Journal of Soft Computing and Information Technology (JSCIT)
Babol Noshirvani University of Technology, Babol, Iran
Journal Homepage: jscit.nit.ac.ir
Volume 9, Number 3, Fall 2020, pp. 180-195
Received: 05/23/2019, Revised: 11/05/2019, Accepted: 05/21/2020

Proposing two quantum audio watermarking schemes with improved robustness

Mohsen Yoosefi Nejad[1], Mohammad Mosleh[2*] and Saeed Rasouli Heikalabad[3]
1- Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran.
2*- Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran.
3- Department of Computer Engineering, Tabriz Branch, Islamic Azad University, Tabriz, Iran.
[1]m_yoosefi@pnu.ac.ir, [2*]mosleh@iaud.ac.ir, and [3]s.rasouli@iaut.ac.ir

Corresponding author address: Mohammad Mosleh, Department of Computer Engineering, Islamic Azad University of Dezful, Dezful, Iran, Post Box: 313.

Abstract- As an important security technology, recently quantum watermarking attracted wide research attention. Up to now, several methods have been proposed for quantum image watermarking, while there are a few achievements in the domain of quantum audio watermarking. This study presents two quantum audio watermarking schemes, with the aim of improving robustness. The first scheme embeds a watermark qubit into odd number of qubits of host audio, and employs majority-voting policy to extract the correct watermark qubit. In the second proposed scheme, k audio samples are grouped as a frame, which holds one qubit of watermark. In order to embed a qubit into a frame, parameter r, which is sum of frame amplitudes, is calculated in module 2^k. The amplitudes are then adjusted to set parameter r in the median of two ranges, $[0, 2^{k-1}-1]$, and $[2^{k-1}, 2^k-1]$ to represent embedding $|0\rangle$ or $|1\rangle$. The parameter r is recalculated in extracting phase, and based on belonging to a range, the extracted qubit is determined. For every procedure of the proposed schemes, the quantum circuit and complexity analysis are presented. The circuit complexity of both proposed schemes is linear. Experimental results show that the proposed schemes offer promising trade-offs in terms of robustness and transparency.

Keywords- Quantum Audio Watermarking, Signal Processing, Quantum Signal Processing, Quantum Computation, Robustness, Time Domain.

مجله علمی پژوهشی رایانش نرم و فناوری اطلاعات
دانشگاه صنعتی نوشیروانی بابل
صفحه مجله: jscit.nit.ac.ir
جلد ۹، شماره ۳، پائیز ۱۳۹۹ ، صفحه ۱۸۰-۱۹۵
دریافت: ۱۳۹۸/۰۳/۰۲، بازنگری ۱۳۹۸/۰۸/۱۴، پذیرش: ۱۳۹۹/۰۳/۰۱

ارائه دو رویکرد نهان‌نگاری صوتی کوانتومی بهبودیافته از نظر مقاومت

محسن یوسفی نژاد[۱]، محمد مصلح*[۲]، سعید رسولی هیکل آباد[۳]
۱- گروه مهندسی کامپیوتر، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران.
*۲- گروه مهندسی کامپیوتر، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران.
۳- گروه مهندسی کامپیوتر، واحد تبریز، دانشگاه آزاد اسلامی، تبریز، ایران.
[1]m_yoosefi@pnu.ac.ir, [2*]mosleh@iaud.ac.ir, and [3]s.rasouli@iaut.ac.ir

* نشانی نویسنده مسئول: محمد مصلح نویسنده مسئول، دزفول، کوی آزادگان، دانشگاه آزاد اسلامی واحد دزفول، گروه مهندسی کامپیوتر، صندوق پستی: ۳۱۳

چکیده- اخیرا نهان‌نگاری کوانتومی به عنوان یک مبحث امنیتی مهم توجه پژوهشگران زیادی را به خود جلب کرده است. تاکنون روش‌های زیادی برای نهان‌نگاری تصاویر کوانتومی پیشنهاد شده است ولی دستاوردهای انگشت‌شماری در حوزه نهان‌نگاری صوت کوانتومی به چشم می‌خورد. این مقاله دو رویکرد نهان‌نگاری صوت کوانتومی را با هدف بهبود مقاومت ارائه می‌دهد. رویکرد اول یک کیوبیت نهان‌نگاره را در تعداد فردی از نمونه‌های صوتی سیگنال میزبان جایگذاری کرده و با استفاده از روش رای گیری اکثریت، کیوبیت صحیح را استخراج می‌کند. در رویکرد پیشنهادی دوم، تعداد k نمونه صوتی از سیگنال میزبان به عنوان یک قاب، گروه بندی می‌شوند که حامل یک کیوبیت از نهان‌نگاره خواهند شد. به منظور جایگذاری یک کیوبیت، مجموع دامنه نمونه‌های صوت در پیمانه 2^k محاسبه می‌شود (r)، و با افزایش یا کاهش جزئی مقدار دامنه نمونه‌ها، مقدار r در مرکز یکی از دسته‌های $[0,2^{k-1}-1]$ و $[2^{k-1},2^k-1]$ به ترتیب برای درج کیوبیت $|0\rangle$ یا $|1\rangle$ تنظیم می‌گردد. در زمان استخراج، مقدار r مجددا محاسبه شده و با توجه به اینکه در کدام یک از دسته‌های مذکور قرار می‌گیرد، کیوبیت استخراج شده مشخص خواهد شد. برای هرکدام از رویکردهای پیشنهادی، مدار کوانتومی و تحلیل پیچیدگی ارائه شده است. پیچیدگی مداری هر دو رویکرد ارائه شده خطی است. نتایج شبیه سازی نشان می‌دهد که رویکرد-های ارائه شده مصالحه قابل قبولی بین مقاومت، شفافیت و ظرفیت ارائه می‌دهند.

واژه‌های کلیدی: نهان‌نگاری صوت کوانتومی، پردازش سیگنال کوانتومی، محاسبات کوانتومی، مقاومت، حوزه زمان

۱- مقدمه

در اوایل دهه ۱۹۸۰، بنیاف نشان داد که می‌توان یک مدل مکانیک کوانتومی میکروسکوپی از کامپیوترهایی ساخت که با ماشین تورینگ نمایش داده می‌شوند[۱]. دو سال بعد، فینمان یک مدل محاسباتی جدید به‌نام کامپیوترهای کوانتومی ارائه داد. کامپیوترهای کوانتومی در واقع ماشین‌های فیزیکی هستند که می‌توانند حالت‌های ورودی را بپذیرند که بیانگر یک برهم‌نهی[۱] منطقی از چندین ورودی مختلف است و آن‌ها را به یک برهم‌نهی متناظر به‌عنوان خروجی تبدیل می‌کنند. محاسبات که دنباله‌ای از تبدیلات واحد[۲] است به‌طور همزمان روی هر مولفه برهم‌نهی تاثیر می‌گذارد که این امر منجر به پردازش داده موازی عظیم خواهد شد. درحالی که موازی‌سازی در کامپیوترهای کلاسیک نیازمند سخت‌افزار اضافی است، در کامپیوترهای کوانتومی، فقط با یک قطعه سخت‌افزار انجام می‌شود. این قابلیت، کامپیوترهای کوانتومی را قادر می‌سازد تا برخی از مسائل را که روی کامپیوترهای کلاسیک رام‌نشدنی محسوب می‌شوند، به صورت بهینه حل کنند[۲].

در سال‌های اخیر، رسانه‌های دیجیتال مانند متن، تصویر، ویدئو و صوت با نمایش‌های گوناگون در محاسبات کوانتومی و شبکه‌های کوانتومی توسعه پیدا کرده‌اند. اولین نمایش تصاویر کوانتومی،

شبکه کیوبیت[۳] بود. این نمایش یک حالت کوانتومی است که از امواج الکترومغناطیس تک‌رنگ از طریق ماشین‌ها و موقعیت‌های ویژه به‌دست می‌آید. نگاشت پیکسل‌ها به کِت حقیقی[۴] فضای هیلبرت[۵] توسط لاتور پیشنهاد شد[۴]. نمایش انعطاف‌پذیر تصاویر کوانتومی (FRQI[6]) که به صورت گسترده ای استفاده می‌شود، اطلاعات رنگ و موقعیت یک تصویر را در یک حالت کوانتومی تجمیع می‌کند[۵]. با تکیه بر FRQI، یک نمایش چندکاناله برای تصاویر کوانتومی (MCRQI[7]) با استفاده از فضای رنگ RGBα توسط سان و همکاران پیشنهاد شد[۶]. یک نمایش نوین بهبود یافته کوانتومی برای تصاویر دیجیتال (NEQR[8]) توسط ژانگ و همکاران ارائه شد که از دنباله دودویی برای نمایش سطح خاکستری استفاده می‌کند[۷].

سانگ و همکاران نمایش کوانتومی نوینی برای تصاویر دیجیتال رنگی (NCQI[9]) پیشنهاد کردند که از سه دنباله دودویی برای کانال‌های RGB استفاده می‌کند تا مقادیر رنگ پیکسل‌ها را نمایش دهد[۸]. در سال ۲۰۱۵، وانگ یک نمایش کوانتومی موثر برای صوت دیجیتال ارائه داد. نمایش کوانتومی صوت دیجیتال (QRDA[10]) از دو دنباله کیوبیتی درهم تنیده[۱۱] برای ذخیره اطلاعات دامنه و زمان استفاده می‌کند و تمام صوت دیجیتال را در برهم‌نهی دو دنباله کیوبیتی نگهداری می‌کند[۹]. در سال ۲۰۱۷، یان و همکاران یک نمایش انعطاف پذیر برای صوت کوانتومی (FRQA[12]) پیشنهاد دادند که از سیستم مکمل دو برای نمایش دامنه سیگنال استفاده می‌کند[۱۰].

با توسعه چندرسانه‌ای در محاسبات کوانتومی و شبکه‌های کوانتومی، امنیت رسانه‌های دیجیتال به مسئله‌ای پراهمیت تبدیل شد. در دهه‌های اخیر فناوری‌های مختلفی برای حفاظت از اطلاعات پا به عرصه گذاشته اند. نهان‌نگاری کوانتومی به عنوان یک فناوری امنیت اطلاعات کوانتومی مهم، گونه‌ای فناوری برای حفاظت از حق کپی است که با جایگذاری سیگنال نامحسوس حاوی اطلاعات شناسه‌ای رسانه در سیگنال‌های حامل چند رسانه-ای کوانتومی گوناگون محقق می‌شود[۱۱].

در سال ۲۰۱۳، ژانگ و همکاران یک راهبرد نهان‌نگاری برای تصاویر مبتنی بر نمایش FRQI ارائه کردند[۱۲]. در همان سال سونگ و همکاران یک طرح نهان‌نگاری تصویر بر مبنای تبدیل موجک کوانتومی (QWT[13]) پیشنهاد دادند[۱۳]. پس از آن سونگ و همکاران یک طرح نهان‌نگاری پویا برای تصاویر بر اساس تبدیل‌هادامارد[۱۴] ارائه دادند[۱۴]. طرح ارائه شده کیفیت بصری بهتر، ظرفیت نهان‌نگاری بالاتر و پیچیدگی کمتری داشت. در سال ۲۰۱۵، وانگ و همکاران یک روش نهان‌نگاری تصویر بر اساس تبدیل کسینوسی کوانتومی (QCT[15]) پیشنهاد کردند[۱۵]. وانگ و لین یک طرح نهان‌نگاری برای تصاویر کوانتومی بر اساس بیت کم ارزش (LSB[16]) ارائه کردند[۱۶]. در این طرح فقط مالک کپی‌رایت که کلید خصوصی را در دست داشت می‌توانست اطلاعات نهان‌نگاری شده را به کمک مدارهای کوانتومی الگوریتم‌های جایگذاری و استخراج به دست آورد. در سال ۲۰۱۶، حیدری و همکاران یک طرح نهان‌نگاری بر اساس بیت کم ارزش ارائه دادند که در آن با استفاده از کلید خصوص که توسط مالک حق کپی ارائه می‌شد، یک تصویر سیاه و سفید در یک تصویر مقیاس خاکستری[۱۷]جایگذاری می‌گردید[۱۷]. جیانگ و همکاران دو الگوریتم پنهان‌نگاری کور مبتنی بر بیت کم‌ارزش برای تصاویر کوانتومی ارائه دادند[۱۸]. در سال ۲۰۱۷، حیدری و همکاران یک رویکرد نهان‌نگاری تصویر پیشنهاد دادند که از تبدیل موجک کوانتومی استفاده می‌کرد[۱۹].

با مرور ادبیات موجود مشخص می‌شود که اکثر دستاوردهای قبلی روی محافظت از حق کپی برای تصاویر کوانتومی است. در خصوص نهان‌نگاری صوت کوانتومی که یک رسانه مهم دیگر است، مقالات اندکی تا کنون به چشم می‌خورد.

در سال ۲۰۱۷، چن و همکاران دو پروتکل پنهان‌نگاری صوت کوانتومی ارائه دادند که بیت کم ارزش سیگنال صوتی کوانتومی میزبان را دستکاری می‌کردند. سیگنال‌های صوت کوانتومی میزبان در نمایش FRQA بودند[۲۰]. پروتکل پنهان نگاری اول در واقع ذخیره کیوبیت‌های پیام در کیوبیت کم‌ارزش است که اگرچه از لحاظ شفافیت به‌خوبی عمل می‌کند، مقاومت بسیار پایینی در مقابل نویز دارد. پروتکل دوم مربوط به ذخیره کیوبیت‌های پیام در کیوبیت‌های لایه‌های بالاتر است. در این پروتکل با حرکت به‌سمت لایه‌های بالاتر مقاومت افزایش یافته و شفافیت کاهش می‌یابد. در سال ۲۰۱۸، کیو و همکاران الگوریتم نهان‌نگاری صوتی کوانتومی بهبود یافته‌ای با تغییر بیت کم ارزش ارائه دادند. در این الگوریتم به منظور افزایش مقاومت، دو بیت کم‌ارزش دامنه بر اساس یک منطق ارائه شده تغییر می‌کرد[۱۱]. باوجود تلاش برای افزایش مقاومت در این روش، فاز استخراج نهان‌نگاره به‌گونه‌ایست که در صورت تغییر کیوبیت کم‌ارزش نمونه سیگنال صوت، در اثر عواملی مانند نویز، کیوبیت نهان نگاره از بین خواهد رفت. مقاله مذکور صرفا به نحوه جایگذاری داده در یک نمونه سیگنال اشاره کرده است و مداری برای جایگذاری در تمام سیگنال ارائه ننموده است. همچنین هر دو مقاله اخیر از ظرفیت موازی‌سازی که دستاورد مهم محاسبات کوانتومی است استفاده ننموده اند.

جایگذاری کیوبیت‌های نهان‌نگاره در بیت کم ارزش نمونه‌های صوتی دارای مزیت شفافیت و ظرفیت است ولی مقاومت پایینی دارد. در این مطالعه به منظور افزایش مقاومت، دو رویکرد ارائه

شده است. رویکرد اول یک کیوبیت نهان‌نگاره را در تعداد فردی از نمونه‌های صوتی سیگنال میزبان جایگذاری کرده و با استفاده از روش رای‌گیری اکثریت، کیوبیت صحیح را استخراج می‌کند. به عنوان مثال در صورتی که سه نمونه صوتی برای جایگذاری یک کیوبیت نهان‌نگاره استفاده شود، در صورت تغییر یک نمونه (مثلا در اثر نویز کانال)، کیوبیت صحیح نهان‌نگاره از طریق دو نمونه دیگر قابل استخراج است. در رویکرد پیشنهادی دوم، تعداد k نمونه صوتی از سیگنال میزبان به عنوان یک قاب، گروه بندی می‌شوند که حامل یک کیوبیت از نهان‌نگاره خواهند شد. به منظور جایگذاری یک کیوبیت، مجموع دامنه نمونه‌های صوت در پیمانه 2^k محاسبه می‌شود که آن را r می‌نامیم. با افزایش یا کاهش مقدار دامنه نمونه‌ها، مقدار r را در مرکز یکی از دسته‌های $[0,2^{k-1}-1]$ و $[2^{k-1},2^k-1]$ به ترتیب برای درج کیوبیت $|0\rangle$ یا $|1\rangle$ تنظیم می‌کنیم. در زمان استخراج، مجددا مقدار r محاسبه شده و با توجه به اینکه در کدام یک از دسته‌های مذکور قرار می‌گیرد، کیوبیت استخراج شده مشخص می‌گردد. به عنوان مثال برای k=3، مجموع دامنه‌های هر سه نمونه محاسبه می‌شوند و باقیمانده تقسیم آن‌ها بر عدد ۸=۲۳ محاسبه می‌شود. از آنجایی که باقیمانده تقسیم هر عدد بر ۸ عددی بین صفر تا ۷ است، این بازه به دو دسته صفر تا ۳ و ۴ تا ۷ تقسیم می‌شود. در زمان استخراج، مجددا مجموع دامنه‌های سه نمونه محاسبه شده و باقیمانده تقسیم آن‌ها بر ۸ محاسبه می‌شود، این مقدار اگر در دسته اول (صفر تا ۳) قرار گرفت بیانگر کیوبیت نهان‌نگاره $|0\rangle$ است و در صورتی که در دسته دوم (۴ تا ۷) جای داشت بیانگر کیوبیت نهان‌نگاره $|1\rangle$ است. برای افزایش مقاومت در زمان جایگذاری با افزایش یا کاهش مقدار نمونه‌ها به شکلی عمل می‌شود که مقدار محاسبه شده در مرکز دسته مورد نظر قرار گیرد. قرار گرفتن مقدار محاسبه شده در مرکز دسته درجه‌ای از آزادی را به وجود می‌آورد که در صورت تغییر مقدار دامنه‌ها، مقدار محاسبه شده کماکان در دسته مورد نظر باقی بماند. با توجه به اینکه دسته‌های ذکر شده اعداد زوج هستند و مرکز آن‌ها یک عدد اعشاری است، عددی به عنوان مرکز انتخاب می‌شود که کمترین تغییرات در اندازه دامنه‌ها را نیاز داشته باشد.

ادامه این مقاله به صورت زیر تنظیم شده است: مفاهیم پایه مورد نیاز در خصوص رویکردهای ارائه شده در بخش ۲ ارائه گردیده است. در بخش ۳ به بیان روش‌های نهان‌نگاری پیشنهادی پرداخته شده است. تحلیل پیچیدگی مدارهای کوانتومی ارائه شده در بخش ۴ و نتایج شبیه سازی و تحلیل آن‌ها در بخش ۵ بیان شده اند. مقاله با بخش جمع بندی و نتیجه گیری به پایان می‌رسد.

۲- مفاهیم پایه

به منظور سازماندهی اطلاعات پشتیبان کننده روش‌های پیشنهادی، مفاهیم پایه مورد نیاز در این بخش ارائه می‌گردد.

۲-۱- نمایش کوانتومی صوت دیجیتال (QRDA)

نمایش کوانتومی صوت دیجیتال (QRDA) از دو دنباله کیوبیتی درهم‌تنیده برای ذخیره سازی اطلاعات دامنه و زمان استفاده می‌کند و تمام سیگنال صوت دیجیتال را در برهم نهی این دو دنباله کیوبیتی نگهداری می‌کند. هر دو دنباله کیوبیتی در پایه $|0\rangle$ و $|1\rangle$ هستند. به‌منظور نمایش سیگنال صوت دیجیتال $A = [a_0, a_1, \dots, a_{L-1}]$ در QRDA که در آن L طول سیگنال صوتی است و $a_i \in \{-2^{q-1}, \dots, -1,0,1, \dots, 2^{q-1}-1\}$، می‌بایست سیگنال به شکل $a_i \in \{0,1, \dots, 2^q-1\}$ برگردانده شود. این انتقال تاثیری روی شکل موج سیگنال ندارد. نمایش QRDA از دنباله دودویی q بیتی $D_T = D_T^0 D_T^1 \dots D_T^{q-2} D_T^{q-1}$ برای کدگذاری مقدار دامنه a_T استفاده می‌کند. بنابراین یک سیگنال صوتی QRDA می‌تواند به شکل رابطه (۱) نوشته شود.

$$
\begin{aligned}
&|A\rangle = \frac{1}{\sqrt{2^l}} \sum_{T=0}^{2^l-1} |D_T\rangle \otimes |T\rangle \\
&|T\rangle = |t_0 t_1 \dots t_{l-1}\rangle, t_i \in \{0,1\} \\
&|D_T\rangle = |D_T^0 D_T^1 \dots D_T^{q-2} D_T^{q-1}\rangle, D_T^i \in \{0,1\} \\
&l = \begin{cases} 1 & L = 1 \\ \lceil log_2^L \rceil & L > 1 \end{cases}
\end{aligned}
\qquad (۱)
$$

که در این رابطه $|T\rangle$ بیانگر اطلاعات زمان و $|D_T\rangle$ مقدار کدگذاری شده دودویی دامنه مربوط به زمان T می‌باشد. در QRDA، اطلاعات زمان T با استفاده از l کیوبیت نمایش داده می‌شود که می‌تواند 2^l نقطه زمانی را بیان کند. با این وجود، فقط L نقطه زمانی ابتدای سیگنال موثر هستند و 2^l-L نقطه زمانی انتهایی زائد بوده که به دلیل ویژگی ذاتی محاسبات دودویی ایجاد شده اند. این نقاط زمانی زائد در QRDA با مقدار دامنه $|0\rangle$ مقداردهی می‌شوند.

۲-۲- نمایش کوانتومی نوین بهبودیافته تصاویر (NEQR)

نمایش کوانتومی نوین بهبود یافته تصاویر (NEQR) از دو دنباله کیوبیتی درهم‌تنیده برای ذخیره سازی اطلاعات سطح خاکستری و موقعیت استفاده می‌کند و تمام تصویر را در برهم‌نهی این دو دنباله کیوبیتی نگهداری می‌کند. برای یک تصویر سطح خاکستری با محدوده خاکستری 2^q دنباله دودویی $C_{yx}^0 \dots C_{yx}^{q-2} C_{yx}^{q-1}, C_{yx}^k$ مقدار سطح خاکستری f(y,x) را برای پیکسل متناظر (y,x) مطابق رابطه (۲) کدگذاری می‌کند.

$$f(y,x) = C_{yx}^{0} \dots C_{yx}^{q-2} C_{yx}^{q-1}, C_{yx}^{k} \in [0,1], \quad f(y,x) \in [0, 2^q - 1] \qquad (۲)$$

نمایش یک تصویر $2^n \times 2^n$ در فرم NEQR به صورت رابطه (۳) بیان می‌شود.

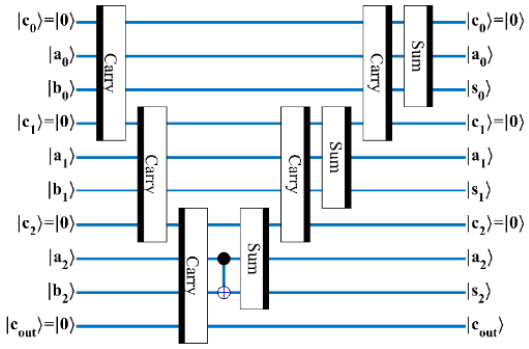
$$|I\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} |f(y,x)\rangle |yx\rangle = \frac{1}{2^n} \sum_{y=0}^{2^n-1} \sum_{x=0}^{2^n-1} \otimes_{i=0}^{q-1} |C_{yx}^{i}\rangle |yx\rangle \qquad (۳)$$

۲-۳- جمع‌کننده کوانتومی پیمانه 2^n

جمع‌کننده کوانتومی یک تبدیل کوانتومی و یا مدار معادل آن است که دو عدد n کیوبیتی $|a\rangle$ و $|b\rangle$ را به عنوان ورودی دریافت کرده و حاصل جمع آن‌ها را در یک حالت کوانتومی نشان می‌دهد. یک عدد مانند $|a\rangle$ به صورت حاصل ضرب مستقیم کیوبیت‌های آن تعریف می‌شود. به عنوان مثال عدد ۶ در مبنای ۲ به صورت ۱۱۰ نوشته می‌شود و بارکردن یک رجیستر کوانتومی با این مقدار با آماده سازی سه کیوبیت در حالت $|1\rangle \otimes |1\rangle \otimes |0\rangle$ انجام می‌گردد. بنابراین منظور از عدد $|a\rangle$ شکل فشرده حاصلضرب مستقیم $|a_n\rangle \otimes |a_{n-1}\rangle \otimes \dots \otimes |a_1\rangle \otimes |a_0\rangle$ است که بیانگر یک رجیستر کوانتومی با مقدار $a = 2^0 a_0 + 2^1 a_1 + \dots + 2^n a_n$ می‌باشد. برای جمع دو عدد در پیمانه 2^n کافیست n بیت کم‌ارزش آن دو عدد را جمع کنیم. شکل ۱ یک جمع‌کننده پیمانه ۸ را نشان می‌دهد که بر اساس طرح ارائه شده توسط ودرال و همکاران[۲] رسم شده است. این مدار از دو ماژول Carry و Sum استفاده می‌کند که در شکل ۲ نشان داده شده‌اند. با افزایش تعداد کیوبیت‌ها می‌توان به جمع‌کننده‌های پیمانه‌های ۱۶ و ۳۲ و بالاتر دست یافت.

۲-۴- افزاینده و کاهنده دودویی کوانتومی

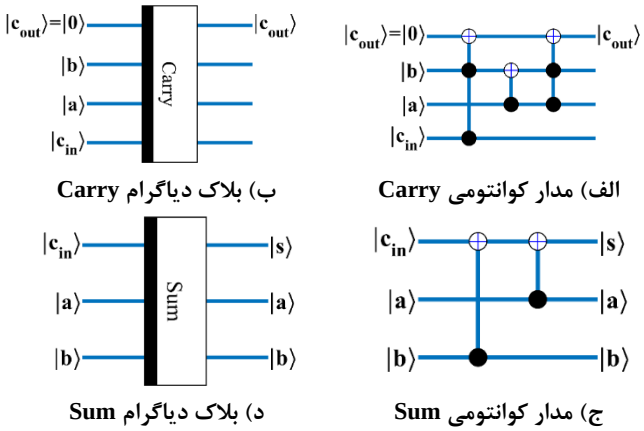
دو مدار پایه مورد نیاز در اجرای الگوریتم جایگذاری روش پیشنهادی دوم، مدارهای افزاینده و کاهنده دودویی هستند. با وجود اینکه می‌توان به کمک یک جمع‌کننده دودویی، عملیات افزایش یا کاهش یک واحد را به درستی انجام داد، ولی به جهت افزایش کارایی و کاهش پیچیدگی مدار نهایی، بهتر است از مدارهای ویژه افزایش و کاهش یک واحدی استفاده کرد. شکل ۳ مدارهای کوانتومی و بلاک دیاگرام افزاینده و کاهنده را بر اساس مرجع[۲۱] نشان می‌دهد.



الف) مدار کوانتومی

ب) بلاک دیاگرام

شکل ۱) مدار کوانتومی جمع‌کننده پیمانه ۸ و بلاک دیاگرام آن براساس مرجع [۲]



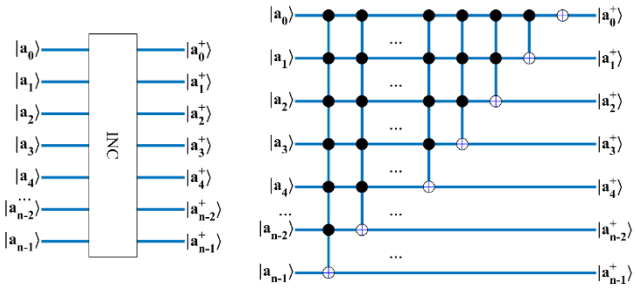
الف) مدار کوانتومی Carry

ب) بلاک دیاگرام Carry

ج) مدار کوانتومی Sum

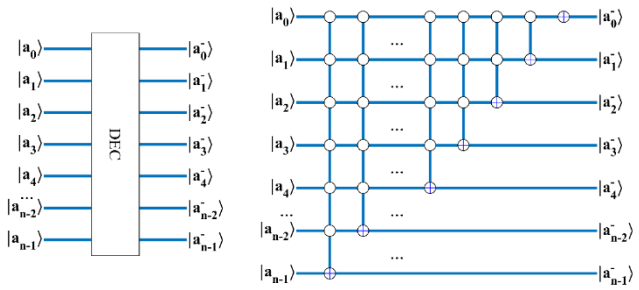
د) بلاک دیاگرام Sum

شکل ۲) مدارهای کوانتومی و بلاک دیاگرام Carry و Sum بر اساس مرجع [۲]



الف) مدار کوانتومی افزاینده

ب) بلاک دیاگرام افزاینده



ج) مدار کوانتومی کاهنده د) بلاک دیاگرام کاهنده

شکل ۳) مدار کوانتومی و بلاک دیاگرام افزاینده و کاهنده رسم شده براساس مرجع [۲۱]

افزایش یک واحد ابتدا با بررسی n-1 کیوبیت کم‌ارزش (تمام کیوبیت‌های عدد بجز کیوبیت پرارزش) صورت می‌گیرد. در صورتی که همه این کیوبیت‌ها یک باشند، پرارزش‌ترین کیوبیت مکمل می‌شود. در مرحل بعد اگر n-2 کیوبیت کم‌ارزش یک باشند، کیوبیت n-2 مکمل می‌شود. آخرین مرحله مکمل نمودن کیوبیت کم‌ارزش است که بدون شرط انجام می‌پذیرد. روال کاهش یک واحد به طور مشابه با بررسی صفر بودن کیوبیت‌ها انجام می‌پذیرد.

۳- روش‌های پیشنهادی

در این مقاله دو رویکرد پیشنهادی برای نهان‌نگاری یک تصویر در سیگنال صوتی بیان شده است. علت انتخاب تصویر به عنوان نهان‌نگاره این است که عموما تولیدکنندگان اثر تمایل دارند لوگوی خود را در اثر صوتی تصنیف شده به عنوان نماد حق کپی قرار دهند. بااین‌وجود هر گونه دنباله کیوبیتی می‌تواند در رویکردهای پیشنهادی جایگزین نهان‌نگاره تصویری شده و نیاز به هیچگونه تغییری در رویکردهای پیشنهادی نیست.

هر دو رویکرد پیشنهادی از سیگنال صوتی کوانتومی $|A\rangle$ در نمایش QRDA با تعداد 2^l نمونه صوتی به عنوان سیگنال میزبان و تصویر دودویی $|WI\rangle$ با ابعاد $2^u \times 2^v$ به عنوان نهان‌نگاره استفاده می‌کنند. با توجه به فرضیات و بر اساس مرجع [۹] $|A\rangle$ به صورت رابطه (۴) تعریف می‌شود.

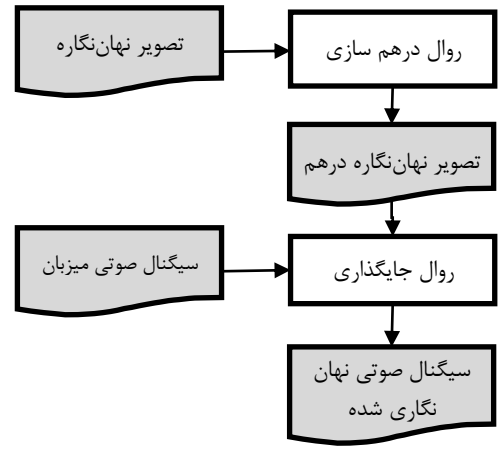
$$|A\rangle = \frac{1}{\sqrt{2^l}} \sum_{T=0}^{2^l-1} |D_T\rangle \otimes |T\rangle \qquad (۴)$$
$$|T\rangle = |t_0 t_1 \dots t_{l-1}\rangle, t_i \in \{0,1\}$$
$$|D_T\rangle = |D_T^0 D_T^1 \dots D_T^{q-2} D_T^{q-1}\rangle, D_T^i \in \{0,1\}$$

همچنین تصویر نهان‌نگاره $|WI\rangle$ بر اساس فرض و مطابق مرجع [۷] به صورت رابطه (۵) قابل تعریف است.

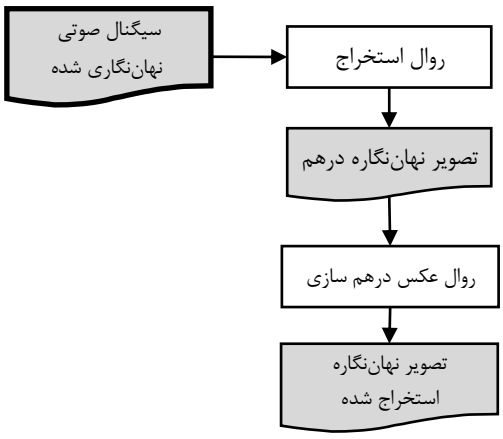
طرح کلی جایگذاری و استخراج روش‌های پیشنهادی در شکل ۴ ارائه شده است. به منظور حذف ویژگی‌های آماری تصویر نهان‌نگاره و دشوارسازی تشخیص این تصویر، پیش از درج نهان‌نگاره در سیگنال صوتی، تصویر درهم‌سازی می‌شود.

$$|WI\rangle = \frac{1}{\sqrt{2^{u+v}}} \sum_{y=0}^{2^u-1} \sum_{x=0}^{2^v-1} |f(y,x)\rangle |yx\rangle = \frac{1}{\sqrt{2^{u+v}}} \sum_{y=0}^{2^u-1} \sum_{x=0}^{2^v-1} |q_{yx}\rangle |yx\rangle, q_{yx} \in \{0,1\} \qquad (۵)$$

روال جایگذاری سیگنال میزبان را دریافت کرده و اطلاعات نهان‌نگاره را در مکان‌های مناسب سیگنال مطابق روش‌های پیشنهادی جایگذاری می‌کند. روال استخراج سیگنال صوتی نهان‌نگاری شده را دریافت کرده و تصویر نهان‌نگاره درهم را از آن استخراج می‌کند. سپس به کمک روال معکوس درهم سازی تصویر اصلی بازسازی می‌شود. در ادامه، ابتدا به‌ارائه روش پیشنهادی درهم‌سازی اشاره خواهد شد. سپس هر کدام از طرح‌های پیشنهادی ارائه می‌گردند.



الف. جایگذاری



ب. استخراج

شکل ۴) طرح کلی روش‌های پیشنهادی. الف. جایگذاری ب. استخراج

۳-۱- درهم سازی تصویر نهان‌نگاره

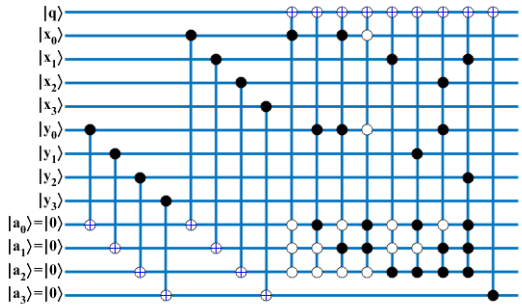
در رویکردهای پیشنهادی ابتدا تصویر نهان‌نگاره $|WI\rangle$ درهم‌سازی می‌شود. درهم سازی یک تصویر، فرایند تبدیل تصویر معنی‌دار به تصویر بی‌معنی است. این علمیات ویژگی‌های آماری تصویر را

حذف می‌کند و در مبحث نهان‌نگاری آشکارسازی تصویر را دشوار می‌کند. روش‌های درهم‌سازی مختلفی تاکنون پیشنهاد شده است. از آن جمله می‌توان به الگوریتم مکعب روبیک[۲۲]، روش درهم-سازی بر اساس تبدیل آرنولد[۲۳]، درهم‌سازی بر مبنای اعداد فیبوناچی[۲۴]، منحنی هیلبرت[۲۵] و معمای سودوکو[۲۶] اشاره کرد. برخی از این روش‌های درهم‌سازی به محاسبات کوانتومی منتقل شده اند که می‌توان به روش‌های درهم‌سازی آرنولد و فیبوناچی[۲۷] و روش درهم‌سازی هیلبرت[۲۸] اشاره کرد. تمام روش‌های یاد شده با تغییر موقعیت پیکسل‌ها، تصویر را درهم-سازی می‌کنند و اکثر آن‌ها نیاز به تصاویر با طول و عرض یکسان دارند. در این مطالعه یک روش درهم‌سازی تصویر متفاوت پیشنهاد شده است که با تغییر مقدار دودویی پیکسل‌ها به جای تغییر مختصات آن‌ها عمل درهم سازی را انجام می‌دهد. شکل ۵ الگوریتم روش درهم‌سازی پیشنهادی را نشان می‌دهد. این الگوریتم به عنوان تابعی بر روی هر پیکسل از تصویر داده شده عمل می‌کند که به صورت مختصات (x,y) و مقدار دودویی آن (q) تعریف شده است. در این روش پیشنهادی پیکسل‌ها بر اساس سه بیت کم ارزش مختصاتشان ($x_2x_1x_0$ xor $y_2y_1y_0$) به هشت گروه مختلف تقسیم می‌شوند. با توجه به اینکه یک پیکسل به کدام گروه تعلق داشته باشد به کمک عملیات منطقی مانند AND، XOR و NOR عملیات متفاوتی روی آن‌ها انجام می‌شود. به منظور اجتناب از تشکیل الگوهای ۸×۸ تکراری، بلوک‌های مجاور با توجه به بیت مرتبه چهارم مختصات تغییر می‌کنند.

```
procedure scramble (x,y,q)
  x=xu-1…x2x1x0
  y=yv-1…y2y1y0
begin
       m=x2x1x0
       n=y2y1y0
       q=q xor (x3 xor y3)
switch (m xor n)
  case 0:q=q xor x0
  case 1:q=q xor y0
  case 2:q=q xor (x0 and y0)
  case 3:q=q xor (x0 nor y0)
  case 4:q=q xor y1;
  case 5:q=q xor y1;
  case 6:q=q xor (x2 and y0)
  case 7:q=q xor (x1 and y2)
end
end procedure
```

شکل ۵) الگوریتم درهم سازی تصویر پیشنهادی

مدار کوانتومی درهم سازی تصویر در شکل ۶ قابل مشاهده است. ورودی‌های مدار $|x_0\rangle \dots |x_3\rangle$، $|y_0\rangle \dots |y_3\rangle$ و $|q\rangle$ و چهار کیوبیت کمکی $|a_0\rangle \dots |a_3\rangle$. کیوبیت کمکی $|a_i\rangle$ حاصل $|x_i\rangle \, XOR \, |y_i\rangle$ را نگهداری می‌کند و به عنوان کیوبیت کنترلی برای انتخاب عملیات مناسب استفاده می‌گردد. شکل ۷ سه تصویر نمونه و نتایج حاصل از اعمال الگوریتم درهم‌سازی پیشنهادی روی آن‌ها را نشان می‌دهد.



شکل ۶) مدار کوانتومی درهم سازی تصویر

شکل ۷) سه تصویر نمونه و نتیجه اجرای درهم‌سازی روی آن‌ها

از آنجایی که ساختار ذاتی تصویر دوبعدی است، تصویر نهان‌نگاره می‌بایست به معادل یک‌بعدی تبدیل شود تا از لحاظ تعداد ابعاد با سیگنال صوت سازگار باشد. برای این تبدیل از نمایش رابطه (۶) استفاده می‌کنیم.

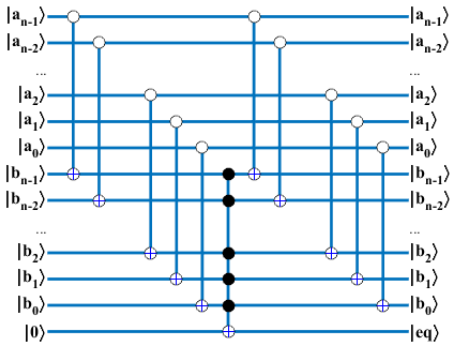
$$|w\rangle = \frac{1}{\sqrt{2^m}} \sum_{j=0}^{2^m-1} |w_j\rangle \otimes |j\rangle$$
$$|j\rangle = |j_0 j_1 \dots j_{m-1}\rangle, j_i \in \{0,1\} \qquad (۶)$$
$$|w_j\rangle \in \{0,1\}$$

تعداد کل پیکسل‌های تصویر نهان‌نگاره برابر با $2^u \times 2^v = 2^{u+v} = 2^m$ می‌باشد. این 2^m پیکسل در حالت کوانتومی $|w\rangle$ با استفاده از دو دنباله کیوبیتی درهم تنیده $|w_j\rangle$ و $|j\rangle$ ذخیره می‌شوند که در مجموع نیاز به m+1 کیوبیت دارد. در این نمایش، $|j\rangle$ همانند اندیس و $|w_j\rangle$ همانند مقدار (کیوبیتی که باید جایگذاری شود) عمل می‌کنند. با توجه به ساختار ذخیره سازی حالت کوانتومی در یک بردار، مشخص می‌گردد که بردار ذخیره سازی تصویر NEQR مطابق رابطه (۵) مشابه حالت کوانتومی پیشنهادی در رابطه (۶) می‌باشد که در آن $|w_j\rangle = |q_{yx}\rangle$ و $|j\rangle = |yx\rangle$ می‌باشد. بنابراین

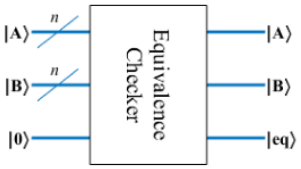
برای تبدیل تصویر به دنباله کیوبیتی، عملا نیاز به هیچ مدار کمکی نیست.

۳-۲- تساوی‌سنج

یک مدار کمکی برای مقایسه تساوی در روال‌های جایگذاری و استخراج نیاز است که در این بخش ارائه می‌گردد. علت عدم استفاده از مدارهای کوانتومی موجود مقایسه گر کاهش پیچیدگی مدار است. مدارهای کوانتومی موجود مقایسه گر، کوچکتر یا بزرگتر بودن را نیز چک می‌کنند که در روال‌های مذکور به آن‌ها نیازی نیست. بنابراین با ساده‌سازی مدارهای کوانتومی مقایسه‌گر می‌توان به مدار کوانتومی تساوی‌سنج دست یافت. شکل ۸ مدار کوانتومی پیشنهادی تساوی‌سنج و بلاک دیاگرام آن را نشان می‌دهد. ورودی‌های مدار دو حالت کوانتومی $|A\rangle$ و $|B\rangle$ هستند که بیانگر دو عدد n بیتی می‌باشند. یک کیوبیت کمکی برای نگهداری حاصل مقایسه نیز مورد نیاز می‌باشد. خروجی‌ها $|A\rangle$ و $|B\rangle$ و $|eq\rangle$ می‌باشند که در حالت تساوی $|A\rangle$ و $|B\rangle$ مقدار $|eq\rangle$ برابر $|1\rangle$ و در حالت عدم تساوی $|0\rangle$ خواهد بود.



الف) مدار کوانتومی



ب) بلاک دیاگرام

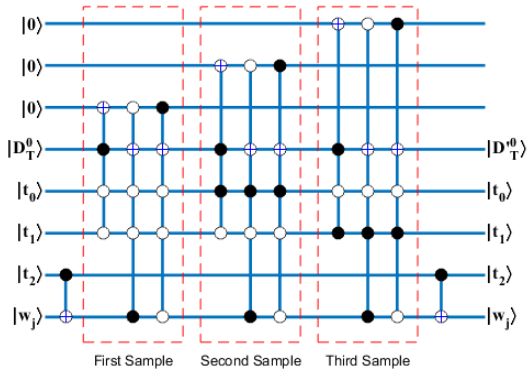
شکل ۸) مدار کوانتومی پیشنهادی تساوی‌سنج و بلاک دیاگرام آن

۳-۳- رویکرد نهان‌نگاری صوت کوانتومی پیشنهادی اول

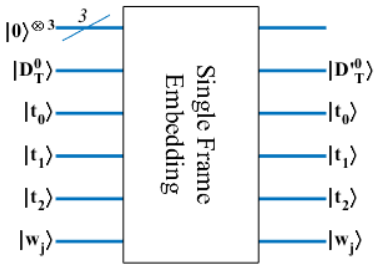
در این رویکرد هر کیوبیت نهان‌نگاره در تعداد فردی نمونه صوتی متوالی جایگذاری می‌شود. جایگذاری در بیت کم‌ارزش هر نمونه صوتی انجام می‌شود. طرح پیشنهادی با تعداد سه نمونه متوالی ارائه می‌گردد که قابل تعمیم به تعداد نمونه‌های بالاتر است. بدیهی است در این روش افزایش تعداد نمونه‌هایی که یک کیوبیت نهان‌نگاره در آن‌ها درج می‌شود باعث کاهش ظرفیت و افزایش مقاومت می‌شود. به منظور کمینه کردن تعداد عملیات کوانتومی، سیگنال صوتی به قاب‌هایی شامل چهار نمونه صوتی تقسیم بندی می‌شود. نمونه چهارم هر قاب دست‌نخورده باقی می‌ماند. برای پرهیز از جایگذاری مستقیم کیوبیت نهان‌نگاره در بیت کم‌ارزش سیگنال میزبان، کیوبیت نهان‌نگاره با بیت سوم زمان، XOR می‌شود. به عبارت دیگر کیوبیت‌های نهان‌نگاره، قبل از جایگذاری به طور یک در میان مکمل می‌شوند. روال کامل جایگذاری یک کیوبیت در نمونه صوتی داده شده به شکل زیر است.

```
if (|t₁t₀>==|00>) then |Dₜ⁰>=|wⱼ> XOR |t₂>;
if (|t₁t₀>==|01>) then |Dₜ⁰>=|wⱼ> XOR |t₂>;
if (|t₁t₀>==|10>) then |Dₜ⁰>=|wⱼ> XOR |t₂>;
```

که در آن $|t_i\rangle$ بیانگر امین کیوبیت $|T\rangle$ و $|D_T^0\rangle$ بیانگر بیت کم‌ارزش نمونه صوتی جاری است. همچنین $|w_j\rangle$ کیوبیت نهان‌نگاره می‌باشد که می‌بایست در سیگنال میزبان درج گردد. شکل ۹ مدار کوانتومی جایگذاری یک کیوبیت نهان‌نگاره در سه نمونه صوتی و بلاک دیاگرام آن را نشان می‌دهد.



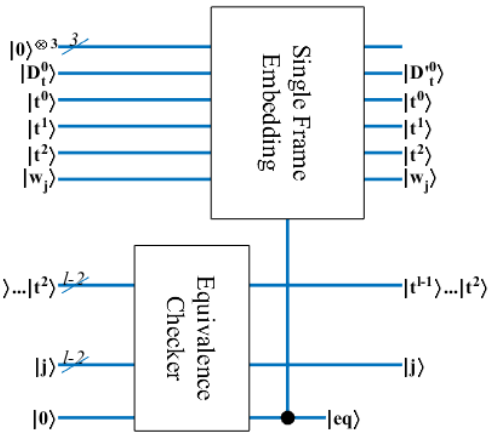
الف) مدار کوانتومی



ب) بلاک دیاگرام

شکل ۹) مدار کوانتومی جایگذاری یک کیوبیت در یک قاب از سیگنال صوتی میزبان به روش پیشنهادی اول و بلاک دیاگرام آن

مدار کوانتومی کامل برای جایگذاری دنباله نهان‌نگاره در سیگنال صوت کوانتومی به‌روش پیشنهادی اول در شکل ۱۰ نشان داده شده است. بلاک تساوی‌سنج قاب‌های صوت متناظر با کیوبیت‌های نهان‌نگاره را انتخاب می‌کند. این کار با مقایسه $|t^2\rangle \dots |t^{l-1}\rangle$ با $|j\rangle$ انجام می‌شود. سه کیوبیت سمت راست مولفه زمان، $|t^0\rangle \dots |t^2\rangle$، کیوبیت کم ارزش نمونه‌های صوت، $|D_t^0\rangle$، و کیوبیت نهان‌نگاره، $|w_j\rangle$، وارد بلاک درج یک کیوبیت در یک قاب می‌شوند که این بلاک، پیشتر توضیح داده شد.



شکل ۱۰) مدار کوانتومی جایگذاری دنباله نهان‌نگاره 2^{l-2} کیوبیتی در سیگنال صوتی میزبان با 2^l نمونه به روش پیشنهادی اول

روال استخراج به این صورت است که ابتدا کیوبیت کم‌ارزش نمونه‌های صوتی اول، دوم و سوم یک قاب داده شده استخراج می‌شوند. اکثریت این سه کیوبیت محاسبه می‌شود و حاصل با سومین کیوبیت کم‌ارزش مولفه زمان XOR می‌شود. منظور از محاسبه اکثریت، شمارش تعداد صفرها و یک‌ها و انتخاب داده‌ای است که فراوانی بیشتر را دارد. به عنوان مثل وجود دو یا سه داده صفر به معنی اکثریت صفر است و وجود دو یا سه داده یک به معنی اکثریت یک است. در تعداد داده فرد، همیشه یکی از داده‌های صفر یا یک اکثریت را دارد و با هم برابر نمی شوند. علت انتخاب تعداد فرد نمونه صوت نیز همین امر است. شکل ۱۱ مدار کوانتومی استخراج یک کیوبیت نهان‌نگاره از قاب مفروض شامل چهار نمونه صوتی و بلاک دیاگرام آن را نشان می‌دهد.

پیش از شروع فرایند استخراج نیاز به تولید یک دنباله کیوبیتی خالی به منظور نگهداری مقادیر استخراج شده نهان‌نگاره است. برای تولید این دنباله، ابتدا حالت کوانتومی $|\psi\rangle_0$ را مطابق رابطه (۷) شامل m+1 کیوبیت صفر تولید می‌کنیم.

$$|\psi\rangle_0 = |0\rangle^{\otimes m+1} \quad (۷)$$

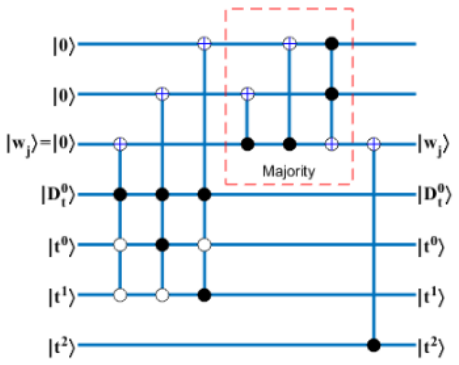
سپس به کمک m گیت‌هادامارد و یک گیت همانی[۱۸] مطابق رابطه (۸) تبدیل U را ایجاد می‌کنیم.

$$U = I \otimes H^{\otimes m} \quad (۸)$$

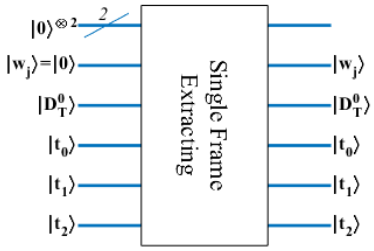
تبدیل یکانی U می‌تواند حالت کوانتومی $|\psi\rangle_0$ را به حالت کوانتومی $|w_{empty}\rangle$ مورد نظر انتقال داده که همان دنباله کیوبیتی خالی مورد نظر است.

همانگونه که در رابطه (۹) قابل مشاهده است حالت کوانتومی بدست آمده از اعمال تبدیل U روی حالت کوانتومی $|\psi\rangle_0$ کاملا مشابه رابطه (۶) می‌باشد که به جای $|w_j\rangle$ ، $|0\rangle$ قرار گرفته است.

$$|w_{empty}\rangle = U(|\psi\rangle_0) = (I|0\rangle)\otimes(H|0\rangle)^{\otimes m} = \frac{1}{\sqrt{2^m}}|0\rangle\otimes\sum_{j=0}^{2^m-1}|j\rangle = \frac{1}{\sqrt{2^m}}\sum_{j=0}^{2^m-1}|0\rangle|j\rangle \quad (۹)$$



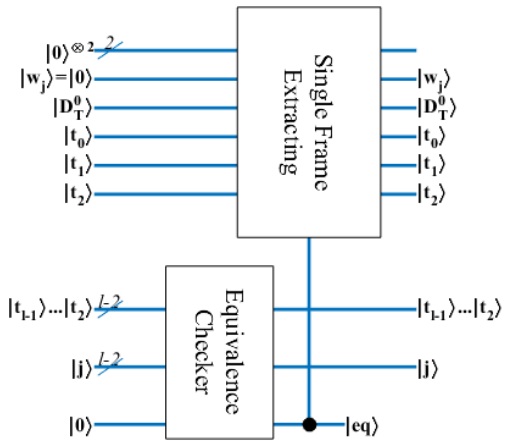
الف) مدار کوانتومی



ب) بلاک دیاگرام

شکل ۱۱) مدار کوانتومی استخراج یک کیوبیت از یک قاب از سیگنال صوتی میزبان به روش پیشنهادی اول و بلاک یاگرام آن

مشابه فرایند جایگذاری، روال استخراج کامل نیازمند یک تساوی‌سنج است تا قاب‌های سیگنال صوتی را با مکان متناظر در دنباله خالی نهان‌نگاره تطبیق دهد. شکل ۱۲ مدار کوانتومی استخراج کامل نهان‌نگاره از سیگنال صوت کوانتومی نهان‌نگاری شده را نشان می‌دهد.



شکل ۱۲) مدار کوانتومی استخراج دنباله نهان‌نگاره 2^{l-2} کیوبیتی از سیگنال صوتی نهان‌نگاری شده با 2^l نمونه به روش پیشنهادی اول

۳-۴- رویکرد نهان‌نگاری صوت کوانتومی پیشنهادی دوم

در این رویکرد تعداد k نمونه صوتی از سیگنال میزبان به عنوان یک قاب، گروه‌بندی می‌شوند که حامل یک کیوبیت از نهان‌نگاره خواهند شد. به منظور جایگذاری یک کیوبیت، مجموع دامنه نمونه‌های صوت در پیمانه 2^k محاسبه می‌شود که آن را r می‌نامیم.

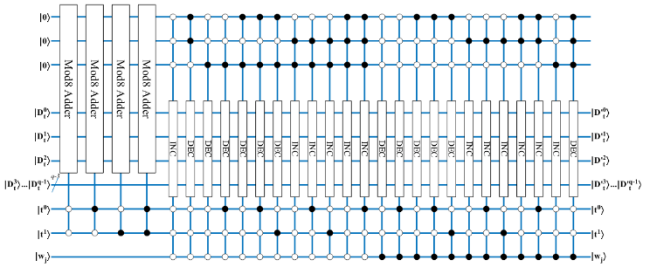
با افزایش یا کاهش یک واحدی مقدار دامنه نمونه‌ها، مقدار r را در مرکز یکی از دسته‌های $[0,2^{k-1}-1]$ و $[2^{k-1},2^{k}-1]$ به ترتیب برای درج کیوبیت $|0\rangle$ یا $|1\rangle$ تنظیم می‌کنیم. در زمان استخراج، مقدار r مجددا محاسبه شده و با توجه به اینکه در کدام یک از دسته‌های مذکور قرار می‌گیرد، کیوبیت استخراج شده مشخص می‌گردد. به‌عنوان مثال برای k=3، مجموع دامنه‌های هر سه نمونه محاسبه می‌شوند و باقیمانده تقسیم آن‌ها بر عدد ۸=$۲^۳$ محاسبه می‌شود. باقیمانده تقسیم هر عدد بر ۸ عددی بین صفر تا ۷ است. این بازه به دو زیر بازه [۳و۰] و [۷و۴] تقسیم می‌شود. در زمان استخراج، مجددا مقدار r محاسبه می‌شود و با توجه به اینکه در کدام زیر بازه قرار می‌گیرد بیانگر کیوبیت نهان‌نگاره $|0\rangle$ یا $|1\rangle$ است. برای افزایش مقاومت در زمان جایگذاری با افزایش یا کاهش مقدار نمونه‌ها به شکلی عمل می‌شود که مقدار محاسبه شده در مرکز زیربازه مورد نظر قرار گیرد. قرار گرفتن مقدار محاسبه شده در مرکز زیربازه درجه‌ای از آزادی را به وجود می‌آورد که در صورت تغییر مقدار دامنه‌ها، مقدار محاسبه شده کماکان در محدوده مورد نظر باقی بماند. با توجه به اینکه مرکز زیربازه‌های ذکر شده یک عدد اعشاری است، عدد صحیحی به عنوان مرکز انتخاب می‌شود که کمترین تغییرات در اندازه دامنه‌ها را نیاز داشته باشد. الگوریتم‌ها و مدارهای کوانتومی ارائه شده در این بخش بر اساس k=3 می‌باشند که به سادگی قابل تعمیم به مقادیر بزرگتر k خواهند بود. شکل ۱۳ الگوریتم جایگذاری رویکرد پیشنهاد دوم را نشان می‌دهد.

```
procedure embed (w,D0,D1,D2)
begin
  r=(D0+D1+D2) mod 8
if (w==0) then
 switch r
   case 0:D0++
   case 3:D0--
   case 4:D0--;D1--
   case 5:D0--;D1--;D2--
   case 6:D0++;D1++;D2++
   case 7:D0++;D1++
end
if (w==1) then
 switch r
  case 0:D0--;D1--
  case 1:D0--;D1--;D2--
  case 2:D0++;D1++;D2++
  case 3:D0++;D1++
  case 4:D0++
  case 7:D0--
end
end procedure
```

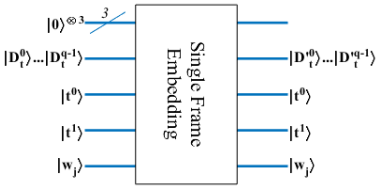
شکل ۱۳) الگوریتم جایگذاری روش نهان‌نگاری پیشنهادی دوم

مدار کوانتومی و بلاک دیاگرام جایگذاری یک کیوبیت نهان‌نگاره در یک قاب از سیگنال صوتی میزبان در شکل ۱۴ ارائه شده است.

کیوبیت‌های دامنه نمونه صوتی، $|D_T^0\rangle \dots |D_T^{q-1}\rangle$، دو کیوبیت کم‌ارزش مولفه زمان، $|t^1\rangle \dots |t^0\rangle$، و سه کیوبیت کمکی با مقدار اولیه $|0\rangle$ به عنوان انباره[۱۹]، به‌همراه کیوبیت نهان‌نگاره، $|w_j\rangle$، ورودی‌های مدار را تشکیل می‌دهند. به کمک دو کیوبیت کم ارزش مولفه زمان، شماره نمونه صوتی تشخیص داده می‌شود و هر کدام از نمونه‌های اول تا چهارم به کمک جمع‌کننده پیمانه ۸، به انباره اضافه می‌شوند. سپس با توجه به مقدار انباره که همان پارامتر محاسبه شده r می‌باشد و مقدار کیوبیت نهان‌نگاره، مطابق الگوریتم جایگذاری، نمونه‌های مورد نظر یک واحد کم یا زیاد می‌شوند.



الف) مدار کوانتومی



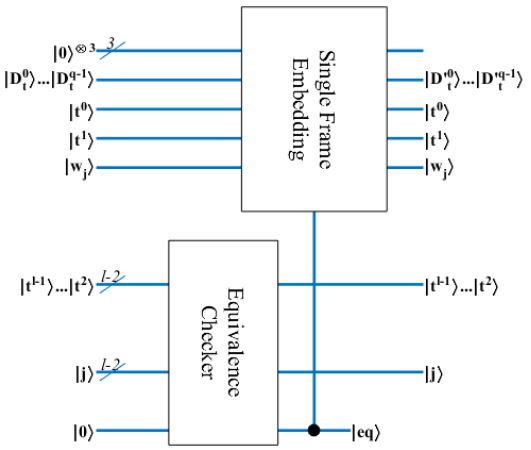
ب) بلاک دیاگرام

شکل ۱۴) مدار کوانتومی جایگذاری یک کیوبیت نهان‌نگاره در یک قاب از سیگنال صوتی میزبان به روش پیشنهادی دوم و بلاک دیاگرام آن

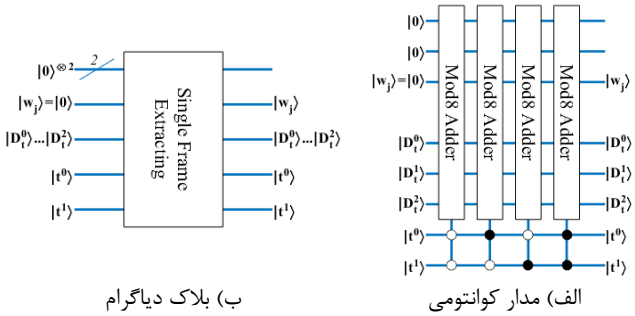
مدار کوانتومی کامل برای جایگذاری دنباله نهان‌نگاره در سیگنال صوت کوانتومی به روش پیشنهادی دوم در شکل ۱۵ نمایش داده شده است. مشابه رویکرد پیشنهادی اول بلاک تساوی‌سنج قاب‌های صوت متناظر با کیوبیت‌های نهان‌نگاره را انتخاب می‌کند. این کار با مقایسه $|t^{l-1}\rangle \dots |t^2\rangle$ با $|j\rangle$ انجام می‌شود. دو کیوبیت کم ارزش مولفه زمان، $|t^1\rangle \dots |t^0\rangle$، دنباله کیوبیت‌های دامنه، $|D_T^0\rangle \dots |D_T^{q-1}\rangle$، سه کیوبیت کمکی با مقدار اولیه $|0\rangle$، و کیوبیت نهان‌نگاره، $|w_j\rangle$، وارد بلاک درج یک کیوبیت در یک قاب می‌شوند و عمل جایگذاری صورت می‌پذیرد.

استخراج یک کیوبیت نهان‌نگاره از یک قاب چهار نمونه ای مفروض، پیچیدگی کمتری نسبت به جایگذاری دارد. همانگونه که پیشتر شرح داده شد، ابتدا مجموع مقادیر چهار نمونه قاب داده شده در پیمانه ۸ محاسبه می‌شود که حاصل یک عدد ۳ کیوبیتی است. کیوبیت با ارزش این عدد مشخص می‌کند که در زیربازه [۳و۰] قرار دارد یا زیربازه [۷و۴]. بنابراین این کیوبیت به عنوان داده استخراج شده لحاظ می‌گردد. شکل ۱۶ مدار کوانتومی

استخراج یک کیوبیت از یک قاب چهارنمونه ای و بلاک دیاگرام آن را نشان می‌دهد. شکل ۱۷ روال کامل استخراج را به صورت مدار کوانتومی نشان می‌دهد که مشابه مدار جایگذاری کامل است.

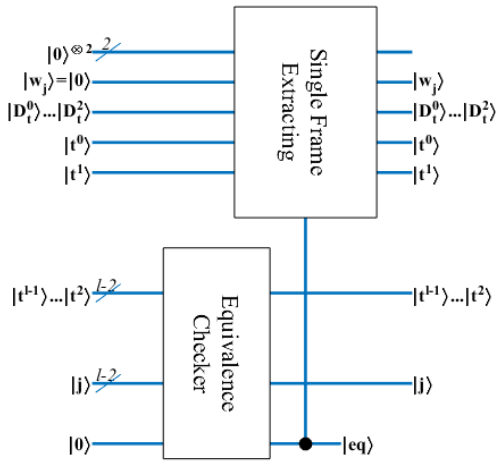


شکل ۱۵) مدار کوانتومی درج دنباله نهان‌نگاره 2^{l-2} کیوبیتی در سیگنال صوتی نهان‌نگاری شده با 2^{l} نمونه به روش پیشنهادی دوم



الف) مدار کوانتومی ب) بلاک دیاگرام

شکل ۱۶) مدار کوانتومی و بلاک دیاگرام استخراج یک کیوبیت نهان‌نگاره از یک قاب چهارنمونه ای مفروض



شکل ۱۷) مدار کوانتومی استخراج دنباله نهان‌نگاره 2^{l-2} کیوبیتی از سیگنال صوتی نهان‌نگاری شده با 2^{l} نمونه به روش پیشنهادی دوم

۳-۵- بازسازی تصویر استخراج شده درهم

تصویری که در دو روش پیشنهادی استخراج شده است، تصویر درهم‌سازی شده است که باید به حالت اصلی خود برگردد. با توجه به اینکه تمام عملیات درهم سازی تصویر شامل XOR می‌باشد و به دلیل متقارن بودن عمل XOR، در صورت اعمال مجدد الگوریتم درهم‌سازی روی تصویر درهم، تصویر اصلی به دست می‌آید. بنابراین نیازی به تعریف روال جدید برای بازسازی تصویر نمی باشد.

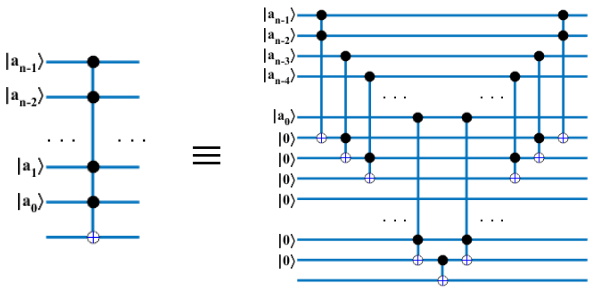
۴- تحلیل پیچیدگی مدار

پیچیدگی یک مدار کوانتومی میزان رشد مدار با افزایش تعداد ورودی‌ها می‌باشد که وابسته به اجزای سازنده مدار است. همچنین پیچیدگی مدار وابسته به این است که چه گیت‌هایی به عنوان گیت پایه در نظر گرفته شود.

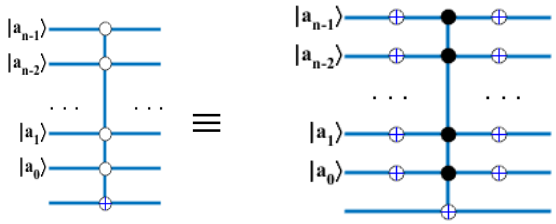
در این مقاله عملگرهای یکانی ۲×۲ شامل گیت هادامارد و گیت نات[۲۰] به عنوان واحد در نظر گرفته شده‌اند. گیت کنترل نات[۲۱] به عنوان واحد پایه در نظر گرفته شده است و سایر گیت‌ها به کمک گیت کنترل‌نات شبیه‌سازی شده‌اند. به عنوان مثال گیت تعویض[۲۲] می‌تواند با سه گیت کنترل نات شبیه‌سازی شده و گیت تافولی[۲۳]با شش گیت کنترل نات ساخته شود. علاوه براین، بر اساس مرجع [۲۹] همانگونه که در شکل ۱۸-الف مشاهده می‌شود، یک گیت n-کنترل نات ($n\geq3$) می‌تواند با استفاده از 2(n-1) گیت تافولی و یک گیت کنترل نات ساخته شود. با جایگزینی هر گیت تافولی با شش گیت کنترل نات، پیچیدگی یک گیت n-کنترل نات برابر با 12n-11 می‌باشد. کنترل‌های صفر (دایره‌های سفید رنگ در مدارهای کوانتومی) می‌توانند به کمک دو گیت نات اضافه، یکی قبل و دیگری بعد از کیوبیت‌های کنترلی شبیه‌سازی شوند و مطابق شکل ۱۸-ب به کنترل‌های یک (دایره‌های سیاه رنگ) تبدیل شوند. بنابراین پیچیدگی مداری یک گیت n-کنترل نات که کیوبیت‌های کنترلی آن تماما یک نیستند دو واحد بیشتر از یک n-کنترل نات با کیوبیت‌های کنترلی تمام یک و برابر 12n-9 می‌باشد. بدیهی است که این دو واحد اضافه معادل پیچیدگی دو گیت نات اضافه شده قبل و بعد از کیوبیت‌های کنترلی است. یک حالت خاص و پر کاربرد گیت نات ۰۱ می باشد. گیت ۲-کنترل نات با یک کنترل صفر و یک کنترل یک که می‌تواند با هشت گیت کنترل نات شبیه سازی شود (۶ کنترل نات مشابه تافولی و دو نات اضافه قبل و بعد از کنترل صفر). جدول ۲ پیچیدگی گیت‌های ذکر شده را جمع‌بندی می‌کند.

جدول ۲- پیچیدگی گیت‌های کوانتومی

گیت	پیچیدگی
نات	۱
هادامارد	۱
کنترل نات	۱
کنترل نات صفر	۳
تعویض	۳
تافولی	۶
۰۱-نات	۸
n-کنترل نات بدون کنترل صفر	12n-11
n-کنترل نات با کنترل صفر	12n-9



الف ساخت گیت n-کنترل نات با گیت‌های تافولی و کنترل نات



ب) ساخت کنترل صفر(○) با استفاده از گیت‌های نات و کنترل یک (●)

شکل ۱۸) شبیه سازی گیت‌های پیچیده با استفاده از گیت‌های ساده تر

تحلیل پیچیدگی هر بخش از مدارهای ارائه شده در ادامه بیان می‌شود و سپس پیچیدگی مدارهای کامل جایگذاری و استخراج هر روش محاسبه می‌گردد.

- ماژول جمع‌کننده پیمانه ۸
  - ماژول Carry استفاده شده در جمع‌کننده مطابق شکل ۲-الف شامل دو گیت تافولی و یک کنترل نات می‌باشد که پیچیدگی آن $O(2 \times 6 + 1) = O(13)$ می‌باشد.
  - ماژول Sum استفاده شده در جمع‌کننده مطابق شکل ۲-ج شامل دو گیت کنترل نات می‌باشد که پیچیدگی آن $O(2 \times 1) = O(2)$ می‌باشد.
  - ماژول جمع‌کننده پیمانه ۸ مطابق شکل ۱-الف شامل پنج ماژول Carry، و سه ماژول Sum و یک گیت کنترل نات می‌باشد که پیچیدگی آن $O(5 \times 13 + 3 \times 2 + 1) = O(72)$ می‌باشد.
- ماژول افزاینده دودویی ۸ کیوبیتی بر اساس شکل ۳-الف و به ازای n=8
  - شامل $\sum_{k=0}^{7} k - ControlNot$ خواهد بود که برای k=0,1,2 به ترتیب منظور گیت‌های نات، کنترل نات و تافولی می‌باشد. بنابراین پیچیدگی مداری به صورت $O(1 + 1 + 6 + \sum_{k=3}^{7}(12k - 11)) = O(253)$ خواهد بود.
- ماژول کاهنده دودویی ۸ کیوبیتی بر اساس شکل ۳-ج و به ازای n=8
  - این ماژول را می‌توان با مکمل کردن تمام کیوبیت‌های عدد، افزایش آن و سپس مکمل کردن مجدد شبیه‌سازی کرد بنابراین پیچیدگی آن برابر $O(1 + 253 + 1) = O(255)$ می‌باشد.
- مدار درهم سازی/بازسازی مطابق شکل ۶ شامل
  - نه گیت کنترل نات با پیچیدگی $O(9 \times 1) = O(9)$
  - چهار گیت ۴-کنترل نات با کنترل صفر با پیچیدگی $O(4 \times (12 \times 4 - 9)) = O(156)$
  - سه گیت ۵-کنترل نات با کنترل صفر با پیچیدگی برابر با $O(3 \times (12 \times 5 - 9)) = 153$
  - یک گیت ۵-کنترل نات بدون کنترل صفر با پیچیدگی $O((12 \times 5 - 11)) = O(49)$
  - در مجموع مدار درهم سازی/بازسازی با پیچیدگی $O(9 + 156 + 153 + 49) = O(367)$ محاسبه می‌گردد.
- تساوی‌سنج مطابق شکل ۸-الف شامل
  - 2n گیت کنترل نات صفر با پیچیدگی $O(6n)$
  - گیت n-کنترل نات با پیچیدگی $O(12n - 11)$
  - در مجموع پیچیدگی این مدار به صورت $O(18n - 11)$ محاسبه می‌گردد.
- ماژول جایگذاری یک کیوبیت در یک قاب سیگنال صوتی (روش اول) مطابق شکل ۹-الف شامل
  - دو گیت کنترل نات با پیچیدگی $O(2 \times 1) = O(2)$
  - سه گیت ۳-کنترل نات با کنترل صفر دارای پیچیدگی $O(3 \times (12 \times 3 - 9)) = O(81)$
  - شش گیت ۴-کنترل نات با کنترل صفر دارای پیچیدگی $O(6 \times (12 \times 4 - 9)) = O(234)$
  - پیچیدگی کل ماژول $O(2 + 81 + 234) = O(317)$ می‌باشد.
- مدار جایگذاری کامل (روش اول) مطابق شکل ۱۰ شامل
  - یک تساوی‌سنج l-2 بیتی با پیچیدگی $O(18(l - 2) - 11) = O(18l - 47)$
  - ماژول جایگذاری یک کیوبیت در یک قاب سیگنال صوتی با پیچیدگی $O(317)$
  - در مجموع پیچیدگی این مدار به صورت $O(18l + 270)$ محاسبه می‌شود.

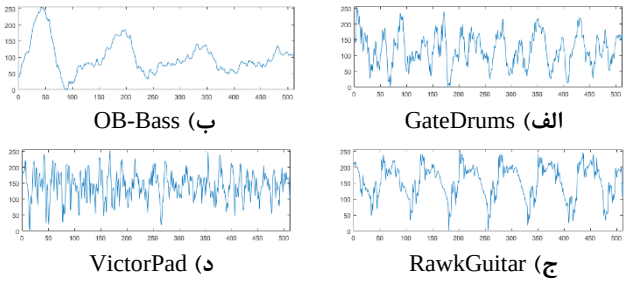
- ماژول استخراج یک کیوبیت از یک قاب سیگنال صوتی مطابق شکل ۱۱-الف شامل
  - سه گیت کنترل نات با پیچیدگی $O(3 \times 1) = O(3)$
  - یک گیت تافولی با پیچیدگی $O(6)$
  - سه گیت ۳-کنترل نات با کنترل صفر و پیچیدگی $O(3 \times (12 \times 3 - 9)) = O(81)$
  - در مجموع این ماژول از پیچیدگی $O(3 + 6 + 81) = O(90)$ برخوردار است.
- مدار استخراج کامل (روش اول) مطابق شکل ۱۲ شامل
  - یک تساوی‌سنج l-2 بیتی با پیچیدگی $O(18(l-2) - 11) = O(18l - 47)$
  - ماژول استخراج یک کیوبیت از یک قاب سیگنال صوتی با پیچیدگی $O(90)$
  - در مجموع پیچیدگی این مدار به صورت $O(18l + 43)$ محاسبه می‌شود.
- ماژول جایگذاری یک کیوبیت در یک قاب سیگنال صوتی (روش دوم) مطابق شکل ۱۴-الف
  - سه گیت ۰۱-نات با پیچیدگی $O(3 \times 8) = O(24)$
  - دو گیت تافولی با پیچیدگی $O(2 \times 6) = O(12)$
  - چهار ماژول جمع‌کننده پیمانه ۸ با پیچیدگی $O(4 \times 72) = O(288)$
  - ۲۴ ماژول ۶-کنترل نات با پیچیدگی $O(24 \times (12 \times 6 - 9)) = O(1512)$
  - ۱۲ ماژول افزاینده دودویی ۸ کیوبیتی با پیچیدگی $O(12 \times 253) = O(3036)$
  - ۱۲ ماژول کاهنده دودویی ۸ کیوبیتی با پیچیدگی $O(12 \times 255) = O(3060)$
  - در مجموع پیچیدگی این ماژول به صورت $O(7932)$ محاسبه می‌شود.
- مدار جایگذاری کامل (روش دوم) مطابق شکل ۱۵ و مشابه مدار جایگذاری روش اول به صورت $O(18(l-2) - 11) + 7932 = O(18l + 7885)$ محاسبه می‌شود.
- ماژول استخراج یک کیوبیت از یک قاب سیگنال صوتی (روش دوم) مطابق شکل ۱۶-الف مشابه ۳ بند اول ماژول جایگذاری یک کیوبیت در یک قاب سیگنال صوتی است و پیچیدگی آن به صورت $O(24 + 12 + 288) = O(324)$ می‌باشد.
- مدار استخراج کامل (روش دوم) مطابق شکل ۱۷ و مشابه روش اول به صورت $O(18(l-2) - 11) + 324 = O(18l + 277)$ محاسبه می‌شود.

بنابر آنچه در بالا محاسبه شد، مدار درهم‌سازی/بازسازی پیشنهادی تصویر با پیچیدگی O(367) در مقایسه با درهم سازی-های هیلبرت با پیچیدگی $O(18n^2+18n-2)$ [۲۸] و آرنولد و فیبوناچی با پیچیدگی O(140n) [۲۷] بسیار ساده‌تر بوده و از مرتبه ثابت است. همچنین پیچیدگی مداری روش پیشنهادی اول شامل مدارهای درهم‌سازی، جایگذاری، استخراج و بازسازی به صورت $O(367 + 18l + 270 + 18l + 43 + 367) = O(36l + 1047)$ و روش دوم نیز به صورت $O(36l + 8896)$ می‌باشد. هر دو روش پیشنهاد شده از پیچیدگی درجه یک برخوردار هستند و با رشد طول سیگنال صوتی به صورت خطی رشد می‌کنند.

۵- نتایج آزمایشگاهی و تحلیل آن‌ها

با توجه به اینکه هنوز کامپیوتر کوانتومی در دسترس پژوهشگران قرار نگرفته است، مشابه سایر پژوهش‌های حوزه محاسبات کوانتوم، در این پژوهش رویکرد شبیه‌سازی دنبال شده است. شبیه‌سازی‌ها روی یک کامپیوتر با پردازنده اینتل Core™ i5 M540 2.53GHz با حافظه ۸ گیگابایت و سیستم‌عامل ۶۴ بیتی به کمک نرم‌افزار Matlab 2016a انجام شد. چهار فایل صوتی از وب سایت MusicRadar [۳۰] دریافت شد. فایل‌های دریافت شده از نرخ ۴۴۱۰۰ هرتز به نرخ ۸۱۹۲ هرتز بازنمونه‌برداری شدند و از هرکدام ۵۱۲ نمونه صوتی (l=9) در شبیه سازی‌ها به کار گرفته شد. نمونه‌های صوتی به ۲۵۶ سطح کوانتیزه شدند (q=8). شکل۱۹ شکل‌موج فایل‌های صوتی استفاده شده در آزمایش‌ها را نشان می‌دهد. همچنین شکل ۲۰، شش تصویر مختلف استفاده شده از آزمایش‌ها را نمایش می‌دهد.

در آزمایش‌های انجام شده، علاوه بر دو روش پیشنهادی، روش‌های ارائه شده توسط کیو و همکاران[۱۱] و چن و همکاران[۲۰] نیز شبیه‌سازی شدند. در این شبیه‌سازی، جایگذاری هر کیوبیت از نهان‌نگاره در یکی از چهار نمونه متوالی سیگنال صوت میزبان انجام شد تا ظرفیت ذخیره‌سازی در تمام روش‌ها یکسان باشد و با ثابت بودن ظرفیت ذخیره‌سازی، بتوان مقایسه عادلانه‌ای بین شفافیت رویکردها و همچنین بین مقاومت آن‌ها انجام داد.



شکل ۱۹) چهار سیگنال صوتی استفاده شده در شبیه‌سازی

۵-۱- ارزیابی شفافیت

شفافیت اطمینان می‌دهد که کیفیت سیگنال به صورت مشهود تغییر نکرده و قابل درک توسط شنونده نیست. به منظور ارزیابی

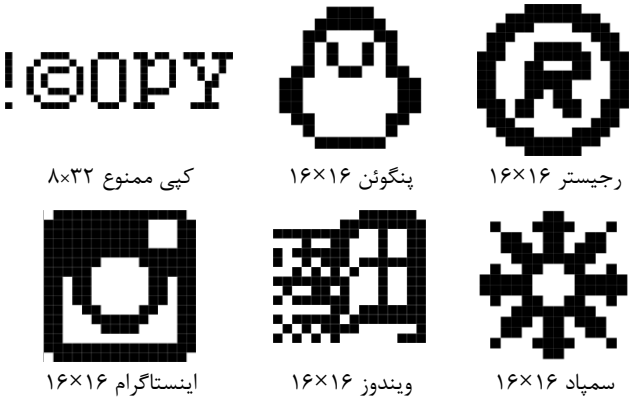
شفافیت روش‌های پیشنهادی از معیار سیگنال به نویز (SNR) استفاده شده است. تعریف این معیار به صورت نسبت توان سیگنال به توان نویز زمینه به دسیبل است که در رابطه (۱۰) محاسبه شده است. همچنین معیار PSNR نسبت اوج سیگنال به نویز را مطابق رابطه (۱۱) نشان می‌دهد.

$$SNR = 10\log\left(\frac{P_s}{P_n}\right) = 10\log\left(\frac{\sum_{t=0}^{2^{l-1}} D_t^2}{\sum_{t=0}^{2^{l-1}}(D_t - D_t')^2}\right) \quad (۱۰)$$

$$PSNR = 10\log\left(\frac{MAX_s^2}{P_n}\right) = 20\log(\mathrm{MAX_s}) - 10\log\left(\sum_{t=0}^{2^{l-1}}(D_t - D_t')^2\right) \quad (۱۱)$$

که P_s و P_n به‌ترتیب بیانگر توان موثر سیگنال و نویز، D_t و $D't$ به ترتیب بیانگر دامنه نمونه صوتی سیگنال میزبان و نهان‌نگاری شده در زمان t و MAX_s بیانگر بیشترین مقدار سیگنال می‌باشند.

نتایج اجرای آزمایش‌ها در جدول ۳ ارائه شده اند. با مقایسه مقادیر به‌دست‌آمده در دو روش پیشنهادی مشخص می‌شود شفافیت دو روش در یک سطح بوده که این مقادیر نسبت به مقادیر رویکرد کیو و همکاران و رویکرد pMSQ2 ارائه شده توسط چن و همکاران بیشتر هستند و اختلاف ناچیزی با رویکرد pMSQ1 دارند.



شکل ۲۰) تصاویر استفاده شده در شبیه سازی

۵-۲- ارزیابی مقاومت

در مباحث امنیت داده و اطلاعات، مقاومت به توانایی تحمل سیگنال ایجاد شده توسط یک تکنیک در برابر تغییراتی است که ممکن است بدنه عملیاتی سیستم را تحت تاثیر قرار دهد. مقاومت پارامتری است که به صورت گسترده پایداری یک الگوریتم نهان‌نگاری را ارزیابی می‌کند. غالبا معیار نرخ خطای بیت(BER) برای اندازه‌گیری مقاومت سیگنال نهان‌نگاری شده در برابر حملات استفاده می‌شود که به صورت تعداد بیت‌های تغییریافته تقسیم بر تعداد کل بیت‌های نهان‌نگاره اصلی محاسبه می‌شود. رابطه (۱۲) نحوه محاسبه BER را بیان می‌کند.

$$BER(|I_{org}\rangle, |I_{ext}\rangle) = \left(\frac{\sum_{i=0}^{2^m-1}|P_i - P_i'|}{2^m}\right) \quad (۱۲)$$

که $|I_{org}\rangle$ و $|I_{ext}\rangle$ به ترتیب تصاویر اصلی و استخراج شده هستند و P_i و P'_i به ترتیب اطلاعات تصویر در موقعیت i از تصویر اصلی و استخراج شده می‌باشند.

در یک کانال کوانتومی باز در تعامل با محیط خارجی، کیوبیت‌های ارسالی مستعد پذیرش نویز می‌باشند. به منظور ارزیابی و نمایش مقاومت روش‌های پیشنهادی، در این بخش، شبیه‌سازی و تحلیل روی چهار حمله نویز پائولی ارائه شده است.

به طور کلی چهار نویز کوانتومی شامل $\sigma_I, \sigma_x, \sigma_y, \sigma_z$ وجود دارد. با توجه به اینکه این نویزها با ماتریس‌های پائولی متناظر هستند به آن‌ها چهار نویز ماتریس پائولی نیز گفته می‌شود. این ماتریس‌ها به صورت زیر تعریف می‌شوند [۱۱].

$$\sigma_I = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix} \qquad \sigma_x = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$
$$\sigma_y = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix} \qquad \sigma_z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \quad (۱۳)$$

که σ_I ماتریس همانی است و به این معنی است که نویزی روی کیوبیت اتفاق نمی‌افتد. σ_x معکوس‌کننده بیت و σ_z معکوس‌کننده فاز است. همچنین $\sigma_y = i\sigma_x\sigma_z$ برهم‌نهی σ_x و σ_z با فاز کلی $\pi/2$ می‌باشد. بدیهی است که انواع نویزی که می‌بایست درمورد آن‌ها بحث کرد σ_x و σ_y و σ_z می‌باشند.

۵-۲-۱- نویز معکوس کننده بیت

برای یک کانال کوانتومی، نویز معکوس‌کننده بیت حالت کیوبیت را با احتمال p-1 از $|0\rangle$ به $|1\rangle$ یا بالعکس انتقال می‌دهد. این عمل می‌تواند به صورت دو عملگر $E_0 = \sqrt{p}I = \sqrt{p}\begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}$ و $E_1 = \sqrt{1-p}X = \sqrt{1-p}\begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$ توصیف شود.

در آزمایش انجام شده، یک تصویر نهان‌نگاره ثابت (تصویر رجیستر ۱۶×۱۶) درون چهار سیگنال صوتی جایگذاری شد. سپس با احتمالات مختلف $1-p \in \{0.01, 0.02, 0.05, 0.1, 0.2, 0.3\}$ نویز معکوس کننده بیت روی سیگنال نهان‌نگاری شده اعمال شد و پس از استخراج تصویر نهان‌نگاری شده معیار BER محاسبه گردید. به منظور افزایش دقت محاسبه فرایند ذکر شده ۱۰۰ بار انجام شد و میانگین BERهای بدست آمده ثبت شد که نتایج در جدول ۴ ارائه شده اند.

به منظور درک بهتر مقادیر ارائه شده در جدول ۴، به ازای مقادیر BER مختلف تصاویر نمونه‌ای در جدول ۵ نشان داده شده است.تصاویر ارائه شده در جدول ۵ به صورت نمونه نشان می‌دهند که مقادیر BER مختلف با چه میزان اعوجاج در تصویر مرتبط می‌باشند. شایان ذکر است که به ازای یک مقدار BER مشخص ممکن است شکل تصویر استخراج شده متفاوت از آنچه در جدول ۵ ارائه شده، باشد ولی میزان اعوجاج تفاوتی ندارند.

جدول ۳. مقادیر SNR برای چهار سیگنال صوتی پس از جایگذاری شش تصویر مختلف با استفاده از دو روش پیشنهادی و روش‌های پیشین

نام تصویر	سیگنال صوت	روش پیشنهادی اول		روش پیشنهادی دوم		روش کیو و همکاران[۱۱]		روش چن و همکاران (pMSQ1) [۲۰]		روش چن و همکاران (pMSQ2) [۲۰]	
		PSNR	SNR	PSNR	SNR	PSNR	SNR	PSNR	SNR	PSNR	SNR
اینستاگرام ۱۶×۱۶	Drums	52.40	46.35	52.86	46.81	50.54	44.50	53.45	47.40	48.70	42.65
	OB-Bass	52.29	46.63	52.25	46.59	50.69	45.03	53.43	47.77	48.31	42.65
	RawkGuitar	52.53	47.54	52.44	47.45	50.74	45.76	53.35	48.36	49.04	44.06
	VictorPad	52.47	47.79	52.69	48.02	51.31	46.64	53.46	48.79	48.73	44.06
ویندوز ۱۶×۱۶	Drums	52.73	46.68	52.12	46.07	50.27	44.23	53.49	47.44	48.93	42.88
	OB-Bass	52.38	46.72	52.16	46.51	51.01	45.35	53.49	47.83	48.92	43.26
	RawkGuitar	52.30	47.31	52.53	47.54	50.66	45.68	53.42	48.43	48.74	43.75
	VictorPad	52.42	47.75	52.39	47.71	50.77	46.10	53.36	48.69	48.47	43.80
کپی ممنوع ۸×۳۲	Drums	52.25	46.20	52.27	46.22	50.23	44.19	53.49	47.44	48.48	42.43
	OB-Bass	52.38	46.72	52.18	46.52	51.12	45.47	53.57	47.91	48.42	42.76
	RawkGuitar	52.37	47.38	52.46	47.47	50.67	45.68	52.84	47.86	48.59	43.60
	VictorPad	52.49	47.82	52.48	47.81	51.18	46.51	53.38	48.70	49.03	44.35
سمپاد ۱۶×۱۶	Drums	52.87	46.82	51.78	45.73	50.25	44.21	53.89	47.84	48.84	42.80
	OB-Bass	52.74	47.09	52.55	46.90	51.23	45.57	53.41	47.75	48.54	42.88
	RawkGuitar	52.18	47.19	52.36	47.37	50.63	45.65	52.86	47.87	48.82	43.83
	VictorPad	52.32	47.65	52.03	47.36	51.18	46.52	53.33	48.66	48.88	44.20
پنگوئن ۱۶×۱۶	Drums	52.51	46.46	52.04	45.99	50.20	44.16	53.29	47.24	48.34	42.30
	OB-Bass	52.44	46.78	52.44	46.78	51.07	45.41	53.02	47.36	48.23	42.56
	RawkGuitar	52.22	47.24	52.38	47.39	50.87	45.89	53.02	48.04	48.82	43.83
	VictorPad	52.65	47.97	52.29	47.62	51.31	46.64	53.78	49.11	49.23	44.55
رجیستر ۱۶×۱۶	Drums	52.37	46.32	52.35	46.29	50.52	44.48	53.11	47.07	48.73	42.68
	OB-Bass	52.51	46.85	52.53	46.87	50.97	45.32	53.58	47.92	48.74	43.08
	RawkGuitar	52.36	47.37	52.45	47.46	50.70	45.72	52.42	47.44	48.33	43.35
	VictorPad	52.41	47.74	52.29	47.62	51.44	46.77	53.61	48.94	48.67	43.99

همانگونه که در جدول ۴ مشاهده می‌شود، با اعمال نویز معکوس کننده بیت با احتمال ۰.۰۱ در روش‌های کیو و همکاران و pMSQ1 اعوجاجی به میزان BER=0.01 مشاهده می‌گردد. در حالیکه هر دو روش پیشنهادی تا مقدار احتمال ۰.۰۵ در برابر نویز از خود مقاومت نشان داده اند (BER=0.00). با افزایش احتمال نویز، روش دوم نسبت به روش اول مقاومت بیشتری نشان می‌دهد و میزان نرخ خطای بیت در روش دوم تقریبا نصف روش اول است.

۵-۲-۲- نویز معکوس کننده فاز (σ_z)

تاثیر این نویز به صورت $|0\rangle \rightarrow |0\rangle$ و $|1\rangle \rightarrow -|1\rangle$ می‌باشد.

همانگونه که پیشتر اشاره شد، باتوجه به اینکه دامنه نمونه‌های سیگنال صوت و پیکسل‌های تصویر نهان‌نگاره همگی به صورت دنباله‌هایی از کیوبیت‌ها کدگذاری شده‌اند، تغییر فاز تاثیری در سیگنال صوت حامل و تصویر نهان‌نگاره ندارد. درنتیجه رویکردهای پیشنهادی به طور موثر در مقابل حمله نویز معکوس‌کننده فاز مقاوم هستند.

۵-۲-۳- نویز معکوس کننده بیت و فاز (σ_y)

نویز معکوس کننده بیت و فاز حاصل برهم‌نهی نویز بیت و نویز فاز با فاز کلی $\pi/2$ می‌باشد. همانگونه که اشاره شد، نویز معکوس کننده فاز، تاثیری در سیگنال صوت حامل و تصویر نهان‌نگاره ندارد و فقط نویز معکوس‌کننده بیت است که اثرگذار است. بنابراین شبیه‌سازی مربوط به نویز معکوس‌کننده بیت (σ_x) مقاومت رویکردهای پیشنهادی را در مقابل نویز معکوس کننده بیت و فاز (σ_y) نیز نشان می‌دهند.

۵-۳- ارزیابی ظرفیت

ظرفیت یک روش نهان‌نگاری به تعداد کیوبیت‌هایی گفته می‌شود که به کمک آن روش می‌توان در سیگنال میزبان جایگذاری کرد.

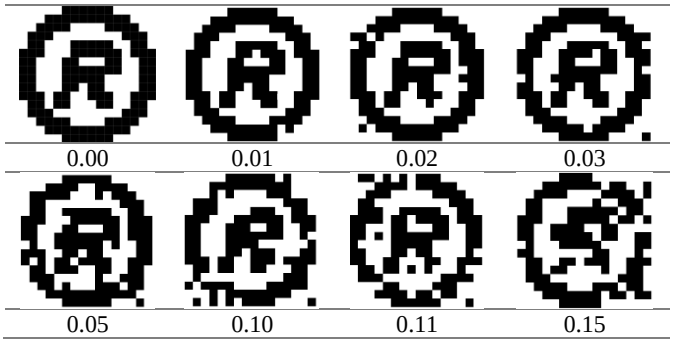
این پارامتر براساس واحد بیت بر ثانیه (bps) بیان شود. با توجه به اینکه هر دو رویکرد پیشنهادی یک کیوبیت نهان نگاره را در یک قاب سیگنال با چهار نمونه صوتی ذخیره می‌کنند ظرفیت این رویکردها با فرض اینکه سیگنال صوت میزبان به صورت ۸۱۹۲ بیت‌برثانیه نمونه برداری شده باشد به صورت زیر محاسبه می‌شود.

$$\text{Payload} = 8192 \text{ bps} / 4 = 2048 \text{ bps} \quad (۱۴)$$

جدول ۴. مقادیر متوسط BER به دست آمده از آزمایش ارزیابی مقاومت پنج الگوریتم در مقابل نویز معکوس کننده کیوبیت با احتمالات متفاوت روی چهار سیگنال صوتی مختلف که تصویر یکسانی در آن‌ها نهان‌نگاری شده است.

	مقادیر BER				
1-p	روش پیشنهادی اول	روش پیشنهادی دوم	روش کیو و همکاران	روش چن و همکاران (pMSQ1)	روش چن و همکاران (pMSQ2)
0.01	0.00	0.00	0.01	0.01	0.00
0.02	0.00	0.00	0.02	0.02	0.01
0.05	0.00	0.00	0.03	0.03	0.02
0.10	0.01	0.01	0.04	0.04	0.03
0.20	0.05	0.02	0.07	0.06	0.06
0.30	0.10	0.05	0.13	0.12	0.11

جدول ۵ تصاویر نهان‌نگاره نمونه استخراج شده از سیگنال نهان‌نگاری شده در معرض نویز و میزان BER مرتبط با آن‌ها



۶- جمع بندی و نتیجه گیری

در سال‌های اخیر، چندرسانه‌ای دیجیتال توسعه پیدا کرده و از شبکه‌های کوانتومی سر برآورده است که در نتیجه آن محافظت از حق کپی چند رسانه‌ای کوانتومی یک موضوع پراهمیت شمرده می‌شود. نهان‌نگاری کوانتومی به عنوان یک فناوری امنیتی بنیادی یک روش اثبات شده برای حفاظت از حقوق مالکین است که اطلاعات مالک را در سیگنال دیجیتال جایگذاری می‌کند. با وجود دستیابی‌های زیادی در حوزه نهان‌نگاری تصاویر کوانتومی، ادبیات محدودی در حوزه نهان‌نگاری صوت کوانتومی به چشم می‌خورد. با توجه به اهمیت معیار مقاومت در مقوله نهان‌نگاری، در این پژوهش دو رویکرد متفاوت نهان‌نگاری صوت کوانتومی پیشنهاد گردید. رویکرد اول یک کیوبیت نهان‌نگاره را در تعداد فردی از نمونه‌های صوتی سیگنال میزبان جایگذاری کرده و با استفاده از روش رای‌گیری اکثریت، کیوبیت صحیح را استخراج می‌کند. در رویکرد پیشنهادی دوم، تعداد k نمونه صوتی از سیگنال میزبان به عنوان یک قاب، گروه بندی می‌شوند که حامل یک کیوبیت از نهان‌نگاره خواهند شد. به‌منظور جایگذاری یک کیوبیت، مجموع دامنه نمونه‌های صوت در پیمانه 2^k محاسبه می‌شود (r)، و با افزایش یا کاهش مقدار دامنه نمونه‌ها، مقدار r را در مرکز یکی از دسته‌های $[0,2^{k-1}-1]$ و $[2^{k-1},2^k-1]$ به ترتیب برای درج کیوبیت $|0\rangle$ یا $|1\rangle$ تنظیم می‌کنیم. در زمان استخراج، مقدار r مجددا محاسبه شده و با توجه به اینکه در کدام یک از دسته‌های مذکور قرار می‌گیرد، کیوبیت استخراج شده مشخص می‌گردد. برای هر کدام از رویکردهای ارائه شده، مدارهای کوانتومی آن‌ها به همراه تحلیل پیچیدگی مدارها ارائه شدند. پیچیدگی مداری در هر دو رویکرد پیشنهادی برای سیگنالی به طول l، از مرتبه $O(l)$ است. این بدین معنی است که با افزایش طول سیگنال، پیچیدگی مدار به صورت خطی رشد می‌کند که از بهترین پیچیدگی‌ها محسوب می‌شود. ارزیابی شفافیت دو رویکرد پیشنهای مقادیر بین ۴۵.۷۳ تا ۴۸.۰۲ دسیبل را نشان داد که برای یک نهان‌نگاری در سیگنال میزبان هشت کیوبیتی (۲۵۶ سطحی) مقادیر بالایی محسوب می‌شوند. همچنین ارزیابی مقاومت صورت گرفته با اعمال نویز معکوس کننده با احتمالات ۰.۰۱ تا ۰.۳۰ نشان داد که رویکرد پیشنهادی دوم از مقاومت بالاتری نسبت به رویکرد پیشنهادی اول برخوردار است. در عین حال هر دو رویکرد با سه روش ارائه شده پیشین مقایسه شدند نتایج این مقایسه نشان داد که هر دو رویکرد پیشنهادی مقاوم‌تر از روش‌های ارائه شده پیشین می‌باشند.

مراجع

[1] P. Benioff, "**The computer as a physical system: A microscopic quantum mechanical Hamiltonian model of computers as represented by Turing machines,**" *Journal of statistical physics*, vol. 22, pp. 563-591, 1980.

[2] V. Vedral, A. Barenco, and A. Ekert, "**Quantum networks for elementary arithmetic operations,**" *Physical Review A*, vol. 54, p. 147, 1996.

[3] S. E. Venegas-Andraca and S. Bose, **"Storing, processing, and retrieving an image using quantum mechanics,"** in *Quantum Information and Computation*, 2003, pp. 137-148.

[4] J. I. Latorre, "**Image compression and entanglement,**" *arXiv preprint quant-ph/0510031*, 2005.

[5] P. Q. Le, F. Dong, and K. Hirota, "**A flexible representation of quantum images for polynomial preparation, image compression, and processing operations,**" *Quantum Information Processing*, vol. 10, pp. 63-84, 2011.

[6] B. Sun, P. Q. Le, A. M. Iliyasu, F. Yan, J. A. Garcia, F. Dong, *et al.*, **"A multi-channel representation for images**

on quantum computers using the RGBα color space," in *Intelligent Signal Processing (WISP), 2011 IEEE 7th International Symposium on*, 2011, pp. 1-6.

[7] Y. Zhang, K. Lu, Y. Gao, and M. Wang, "**NEQR: a novel enhanced quantum representation of digital images,**" *Quantum information processing*, vol. 12, pp. 2833-2860, 2013.

[8] J. Sang, S. Wang, and Q. Li, "**A novel quantum representation of color digital images,**" *Quantum Information Processing*, vol. 16, p. 42, 2017.

[9] J. Wang, "**QRDA: quantum representation of digital audio,**" *International Journal of Theoretical Physics*, vol. 55, pp. 1622-1641, 2015.

[10] F. Yan, A. M. Iliyasu, Y. Guo, and H. Yang, "**Flexible representation and manipulation of audio signals on quantum computers,**" *Theoretical Computer Science*, 2017.

[11] Z.-G. Qu, H.-X. He, and T. Li, "**Novel quantum watermarking algorithm based on improved least significant qubit modification for quantum audio,**" *Chinese Physics B*, vol. 27, p. 010306, 2018.

[12] W.-W. Zhang, F. Gao, B. Liu, H.-Y. Jia, Q.-Y. Wen, and H. Chen, "**A quantum watermark protocol,**" *International Journal of Theoretical Physics*, vol. 52, pp. 504-513, 2013.

[13] X.-H. Song, S. Wang, S. Liu, A. A. A. El-Latif, and X.-M. Niu, "**A dynamic watermarking scheme for quantum images using quantum wavelet transform,**" *Quantum information processing*, vol. 12, pp. 3689-3706, 2013.

[14] X. Song, S. Wang, A. A. A. El-Latif, and X. Niu, "**Dynamic watermarking scheme for quantum images based on Hadamard transform,**" *Multimedia systems*, vol. 20, pp. 379-388, 2014.

[15] S. Wang, X. Song, and X. Niu, "**Quantum cosine transform based watermarking scheme for quantum images,**" *Chinese Journal of Electronics*, vol. 24, pp. 321-325, 2015.

[16] N. Wang and S. Lin, "**A watermarking strategy for quantum image based on least significant bit,**" *Chin. J. Quantum Electron*, vol. 32, pp. 263-269, 2015.

[17] S. Heidari and M. Naseri, "**A novel LSB based quantum watermarking,**" *International Journal of Theoretical Physics*, vol. 55, pp. 4205-4218, 2016.

[18] N. Jiang, N. Zhao, and L. Wang, "**LSB based quantum image steganography algorithm,**" *International Journal of Theoretical Physics*, vol. 55, pp. 107-123, 2016.

[19] S. Heidari, M. Naseri, R. Gheibi, M. Baghfalaki, M. R. Pourarian, and A. Farouk, "**A new quantum watermarking based on quantum wavelet transforms,**" *Communications in Theoretical Physics*, vol. 67, p. 732, 2017.

[20] K. Chen, F. Yan, A. M. Iliyasu, and J. Zhao, "**Exploring the Implementation of Steganography Protocols on Quantum Audio Signals,**" *International Journal of Theoretical Physics*, vol. 57, pp. 476-494, 2017.

[21] X. Li, G. Yang, C. M. Torres Jr, D. Zheng, and K. L. Wang, "**a Class of Efficient Quantum Incrementer Gates for Quantum Circuit Synthesis,**" *International Journal of Modern Physics B*, vol. 28, p. 1350191, 2014.

[22] L. Zhang, X. Tian, and S. Xia, **"A scrambling algorithm of image encryption based on Rubik's cube rotation and Logistic sequence,"** in *Multimedia and Signal Processing (CMSP), 2011 International Conference on*, 2011, pp. 312-315.

[23] M. Li, T. Liang, and Y.-j. He, **"Arnold transform based image scrambling method,"** in *3rd International Conference on Multimedia Technology*, 2013.

[24] J. Zou, R. K. Ward, and D. Qi, **"A new digital image scrambling method based on Fibonacci numbers,"** in *Circuits and Systems, 2004. ISCAS'04. Proceedings of the 2004 International Symposium on*, 2004, pp. III-965.

[25] X.-H. Lin and L.-D. Cai, "**Scrambling research of digital image based on Hilbert curve [J],**" *Chinese Journal of Stereology and Image Analysis*, vol. 9, pp. 224-227, 2004.

[26] Y. Zou, X. Tian, S. Xia, and Y. Song, **"A novel image scrambling algorithm based on Sudoku puzzle,"** in *Image and Signal Processing (CISP), 2011 4th International Congress on*, 2011, pp. 737-740.

[27] N. Jiang, W.-Y. Wu, and L. Wang, "**The quantum realization of Arnold and Fibonacci image scrambling,**" *Quantum information processing*, vol. 13, pp. 1223-1236, 2014.

[28] N. Jiang, L. Wang, and W.-Y. Wu, "**Quantum Hilbert image scrambling,**" *International Journal of Theoretical Physics*, vol. 53, pp. 2463-2484, 2014.

[29] A. Barenco, C. H. Bennett, R. Cleve, D. P. DiVincenzo, N. Margolus, P. Shor, *et al.*, "**Elementary gates for quantum computation,**" *Physical review A*, vol. 52, p. 3457, 1995.

[30] www.MusicRadar.com. (2015, 01/08/2018). *SampleRadar: 235 free '80s heat samples*. Available: https://www.musicradar.com/news/tech/sampleradar-235-free-80s-heat-samples-628852

زیرنویس‌ها:

[1] Superposition
[2] Unitary
[3] Qubit Lattice
[4] Real Ket
[5] Hilbert
[6] Flexible Representation of Quantum Images
[7] Multi-Channel Representation for Quantum Images
[8] Novel Enhanced Quantum Representation for digital images
[9] Novel Quantum representation of Color digital Images
[10] Quantum Representation of Digital Audio
[11] Entangled
[12] Flexible Representation of Quantum Audio
[13] Quantum Wavelet Transform
[14] Hadamard Transform
[15] Quantum Cosine Transform
[16] Least Significant Bit
[17] Grayscale
[18] Identity Gate
[19] Accumulator
[20] NOT
[21] Control-NOT
[22] Swap
[23] Toffoli