یک رویکرد نهان‌نگاری صوت کوانتومی مقاوم مبتنی بر هم‌افزایی مخفی‌سازی پژواک و تکنیک کم‌ارزش‌ترین بیت

معصومه ولایتی پور[۱]، محمد مصلح[*۲]، محسن یوسفی‌نژاد[۳]، محمد خیراندیش[۴]

۱- دانشجوی دکتری، گروه مهندسی کامپیوتر، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران ۲- دانشیار، گروه مهندسی کامپیوتر، واحد دزفول، دانشگاه آزاد اسلامی، دزفول، ایران ۳- استادیار، گروه مهندسی کامپیوتر و فناوری اطلاعات، دانشگاه پیام نور، تهران، ایران ۴- استادیار، گروه مهندسی کامپیوتر، واحد دزفول، دانشگاه آزاداسلامی، دزفول، ایران

(دریافت: ۱۴۰۲/۱۰/۰۴، بازنگری: ۱۴۰۳/۰۱/۲۷، پذیرش: ۱۴۰۲/۰۲/۱۶، انتشار: ۱۴۰۳/۰۳/۱۳)

2- DOR: https://dorl.net/dor/

-۳

چکیده

با ظهور رایانه‌های کوانتومی، لزوم حفاظت از داده‌های کوانتومی به‌عنوان یک موضوع اساسی، توجه محققین را به خود جلب کرده است. در این مقاله، یک رویکرد نهان‌نگاری صوت کوانتومی، مبتنی بر تلفیقی از روش‌های مخفی‌سازی پژواک(Echo Hiding) و روش کم‌ارزش‌ترین بیت(LSB) پیشنهاد می‌شود. رویکرد پیشنهادی در مرحله درج، ابتدا سیگنال صوت میزبان را به برگه نمایش کوانتومی QRDS تبدیل کرده و سپس یک سیگنال پژواک کوانتومی، از آن تولید می‌کند. در ادامه کیوبیت‌های داده نهان نگاره را به روش کم‌ارزش‌ترین بیت در سیگنال پژواک کوانتومی حاصل درج می‌نماید. در نهایت، سیگنال کوانتومی نهان‌نگاری شده از برآیند سیگنال کوانتومی اصلی و سیگنال کوانتومی پژواک حاصل می‌شود. در مرحله استخراج رویکرد پیشنهادی، بر اساس تفاضل نمونه‌های سیگنال کوانتومی اصلی با سیگنال کوانتومی دریافت شده، کیوبیت‌های نهان نگاره بازیابی می‌شوند. علاوه بر این، مدارات برگشت‌پذیر کوانتومی برای فرایندهای درج و استخراج، طراحی و پیاده سازی شده‌اند. نتایج حاصل از ارزیابی و مقایسه رویکرد پیشنهادی، از نظر شفافیت، مقاومت‌پذیری در برابر حملات و نیز ظرفیت درج، نشان می‌دهند که این رویکرد، در مقایسه با روش‌های نهان‌نگاری کوانتومی مبتنی بر روش بیت کم‌ارزش، از مقاومت‌پذیری بالاتری برخوردار است. علاوه بر این، روش پیشنهادی از شفافیت بسیار مناسبی (SNR=66.26dB) در نرخ جادهی ۵۱۲ کیوبیت در ثانیه برخوردار است که نشان می‌دهد روش پیشنهادی توانسته مصالحه بین مقاومت‌پذیری، شفافیت و ظرفیت را بهبود بخشد.

کلیدواژه‌ها: نهان‌نگاری صوت کوانتومی، محاسبات کوانتومی، مخفی‌سازی پژواک، بیت کم‌ارزش

*Corresponding Author E-mail: Mosleh@iaud.ac.ir

۱. مقدمه

امروزه، در دسترس بودن کامپیوترهای خانگی، پیشرفت روزافزون فناوری اطلاعات دیجیتال، پردازنده‌های سریع، دسترسی آسان به اینترنت و شبکه، حافظه‌های قابل جابجایی، تلفن همراه و شبکه‌های اجتماعی، انفجاری در توزیع و استفاده آسان از داده دیجیتال چندرسانه‌ای را فراهم ساخته است. به همین دلیل، اطلاعات دیجیتالی به سهولت در دسترس همگان قرار می‌گیرند و این موضوع، ارائه دهندگان خدمات چندرسانه‌ای را نگران پخش و انتشار غیرمجاز محصولات خود کرده است. یکی از مشکلات در این حوزه، توانایی دستکاری، کپی‌برداری و توزیع غیرقانونی اسناد دیجیتالی، توسط کاربرانی است که از این اسناد استفاده می‌کنند و چناچه مسائل امنیتی محصولات دیجیتالی حل نشود، مالکان این محصولات انگیزه خود را برای وارد کردن این محصولات در دنیای تجارت الکترونیک از دست خواهند داد. به‌منظور حل این مشکلات، تکنیک‌های نهان‌نگاری توسعه یافتند [۱-۵]. نهان‌نگاری عبارت است از درج اطلاعات در سیگنال حامل به‌گونه‌ای که قابل درک نباشد و نتوان به آسانی آن را حذف یا دستکاری نمود. نهان‌نگاری می‌تواند بر روی داده‌های متنی، تصویری، ویدیویی و یا صوتی انجام گیرد[۶, ۷]. از جمله کاربردهای نهان‌نگاری می‌توان به محافظت از حق مالکیت، اثر انگشت، نظارت بر پخش برنامه‌ها، تعیین اعتبار و مخابرات مخفی اشاره کرد [۲, ۸, ۹]. با توجه به میزان حساسیت سیستم شنیداری انسان، نهان‌نگاری صوت از پیچیدگی بالاتری برخوردار است. از جمله روش‌های نهان‌نگاری صوت می‌توان به روش مبتنی بر کم‌ارزش‌ترین بیت (LSB) [۱۰, ۱۱]، روش مخفی-سازی پژواک (Echo hiding) [۱۲, ۱۳]، روش مخفی‌سازی در سکوت (Audio silence interval) [۱۴, ۱۵] و روش دوتکه‌ای (Patchwork) [۱۶, ۱۷].

۲.کارهای پیشین

در سال‌های اخیر، محاسبات کوانتومی به دلیل سرعت پردازش بسیار بالا در مقایسه با محاسبات کلاسیک، مورد توجه بسیاری از پژوهشگران قرارگرفته‌اند [۱۸]. این محاسبات، دارای ماهیت توازی بوده و بنابراین قادرند مسائلی که حل آن‌ها در محاسبات کلاسیک بسیار سخت و پیچیده است را با سرعت بالا و به‌آسانی حل نمایند [۱۹]. به واسطه پیشرفت‌هایی که امروزه در حوزه محاسبات کوانتومی صورت گرفته، امکان ذخیره، بازیابی، انتقال و نمایش صوت و تصویر در کامپیوترهای کوانتومی و شبکه‌های انتقال اطلاعات کوانتومی به‌وجود آمده است. لزوم حفظ حق مالکیت، احراز هویت و مسائلی از این قبیل، ضرورت نهان‌نگاری کوانتومی را بیش از پیش نشان می‌دهد [۲۰]. در این راستا، تاکنون چندین رویکرد نهان‌نگاری کوانتومی در صوت معرفی شده‌اند که در ادامه مورد بررسی قرار می‌گیرند.

J. Wang برای اولین بار تلاش کرد که سیگنال صوت دیجیتالی را به‌صورت کوانتومی نمایش دهد. این پژوهش در سال ۲۰۱۵ انجام شد و QRDA نامیده شد. در این روش نمایش، اطلاعات دامنه و زمان نمونه‌های سیگنال صوتی، در دو دنباله کوانتومی ذخیره می‌شوند [۲۱]. در پژوهشی در سال ۲۰۱۸، F. Yan و همکاران یک نمایش کوانتومی جدید به نام نمایش انعطاف‌پذیر صوت کوانتومی[1] (FRQA) را پیشنهاد کرد [۲۲]. همچنین، P. Li و همکاران در سال ۲۰۱۸، روش نمایش کوانتومی سیگنال‌های دیجیتال (QRDS) را به‌منظور نمایش کونتوامی اعداد اعشاری ارائه نمودند [۲۳]. در تلاشی دیگر در سال ۲۰۱۸، K. Chen و همکاران یک طرح دوگانه نهان‌نگاری صوت کوانتومی را بر مبنای تبدیل کسینوسی گسسته کوانتومی (QDCT)[2] پیشنهاد کردند [۲۴]. با استفاده از تکنیک QDCT، ویژگی‌های سیگنال از حوزه زمان به حوزه فرکانس تبدیل می-شوند. در طرح اول، کیوبیت‌های نهان نگاره با فرکانس بالا جای‌گذاری می‌شوند و در طرح دوم، سیگنال کوانتومی در ابتدا به ۸ زیربخش تقسیم می‌شود و عملیات نهان‌نگاری روی این بخش‌ها، به‌صورت جداگانه انجام می‌شود. مجموع این زیربخش‌ها در انتها، کل سیگنال نهان نگاره را تولید می‌کند. علیرغم تذکر نویسندگان درباره شفافیت و مقاومت بالا، روش آنها در مقایسه با سایر پژوهش‌های نهان‌نگاری کوانتومی، نرخ مقاومتی در حد متوسط از خود نشان داده است و همچنین، شفافیت آن کمتر از سایر روش‌های کوانتومی است. نکته قابل تامل دیگر این است که برخلاف پژوهش‌های علمی، این روش با هیچ روش نهان‌نگاری کوانتومی مقایسه نشده است.

یک الگوریتم نهان‌نگاری صوت کوانتومی مبتنی بر بیت کم‌ارزش پیشرفته، توسط Qu و همکاران در سال ۲۰۱۸ پیشنهاد شد [۲۵]. به‌منظور نهان‌نگاری در صوت کوانتومی، M.Y. Nejad و همکاران یک تصویر کوانتومی را با روش‌های درهم‌سازی به یک دنباله دودویی تبدیل کردند و در سیگنال صوتی میزبان جای‌گذاری کردند [۲۶]. روش جای‌گذاری بدین صورت است که اگر پر ارزش‌ترین کیوبیت (MSB)[3] نمونه سیگنال برابر $|0\rangle$ باشد، کیوبیت تصویر نهان نگاره در کم‌ارزش-ترین کیوبیت و اگرMSB برابر $|1\rangle$ باشد، در دومین کیوبیت کم-ارزش قرار داده می‌شود. در این روش، از کیوبیت پر ارزش

[1] Flexible representation of quantum audio (FRQA)
[2] Quantum Discrete Cosine Transform(QDCT)
[3] Most Significant Bit (MSB)

به‌عنوان یک داور استفاده شده است. شفافیت این روش با استفاده از جای‌گذاری تصاویر مختلف، بین ۴۵ تا ۴۸ دسیبل گزارش شده است. نرخ BER این روش که تقریبا بین ۰,۲تا۰,۴ گزارش شده، بیانگر مقاومت بالا در مقابل حملات نویزی است.

در سال ۲۰۲۰ یک روش نهان‌نگاری صوت کوانتومی شفاف و مقاوم، توسط M.Y. Nejad و همکاران معرفی شد [۲۷] که بهبود یافته پژوهش پیشین این محققان بود و از ELSB و کد گری به‌منظور بهبود مقاومت استفاده می‌کرد. در ابتدا، تصاویر کوانتومی توسط ماژول‌های چرخشی درهم‌سازی شده و با استفاده از کلید، در سیگنال حامل جای‌گذاری می‌شدند. شفافیت ۶۰ دسیبلی و مقاومت کمتر از ۰,۱ این رویکرد نهان‌نگاری، از مزایای چشمگیر این روش به‌شمار می‌رود.

یک روش نهان‌نگاری کوانتومی صوتی، مبتنی بر تبدیل کسینوسی گسسته کوانتومی (qDCT) توسط M.Y. Nejad و همکاران پیشنهاد شد [۲۸]. روش استخراج داده نهان نگاره در این رویکرد، مبتنی بر یک روش کور است. آن مقاله، داده‌های نهان نگاره را در باند فرکانس متوسط سیگنال صوتی جاسازی می‌کند و مقاومت بهتر و حفظ ظرفیت و شفافیت یکسان را نشان می‌دهد. رویکرد آن‌ها، با استفاده از پردازش موازی و مدارهای کوانتومی، روش‌های جاسازی و استخراج، کاهش دروازه‌های کوانتومی و بهبود کارایی را به وضوح نشان داد.

M.velayatipour و همکاران در سال ۲۰۲۲ یک روش نهان-نگاری صوت کوانتومی مقاوم، مبتنی بر مخفی‌سازی پژواک پیشنهاد کردند. آن‌ها پژواک‌های کوانتومی را توسط مدارات کوانتومی تولید و به سیگنال صوتی کوانتومی اضافه کردند [۲۹]. در رویکرد آن‌ها، برای قرار دادن کیوبیت $|0\rangle$ و $|1\rangle$ پژواک‌های جداگانه‌ای ایجاد شده و به هر قاب سیگنال حامل اضافه می‌شدند. این پژواک‌های کوانتومی، برخلاف روش‌های کلاسیک، کمترین تاثیر را بر روی شفافیت دارند. نرخ BER صفر و یا نزدیک به صفر بیانگر مقاومت‌بالای آن روش است.

به‌منظور ارتقا امنیت تکنیکهای کوانتومی، در کنار روش‌های نهان‌نگاری، روش‌های پنهان‌نگاری کوانتومی نیز مورد توجه پژوهشگران قرارگرفته‌اند. K. Chen و همکاران، یک پروتکل نهان‌نگاری برای صوت کوانتومی را در سال ۲۰۱۸ پیشنهاد کردند [۳۰]. در ۲۰۱۹، A. Abd EL و همکاران، از الگوریتم پیاده‌روی کوانتومی (QWs) در یک روش پنهان‌نگاری تصویر استفاده کردند [۳۱]. در پنهان‌نگاری صوت کوانتومی، J. Chaharlang و همکاران، یک روش مبتنی بر بیت کم‌ارزش کسری LSFQ[1] پیشنهاد دادند [۳۲]. در ۲۰۲۲، یک روش پنهان‌نگاری صوت کوانتومی درحوزه فرکانس، توسط S. N. Larki و همکاران ارائه شد که از تکنیک‌های یادگیری ماشین استفاده می‌کرد [۳۳].

همواره طراحی و پیاده‌سازی یک سیستم نهان‌نگاری شفاف که در مقابل حملات نیز مقاوم باشد به‌عنوان مهم‌ترین چالش این حوزه بشمار می‌رود؛ بنابراین پژوهشگران این حوزه سعی در مرتفع کردن این چالش داشتند. می‌توان به مهم‌ترین دستاوردهای این پژوهش به شرح زیر اشاره کرد:

- تولید پژواک‌های نامحسوس کوانتومی توسط مدارات کوانتومی
- بهبود شفافیت روش‌های نهان‌نگاری مبتنی بر پژواک
- افزایش چشمگیر مقاومت روش‌های نهان‌نگاری مبتنی بر کم‌ارزش‌ترین بیت
- تقویت پارامترهای مهم نهان نگاره با هم‌افزایی دو رویکرد مخفی‌سازی پژواک و LSB

سایر بخش‌های مقاله در ادامه بیان شده‌اند: در بخش ۲ مروری بر شیوه نمایش سیگنال کوانتومی و مدارات کوانتومی پایه انجام شده است. روش پیشنهادی و مدارات کوانتومی آن در بخش سوم به‌تفصیل ارائه شده‌اند و در بخش چهارم، روش پیشنهادی با سایر روش‌های کوانتومی مقایسه شده است و مقاومت و شفافیت آن بیان شده است. بخش انتهایی مقاله، پیشنهادهای آتی است.

۳. مقدمه‌ای بر محاسبات کوانتومی

مصرف توان در رایانه‌های مدرن امروزی، یکی از مهم‌ترین مسائل طراحی است. بخشی از مصرف توان در رایانه‌های کلاسیک به دلیل برگشت‌ناپذیر بودن محاسبات است. با انجام محاسبات به روش برگشت‌پذیر، بخشی از انرژی مصرفی که به دلیل ازدست‌رفتن اطلاعات رخ می‌دهد، در فرایند برگشت‌پذیری حذف می‌شود. علاوه‌برآن، ظهور فناوری‌های محاسبات کوانتومی که قادر به اجرای الگوریتم‌های خاصی با سرعت‌هایی بسیار بیشتر از محاسبات کلاسیک می‌باشند و همچنین برگشت‌پذیر بودن محاسبات کوانتومی، باعث ارتباط تنگاتنگ این دو روش محاسبات با یکدیگر شده است. در سال‌های اخیر، طراحی مدارهای محاسباتی مختلف موردنیاز، با استفاده از روش‌های محاسبات کوانتومی و برگشت‌پذیر که پایه محاسبات کوانتومی می‌باشند، انجام‌گرفته است. در ابتدای این زیربخش، سیگنال دیجیتال به‌صورت کوانتومی نمایش داده می‌شود. بعضی ماژول‌های محاسباتی کوانتومی و مدارات آنها که در پژوهش‌های

[1] Least Significant Fractional Qubit (LSFQ)

پیشین توسط سایر محققان ترسیم شده‌اند، به‌تفصیل تشریح شده‌اند.

۳-۱. نمایش کوانتومی سیگنال‌های دیجیتال (QRDS)

در سال ۲۰۱۸، برای نمایش کوانتومی یک سیگنال صوت دیجیتال، به فرم اعشاری، یک روش جدید با نام QRDS پیشنهاد شد [۲۳]. این شیوه نمایش، مشابه روش FRQA، اطلاعات دامنه و زمان سیگنال دیجیتال را در دو ثبات کوانتومی $|x_i^t\rangle$ و $|t\rangle$ ذخیره می‌کند. نمایش کوانتومی QRDS به‌صورت رابطه ریاضی، در رابطه(۱) بیان شده است. اگر فرض کنیم سیگنال صوت در حالت مکمل۲، به‌صورت $x_t = x_t^m, x_t^{m-1}, x_t^{m-2} \dots x_t^0 . x_t^{-1} \dots x_t^{m-n}$ نمایش داده شود. در این نمایش، از سمت چپ به راست ارزش بیتها کم و کمتر می‌شود.

$$|x\rangle = \frac{1}{\sqrt{2^k}}\sum_{t=0}^{2^k-1}|x_t\rangle\otimes|t\rangle = \frac{1}{\sqrt{2^k}}\sum_{t=0}^{2^k-1}\otimes_{i=m-n}^{m}|x_i^t\rangle\otimes|t\rangle \quad (۱)$$

۳-۲ . جمع کوانتومی و مجموع کوانتومی

جمع کننده کوانتومی عملگری است که برای جمع دو عدد کوانتومی بکار برده می‌شود. این دروازه کوانتومی، مانند عملگرهای کلاسیک، عملیات جمع دو عددکوانتومی را با استفاده از ماژول‌های carry و sum پیاده سازی می‌کند. پیاده‌سازی‌های متفاوتی از مدارات کوانتومی، برای جمع دو عدد کوانتومی در منابع مختلف ارائه شده است [۲۳, ۳۴]. شبکه مدار کوانتومی و ماژول این جمع‌کننده در شکل(۱) نشان داده شده است و عملکرد آن در رابطه (۲) بیان شده است [۲۳]. قابل مشاهده است که ورودی‌های این مدار، دو عدد علامتدار n+1 کیوبیتی a و b و کیوبیت کمکی $|0\rangle$ هستند. همچنین در این پیاده‌سازی، $n+1$ کیوبیت کمکی $|0\rangle$ برای ذخیره نتیجه نهایی عملیات مجموع مورد استفاده قرار گرفته است. در [۳۴] یک پیاده‌سازی دیگر از جمع‌کننده کوانتومی ارائه شده است.

$$\text{add}|a\rangle|b\rangle = |a\rangle|a+b\rangle \quad (۲)$$

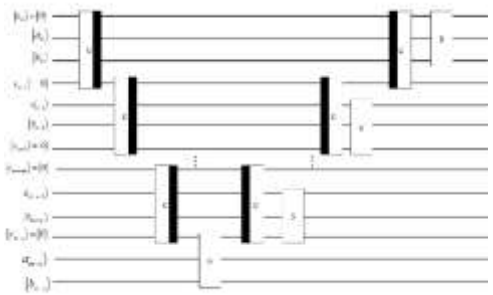
برای محاسبه مجموع اعداد کوانتومی در رشته‌های ریاضی، از قبیل جمع مقادیر رنگ پیکسل‌های یک تصویر یا جمع مقادیر نمونه‌های یک سیگنال، به مدارات جمع‌کننده نیاز است. این ماژول در شکل (۲) نشان داده‌شده است که در آن $|t\rangle = |t_{l-1} \dots t_1 t_0\rangle$ یک دنباله کوانتومی با طول l، برای نمایش اطلاعات زمان سیگنال و $|a_t\rangle = |a_n \dots t_1 t_0\rangle$ یک دنباله کوانتومی با طول n، برای نشان دادن اطلاعات دامنه نمونه‌های سیگنال صوت کوانتومی است. در این مدار، تعداد 2^l ماژول جمع‌کننده برای محاسبه مجموع $|a_t\rangle$ در 2^l موقعیت زمانی $|t\rangle$ استفاده شده است.

۳-۳. تفریق کوانتومی

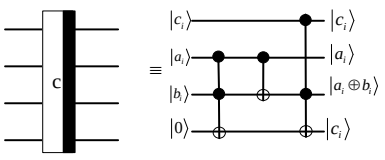
برای انجام عملیات تفریق کوانتومی (a-b)، می‌توان از ماژول FP+1 استفاده کرد و عبارت (-b) را توسط این ماژول تولید کرد [۲۳]. ماژول FP+1 و ماژول تفریق‌کننده دو عدد کوانتومی (n+1) کیوبیتی [۲۳] در شکل (۳) نشان داده شده‌اند. می‌توان عملکرد این ماژول را به این‌گونه تعریف کرد که در ابتدا، توسط بخش اول ماژول، مکمل کیوبیت‌های دنباله x محاسبه می‌شود و در ادامه، باکس بعدی ماژول آن را با مقدار یک جمع می‌کند.

۳-۴. مقایسه‌گر و تساوی‌سنج کوانتومی

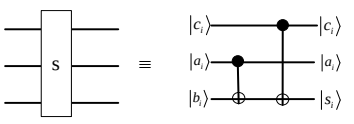
به‌منظور مقایسه مقدار تک‌تک کیوبیت‌ها، به یک مقایسه‌گر کوانتومی نیاز است. ماژول مقایسه‌گر، عموماً به همراه سایر ماژول ها، برای تعیین موقعیت‌های زمانی یکسان (نمونه‌های هم‌زمان) از دو سیگنال صوتی به کار می‌رود. ماژول و مدار کوانتومی این مقایسه‌گر در شکل (۴) نمایش داده شده است [۳۵].



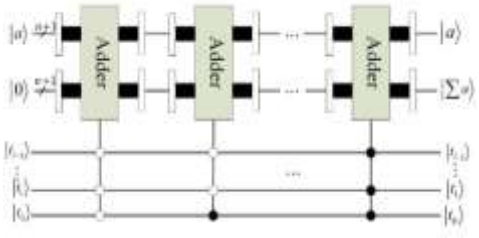
(الف)



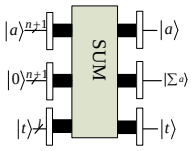
(ب)



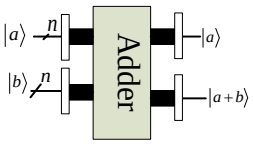
(ج)



(الف)

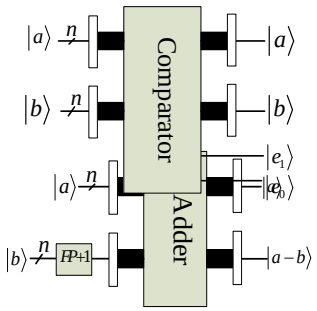


(ب)



(د)

شکل (۱). مدارهای کوانتومی جمع دو عدد علامتدار (الف) مدارات کوانتومی برای جمع‌کننده کوانتومی (ماژول 2^M) (ب) مدارکوانتومی برای carry(ج) مدارکوانتومی برای sum (د) نمودار بلوکی جمع‌کننده کوانتومی[19]



شکل (۲). مدارات کوانتومی مربوط به محاسبه مجموع تمام مقادیر دامنه (الف) مدارکوانتومی (ب) نموداربلوکی [۲۳].

شکل (۳). نمودار بلوکی تفریق دو عدد کوانتومی n+1 کیوبیتی باکمک ماژول FP +1 [۲۳].

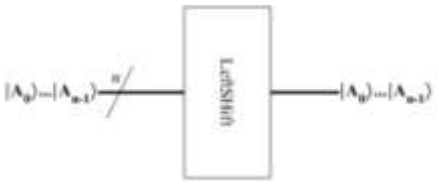
در این شکل، مشخص است که $|b\rangle$ و $|a\rangle$ ورودی‌های این مدار و e_0 و e_1 دو کیوبیت خروجی این مدار هستند. نتایج خروجی این مدار در قالب رابطه(۳) قابل بیان هستند:

$$\begin{cases} a > b,\ e_1e_0 = 10 \\ a < b,\ e_1e_0 = 01 \\ a = b, e_1e_0 = 00 \end{cases} \quad (۳)$$

تفاوت تساوی سنج کوانتومی با مقایسه‌گر کوانتومی در این است که این مدار، کوچک‌تر یا بزرگ‌تر بودن را بررسی نمی‌کند و فقط مساوی بودن را بررسی می‌کند [۲۶]. از مزایای این مدار نسبت به مقایسه‌گر، می‌توان به برخورداری آن از پیچیدگی مداری کمتر اشاره کرد. شکل(۵) مدار کوانتومی تساوی‌سنج و ماژول آن را نمایش می‌دهد.

۵-۳. ثبات انتقالی کوانتومی

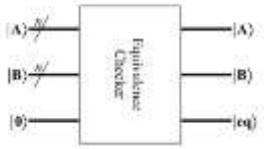
ثبات‌های انتقال یکی از انواع مدارات منطقی هستند که در ذخیره‌سازی و انتقال داده‌های دیجیتال کاربرد دارند. یک نوبت یا چرخش منطقی در واقع یک عملگر بیتی است که قادر به حرکت‌دادن تمامی بیت‌های عملوند است [۳۶]. چرخش بیت به چپ یک عملوند با علامت یا بدون علامت، برابر با ضرب کردن آن در 2^nاست و چرخش n بیت به راست یک عملوند بدون-علامت، برابر با تقسیم آن بر2^n است. این عدد با $|B_i\rangle$ نمایش داده می‌شود. مدارات کوانتومی ثبات انتقالی نسبت به مدارات تقسیم‌کننده، از پیچیدگی کمتری برخوردارند. ثبات انتقالی کوانتومی در شکل(۶) نمایش داده شده است. اگر $|A\rangle$ یک عدد n کیوبیتی باشد و داشته باشیم $n= 2^i$، می‌توان تا i-1 رقم آن را به راست یا چپ شیفت داد.



(الف)

(ب)

شکل (۴). نمودار بلوکی مقایسه‌کننده‌کوانتومی [۳۵]



شکل (۵). نمودار بلوکی تساوی سنج کوانتومی [۲۶]

شکل (۶). (الف) نمودار بلوکی ثبات انتقالی چپ (ب) نمودار بلوکی ثبات انتقالی راست [۲۳]

۴. روش پیشنهادی

نهان‌نگاری صوتی فرایند نهفتن اطلاعات اضافی در سیگنال میزبان به‌منظور اثبات حق مالکیت است. یکی از فن‌هایی که در روش نهان‌نگاری به‌منظور جاسازی اطلاعات استفاده می‌شود، روش مخفی‌سازی پژواک است. هدف در روش مخفی‌سازی پژواک، تولید پژواک‌هایی در محدوده شنوایی انسان و افزودن آن‌ها به سیگنال میزبان است. در این مقاله، یک روش نهان‌نگاری کوانتومی مبتنی بر تلفیق روش مخفی‌سازی پژواک و بیت کم‌ارزش پیشنهاد شده است که همانند سایر روش‌های نهان نگاری، در دو مرحله انجام می‌شود: مرحله جای‌گذاری داده نهان نگاره (بخش کدکننده) و مرحله استخراج داده نهان نگاره (بخش کدگشا). در مرحله اول، داده نهان نگاره در سیگنال حامل جای‌گذاری می‌شود که به آن، مرحله جای‌گذاری گفته می‌شود. در این مرحله پیشنهادی، بعد از تبدیل سیگنال به یک سیگنال کوانتومی، عملیات قاب‌بندی انجام می‌شود و نمونه‌های کوانتومی در قاب‌هایی دسته‌بندی می‌شوند. برای هر قاب، یک سیگنال پژواک کوانتومی به روش مخفی‌سازی پژواک، ساخته می‌شود. سپس، در هر قاب از این سیگنال، یک کیوبیت داده نهان نگاره، به روش بیت کم‌ارزش جای‌گذاری می‌شود. سیگنال حاصله با سیگنال اصلی جمع می‌شود و درنهایت سیگنال نهان‌نگاری تولید می‌شود. در مرحله دوم، تکنیکی ارائه می‌شود تا داده جای‌گذاری شده در سیگنال استخراج شود و به آن، مرحله استخراج گفته می‌شود. روش استخراج رویکرد پیشنهادی، بدین صورت طراحی شده است که در ابتدا، تفاضل تک‌تک نمونه‌های سیگنال نهان نگاری شده از سیگنال اصلی برای هر قاب محاسبه می‌شود و سپس مجموع این مقادیر حاصله، برای هر قاب محاسبه می‌شود. همچنین، مشابه مرحله جای‌گذاری، یک سیگنال پژواک کوانتومی ایجاد می‌شود و مجموع نمونه‌های آن برای هر قاب، جداگانه حساب می‌شود. وقتی کیوبیت $|1\rangle$ جای‌گذاری شود، نمونه تغییر نمی‌کند یا حداکثر به اندازه یک واحد مقدار نمونه افزایش پیدا می‌کند (و برای نهان‌نگاری کیوبیت$|0\rangle$ یا نمونه تغییر نمی‌کند یا به اندازه یک واحد کاهش می‌یابد). بنابراین، باتوجه به نکته ذکرشده، می‌توان گفت: اگر مجموع نمونه‌های سیگنال اکو از مجموع نمونه‌های سیگنال تفاضل، کمتر باشد بیانگر این است که کیوبیت نهان‌نگاری $|1\rangle$ است و بالعکس کیوبیت نهان‌نگاری شده $|0\rangle$ است. در ادامه، ابتدا شیوه نمایش سیگنال کوانتومی معرفی می‌شود و در دو بخش بعدی، مرحله جای‌گذاری و مرحله استخراج داده نهان نگاره روش پیشنهادی مفصلا مورد بحث قرار می‌گیرد.

۴-۱. نمایش سیگنال صوت کوانتومی

در ابتدا لازم است سیگنال دیجیتال میزبان به یک صوت کوانتومی تبدیل شود. بدین منظور، از روش نمایش QRDS استفاده شده و سیگنال صوتی کوانتومی $|x\rangle$ حاصل شده است. QRDS نمونه‌های سیگنال صوتی را به‌صورت اعداد اعشاری نمایش می‌دهد. با فرض این‌که سیگنال میزبان دارای L نمونه است و عدد L در مبنای دودویی، به شکل $L = 2^l$ نوشته می‌شود، لازم است نمونه‌ها قاب بندی شوند. ظرفیت نهان‌نگاری مشخص می‌کند قاب‌ها شامل چند نمونه باشند و در هر قاب، چند کیوبیت باید قرارداده شود. به‌عنوان مثال، اگر قاب $|x_0x_1\dots x_{n-1}\rangle$ شامل n نمونه باشد، برای نمایش کوانتومی دامنه و زمان نمونه‌های سیگنال، نیاز به دو رجیستر کوانتومی است؛ به ترتیب $|D_T\rangle$و$|T\rangle$. این رجیسترهای نگهدارنده اطلاعات دامنه و زمان، به‌همراه خاصیت برهم نهی یا ضرب تانسوری، کیوبیت‌های سیگنال کوانتومی را تولید می‌کنند. در ادامه، نمایش کوانتومی مدل QRDS در رابطه (۴) بیان شده است.

$$|x\rangle = \frac{1}{\sqrt{2^l}}\sum_{T=0}^{L-1}|D_T\rangle\otimes|T\rangle \qquad (۴)$$

$$|D_T\rangle = \left|D_T^q D_T^{q-1}\dots D_T^0 D_T^{-1} D_T^{-p}\right\rangle, D_T^i \in \{0,1\}$$

$$|T\rangle = |t_0 t_1\dots t_{l-1}\rangle, t_i \in \{0,1\}$$

$$l = \begin{cases}\lceil \log 2L \rceil, L>1\\ 1, L=1\end{cases}$$

۴-۲. مرحله جای‌گذاری روش پیشنهادی

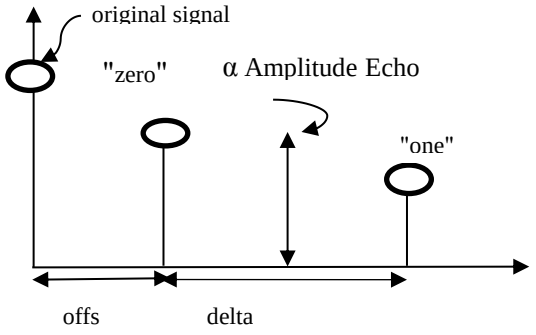
در مرحله جای‌گذاری، فرایندی معرفی می‌گردد که متناسب با آن، کیوبیت‌های داده نهان نگاره در سیگنال حامل جای‌گذاری می‌شوند. مخفی‌سازی پژواک یک روش از فن‌های نهان‌نگاری است که با استفاده از تشدید، پژواک (تأخیر زمانی) کوتاهی ایجاد کرده و به سیگنال صوتی اضافه می‌کند. در حقیقت، پژواک یا پژواک، تضعیف شده‌ای از همان سیگنال صوت است که به سیگنال اصلی اضافه می‌شود و سیگنال نهان نگاره را تولید می کند. اگر دامنه این پژواک‌ها از حد آستانه‌ای کمتر باشند، برای

سیستم شنیداری انسان محسوس نیستند. مطلوب این است که تلاش شود پژواک‌های حاصله در صوت اصلی محسوس و قابل‌تشخیص نباشند و در سیگنال اصلی درآمیخته باشند و سیگنال نهان نگاره حاصله، شفاف باشد.

پارامترهای اصلی در روش مخفی‌سازی پژواک عبارت‌اند از: دامنه اولیه (مقدار دامنه سیگنال اصلی)، ضریب دامنه α (ضریب تشدید که مقداری بین ۰ و ۱ دارد و در دامنه سیگنال اصلی ضرب می‌شود)، تأخیر زمانی برای هر قاب (زمانی که به‌عنوان تأخیر به زمان سیگنال اضافه می‌شود)، Offset (تأخیر زمانی برای نهان‌نگاری بیت «صفر») و delta (تأخیر زمانی برای نهان‌نگاری بیت «یک»). علاوه بر کاهش زمان تأخیر، می‌توان عامل دامنه و ضریب میرایی سیگنال پژواک را نیز به‌گونه‌ای تنظیم کرد که برای گوش انسان قابل‌تفکیک نباشد [۱۳]. شکل(۷) روش مخفی‌سازی پژواک تکی را نشان می‌دهد که به‌عنوان رویکرد پایه در مخفی‌سازی به‌شمار می‌رود. برخلاف روش مخفی‌سازی پژواک (با فرمول کلی بیان شده در رابطه (۵)) که در آن، برای جای‌گذاری کیوبیت های $|0\rangle$ یا $|1\rangle$ اکوهای جداگانه‌ای تعریف شده، در این مقاله، برای نهان‌نگاری $|0\rangle$ یا$|1\rangle$ از یک سیگنال اکو استفاده شده است و با کمک روش جای‌گذاری بیت کم‌ارزش، داده نهان نگاره در نمونه‌ها جای‌گذاری شده است. در روش نهان‌نگاری به شیوه بیت کم‌ارزش، مخفی‌سازی بدین شکل انجام می‌شود که در کم‌ارزش‌ترین کیوبیت نمونه کوانتومی، داده نهان‌نگاری جای‌گذاری می‌شود. به‌عنوان مثال، اگر کیوبیت نهان نگاره $|1\rangle$ و نمونه مورد نظر به شکل $|10001100\rangle$ تعریف شده باشد، بعد از جای‌گذاری، نمونه مذکور به شکل $|10001101\rangle$ تغییر پیدا می‌کند. طرح کلی جای‌گذاری روش پیشنهادی در شکل(۸) ارائه شده است و شبه کد آن در شکل(۹) نمایش داده شده است.

(۵)

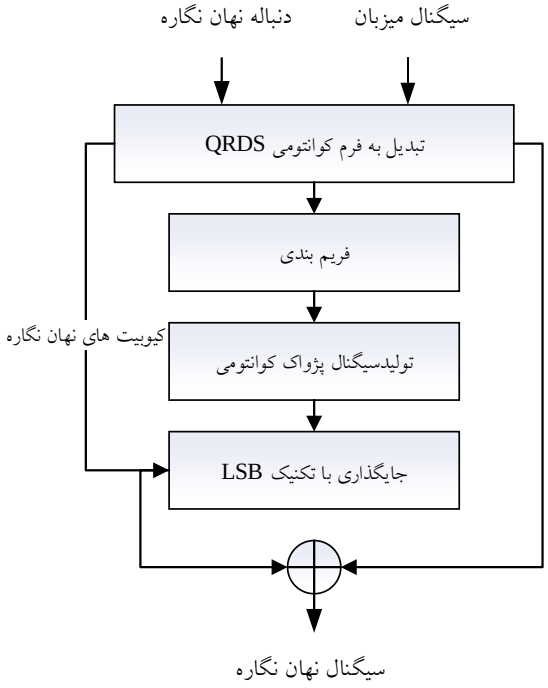
$$x_0[n] = S_i[n]+\alpha S_i[n+d]$$



شکل (۷). پارامترهای قابل تنظیم در روش مخفی‌سازی پژ واک

۳-۴. تولید هسته پژواک کوانتومی

بر خلاف بعضی از روش‌های نهان‌نگاری کوانتومی که عمل جای‌گذاری را در همه یا برخی نمونه‌ها انجام می‌دهند، در روش پیشنهادی، در هر قاب یک کیوبیت جای‌گذاری می‌شود. در نتیجه در ابتدا سیگنال میزبان باید قاب‌بندی شود. با فرض اینکه R تعداد کل نمونه‌های سیگنال میزبان و N تعداد قاب‌ها باشد (R=2^r =n×N)، دنباله نهان‌نگاری $|w_0 w_1 \dots w_{N-1}\rangle$ به صورت دنباله‌ای تصادفی از $|1\rangle$ها یا $|0\rangle$ها تعریف شده است. طی فرآیند جای‌گذاری، هر کیوبیت این دنباله تصادفی، در یک قاب نهان-نگاری می‌شود. به‌منظور مقایسه شماره هر قاب با $|j\rangle$ امین اندیس دنباله نهان نگاره، از یک تساوی سنج کوانتومی استفاده شده است [۲۶]. رجیسترکوانتومی $|T\rangle$ برای نما دادن زمان سیگنال کوانتومی استفاده شده است. بنابراین، اگر اندیس $|j\rangle$ امین کیوبیت نهان نگاره با $|T_{l-1}\rangle \dots |T_r\rangle$ برابر باشد، مقدار خروجی تساوی سنج، $|eq\rangle$ ، یک می‌شود و جای‌گذاری انجام می‌شود. در غیر اینصورت، $|eq\rangle$ برابرصفرمی‌شود.



شکل (۸). طرح کلی مرحله جای‌گذاری روش پیشنهادی

```
for j = 1 to N:
  # Apply Quantum Echo Kernel
```

```
echoed_frame = quantum_echo_kernel
(delay_times, amplitude_coefficient)
 watermark_bit=watermark_sequence[j]
    # Embed watermark using Quantum
Echo LSB for watermark bit
watermarked_frame = quantum_echo_lsb
(echoed_frame, delay_times,
amplitude_coefficient, watermark_bit)
    # Combine watermarked frame with
the host signal
watermarked_signal = watermarked_frame
+ host_signal
```

شکل (۹). شبه‌کد مرحله جای‌گذاری روش پیشنهادی

این عملیات برای هر N قاب تکرار می‌شود، تا عملیات جای‌گذاری به اتمام برسد و هر کیوبیت دنباله نهان‌نگاری $|w_0\rangle, |w_1\rangle, \ldots, |w_{N-1}\rangle$، در هر قاب سیگنال حامل نهان‌نگاری شود. همان‌گونه که در مدار قابل‌مشاهده است، نتیجه،

$$|eq\rangle$$

بعلاوه مقدار $|w_j\rangle$ فعال‌کننده ماژول‌های جای‌گذاری هستند. سیگنال

$$|D_0\rangle, |D_1\rangle, \ldots, |D_{n-1}\rangle$$

که یک سیگنال خالی است و سیگنال میزبان

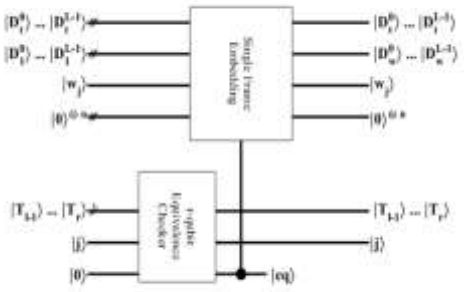
$$|D_t\rangle$$

و داده نهان نگاره $|w_j\rangle$، به‌عنوان ورودی‌های بلوک جای‌گذاری هستند که به ترتیب برای ذخیره‌سازی نمونه‌های سیگنال نهان نگاره و سیگنال اصلی در نظر گرفته شده‌اند. اگر مقدار

$$|eq\rangle$$

برابر یک باشد، ماژول جای‌گذاری فعال می‌شود و با فعال‌شدن آن، کیوبیت متناظر با نمایه قاب در آن، جاگذاری می‌شود. سپس نتیجه در کیوبیت کمکی $|0\rangle$ ذخیره می‌شود. در شکل(۱۰) مدارکلی مرحلهجای‌گذاری پیشنهادی نمایش داده شده‌است.

از پارامترهای مهم قابل‌تنظیم روش مخفی‌سازی پژواک، می‌توان به «ضریب تشدید مقدار دامنه» و «تأخیر زمانی» اشاره کرد که در اکثر پژوهش‌ها مورد بررسی قرار گرفته‌اند و میزان تأثیر آنها در شفافیت و مقاومت سیگنال آزمایش شده است. برای تولید یک سیگنال پژواک کوانتومی، باتوجه‌به بیت‌های داده نهان‌نگاری $|w\rangle$، در هر قاب، تأخیر مناسب $|d\rangle$ اضافه می‌شود و سپس دامنه نمونه‌ها به یک پارامتر خاص تقسیم می‌شوند. در روش مخفی-سازی پژواک تلاش می‌شود که سیگنال پژواک تولید شده برای سیستم شنوایی انسان محسوس نباشد و از شفافیت خوبی برخوردار باشد.

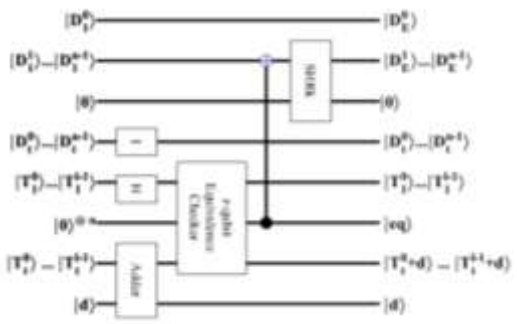


شکل (۱۰). پیاده‌سازی مدارکوانتومی مرحله جای‌گذاری روش پیشنهادی برای یک قاب از سیگنال کوانتومی

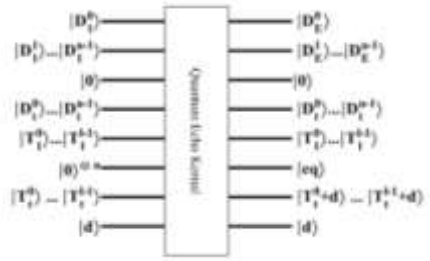
در ابتدا، مدار کوانتومی به‌منظور ایجاد هسته پژواک طراحی شده است (شکل ۱۱). $|D_t^0 \ldots\ldots D_t^{n-1}\rangle$ و $|T_t^0 \ldots\ldots T_t^{l-1}\rangle$ و$|k_i\rangle$ و$|d\rangle$ ورودی‌های مدار کوانتومی هستند. $|D_1^0 \ldots\ldots D_1^{n-1}\rangle$ و $|T_1^0 \ldots\ldots T_1^{l-1}\rangle$ و $|0\rangle$ به‌عنوان ورودی‌های کمکی مدار، جهت نگهداری اطلاعات زمان و دامنه نمونه‌های یک قاب از سیگنال صوت کوانتومی عمل می‌کنند. در قاب مربوطه، کلیه کیوبیت‌های پارامتر زمان$|T_t^0 \ldots\ldots T_t^{l-1}\rangle$ ، توسط مدار جمع‌کننده با کیوبیت $|d\rangle$ جمع می‌شوند و در حقیقت، به اندازه $|d\rangle$ کیوبیت شیفت پیدا می‌کنند. خروجی این مدار جمع کننده، به یک تساوی‌سنج وارد می‌شود. تساوی‌سنج تک‌تک کیوبیت‌های زمان سیگنال خالی$|T_1^0 \ldots\ldots T_1^{l-1}\rangle$ و سیگنال تاخیریافته را باهم مقایسه می‌کند. اگر کیوبیت‌های زمان باهم برابر بودند، تساوی‌سنج مقدار ۱ را برمی‌گرداند و مقدار دامنه سیگنال اصلی$|D_t^0 \ldots\ldots D_t^{n-1}\rangle$ را در کیوبیت دامنه سیگنال خالی $|D_1^0 \ldots\ldots D_1^{n-1}\rangle$ کپی می‌کند. در نتیجه، یک سیگنال کوانتومی با پارامترهای زمانی تأخیریافته و دامنه‌ای مشابه با سیگنال اصلی حاصل می‌شود. مدار کوانتومی این بخش، برای یک قاب به‌صورت یک مدار جداگانه ترسیم شده است (شکل۱۱). بعد از ایجاد تاخیر زمانی، به‌منظور ایجاد یک سیگنال پژواک، لازم است دامنه سیگنال به α تقسیم شود. به‌علت پیچیدگی مداری پایین‌تر ثبات‌های انتقالی، نسبت به تقسیم‌کننده‌های کوانتومی، از ثبات انتقالی منطقی SHRi برای انجام عملیات تقسیم استفاده شده است. زمانی که SHRi فعال می‌شود، دامنه تک‌تک کیبویت‌ها به پارامتر α تقسیم می‌شوند. با اشاره به مفهوم منطقی اعداد در نمایش کیوبیتی، پارامتر $\alpha = 2^{-i}$ قابل تعریف است و در نتیجه، با توجه به میزان تضعیف دامنه، دامنه‌ها به مضربی از۲ تقسیم می‌شوند. خروجی مدارات چرخشی (ثبات انتقالی‌ها)، سیگنال پژواک است که در نهایت در رجیستر$|D_E^0 \ldots\ldots D_E^{n-1}\rangle$ ذخیره می‌شود و هسته اکو توسط این مدار کوانتومی طراحی می‌شود. در ادامه مرحله جای‌گذاری و به عنوان مرحله بعد از تولید سیگنال اکو، مرحله جای‌گذاری کیوبیت نهان نگاره فرا می‌رسد. به همین منظور، یک مدار کوانتومی طراحی شده است. همانطور که در شکل(۱۲) قابل مشاهده است، کم‌ارزش‌ترین کیوبیت نمونه $|D_1^0\rangle$ برای دقیق‌تر شدن محاسبات به‌صورت جداگانه در نظر گرفته شده است و در مرحله طراحی مدار اکو، وارد مدار نشده است. اگر $|w_j\rangle$که jامین کیوبیت نهان نگاره است، برابر $|1\rangle$باشد، کم ارزش‌ترین کیوبیت نمونه نیز $|1\rangle$می‌شود و کم ارزش‌ترین کیوبیت دستخوش تغییرات می‌شود. همچنین، اگر $|1\rangle$ نباشد دروازه شرطی وارونگر عمل نمی‌کند و جای‌گذاری انجام نمی‌شود. در ادامه، سیگنال تولید شده $|D_E^0 \ldots\ldots D_E^{n-1}\rangle$ با سیگنال اصلی $|D_t^0 \ldots\ldots D_t^{n-1}\rangle$ وارد جمع‌کننده می‌شوند و سیگنال نهان‌نگاری نهایی حاصل می‌شود که در رجیستر $|D_w^0 \ldots\ldots D_w^{n-1}\rangle$ ذخیره و نگهداری می‌شود.

۴-۴ . مرحله استخراج داده نهان نگاره

مرحله دوم هر روش نهان‌نگاری مرحله استخراج داده جای‌گذاری شده است. هدف مرحله استخراج، بازیابی داده‌ای است که در مرحله جای‌گذاری، در سیگنال اصلی جاسازی شده است. روش استخراج در این مقاله، بر اساس مرحله جای‌گذاری طراحی شده است. نمودار بلوکی کلی مرحله استخراج در شکل (۱۳) ترسیم شده است. در مرحله جای‌گذاری، بعد از ایجاد سیگنال پژواک و انجام عملیات جای‌گذاری کیوبیت نهان نگاره در کیوبیت کم‌ارزش، سیگنال حاصله با سیگنال اصلی جمع شد و سیگنال نهان نگاره ایجاد شد. اکنون، باتوجه‌به عکس مرحله جای‌گذاری، در مرحله استخراج، ابتدا تفاضل سیگنال نهان‌نگاری شده از سیگنال اصلی، برای هر قاب محاسبه می‌شود.

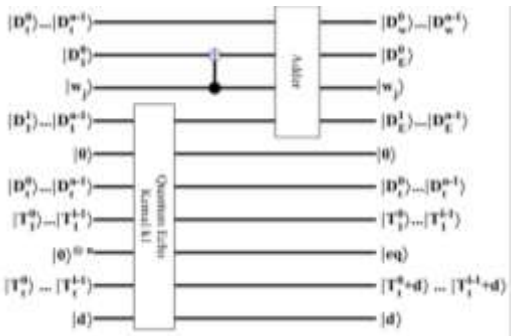


(الف)

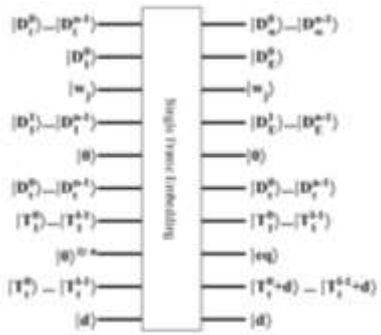


(ب)

شکل (۱۱). مدار کوانتومی هسته اکو طراحی شده در روش پیشنهادی (الف) مدارکوانتومی (ب) نمودار بلوکی



(الف)



(ب)

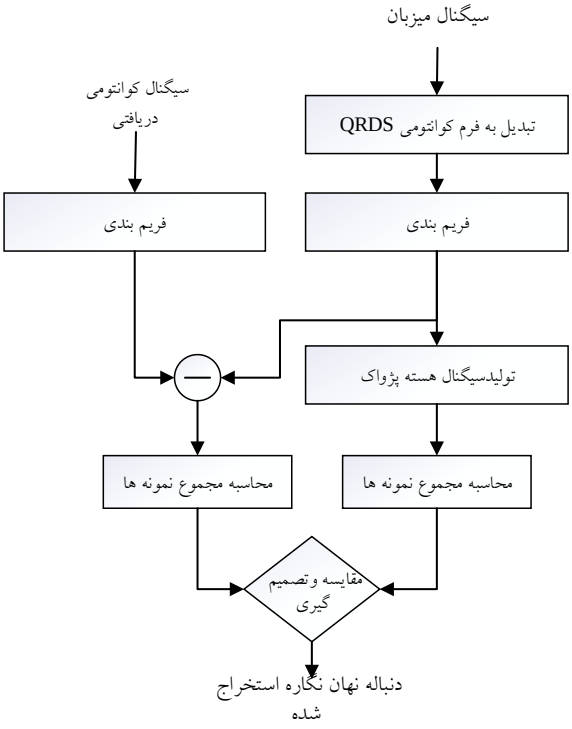
شکل (۱۲). مدارکوانتومی مرحله جای‌گذاری روش پیشنهادی برای یک قاب از سیگنال کوانتومی (الف) مدارکوانتومی (ب) نموداربلوکی

سپس، مجموع مقادیر نمونه‌های این قاب حساب می‌شود. از طرفی، یک سیگنال پژواک مشابه با مرحله جای‌گذاری نیز تولید می‌شود و برای هر قاب، مجموع نمونه‌های این سیگنال پژواک نیز حساب می‌شود. باتوجه‌به توضیحات ارائه شده در بخش جای‌گذاری، اگر مجموع نمونه‌های سیگنال پژواک از مجموع نمونه‌های سیگنال تفاضل کمتر باشد بیانگر این است که کیوبیت نهان‌نگاری $|1\rangle$ است؛ در غیر این صورت، کیوبیت نهان‌نگاری شده $|0\rangle$ است. علت این امر این است که هنگامی که کیوبیت $|1\rangle$در تک‌تک نمونه‌های سیگنال اکو جای‌گذاری می‌شود، در صورتی که کم ارزشترین کیوبیت $|1\rangle$باشد، نمونه تغییر پیدا نمی‌کند؛ ولی اگر $|0\rangle$باشد، کیوبیت LSB به $|1\rangle$ تغییر پیدا می‌کند. در نتیجه، این تغییر باعث افزایش۱ واحدی نمونه می‌شود و مجموع نمونه‌های این قاب نسبت به مجموع نمونه‌های قبل از جای‌گذاری بیشتر می‌شود. همچنین، در هنگام نهان‌نگاری کیوبیت $|0\rangle$، زمانی که کیوبیت LSB برابر $|1\rangle$ است باید به $|1\rangle$ تغییر پیدا کند. بنابراین مقدار نمونه به اندازه یک واحد کاهش پیدا می‌کند و در نهایت، مجموع نمونه‌های سیگنال اکو کاهش پیدا می‌کند. این روش نسبت به سایر روشهای نهان‌نگاری مبتنی بر LSB، در مقابل حملات بسیار مقاوم است که مزیت اصلی این روش به‌شمار می‌رود. پرواضح است که چون مرحله استخراج این روش به کیوبیت LSB وابسته نیست، در مقابل حملات احتمالی و تغییر کیوبیتها مقاوم است و حتی در حضور حملات کیوبیت نهان‌نگاری شده به‌درستی استخراج می‌شود. شبه کد مرحلهاستخراج در شکل (۱۴) نمایش داده‌شده است.

مدار مرحله استخراج کیوبیت نهان‌نگاری شده در شکل (۱۵) بیان شده است. همان‌طور که در بخش پایینی مدار قابل‌مشاهده است، یک سیگنال پژواک کوانتومی توسط ماژول هسته پژواک ایجاد می‌شود که در بخش جای‌گذاری مفصلاً جزئیات آن تشریح شد. خروجی این بخش از مدار در خطهای $|D_E^0\rangle$و $|D_E^1 \ldots\ldots D_E^{n-1}\rangle$منتقل می‌شود. در ادامه، ورودی مدار sum ثبات‌های $|D_E^0\rangle$ و $|D_E^1 \ldots\ldots D_E^{n-1}\rangle$ و ثبات مربوط به کیوبیت های زمان $|T_1^0 \ldots\ldots T_1^{l-1}\rangle$ و رجیستر کمکی $|0\rangle$ هستند که رجیستر کمکی $|0\rangle$ نتیجه مجموع در آن ذخیره خواهدشد. این ماژول sum مجموع تک تک نمونه‌های سیگنال اکو را حساب می‌کند که در خط خروجی $\sum|D_E^0 - D_E^{n-1}\rangle$ نگهداری می‌شود.

حال لازم است تفاضل سیگنال نهان‌نگاری از سیگنال اصلی محاسبه شود. مشخصات سیگنال اصلی در رجیستر $|D_t^0 \ldots\ldots D_t^{n-1}\rangle$ نگهداری می‌شود. ماژول FP+1 علامت این سیگنال را منفی می‌کند ($|D_t^0 \ldots\ldots D_t^{n-1}\rangle$ -).ماژول جمع کننده Adder برای پیاده‌سازی عملیات تفاضل به‌صورت $|D_w\rangle +$ $((-|D_t\rangle)$ بکار برده شده است. بعد از ماژول جمع کننده یک ماژول مجموع sum در مدار تعریف شده است. ماژول sum که در بالای مدار قرار دارد، مجموع تک‌تک نمونه‌های $|D_w\rangle + ((-|D_t\rangle)$

را حساب می‌کند.



شکل (۱۳). نمودار بلوکی مرحله استخراج روش پیشنهادی

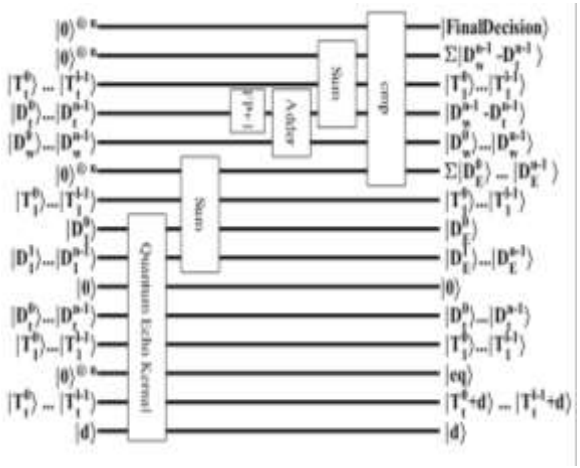
```
for j = 1 to N:
    # Calculate the difference between
host and watermarked signals
    difference_signal = host_signal -
watermarked_signal
    # Calculate the sum of the
difference signal
      sum_difference = sum
(difference_signal)
    # Apply Quantum Echo Kernel
    echoed_frame =
quantum_echo_kernel(delay_times,
amplitude_coefficient)
    sum_echoed = sum(echoed_frame)
    # Compare sums to determine the
watermark bit
    if sum_difference < sum_echoed:
        watermark_sequence[j] = 0
    else:
        watermark_sequence[j] = 1
```

شکل (۱۴). شبه کد مرحله استخراج روش پیشنهادی

ورودی‌های این مدار، $|T_1^0 \ldots\ldots T_1^{l-1}\rangle$ و رجیستر کمکی $|0\rangle$و رجیستر $(|D_w\rangle + (-|D_t\rangle)$ هستند. این ماژول مجموع را حساب می‌کند و به خط $\sum|D_w\rangle - |D_t\rangle$ منتقل می‌کند. ورودی‌های ماژول مقایسه‌کننده cmp دو مقدار $\sum|D_w\rangle - |D_t\rangle$ و $\sum|D_E^0 - D_E^{n-1}\rangle$ و رجیستر کمکی $|0\rangle$ هستند که با مقایسه این دو مقدار، نتیجه نهایی در کیوبیت کمکی $|0\rangle$ ذخیره می‌شود و کیوبیت جای‌گذاری شده تشخیص داده می‌شود. نکته قابل توجه این است که در طراحی مدارات، بعضی خطوط به‌صورت زاید و اضافی قابل مشاهده هستند که در کارکرد مدار تاثیری ندارند، ولی در طراحی مدارات ناچارا وجود دارند و در مدار دیده می‌شوند.

۵. ارزیابی روش پیشنهادی

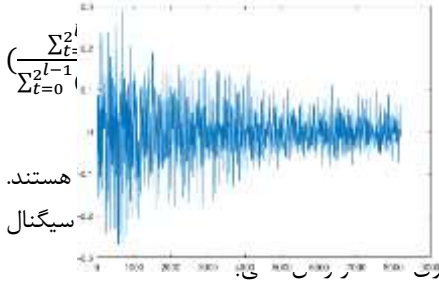
در این مقاله، به علت در دسترس نبودن رایانه‌های کوانتومی، از رویکرد شبیه‌سازی برای انجام ارزیابی‌ها استفاده شده است. آزمایش‌ها با استفاده از یک رایانه با پردازنده اینتل Corei5 u 2.7GHz با حافظه 8 گیگابایت و به کمک نرم‌افزار Matlab 2016a انجام شد. برای شبیه‌سازی نتایج ۳ فایل صوتی متعلق به آزمایشگاه علوم و کامپیوتر دانشگاه امیرکبیر استفاده شده که همگی موسیقی بی‌کلام هستند.



شکل (۱۵). مدارکوانتومی مرحله استخراج روش پیشنهادی برای یک قاب از سیگنال کوانتومی

طول‌موج ۱ ثانیه ازاین داده‌ها در شکل (۱۶) نمایش داده-شده است. در تمامی آزمایش‌ها، نرخ نمونه‌برداری ۸۱۹۲ است. نمونه‌های صوتی به 256 (q=8)سطح کوانتیزه شده و تا ۴ رقم اعشار گرد شده‌اند. هر ۱۶ نمونه یک قاب را تشکیل می‌دهند و

از ۱۶ قاب برای نهان‌نگاری ۱۶ کیوبیت داده تصادفی استفاده شده است (l = 9). به این ترتیب، ظرفیت نهان‌نگاری[۲۹] bps است (۸۱۹۲/۱۶×۱۶=۵۱۲). داده نهان نگاره یک دنباله تصادفی ۱۶ کیوبیتی متشکل از |1⟩ و |0⟩ در نظرگرفته شده است. تمام روش-های بررسیشده با ظرفیت ۲[۹]نهان‌نگاری شده‌اند و با ظرفیت یکسان، نرخ شفافیت و مقاومت آنها باهم مقایسه شده است.



شکل (۱۶). شکل موج فایل‌های صوتی بکار برده شده جهت انجام شبیه‌سازی‌ها و انجام ارزیابی‌ها

۱-۵. ارزیابی شفافیت

در فرایند نهان‌نگاری، یکی از مهم‌ترین فاکتورهای کیفی که باید بر روی سیگنال نهان‌نگاری شده بررسی شود، نرخ شفافیت است که تغییرناپذیری کیفیت سیگنال دست‌کاری شده و شنوایی ناپذیری داده نهان نگاره برای شنونده را مشخص می‌کند. شفافیت بالا به این معناست که سیگنال نهان نگاره نسبت به سیگنال اصلی تغییر محسوسی نکرده است. به‌منظور ارزیابی شفافیت روش‌های پیشنهادی، از معیار نسبت سیگنال به نویز (SNR) استفاده شده است که به‌صورت نسبت توان سیگنال به توان نویز زمینه بر حسب دسی‌بل و در قالب رابطه (۶) محاسبه می‌شود:

$$SNR = 10\log\left(\frac{p_s}{p_n}\right) = 10log_{10}\left(\frac{\sum_{t=}^{2^l}}{\sum_{t=0}^{2^{l-1}}}\right) \quad (۶)$$

p_n و p_s به هستند. همچنین، D_t و سیگنال میزبان ونهان‌نگاری

به‌منظور بررسی پارامترهای تأثیرگذار (d) نهان‌نگاری در روش‌های مبتنی بر مخفی‌سازی پژواک، ضرایب تشدید دامنه α و عامل d به‌عنوان تأخیر زم حلیل قرار می‌گیرند. در پ کلاسیک مخفی‌سازی پژوا کوچک‌تر باشد، سیگنال نه هان‌نگاری کوانتومی مبتنی ب بات رسید [۲۹]. این پژوهش نیز در پی اثبات این ادعا است. بدین منظور، تأثیر α در جدول (۱)بررسی شده(۲) است. باتوجه به ماهیت کیوبیت‌ها در نمـ به‌صورت ضرایبی از 2^{-k} ؛ بت روش پیشنهادی بر رو ست. قابل مشاهده است که شفافیت وجود دارد. هرچه α کمتر و ضعیف‌تر باشد، ج کمتری خواهد بود و نرخ شفافیت بالا می‌رود و SNR افزایش می‌یابد.

در جدول (۲) پارامتر تأخیر زمانی d بر روی شفافیت سیگنال نهان‌نگاری شده حاصل از رویکرد پیشنهادی، بررسی شده است. سیگنال پژواک سیگنالی تضعیف شده با تأخیر زمانی از همان سیگنال اصلی است. تأخیر زمانی d با اعداد ۲و ۴و ۸و ۱۰ مورد آزمایش قرار گرفته است؛ d=2 بدین معناست که نمونه‌های سیگنال به اندازه ۲ نمونه شیفت پیدا کرده‌اند و زمان نمونه‌ها به‌اندازه d واحد افزایش پیدا کرده است.

نتایج نشان می‌دهند که در اکثر سیگنال‌های صوتی، با افزایش مقدار d، اعوجاج بیشتری در سیگنال نهان‌نگاری شده ایجاد می‌شود و شفافیت کاهش می‌یابد. البته باتوجه‌به پیچیدگی ماهیت سیگنال صوت و متغیر بودن شکل موج سیگنال‌های صوتی، گاهی خلاف این گفته مشاهده می‌شود. به‌عنوان‌مثال، در جدول (۲)دیده می‌شود که برای داده صوتی ۱، علیرغم افزایش

مقدار d، اعوجاج کمتری نسبت به سیگنال اصلی ایجاد می‌شود و با افزایش تأخیر زمانی بین نمونه‌ها، نرخ شفافیت بهبود یافته است. ولی در اکثر داده‌های صوتی، هرچه پارامتر d کوچک‌تر انتخاب شود مقدار SNR افزایش می‌یابد.

جدول (۱). بررسی نرخ تأثیر پارامتر ضریب تشدید α به‌عنوان یک فاکتور مؤثر در تولید هسته پژواک کوانتومی بر SNR

k	α	Data1	Data2	Data3
-۳	۰/۱۲۵	۱۸/۰۳	۱۸/۰۱	۱۸/۰۹
-۵	۰/۰۳۱	۳۰/۰۷	۳۰/۰۵	۳۰/۱۳
-۶	۰/۰۱۵	۳۶/۰۹	۳۶/۰۷	۳۶/۱۶
-۷	۰/۰۰۷	۴۲/۱۱	۴۲/۰۹	۴۲/۱۸
-۸	۰/۰۰۳	۴۸/۱۳	۴۸/۱۱	۴۸/۲۰
-۹	۰/۰۰۳	۴۵/۱۵	۵۴/۱۳	۵۴/۲۲
-۱۰	۰/۰۰۰۹	۶۰/۱۷	۶۰/۱۵	۶۰/۲۴
-۱۱	۰/۰۰۰۴	۶۶/۱۹	۶۶/۱۸	۶۶/۲۶

در جدول (۳) شفافیت روش پیشنهادی با سایر روش‌های نهان‌نگاری کوانتومی در شرایط یکسان مقایسه شده است. پارامترهای بکار برده شده برای روش پیشنهادی d=2 و α با مقدار K=11 استخراج شده‌اند. نتایج حاکی از آن است که شفافیت روش پیشنهادی از سایر روش‌ها بالاتر یا در حد معقول و قابل‌پذیرشی است.

جدول (۲). بررسی نرخ تأثیر پارامتر تأخیر زمانی d به‌عنوان یک فاکتور مؤثر در تولید هسته پژواک کوانتومی بر SNR

d	مجموعه‌داده‌ها		
	Data1	Data2	Data3
۲	۶۶/۱۹	۶۶/۱۸	۶۶/۲۶
۴	۶۶/۱۸	۶۶/۱۳	۶۶/۲۷
۸	۶۶/۲۰	۶۶/۰۶	۶۶/۱۵
۱۰	۶۶/۲۳	۶۶/۰۴	۶۶/۰۱

۲-۵. ارزیابی مقاومت

میزان عدم تغییراتی که نهان نگاره ادغام شده به‌واسطه دسته‌ای از تبدیلات یا حملات مشخص متحمل می‌شود را مقاومت می‌گویند. الگوریتمی که تغییرات آن در اثر این حملات زیاد باشد، شکننده نامیده می‌شود و الگوریتمی که در برابر طیف وسیعی از حملات، کمترین تغییرات را متحمل می‌شود، مقاوم نامیده می‌شود. معیار Bit Error Ratio (BER) میزان خطاهای موجود در داده‌های استخراج شده در یک روش نهان‌نگاری را مشخص می‌کند. اگر N_w تعداد بیت‌های نهان نگاره، w سیگنال نهان نگاره اصلی و w' سیگنال نهان نگاره بازیابی شده باشد، BER بر اساس رابطه (۷) محاسبه می‌شود [۲۳].

$$BER = \frac{Number\ of\ Error\ Bits}{Total\ Number\ of\ Bits} = \frac{1}{N_w}\sum_{n=1}^{N_w} w(n) \oplus w'(n) \quad (۷)$$

در ادامه، به‌منظور بررسی مقاومت روش پیشنهادی، سه آزمایش انجام شده است. در آزمایش اول، تأثیر نویز flip بر روی LSB، در آزمایش دوم، تأثیر حمله صفر بر روی بیت LSB و در آزمایش سوم، تأثیر نویز flip بر روی داده‌های نهان‌نگاری شده مورد بررسی قرار گرفته است. در آزمایش‌های انجام شده، با احتمالات مختلف $p \in \{0.01,0.02,0.05,0.1,0.2,0.3\}$ -، نویزهایی روی سیگنال نهان نگاری شده اعمال شده و پس از استخراج دنباله نهان نگاری شده، معیار BER محاسبه گردید. به‌منظور افزایش دقت محاسبه، فرایند ذکر شده ۱۰۰ بار انجام شد و میانگین BER های بدست آمده ثبت شد.

نتایج تأثیر نویز معکوس‌کننده بر روی LSB در جدول (۴) بیان شده‌اند. در یک کانال کوانتومی، نویز معکوس‌کننده، با احتمال p-1، کیوبیت را از $|0\rangle$ به $|1\rangle$ و یا بالعکس تبدیل می‌کند. نتایج، نشان دهنده مقاومت بسیار بالای روش پیشنهادی است. روش ترکیبی پیشنهادی، برخلاف سایر روش‌های مبتنی بر کیوبیت کم‌ارزش، در مقابل حملات LSB مقاوم است. علت این امر این است که در مرحله استخراج روش پیشنهادی، تشخیص کیوبیت نهان نگاره وابسته به کیوبیت LSB نمی‌باشد و در نتیجه، مقاومت بهبود می‌یابد و هرچند کیوبیت LSB نویزی شود و تغییر یابد، تشخیص کیوبیت نهان نگاره به‌درستی انجام می‌شود. مقاومت این روش در حد مقاومت روش کوانتومی مبتنی بر مخفی‌سازی پژواک ارائه شده در مقاله می‌باشد.

در جدول (۵)، حمله صفر مورد بررسی قرار گرفته است که کم ارزشترین کیوبیت نمونه نهان‌نگاری شده را به صفر تبدیل می‌کند. مقاومت بالای روش پیشنهادی در این آزمایش نیز مشهود است و نسبت به سایر روش‌ها، در وضعیت برابر یا بالاتر گزارش شده است. مقاوم بودن در مقابل تغییر کیوبیت کم‌ارزش، نسبت به نویزهایی که مستقیماً کیوبیت LSB را تحت تاثیر قرار می‌دهند، به‌عنوان بارزترین مزیت این روش به‌شمار می‌رود. با توجه به اینکه این روش جزء روش‌های نهان‌نگاری ترکیبی مبتنی بر کیوبیت کم‌ارزش در نظر گرفته می‌شود.

تأثیر نویز flip بروی داده‌های نهان‌نگاری در جدول (۶) بررسی شده و نتایج ارائه شده‌اند. با بالارفتن مقدار احتمال نویزی شدن داده‌ها (p-1)، مقدار کیوبیت‌های نویزی شده بیش‌تر

می‌شود، مقاومت روش‌ها کاهش می‌یابد و نرخ BER افزایش پیدا می‌کند. نرخBER روش پیشنهادی در مقایسه با سایر روش‌ها، دارای مقدار کمتری است. حتی مقاومت این روش در مقایسه با روش مخفی‌سازی پژواک تکی نیز بیشتر گزارش شده است که مزیت دیگر این روش به‌حساب می‌آید و نشان‌دهنده بهبود روش مخفی‌سازی پژواک کوانتومی پیشین است. روش مخفی‌سازی پژوات تکی کوانتومی در احتمال‌های بالا، در مقابل روش کد گری دارای ضعف بود و در احتمال ۰,۳ نسبت به روش نهان‌نگاری کوانتومی مبتنی بر کد گری ضعیف‌تر بود و مقاومت پایین‌تری داشت. روش کد گری، در مباحث کنترل خطا نتایج خوبی ارائه می‌کند و همین امر علت مقاومت نسبی آن به شمار می‌رود. ولی روش پیشنهادی این ضعف را جبران کرد و نتایج مقاومت را حتی با احتمال‌های بالا بهبود بخشید.

۶. تحلیل روش پیشنهادی

در این بخش از مقاله تحلیل‌هایی بر روی روش پیشنهادی صورت‌گرفته است. در بخش اول، تحلیل سخت‌افزاری مدارات پیشنهادی صورت‌گرفته است و هزینه کوانتومی مدارات محاسبه شده است. هزینه کوانتومی، به‌عنوان یک عامل مهم در ارزیابی سخت‌افزاری مدارات همیشه موردتوجه پژوهشگران قرار گرفته است. در بخش دوم، تحلیل آماری داده‌های اطلاعاتی قبل و بعد از جای‌گذاری روش پیشنهادی با کمک نمودار هیستوگرام انجام شده است.

۱-۶. هزینه کوانتومی مدار

در پردازش محاسبات کوانتومی، هزینه کوانتومی مداری، بستگی به تعداد و نوع دروازه‌های بکار برده شده دارد. بدیهی است که هرچه تعداد دروازه‌های بکار برده شده بیشتر باشد، هزینه کوانتومی سخت‌افزاری و مداری رشد می‌کند. عملگرهای یکانی ۲×۲، شامل دروازه‌ها دا ما رد و دروازه وارونگر[1]، به‌عنوان واحد در نظر گرفته شده‌اند. دروازه وارونگر کنترل، به‌عنوان واحد پایه در نظر گرفته شده و سایر دروازه‌ها می‌توانند به‌وسیله دروازه وارونگر کنترل، ایجاد و شبیه‌سازی شوند [۲۴]. هزینه کوانتومی دروازه-های پایه و بعضی مدارات در جدول (۷) نمایش داده شده‌اند [۲۳, ۲۶]. در ادامه، مدارات کوانتومی روش پیشنهادی از نظر هزینه کوانتومی آنالیز می‌شوند.

۱-۱-۶. مرحله جای‌گذاری

مرحله جای‌گذاری از یک ماژول هسته پژواک کوانتومی و دروازه کنترل وارونگر و یک جمع‌کننده تشکیل شده است. ماژول هسته پژواک کوانتومی نیز خود شامل یک دروازه‌ها دا ما رد، یک دروازه یکانی، یک تساوی سنج r-کیوبیتی، یک دروازه کنترل وارونگر و یک ثبات انتقالی راست تشکیل شده است .

[3]NOT Gate

جدول (۳). مقایسه پارامتر SNR روش پیشنهادی با سایرروش‌های نهان‌نگاری کوانتومی

مجموعه‌داده	cLSQ1[30]	cLSQ2[30]	cLSQ3[30]	QLSB [27]	QLSB[26]	QSEH[29]	روش پیشنهادی
Data1	۵۵/۸۶	۵۱/۶۰	۴۴/۱۹	۵۸/۸۷	۴۱/۶۲	۶۶/۷۰	۶۶/۱۸
Data2	۵۸/۶۰	۵۱/۶۱	۴۷/۸۰	۵۸/۶۰	۵۴/۲۰	۶۶/۴۰	۶۶/۱۹
Data3	۵۸/۱۳	۵۱/۴۴	۴۳/۸۷	۵۷/۴۶	۵۵/۱۲	۶۶/۲۹	۶۶/۲۶
میانگین	۵۷/۵۳	۵۱/۵۵	۴۵/۲۸	۵۸/۳۱	۵۰/۳۱	۶۶/۴۶	۶۶/۲۱

جدول (۴). نتایج تأثیر flip noise بر روی بیت LSB

مجموعه‌داده	1-p	cLSQ1[30]	cLSQ2[30]	cLSQ3[30]	QLSB[27]	QLSB[26]	QSEH[29]	روش پیشنهادی
Data1	۰/۰۱	۰/۰۱۱	۰/۰۰۰	۰/۰۰۰	۰/۰۰۶	۰/۰۰۶	۰/۰۰۰	۰/۰۰۰
	۰/۰۲	۰/۰۲۳	۰/۰۰۰	۰/۰۰۰	۰/۰۱۳	۰/۰۰۹	۰/۰۰۰	۰/۰۰۰
	۰/۰۵	۰/۰۴۸	۰/۰۰۰	۰/۰۰۰	۰/۰۴۱	۰/۰۳۹	۰/۰۰۰	۰/۰۰۰
	۰/۱	۰/۰۹۲	۰/۰۰۰	۰/۰۰۰	۰/۰۸۵	۰/۰۸۹	۰/۰۰۰	۰/۰۰۰
	۰/۲	۰/۱۹۰	۰/۰۰۰	۰/۰۰۰	۰/۱۸۳	۰/۱۷۰	۰/۰۰۰	۰/۰۰۰
	۰/۳	۰/۲۹۱	۰/۰۰۰	۰/۰۰۰	۰/۲۹۲	۰/۲۰۷	۰/۰۰۰	۰/۰۰۰
Data2	۰/۰۱	۰/۰۰۶	۰/۰۰۰	۰/۰۰۰	۰/۰۰۷	۰/۰۰۳	۰/۰۰۰	۰/۰۰۰
	۰/۰۲	۰/۰۱۲	۰/۰۰۰	۰/۰۰۰	۰/۰۱۵	۰/۰۰۹	۰/۰۰۰	۰/۰۰۰
	۰/۰۵	۰/۰۴۶	۰/۰۰۰	۰/۰۰۰	۰/۰۴۵	۰/۰۲۲	۰/۰۰۰	۰/۰۰۰
	۰/۱	۰/۰۸۸	۰/۰۰۰	۰/۰۰۰	۰/۰۸۰	۰/۰۴۶	۰/۰۰۰	۰/۰۰۰
	۰/۲	۰/۱۷۹	۰/۰۰۰	۰/۰۰۰	۰/۱۸۲	۰/۱۱۵	۰/۰۰۰	۰/۰۰۱
	۰/۳	۰/۲۲۰	۰/۰۰۰	۰/۰۰۰	۰/۲۷۲	۰/۱۵۳	۰/۰۰۱	۰/۰۰۶
Data3	۰/۰۱	۰/۰۰۹	۰/۰۰۰	۰/۰۰۰	۰/۰۰۷	۰/۰۰۳	۰/۰۰۰	۰/۰۰۰
	۰/۰۲	۰/۰۱۶	۰/۰۰۰	۰/۰۰۰	۰/۰۱۳	۰/۰۰۸	۰/۰۰۰	۰/۰۰۰
	۰/۰۵	۰/۰۳۸	۰/۰۰۰	۰/۰۰۰	۰/۰۴۳	۰/۰۲۵	۰/۰۰۰	۰/۰۰۰
	۰/۱	۰/۰۸۹	۰/۰۰۰	۰/۰۰۰	۰/۰۹۱	۰/۰۴۵	۰/۰۰۰۶	۰/۰۰۰
	۰/۲	۰/۱۸۸	۰/۰۰۰	۰/۰۰۰	۰/۱۸۰	۰/۱۰۰	۰/۰۰۱	۰/۰۰۰
	۰/۳	۰/۲۷۶	۰/۰۰۰	۰/۰۰۰	۰/۲۹۶	۰/۱۵۳	۰/۰۰۵	۰/۰۰۰

جدول (۵). نتایج تأثیر حمله صفر بر LSB

مجموعه‌داده	1-p	cLSQ1[30]	cLSQ2[30]	cLSQ3[30]	QLSB[27]	QLSB[26]	QSEH[29]	روش پیشنهادی
Data1	۰/۰۱	۰/۰۰۴	۰/۰۰۰	۰/۰۰۰	۰/۰۰۱	۰/۰۰۱	۰/۰۰۰	۰/۰۰۰
	۰/۰۲	۰/۰۰۸	۰/۰۰۰	۰/۰۰۰	۰/۰۰۴	۰/۰۰۴	۰/۰۰۰	۰/۰۰۰

	۰/۰۵	۰/۰۱۷	۰/۰۰۰	۰/۰۰۰	۰/۰۱۴	۰/۰۱۱	۰/۰۰۰	۰/۰۰۰
	۰/۱	۰/۰۴۰	۰/۰۰۰	۰/۰۰۰	۰/۰۳۴	۰/۰۳۴	۰/۰۰۰	۰/۰۰۰
	۰/۲	۰/۰۸۰	۰/۰۰۰	۰/۰۰۰	۰/۰۸۰	۰/۰۶۰	۰/۰۰۰	۰/۰۰۰
	۰/۳	۰/۱۱۷	۰/۰۰۰	۰/۰۰۰	۰/۰۸۶	۰/۰۹۱	۰/۰۰۰	۰/۰۰۰
Data2	۰/۰۱	۰/۰۰۲	۰/۰۰۰	۰/۰۰۰	۰/۰۰۰۶	۰/۰۰۰	۰/۰۰۰	۰/۰۰۰
	۰/۰۲	۰/۰۰۵	۰/۰۰۰	۰/۰۰۰	۰/۰۰۷	۰/۰۰۱	۰/۰۰۰	۰/۰۰۰
	۰/۰۵	۰/۰۱۸	۰/۰۰۰	۰/۰۰۰	۰/۰۲۱	۰/۰۰۷	۰/۰۰۰	۰/۰۰۰
	۰/۱	۰/۰۳۵	۰/۰۰۰	۰/۰۰۰	۰/۰۳۰	۰/۰۱۹	۰/۰۰۰	۰/۰۰۰
	۰/۲	۰/۰۷۶	۰/۰۰۰	۰/۰۰۰	۰/۰۷۳	۰/۰۳۳	۰/۰۰۰	۰/۰۰۰
	۰/۳	۰/۱۱۷	۰/۰۰۰	۰/۰۰۰	۰/۱۲۲	۰/۰۵۰	۰/۰۰۰	۰/۰۰۰
Data3	۰/۰۱	۰/۰۰۲	۰/۰۰۰	۰/۰۰۰	۰/۰۰۳	۰/۰۰۱	۰/۰۰۰	۰/۰۰۰
	۰/۰۲	۰/۰۰۴	۰/۰۰۰	۰/۰۰۰	۰/۰۰۹	۰/۰۰۵	۰/۰۰۰	۰/۰۰۰
	۰/۰۵	۰/۰۱۷	۰/۰۰۰	۰/۰۰۰	۰/۰۲۴	۰/۰۱۳	۰/۰۰۰	۰/۰۰۰
	۰/۱	۰/۰۳۸	۰/۰۰۰	۰/۰۰۰	۰/۰۴۸	۰/۰۲۵	۰/۰۰۱	۰/۰۰۰
	۰/۲	۰/۰۸۰	۰/۰۰۰	۰/۰۰۰	۰/۱۱۴	۰/۰۵۳	۰/۰۰۸	۰/۰۰۰
	۰/۳	۰/۱۱۶	۰/۰۰۰	۰/۰۰۰	۰/۱۷۳	۰/۰۸۵	۰/۰۱۷	۰/۰۰۰

جدول (۶). نتایج تأثیر flip noise

مجموعه‌داده	1-p	cLSQ1[30]	cLSQ2[30]	cLSQ3[30]	QLSB[27]	QLSB[26]	QSEH[29]	روش پیشنهادی
Data1	۰/۰۱	۰/۰۹۱	۰/۰۶۶	۰/۰۶۲	۰/۰۳۰	۰/۰۷۱	۰/۰۰۰۱	۰/۰۰۰۶
	۰/۰۲	۰/۱۵۸	۰/۱۳۰	۰/۱۲۰	۰/۰۶۱	۰/۰۷۶	۰/۰۰۰۶	۰/۰۰۱۲
	۰/۰۵	۰/۳۳۸	۰/۲۸۰	۰/۲۵۸	۰/۱۱۰	۰/۲۸۰	۰/۰۰۴	۰/۰۰۲۱
	۰/۱	۰/۵۲۱	۰/۴۷۰	۰/۴۶۵	۰/۱۹۶	۰/۴۷۴	۰/۰۸۸	۰/۰۰۴۶
	۰/۲	۰/۶۲۰	۰/۶۰۱	۰/۵۹۰	۰/۲۶۸	۰/۵۳۱	۰/۱۰۶	۰/۰۰۵۳
	۰/۳	۰/۶۶۰	۰/۶۱۶	۰/۶۱۱	۰/۳۱۷	۰/۵۳۸	۰/۴۲۶	۰/۰۰۸۲
Data2	۰/۰۱	۰/۰۷۲	۰/۰۵۳	۰/۰۵۰	۰/۰۱۶	۰/۰۵۳	۰/۰۰۰	۰/۰۰۰۶
	۰/۰۲	۰/۱۳۱	۰/۱۲۰	۰/۰۹۴	۰/۰۲۸	۰/۱۱۸	۰/۰۰۱	۰/۰۰۱۳
	۰/۰۵	۰/۳۱۶	۰/۲۸۹	۰/۲۴۰	۰/۰۶۹	۰/۲۸۴	۰/۰۰۵	۰/۰۰۲۵
	۰/۱	۰/۵۵۵	۰/۵۰۵	۰/۴۴۰	۰/۰۹۸	۰/۴۶۰	۰/۰۴۱	۰/۰۰۳۱
	۰/۲	۰/۸۱۷	۰/۷۸۱	۰/۷۲۳	۰/۱۰۰	۰/۶۸۶	۰/۲۲۹	۰/۰۰۳۵
	۰/۳	۰/۹۳۸	۰/۹۰۱	۰/۷۳۹	۰/۱۶۰	۰/۷۱۰	۰/۳۷۸	۰/۰۰۳۹
Data3	۰/۰۱	۰/۰۶۸	۰/۰۵۰	۰/۴۰۹	۰/۰۱۱	۰/۰۶۰	۰/۰۰۰	۰/۰۰۶
	۰/۰۲	۰/۱۳۶	۰/۱۲۱	۰/۱۰۹	۰/۰۳۳	۰/۱۱۵	۰/۰۰۱	۰/۰۱۸
	۰/۰۵	۰/۳۳۲	۰/۲۸۳	۰/۲۳۴	۰/۰۶۵	۰/۲۶۷	۰/۰۱۰	۰/۰۴۵

۰/۱	۰/۵۵۰	۰/۴۹۴	۰/۴۴۸	۰/۰۹۹	۰/۴۷۹	۰/۰۶۵	۰/۰۵۷
۰/۲	۰/۸۲۱	۰/۷۸۰	۰/۷۲۵	۰/۱۰۱	۰/۶۸۱	۰/۲۷۸	۰/۰۷۳
۰/۳	۰/۹۳۵	۰/۹۰۴	۰/۸۵۳	۰/۱۷۰	۰/۷۶۱	۰/۴۳۷	۰/۰۹۸

به‌منظور محاسبه هزینه کوانتومی مدار کوانتومی هسته پژواک کوانتومی ارائه شده در شکل (۱۱) به شرح زیر اقدام می‌شود:

- هزینه کوانتومی مدار جمع‌کننده از مرتبه $O(n)\approx O(28n+2)$ می‌باشد. همان‌طور که در شکل (۲) قابل‌مشاهده است، دروازه جمع‌کننده از 2n دروازه carry و (n+1) دروازه sum تشکیل شده است. هر ماژول carry متشکل از دو دروازه تافولی و یک دروازه وارونگر کنترل است و هر ماژول sum، بر اساس شکل (۲)، شامل دو دروازه کنترل وارونگر است [۲۳].

جدول (۷). هزینه کوانتومی دروازه‌های کوانتومی

دروازه	پیچیدگی
وارونگر	۱
هادا مارد	۱
کنترل وارونگر	۱
وارونگر صفر	۳
تعویض	۳
تافولی	۶
جمع‌کننده	$28n+2$
مجموع	$N(l^2+n^3)$
مقایسه‌کننده	$48l^2-36l+18$
ثبات انتقالی راست	l^2+n^3
تساوی سنج -rکیوبیتی	$18n-11$

- هزینه کوانتومی دروازه یکانی برابر یک می‌باشد
- هزینه کوانتومی دروازه هادامارد برابر یک می‌باشد
- هزینه کوانتومی تساوی سنج r کیوبیتی برابر $O(12n+6n-11)=O(18n-11)\approx O(18n)$ می‌باشد چرا که دارای 2n دروازه کنترل وارونگر صفر با هزینه کوانتومی $O(2n\times3)=O(6n)$ و نیز دارای n دروازه کنترل وارونگر با پیچیدگی $O(12n-11)$
- هزینه کوانتومی مدار دروازه کنترل وارونگر برابر یک می‌باشد
- پیچیدگی مدار ثبات انتقالی راست از مرتبه $O(3n+1)\approx O(3n)$ برخوردار است چرا که شامل n دروازه تعویض[1] و یک دروازه کنترل وارونگر است و هر دروازه تعویض شامل سه دروازه کنترل وارونگر است.

بر اساس، مجموع هزینه‌های کوانتومی تک‌تک دروازه‌ها و ماژول‌ها، هزینه کوانتومی کلی مدار ارائه شده در شکل (۱۲) به‌صورت زیر محاسبه می‌شود:

$$O(28n+2+1+1+18n-11+1+3n+1)=O(49n-5)\approx O(n)$$

بنابراین، نتیجه شده که هزینه کوانتومی مدار هسته پژواک کوانتومی، خطی و از مرتبه n است.

علاوه بر این، به‌منظور محاسبه هزینه کوانتومی مدار کوانتومی هسته پژواک کوانتومی ارائه شده در شکل (۱۱) به‌صورت زیر اقدام می‌شود:

- هزینه کوانتومی مدار هسته پژواک کوانتومی که در مرحله قبل محاسبه شد برابر $O(49n-5)$ می‌باشد
- هزینه کوانتومی دروازه کنترل وارونگر برابر یک است
- هزینه کوانتومی مدار جمع‌کننده از مرتبه $O(28n+2)\approx O(n)$ برخوردار است

هزینه کوانتومی کلی مدار ارائه شده در شکل (۱۲) که مدار کلی مرحله جای‌گذاری است به‌قرار زیر است:

$$O(49n-5+1+28n+2)=O(77n-2)\approx O(n)$$

در طراحی‌های سخت‌افزاری هزینه‌های کوانتومی خطی نسبت به هزینه‌های نمایی بسیار مطلوب‌تر و کم‌هزینه‌تر هستند و در این مدار، ثابت شد که هزینه کوانتومی خطی است.

۲-۱-۶. مرحله استخراج

مدار مرحله استخراج در شکل (۱۵)ترسیم شده است. این مدار از یک ماژول هسته کوانتومی، دو دروازه مجموع، یک دروازه FP+1 و یک مقایسه‌کننده تشکیل شده است که در ادامه هزینه

[4] swap

کوانتومی تک‌تک ماژول‌ها محاسبه می‌شوند.

- هزینه کوانتومی مدار کوانتومی هسته پژواک کوانتومی مطابق با شکل (۱۱)
  - هزینه کوانتومی مدار هسته پژواک کوانتومی که در مرحله قبل محاسبه شد برابر $O(49n-5)\approx O(n)$
  - هزینه کوانتومی ماژول مجموع $O(l^2+n^3)$
  - هزینه کوانتومی ماژول FP+1 برابر $O(n^2+n+1)\approx O(n^2)$
  - هزینه کوانتومی ماژول مقایسه‌کننده از مرتبه $O(48l^2-36l+18)\approx O(l^2)$ برخوردار است.

هزینه کوانتومی کلی مدار ارائه شده در شکل (۱۵)که مدار کلی مرحله استخراج است به‌قرار زیر است:

$$O(49n-5+ l^2+n^3+l^2+n^3+ n^2+n+1+48l^2-36l+18)=O(l^2+n^3)$$

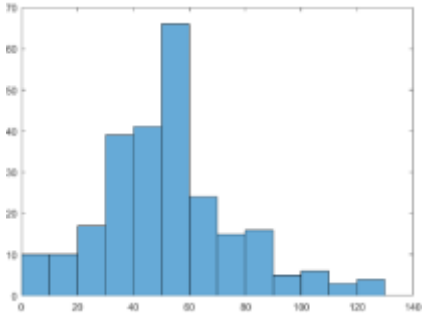
چون $l < n$

$$O(l^2+n^3) \approx O(n^3)$$

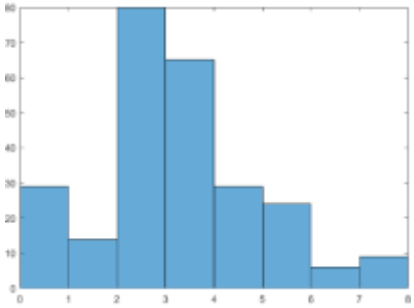
اگرچه هزینه کوانتومی مدار استخراج به‌صورت نمایی حاصل شد؛ ولی باتوجه‌به مقاله [۲۶] و کوچک بودن عدد n، در حد قابل قبولی ارائه شده است.

۲-۶. نمایش هیستوگرام و پاسخ فرکانسی

هیستوگرام[1]، مجموعه‌ای از ستون‌های در کنار یکدیگر است که ارتفاع هر ستون بیانگر میزان فراوانی دسته آن ستون است. نمایش‌های هیستوگرام سیگنال اصلی(۱) به همراه سیگنال پژواک تولید شده در شکل (۱۷) نشان‌داده‌شده است.



(الف)

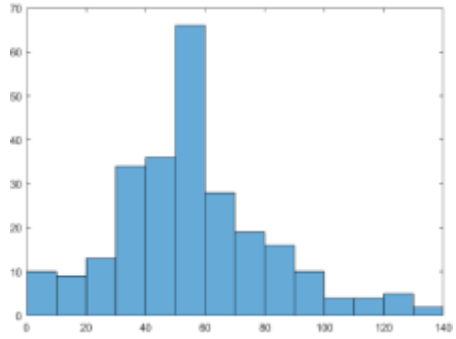


(ب)

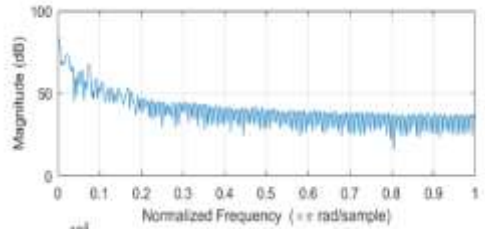
شکل (۱۷). نمودارهیستوگرام (الف) سیگنال اصلی (۱)، و (ب) سیگنال پژواک

هیستوگرام سیگنال نهان‌نگاری شده که از مجموع سیگنال اصلی و سیگنال پژواک تشکیل می‌شود، در شکل (۱۹) نشان داده شده است. همانطوری که مشاهده می‌شود، هیستوگرام سیگنال‌های اصلی و نهان-نگاری شده از توزیع گوسی شکل تبعیت می‌کنند به طوری که مقادیر نمونه‌های هیستوگرام سیگنال نهان‌نگاری شده نسبت به نمونه‌های هیستوگرام سیگنال اصلی افزایش یافته است که این افزایش در محورافقی قابل ملاحظه است. علاوه بر این، نمایش اندازه پاسخ فرکانسی سیگنال اصلی (۱) بهمراه سیگنال نهان‌نگاری شده در شکل (۱۹) نشان داده شده است.

همان‌طور که در شکل (۱۹) مشاهده می‌شود، درج سیگنال نهان نگاره در سیگنال اصلی، موجب ایجاد قله‌هایی در پاسخ فرکانسی سیگنال نهان‌نگاری نسبت به سیگنال اصلی شده‌است که این نشان‌دهنده ایجاد تشدید در برخی از فرکانس‌ها به واسطه عملیات جاسازی نهان نگاره می‌باشد.

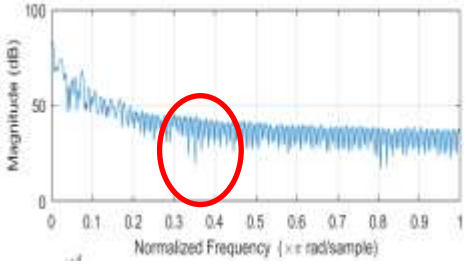


شکل (۱۸). نمودارهیستوگرام سیگنال نهان‌نگاری‌شده با روش پیشنهادی



[1] Histogram

(الف)



(ب)

شکل (۱۹). اندازه پاسخ فرکانسی (الف) سیگنال اصلی (۱)، و (ب) سیگنال نهان‌نگاری شده

۷. نتیجه‌گیری و پیشنهادهای آتی

در این مقاله، یک روش نهان‌نگاری مقاوم پیشنهاد شد که از روش مخفی‌سازی پژواک – بیت کم‌ارزش، به‌منظور نهان‌نگاری بهره می‌برد. در مرحله جای‌گذاری، به‌منظور جای‌گذاری بیشتر از یک کیوبیت داده، سیگنال میزبان، به قاب‌هایی تقسیم شد. در ادامه، یک هسته پژواک کوانتومی تولید شد و داده نهان نگاره در کیوبیت کم‌ارزش آن جای‌گذاری شد. سیگنال حاصله با سیگنال اصلی جمع شد و سیگنال نهان نگاره نهایی تولید شد. در مرحله استخراج، تفاضل سیگنال نهان نگاره و سیگنال اصلی محاسبه‌شده و مجموع نمونه‌های این سیگنال تفاضل محاسبه شد و در ثبات کوانتومی ذخیره شد. یک سیگنال پژواک کوانتومی مشابه با مرحله جای‌گذاری تولید شد و مجموع تک‌تک نمونه‌های آن محاسبه شد و مجموع حاصل در ثبات دیگر ذخیره شد. نتایج این ثبات‌ها توسط یک مقایسه‌کننده کوانتومی با یکدیگر مقایسه شدند و کیوبیت نهان‌نگاری شده تشخیص داده شد. رویکرد پیشنهادی هم از شفافیت قابل‌قبولی برخوردار بود و هم نسبت به حملات کانال‌های نویزی مقاوم بود و می‌توان گفت مصالحه خوبی بین سه عامل اصلی نهان‌نگاری، یعنی شفافیت، ظرفیت و مقاومت برقرار کرد. همچنین سایر روش‌های کوانتومی صوتی را بهبود بخشید. انجام پژوهش‌های امن و شفاف و مقاوم در حوزه نهان‌نگاری کوانتومی و ایجاد تعادل کارا و مطلوب بین این عامل‌ها، هدف نهایی در این حوزه به شمار می‌رود که می‌تواند به‌عنوان پژوهش‌های آینده موردتوجه پژوهشگران قرار گیرد. همچنین، می‌توان به بررسی موضوع امنیت نهان‌نگاری به‌عنوان موضوع مهم در حوزه نهان‌نگاری کوانتومی پرداخت.

۸. مراجع

[1] S. M. Mohsenfar, M. Mosleh, and A. Barati, "Audio watermarking method using QR decomposition and genetic algorithm," Multimedia Tools and Applications, vol. 74, pp. 759-779, 2015. https://doi.org/10.1007/s11042-013-1694-3.

[2] R. Chandramouli and N. Memon, "Analysis of LSB based image steganography techniques," Proceedings 2001 international conference on image processing, vol. 3, pp. 1019-1022, 2001.

[3] H. Hai, X. D. Qing, and Q. Ke, "A watermarking-based authentication and image restoration in multimedia sensor networks," International Journal of High Performance Computing and Networking, vol. 12, pp. 65-73, 2018. https://doi.org/10.1504/IJHPCN.2018.093846

[4] G. Hua, J. Huang, Y. Q. Shi, J. Goh, and V. L. Thing, "Twenty years of digital audio watermarking—a comprehensive review," Signal processing, vol. 128, pp. 222-242, 2016. https://doi.org/10.1016/j.sigpro.2016.04.005

[5] A. A. Hassani, H. Dehghani, M. Dehghani, and R. Esfahani, "Improvement Capacity and Transparency, In Steganography Based On Mod4," (in Fa), Journal of Electronic and Cyber Defense, vol. 4, pp. 15-21, 2016. https://www.magiran.com/paper/1573331.

[6] M. A. S. Baei, "Designing a combinatorial Image Steganography algorithm based on game theory," (in Fa), Journal of Electronic and Cyber Defense, vol. 8, pp. 133-145, 2020. https://dorl.net/dor/20.1001.1.23224347.1399.8.1.11.1

[7] M. Shoaei and V. Sabeti, "Review and Comparison of Network Steganography Methods Based On Different Classifications," (in Fa), Passive Defense Quarterly, vol. 10, pp. 95-109, 2019. https://www.magiran.com/paper/2081090.

[8] I. Cox, M. Miller, J. Bloom, J. Fridrich, and T. Kalker, "Digital watermarking and steganography". Morgan Kaufmann google scholar, pp. 893-914, 2007.

[9] E. Gholampour, "Relating the Detection Rate, Capacity and the Cost of Steganography by Steganographer Modeling," (in Fa), Journal of Electronic and Cyber Defense, vol. 6, pp. 81-94, 2019. https://dorl.net/dor/20.1001.1.23224347.1397.6.3.7.7

[10] M. Chetan, P. P. Bhat, V. Shet, S. B. Husenbhai, and A. Bhat, "Audio Watermarking Using Modified Least Significant Bit Technique," International Conference on Circuits, Controls and Communications (CCUBE), 2021, doi: 10.1109/CCUBE53681.2021.9702715 .

[11] R. K. Singh, D. K. Shaw, and M. J. Alam , "Experimental Studies of LSB Watermarking with Different Noise," Procedia Computer Science, vol. 54, pp. 612-620, 2015.

"Dual quantum audio watermarking schemes based on quantum discrete cosine transform," International Journal of Theoretical Physics, vol. 58, pp. 502-521, 2019. https://doi.org/10.1007/s10773-018-3950-9

[25] 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, pp. 010306, 2018.

[26] M. Y. Nejad, M. Mosleh, and S. R. Heikalabad, "An LSB-based quantum audio watermarking using MSB as arbiter," International Journal of Theoretical Physics, vol. 58, pp. 3828-3851, 2019. https://doi.org/10.1007/s10773-019-04251-z

[27] M. Y. Nejad, M. Mosleh, and S. R. Heikalabad, "An enhanced LSB-based quantum audio watermarking scheme for nano communication networks," Multimedia Tools and Applications, vol. 79, pp. 26489-26515, 2020. https://doi.org/10.1007/s11042-020-09326-2

[28] M. Y. Nejad, M. Mosleh, and S. R. Heikalabad, "A blind quantum audio watermarking based on quantum discrete cosine transform," Journal of Information Security and Applications, vol. 55, pp. 102495, 2020. https://doi.org/10.1016/j.jisa.2020.102495

[29] M. Velayatipour, M .Mosleh, M. Y. Nejad, and M. Kheyrandish, "Quantum reversible circuits for audio watermarking based on echo hiding technique," Quantum Information Processing, vol. 21, pp. 316, 2022. https://doi.org/10.1007/s11128-022-03657-9

[30] 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, 2018. https://doi.org/10.1007/s10773-017-3580-7

[31] A. A. Abd EL-Latif, B. Abd-El-Atty, and S. E. Venegas-Andraca, "A novel image steganography technique based on quantum substitution boxes," Optics & Laser Technology, vol. 116, pp. 92-102, 2019. https://doi.org/10.1016/j.optlastec.2019.03.005

[32] J. Chaharlang, M. Mosleh, and S. R. Heikalabad, "A novel quantum audio steganography–steganalysis approach using LSFQ-based embedding and QKNN-based classifier," Circuits, Systems, and Signal Processing, vol. 39, pp. 1-33, 2020. https://doi.org/10.1007/s00034-020-01345-6

[33] S. Norouzi Larki, M. Mosleh, and M. Kheyrandish, "Quantum Audio Steganalysis Based on Quantum Fourier Transform and Deutsch–Jozsa Algorithm," Circuits, Systems, and Signal Processing, vol. 34, pp.2235-2258, 2023. doi: 10.1007/s00034-022-02208-y.

[34] V. Vedral, A. Barenco, and A. Ekert, "Quantum networks for elementary arithmetic operations," Physical Review A, vol. 54, pp. 147, 1996. doi: https://doi.org/10.1016/j.procs.2015.06.071.

[12] S. Wang, W. Yuan, J. Wang, and M. Unoki, "Inaudible speech watermarking based on self-compensated echo-hiding and sparse subspace clustering," International Conference on Acoustics, Speech and Signal Processing (ICASSP), 2019.

[13] D. Gruhl, A. Lu, and W. Bender, "Echo hiding ", International Workshop on Information Hiding, 1996. https://doi.org/10.1007/3-540-61996-8_48.

[14] M. Fahad Khan, F. Baig, and S. Beg, "Steganography between Silence Intervals of Audio in Video Content Using Chaotic Maps," Circuits, Systems, and Signal Processing, vol. 33, pp. 3901-3919, 2016. https://doi.org/10.1007/s00034-014-9830-5

[15] M. H. Shirali-Shahreza and S. Shirali-Shahreza, "Real-time and MPEG-1 layer III compression resistant steganography in speech," IET Information security, vol. 4, pp. 1-7, 2010.

[16] Y. Xiang, I. Natgunanathan, S. Guo, W. Zhou, and S. Nahavandi" ,"Patchwork-based audio watermarking method robust to de-synchronization attacks," IEEE/ACM Transactions on Audio, Speech, and Language Processing, vol. 22, pp. 1413-1423, 2014.

[17] N. K. Kalantari, M. A. Akhaee, S. M. Ahadi, and H. Amindavar, "Robust multiplicative patchwork method for audio watermarking," IEEE Transactions on Audio, speech, and language processing, vol. 17, pp. 1133-1141, 2009.

[18] P. W. Shor, "Algorithms for quantum computation: discrete logarithms and factoring," Proceedings 35th annual symposium on foundations of computer science, 1994.

[19] 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. https://doi.org/10.1007/BF01011339

[20] R. P. Feynman, "Simulating physics with computers," International Journal of Theoretical Physics, vol. 21, pp. 467-488, 1982.

[21] J. Wang, "QRDA: quantum representation of digital audio," International Journal of Theoretical Physics, vol. 55, pp. 1622-1641, 2016. https://doi.org/10.1007/s10773-015-2800-2

[22] F. Yan, A. M. Iliyasu, Y. Guo, and H. Yang, "Flexible representation and manipulation of audio signals on quantum computers," Theoretical Computer Science, vol.752, pp. 71-85, 2018. https://doi.org/10.1016/j.tcs.2017.12.025

[23] P. Li, B. Wang, H. Xiao, and X. Liu, "Quantum Representation and Basic Operations of Digital Signals," International Journal of Theoretical Physics, vol. 57, pp. 3242-3270, 2018. https://doi.org/10.1007/s10773-018-3841-0

[24] K. Chen, F. Yan, A. M. Iliyasu, and J. Zhao,

https://doi.org/10.48550/arXiv.quant-ph/9511018.

[35] D. Wang, Z.-H. Liu, W.-N. Zhu, and S.-Z. Li, "Design of quantum comparator based on extended general Toffoli gates with multiple targets," Computer Science, vol. 39, pp. 302-306, 2012.

[36] M. N. Divshali, A. Rezai, and A. Karimi, "Towards multilayer QCA SISO shift register based on efficient D-FF circuits," International Journal of Theoretical Physics, vol. 57, pp. 3326-3339, 2018.

https://doi.org/10.1007/s10773-018-3846-8

A Robust Quantum Audio Watermarking Using Synergy of Echo Hiding and Least Significant Bit Technique

Velayatipour, Masoumeh	Mosleh, Mohammad	Yoosefi Nejad, Mohsen	Kheyrandish, Mohammad
Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran	Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran	Payam Noor University	Department of Computer Engineering, Dezful Branch, Islamic Azad University, Dezful, Iran

With the advent of quantum computers, the need to protect quantum data as a fundamental issue has attracted the attention of researchers. In this article,, a quantum audio watermarking approach based on a combination of echo hiding and least significant bit (LSB) methods is proposed. In the embedding stage, the proposed approach first converts the host audio signal into QRDS quantum display form and then generates a quantum echo signal from it. Next, ,it inserts the watermark data qubits into the resulting quantum echo signal using the least significant bit method. Finally, the watermarked quantum signal is obtained from the result of the original quantum signal and the echo quantum signal. In the extraction phase, of the proposed approach, based on the difference between the samples of the original quantum signal and the received quantum signal, the watermark qubits are recovered. In addition, quantum reversible circuits for insertion and extraction processes have been designed and implemented. The results obtained from the evaluation and comparison of the proposed approach, in terms of transparency, robustness to attacks and also the embedding capacity, show that the proposed scheme compared to the quantum watermarking methods based on the LSB method, has a higher resistance . In addition, the proposed method has a very good transparency (SNR=66.26dB) at the embedding capacity of 512 kbps, which shows that the proposed method has been able to improve the compromise between robustness, transparency and capacity.

Quantum Audio watermarking, Quantum computing, Echo Hiding, Least Significant Bit