2$

实验中选取常数 $a=1.51$ 和 $b=0.2$，同时 $x(0)=0.6$ 和 $y(0)=0.7$ 来获取所需的随机序列，利用式(17)计算出的随机序列为 0.600 0，1.156 4，0.899 3，0.010 2，0.820 0，0.013 3，1.163 7，1.047 6. 把 3 位二进制数序列，即 000，001，…，111 与随机序列中的元素一一对应，再对此数列进行降序排列，同时二进制数列会重新排序，形成置乱后的二进制数列. 此过程如图 5 所示.

与图 5 置乱过程对应的 Henon 映射量子线路图如图 6 所示，其中 t_0、t_1、t_2 是线路图的 3 个输入量子位，其存储了 8 个量子叠加态，即 $|000>$，…，$|111>$. 与之对应的是 3 个 Ancillary 量子位，其是 8 个 $|000>$ 量子态的叠加. t_0、t_1、t_2 上的控制位可以确定其所处的量子态，触发与之对应的 3 个 Ancillary 量子位上的量子非门(NOT 门)，使初始态 $|000>$ 变为 Henon 映射后的量子态. 如利用式(17)计算出的随机序列中的第 1 位小数为 0.600 0，与之对应的二进制数为 000. 如图 5 所示，经过降序排列后的第 1 位二进制数为 110. 因此在图 6 中，如果令量子态 $|000>$ 变为 $|110>$，需要在两个高位量子位执行取反操作. 同理第 2 组变换是从量子态 $|000>$ 变为 $|001>$（NOT 门作用于最低位），第 3 组为 $|000>$ 变为 $|111>$（NOT 门作用于 3 个量子位）. 经过 7 轮控非门操作后，$|T_0T_1T_2>$ 为线路图的 3 个量子输出位，为二进制置乱后顺序(如图 5 最右侧一列)的叠加态. 由于二进制 101 置乱后对应的二进制数是 000，这与 3 个 Ancillary 量子位初始化量子态 $|000>$ 相同，此种情况下不需要控非门的变换，因此图 5 中虽然有 8 个二进制数，但图 6 的线路图中仅有 7 个控非门.

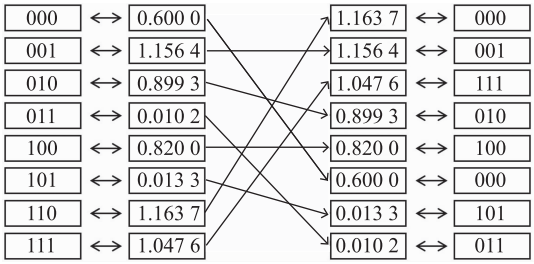


图 5　随机序列降序排列置乱二进制数

Fig.5　Scramble binary numbers utilizing random sequence in descending order

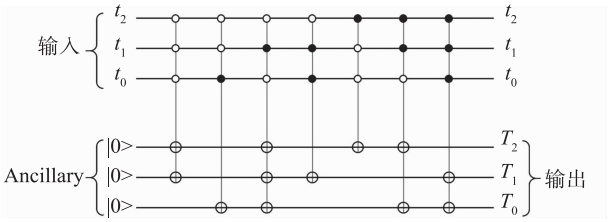


图 6　Henon 映射治乱线路图

Fig.6　Scrambling circuit based on Henon map

4　基于 Henon 映射的量子音频零水印

4.1　量子零水印概述

量子零水印算法示意图如图 7 所示，首先利用量子离散余弦变换 qDCT 对 FRQA 格式编码的量子音频进行运算，其计算过程如下：

$$\begin{aligned} & q\mathrm{DCT}|Q_A> \\ &= \frac{1}{2^{l/2}}\sum_{t=0}^{2^l-1}|A_t> \otimes q\mathrm{DCT}(|t>) \\ &= \frac{1}{2^{l/2}}\sum_{t=0}^{2^l-1}|A_t> \otimes g(t)\sum_{c=0}^{2^l-1}\cos\left[\frac{\pi}{N}\left(c+\frac{1}{2}\right)t\right]|c> \\ &= \frac{1}{2^{l/2}}\sum_{t=0}^{2^l-1}g(t)\sum_{c=0}^{2^l-1}\cos\left[\frac{\pi}{N}\left(c+\frac{1}{2}\right)t\right]|A_t>|c> \end{aligned} \tag{19}$$

qDCT 将 FRQA 量子音频从时域转换为频域. $|c\rangle$ 与 $|t\rangle$ 有一样的取值范围，即从 $|0\rangle$ 到 $|2^{l}-1\rangle$，并记录 FRQA 音频在频域内的采样位置. 其次，提取宿主量子音频在频域内的低频分量，通过振幅二进制的最高位生成一个二进制序列，此为该宿主量子音频的量子水印信息. 这种提取算法保留了原宿主量子音频的所有信息，因此在算法的不可感知性方面有很大优势. 同时，水印信息的提取位置设定为低频分量，降低了传输过程中噪声对水印信息的影响，提高了算法的鲁棒性. 最后通过 Henon 映射加密算法对水印信息进行加密，从而获得最终的已加密的量子水印信息.

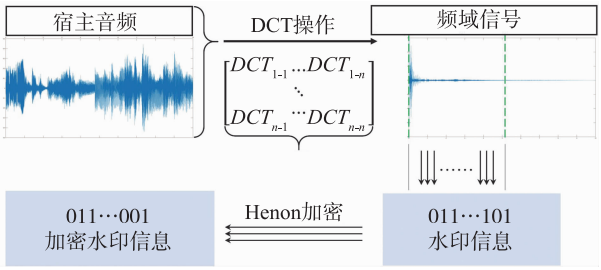


图 7 量子零水印算法

Fig.7 Quantum zero-watermark algorithm

对于量子零水印的提取算法，首先仍然对含水印信息的量子音频进行 qDCT 处理，然后在频域内的低频区域用与提取算法相同的方法计算出一组二进制序列，最后利用特定的量子计算线路图对该组序列执行 Henon 映射，生成提取出的零水印二进制序列.

4.2 量子零水印生成算法

量子零水印生成算法如算法 1 所示，与之对应的线路图如图 8 所示，其输入为 FRQA 格式编码的宿主量子音频以及初始化为 $|0\rangle$ 态的量子比特序列. 首先利用 H 门对处于 $|0\rangle$ 态的量子比特序列执行式(2)中的操作生成 $|0\cdots0\rangle$，$|0\cdots1\rangle$，…，$|1\cdots1\rangle$ 的叠加态. 图中的 qDCT 表示量子离散余弦变换，作用于宿主量子音频存贮时间信息的量子比特序列，即 $|t_0t_1\cdots t_{n-1}\rangle$，使量子音频由时间域转换为频域. 虚线框中被命名为“Set watermark”区域完成了量子零水印的设置工作，这个过程中宿主量子音频中的量子控制位 $t_0\cdots t_{m-1}$ 与 Hadamard 门作用后的量子比特序列在每个控非门执行时保持一致. 表示量子振幅比特序列的最高量子位 H_t^{q-1} 控制下方二进制序列每个位置的具体值，当 $|H_t^{q-1}\rangle=|1\rangle$ 时，控非门在对应量子位上执行取反操作，实现 $|0\rangle\rightarrow|1\rangle$ 的转变，否则该量子位保持 $|0\rangle$ 态不变. 在经过 2^m 个控非操作后，“Set watermark”部分完成. 之后对该二进制序列执行量子 Henon 映射加密算法(见第 3 小节)，生成已置乱的二进制序列，即量子零水印，图中用 $|z_0\cdots z_{m-1}W_z\rangle$ 表示，其中 W_z 表示零水印序列每一位二进制的值，$|z_0\cdots z_{m-1}\rangle$ 表示零水印序列的下标序号. 最后的 iqDCT 表示量子反向离散余弦变换，使得宿主量子音频由频域转换回时间域，从而完成量子零水印的生成算法.

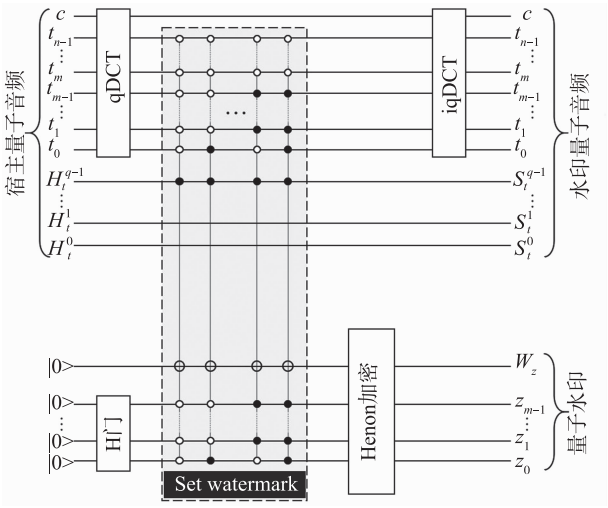


图 8 量子零水印生成算法线路图

Fig.8 Quantum zero-watermark generation algorithm circuit

算法 1 量子零水印生成算法

1：宿主量子音频 FRQA 作为输入
利用 H 门初始化量子零水印序列的时间信息
2：qDCT 作用于 FRQA 的时间域完成时域到频域的转换
3：根据宿主音频低频区域的振幅值为零水印序列赋值
4：利用密钥生成的 Henon 映射线路图对零水印加密
5：iqDCT 令宿主量子音频完成频域到时域的转换

4.3 量子零水印提取算法

量子零水印提取算法如算法 2 所示，与之对应的量子零水印提取算法线路图如图 9 所示，其线路图的两个输入与零水印生成算法相同，分别为宿主量子音频与初始化为 $|0\rangle$ 态的量子比特序列. 首先，与图 8 相同，利用 H 矩阵与 qDCT 变换初始化量子比特序列和完成宿主量子音频从时域向频域的转变. 其次，利用与零水印生成算法相同的线路图对量子比特序列进行设置，生成值为 $|0\rangle$ 或 $|1\rangle$ 的二进制量子比特序列. 之后，利用量子 Henon 映射加密算法对该二进制量子比特序列进行处理，其线路图必须与量子零水印生成算法中 Henon 映射的线路图完全一致，从而获得提取出的量子零水印.

算法 2 量子零水印提取算法

1：宿主量子音频 FRQA 作为输入
利用 H 门初始化量子零水印序列的时间信息
2：qDCT 作用于 FRQA 的时间域完成时域到频域的转换
3：根据宿主音频低频区域的振幅值为零水印序列赋值
4：利用密钥生成的 Henon 映射线路图对零水印解密
5：提取出的量子零水印与标准水印对比求相似性测度

图 9 中“Calculate similarity”把生成的量子零水印序列与标准的水印量子比特序列进行逐位比较，同时计算两个序列的相似度. $|z_0\cdots z_{m-1}W_t\rangle$ 表示标准量子零水印，$|x_0\cdots x_{m-1}W_x\rangle$ 表示从量子音频中提取的零水印信息. “Adder”表示量子加法器(见 1.3 节)，其两个输入是两个量子位

$|W_t\rangle$ 和 $|W_x\rangle$，$|z_0\cdots z_{m-1}\rangle$ 与 $|x_0\cdots x_{m-1}\rangle$ 是加法器的 $2m$ 个量子控制位，控制加法器的执行条件，即在两个量子零水印序列的相同位置执行量子加法的操作，$|k_0 l_1\rangle$ 两个量子位记录加法器的结果. 此处有一个规律，即两个二进制数相加，如果它们的值相等(即相加的两个二进制数都为 0 或都为 1)，则它们和的低位一定为 0，如 00 + 00 = 00 或 01 + 01 = 10，因此可以看出，相同的两个二进制数相加，其结果的低位一定为 0. 相反地，如果相加的两个二进制数的值不同(即相加的两个二进制数一个为 0，而另一个为 1)，则它们和的低位一定为 1，如 00 + 01 = 01 或 01 + 00 = 01，故当两个相加的二进制数不同时，它们和的低位一定为 1. 因此，只需把量子加法器相加结果的低位执行叠加操作，其结果就是两个零水印序列的相似性测度，其结果越小说明相似度越高.

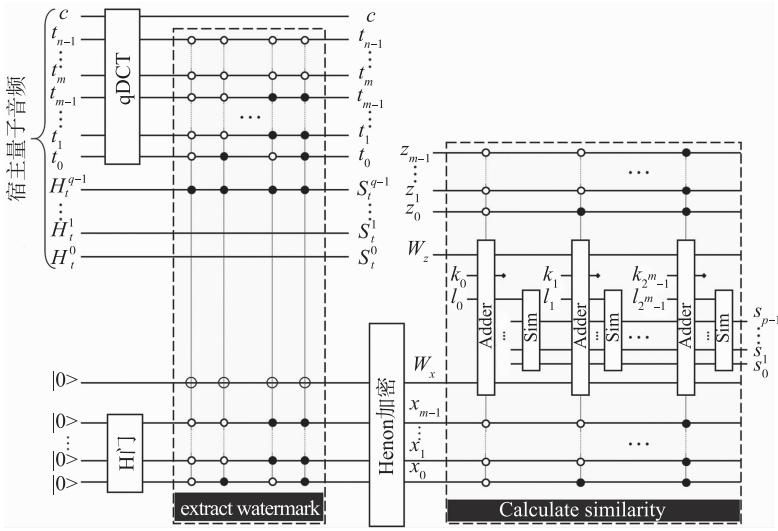


图 9　量子零水印提取算法线路图

Fig.9　Flowchart of quantum zero-watermark extraction algorithm

图 9 中的“Sim”模块计算相似性测度，其输入为多个初始化为 $|0\rangle$ 态的量子比特. 另一个输入为“Adder”的低位输出量子位 $|l_0\rangle$，在“Sim”中同样执行量子加法的操作，其结果为下一个“Sim”模块的输入，同时另一个输入为第二个“Adder”的低位输出量子位 $|l_1\rangle$，由此经过 2^m 个叠加操作后可以计算出相似性测度，图中为整个线路图的输出 $|s_0 s_1\cdots s_{p-1}\rangle$.

5　仿真实验

利用 Matlab 进行仿真实验模拟量子音频零水印算法的执行过程. 宿主量子音频利用 FRQA 的量子音频表达式进行编码，分配 9 个量子位表示振幅信息，19 个量子位表示时间信息. 利用 19 个量子位存储二进制序列零水印，零水印的大小为 2^{18}，利用 18 个量子位表示零水印序列的下标，用一个量子位表示零水印序列的大小.

量子水印算法的目的是通过隐藏水印信息实现对量子音频的版权保护. 不可感知性可以度量在宿主音频内是否容易察觉到水印的存在. 水印算法的这种性质是判定消息安全性的重要指标. 鲁棒性可以测试含水印的音频在遭受恶意攻击或受到信道中噪声的作用时，保证水印信息不受影响的能力. 不可感知性和鲁棒性是评价水印算法性能优劣的两个重要参数.

5.1　不可感知性

不可感知性是为了测试量子零水印算法执行了嵌入操作后，含水印的音频与嵌入前的宿主音频之间的不同. 通常计算两种音频信号间的信噪比(signal-to-noise ratio，SNR)来对零水印算法的不可感知性进行量化. 信噪比计算信号功率与噪声功率的比值，单位为分贝(dB)，其公式为

$$\mathrm{SNR}(H_t, S_t) = \lg \frac{\sum_{t=0}^{2^n-1} H_t^2}{\sum_{t=0}^{2^n-1} (H_t - S_t)^2} \tag{20}$$

其中，H_t 为宿主量子音频，S_t 为嵌入水印后的含水印信息的量子音频，n 为编码两种量子音频时间信息的量子位个数. 信噪比的值越高证明算法不可感知性越强. 实验中选取 10 种不同的宿主音频(如图 10)进行测试，分别对其进行零水印处理及文[19]中两种量子音频水印算法的嵌入操作，进而生成对应的已嵌入水印信息的量子音频. 最后将嵌入前的宿主量子音频与嵌入后的含水印量子音频代入式(20)计算 SNR 值.

3 种不同的量子音频水印算法针对 10 种宿主音频执行水印嵌入操作后所计算出的 SNR 值如图 11 所示. 蓝色、红色和绿色分别对应零水印、QAW-I(quantum audio watermarking-I)和 QAW-II(quantum audio watermarking-II)水印嵌入算法，从图中数据分析可知 10 种宿主音频的零水印嵌入算法获得的 SNR 值要远远高于 QAW-I 和 QAW-II 水印嵌入算法，说明零水印的不可感知性要高于其他两种量子音频水印算法. 这是因为与普通水印嵌入算法不同，零水印算法是从宿主量子音频本身提取出水印信息，在产生水印的过程中宿主音频的状态完全不受影响，这也是零水

印算法最大的优势，即具有强健的不可感知性.

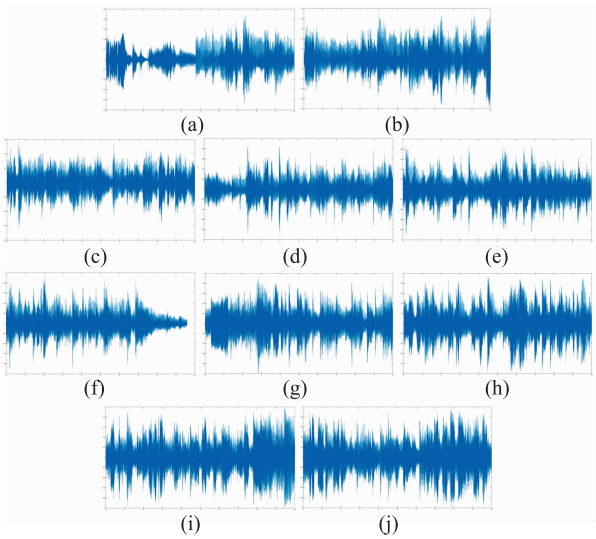


图 10 10 种不同的宿主音频信息

Fig.10 Ten types of host audio signals

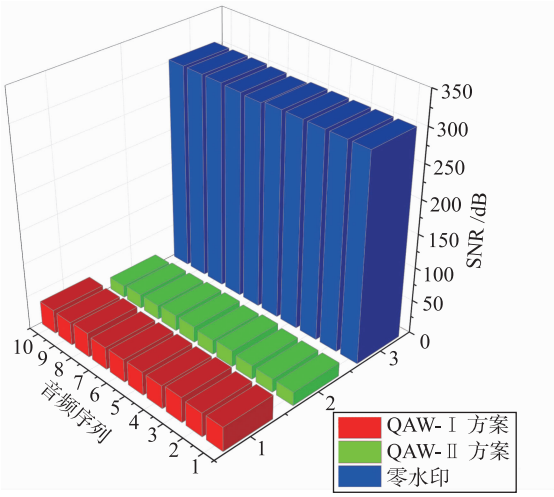


图 11 3 种量子音频水印算法的 SNR 值

Fig.11 The SNR values among three quantum audio watermarking algorithms

5.2 鲁棒性

利用鲁棒性对量子音频零水印算法的稳健性(抗干扰和抗攻击能力)进行探讨. 通常使用归一化互相关系数(normalized correlation coefficient, NCC)来对零水印算法的鲁棒性进行量化. NCC 可以确定两个序列之间的相似性，数值越大，表示算法的鲁棒性越强. NCC 的计算公式为

$$\mathrm{NCC}(W, W_{\mathrm{ex}}) = \frac{\sum_{i=0}^{2^n-1} w(i) w_{\mathrm{ex}}(i)}{\sqrt{\sum_{i=0}^{2^n-1} w^2(i)} \sqrt{\sum_{i=0}^{2^n-1} w_{\mathrm{ex}}^2(i)}} \tag{21}$$

其中，W 和 W_{ex} 表示原始水印序列和从含水印的量子音频中提取的水印序列. $w_{\mathrm{ex}}(i)$ 表示坐标位置为 i 的水印信息. NCC 值越高(NCC∈[0, 1])，表明原始量子水印与提取出的量子水印越相似.

与文[19]中提出的两种量子水印算法的鲁棒性进行对比，设置相同的实验条件. 在执行了零水印生成算法后，对量子音频进行不同类型的攻击，从零水印提取方法中获得的水印序列与标准零水印序列进行比较，可以用式(21)中的 NCC 值对鲁棒性进行量化分析，NCC 值越高，说明算法具有更强的鲁棒性. 在实验中利用 MP3 压缩、高斯白噪声(WGN)、巴特沃思(Butterworth)低通滤波器和重采样四种攻击方法，对本文提出量子零水印算法的鲁棒性进行测试并与文[19]中的两种算法进行比较. MP3 压缩又分为两种压缩情况：128 kbit/s 和 64 kbit/s. 表 2 中总结了 3 种量子音频水印算法的 NCC 值. 显然，本文提出的量子零水印算法在 5 种不同仿真攻击下 NCC 值最大，说明其算法的鲁棒性最强，同时表明量子零水印算法对旨在破坏量子音频水印的攻击方面具有更好的鲁棒性.

表 2 3 种水印算法 NCC 值比较

Tab.2 The NCC comparison among three watermarking algorithms

攻击类型	NCC 值(QAW-I)	NCC 值(QAW-II)	NCC 值(零水印)
MP3 压缩(128 kbit/s)	0.382 5	0.461 7	0.944 2
MP3 压缩(64 kbit/s)	0.207 3	0.321 5	0.864 5
重采样	0.001 2	0.405 2	0.817 8
高斯白噪声	0.332 1	0.472 8	0.952 6
巴特沃思低通滤波器	0.216 6	0.372 7	0.900 9

图 12 更加明确地展示了 3 种水印算法在不同攻击下 NCC 值的不同，很明显图中蓝色所代表的零水印算法在 5 种不同攻击下的 NCC 值比其它两种量子音频水印算法都要高出很多. 因此，量子音频零水印算法具有较高的鲁棒性.

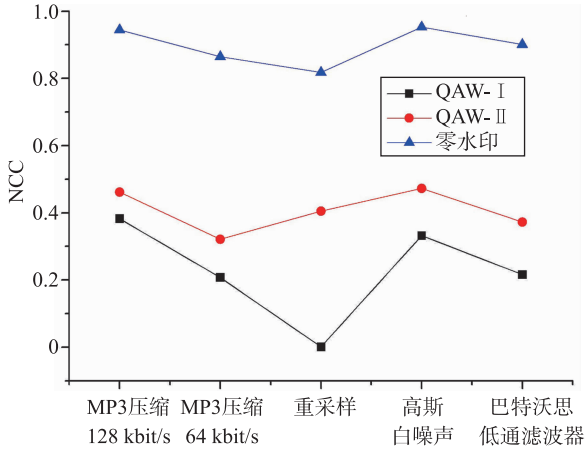


图 12 3 种水印算法 NCC 值比较

Fig.12 The NCC comparison among three watermarking algorithms

根据本小节的仿真实验可以证明量子音频零水印算法在不可感知性和鲁棒性方面相比于同样基于量子离散余弦变换的将水印信息直接嵌入的量子音频水印算法具有更大的优势.

6　总结

本文提出了一种基于量子离散余弦变换的量子零水印算法，宿主量子音频被编码为 FRQA 格式，利用 qDCT 获得宿主量子音频的频域，再根据其低频区域的大小形成一组量子比特序列. 为了对生成的量子比特序列加密，本文根据 Henon 映射加密算法提出一种量子映射加密算法，对量子比特序列进行加密操作，从而获得量子零水印，用于保护量子音频的版权信息. 此处，量子 Henon 映射的线路图即为提取量子零水印的秘钥. 可以用相似的方法完成量子零水印的提取工作，但前提是需要掌握 Henon 映射完整的量子线路图才有可能提取出正确的量子零水印信息. 最后利用仿真实验，验证了本文提出算法具有强健的不可感知性和更强的鲁棒性.

参考文献

[1] Feynman R. Simulating physics with computers[J]. International Journal of Theoretical Physics, 1982, 21(6/7): 467 – 488.

[2] Deutsch D. Quantum theory, the church-turing principle and the universal quantum computer[C]//Royal Society of London A. London, UK: Royal Society, 1985: 97 – 117.

[3] Shor P. Algorithms for quantum computation: Discrete logarithms and factoring[C]//35th Annual Symposium on Foundations of Computer Science. Piscataway, USA: IEEE, 1994: 124 – 134.

[4] Rivest R, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems[J]. Communications of the ACM, 1987, 21(2): 120 – 126.

[5] Biamonte J, Wittek P. Quantum machine learning[J]. Nature, 2017, 549: 195 – 202.

[6] Yan F, Venegas-Andraca S. Quantum image processing[M]. Berlin, Germany: Springer, 2020.

[7] Ge W, Sawyer B C, Britton J W, et al. Trapped ION quantum information processing with squeezed phonons[J]. Physical Review Letters, 2019, 122(3): 030501.

[8] Molotkov S. Concatenation of keys in quantum cryptography: How quantum entanglement "penetrates to" classical devices[J]. Journal of Experimental and Theoretical Physics, 2018, 127(4): 627 – 637.

[9] Bouwmeester D, Pan J, Mattle K, et al. Experimental quantum teleportation[J]. Nature, 1997, 390: 575 – 579.

[10] Yoshida B, Yao N Y. Disentangling scrambling and decoherence via quantum teleportation[J]. Physical Review X, 2019, 9(1): 011006.

[11] Roy S, Chanda T, Das T, et al. Deterministic quantum dense coding networks[J]. Physics Letters A, 2018, 382(26): 1709 – 1715.

[12] Zhang W W, Gao F, Liu B, et al. A quantum watermark protocol[J]. International Journal of Theoretical Physics, 2013, 52(2): 504 – 513.

[13] Yang Y G, Jia X, Xu P, et al. Analysis and improvement of the watermark strategy for quantum images based on quantum Fourier transform [J]. Quantum Information Processing, 2013, 12(8): 2765 – 2769.

[14] Song X H, Wang S, Liu S, et al. A dynamic watermarking scheme for quantum images using quantum wavelet transform[J]. Quantum Information Processing, 2013, 12(2): 3689 – 3706.

[15] Yang Y G, Xu P, Tian J, et al. Analysis and improvement of the dynamic watermarking scheme for quantum images using quantum wavelet transform[J]. Quantum Information Processing, 2014, 13(9): 1931 – 1936.

[16] Song X H, Wang S, Abd El-Latif A, et al. Dynamic watermarking scheme for quantum images based on Hadamard transform[J]. Multimedia Systems, 2014, 20(4): 379 – 388.

[17] Wang J. QRDA: Quantum representation of digital audio[J]. International Journal of Theoretical Physics, 2016, 55: 1622 – 1641.

[18] Yan F, Iliyasu A, Guo Y M, et al. Flexible representation and manipulation of audio signals on quantum computers[J]. Theoretical Computer Science, 2017, 752(15): 71 – 85.

[19] Chen K H, Yan F, Iliyasu A, et al. Dual quantum audio watermarking schemes based on quantum discrete cosine transform[J]. International Journal of Theoretical Physics, 2019, 58(2): 502 – 521.

[20] Vlatko V, Adriano B, Artur E. Quantum networks for elementary arithmetic operations[J]. Physical Review A, 1996, 54(1): 147 – 153.

[21] Deutsch D. Quantum computational networks[J]. Royal Society of London A: Mathematical, Physical and Engineering Sciences, 1989, 425 (1868): 73 – 90.

[22] Ahmed N, Natarajan T, Rao K. Discrete cosine transform[J]. IEEE Transactions on Computers, 1974, C-23(1): 90 – 93.

[23] Klappenecker A, Rotteler M. Discrete cosine transforms on quantum computers[C]//2nd International Symposium on Image and Signal Processing and Analysis. Piscataway, USA: IEEE, 2001: 464 – 468.

[24] Hénon M. A two-dimensional mapping with a strange attractor[J]. Communications in Mathematical Physics, 1976, 50: 69 – 77.

作者简介

张景波(1982 –)，男，硕士，副教授. 研究领域为软件工程，信息安全与数据理论，量子信息处理.

张云琦(1981 –)，女，硕士，副教授. 研究领域为量子信息处理，量子计算，通讯工程，程控交换技术.