Journal of Engineering Science and Technology
Vol. 15, No. 3 (2020) 1562 - 1588
© School of Engineering, Taylor's University

QUANTUM AUDIO STEGANOGRAPHY SYSTEM

ALHARITH A. ABDULLAH[1,*], YASEEN KHUDAIR ABBAS[2]

[1] Department of Network, College of Information Technology, University of Babylon, Iraq
[2] Department of software, College of Information Technology, University of Babylon, Iraq
*Corresponding Author: alharith@itnet.uobabylon.edu.iq

Abstract

The increasing reliance on the internet as a means for data transferring among distributed parties in the world makes keeping the security of these data an essential manner. In order to achieving this goal, there are two ways, the first way depending on coding the data in some way that seen un-understandable. This way is known as cryptography. The second way relies on hiding the data in a cover media which seen unnoticeable without effect on the quality of the cover, it is known as steganography. In audio steganography, the hosting medium will be an audio file while the secret data need to be hidden can take any form of data. Due to the hypersensitivity of the Human Audio System when contrasting with the Human Visual System, this makes challenge to hide data in audio files. The drawback of conventional steganography is that it can detect or restore the embedding data easily when known the used method. The quantum computation relies on quantum properties that came with powerful features that could perform super-fast data processing. Also, it has the ability to solve the problem which cannot be solved when using the classical computer such as breaking the RSA algorithm. The quantum steganography is considered an important emerging technology that is being developed, where it can provide data protection in a new way. Therefore, in this paper, we introduce and describe a new way in audio steganography depending on the quantum computing mechanism. In this proposed quantum audio steganography system (QASS), the Adaptive Least Significant Qubits (ALSQ) is using as the designed algorithm which considered a new version of the classical least significant bit (LSB). This algorithm work with qubits in both embedding and extraction stages where it modifies the state of selected least significant qubits of the host quantum audio signal relies on the state of the secret quantum audio signal. Both the host and the secret audio must converted to the quantum state through using the photon polarization which represents one form of the quantum state. The used method ensures a high imperceptibility between the host quantum audio and its stego version as explain in this paper, which it is an important thing in all vary steganography systems. This new environment can detect any un-authorize access on the channel to modifying the data.

Keywords: Least significant bit, Least significant qubits, Quantum audio, Quantum steganography, Steganography.

1. Research Motivation

Information security act a very essential role in the communication field due it provides protecting data services, especially in current times according to the huge transition of important information over an open network. Therefore, access to the information through an open network not limited by a specific location where anyone in the world can access them. Hence, this information can be intercepted by unauthorized persons. The information hiding technique is widely used to minimize security risk in various areas such as medical imaging, online elections, military, internet banking, and intelligence agencies. Steganography is one of these techniques that provides secure communication without being noticeable.

The steganography has received the attention of many researchers in recent years [1]. Because of the two main important reasons, Steganography increases its significance. Firstly, restricting the encryption services by many various governments leads people to think in a way to hide their secret information in a host medium without effect on its quality. Secondly, the needing for broadcasting services and publishing houses for techniques that provide hide identification information such as embedding the serial numbers and encrypted copyright marks in the book, multimedia products, digital films and audio recordings [2]. Furthermore, using the quantum computation provides a secret environment that can ensure communication between parties secretly through many principles and concepts that support its work which not applicable and consider impossible in the classical environment.

2. Research objective

The aim of the thesis is to develop a technique that enhance the performance of the audio steganography through exploiting the quantum computation that derived from the physic quantum theory which provides a secure environment to many applications that specialize in the security and other science fields. This enhancement can be achieved by depending on two-stage, the first stage is done by preparing the information system with both parts (the cover medium, the host medium) to be coding and transformation into the quantum state during polarization stage. The second stage is performing by the development of the existing classical steganography algorithm to able to work on the qubits that represent the quantum state.

3. Introduction

It is very important to ensure the security manner of our information in the communication to keep on the privacy principle. The private data can face a potential threat in many important filed such as defense, healthcare, banking and many other organizations [3]. There are two ways to achieve this purpose: cryptography and data hiding. The cryptography works on code data (encrypt) in some way that appears to the adversary not understandable, it needs to decode the data (decrypt) to be understandable which performed often by authorized parties [4]. The other way is by using the data hiding technique which consists of two-part, watermarking and steganography. Digital watermarking is considering an appropriate tool for identifying the creator, source, distributor owner, or authorized consumer of an image or a document where the copy of the data may happen without the knowledge of the owner for several purposes like copyright violation, lawlessly accessed or for tampering. Therefore, it needs to hide secret identification in any type of data where the owner can prove copyright possession. Also, it can be used to detect a document or an image that has been illegally modified or distributed. When the host media be an audio file it refers to audio watermarking.

The steganography word is consisting of two Greek words the first is stegos which means the cover and the second is grafia which means the writing [5]. Steganography is the technique that interested in protection digital data by concealing it into another host media where nobody should know about that secret message except the meant receiver. The cover or host message is refers to the media that is responsible for hiding the secret message. It is important to secure the important information like image, text, audio, videos because it may be vulnerable to many attacks and threats [6]. The major goal of steganography is to keep the communication between parties secretly in such a way where it cannot be detecting to accomplish the main task in this field such as storing or conceal sensitive and important information in any kind of digital data [7].

The result of the combination process between the host medium with the secret message is called stego message [8]. Different media types can use to perform steganography, such as texts, audios, and videos. By taking advantage of the data redundancy in video and audio files, they are considering as excellent carriers for the purpose of steganography [9]. When the audio file use as a cover media, this called audio steganography.

Audio steganography has an advantage over audio watermarking, wherein watermarking, the concealed information is related to an attribute of the host media and has further information about the properties of the host. The carrier medium is the primary object of the communication channel. A balance between robustness and audio perceptual quality should be maintaining. Where the constraints in maintaining audio quality resort to reduce the capacity of the embedding information while in steganography the embedded information is often not related to the host media and the object of the communication channel is the concealed message. The embedded capacity in the steganography is higher than the capacity in watermarking because it is free to modify the host file while maintaining quality without paying attention to the sensitivity of the embedding process which exists in the watermarking [10].

Performing steganography with an audio file is consider a hard matter since the sensitivity of the Human Audio System (HAS) goes higher than the sensitivity of the Human Visual System (HVS) [11]. The drawback of traditional steganography is that it is easy to reach the content of messages and restore the embedded message. Quantum computation through its depending on quantum mechanics which provides a powerful feature such as non-cloning theory, can be used to accomplish secure communication between parties because of three main reasons. The first is the quantum no-cloning theorem which states that an unknown quantum state cannot be cloned. The second reason, in a quantum system, when trying to measure the quantum state this process leads to change current qubits state. A quantum message which is intercepted and read by an interceptor will become garbled and useless to the intended receiver. The third reason is the measuring a quantum system property are considered one way, which means an eavesdropper cannot return a quantum message to its original state. These three properties provide the power of the quantum system [12].

There are some features in quantum computation and information that can effectively solve the intractable problems of today's computing technologies [13]. It also depends on the indiscriminate nature of the measurement of quantum mechanical systems. This indiscrimination is used to protect the information, even if the line of communication is eavesdropped [14-16].

Merging between quantum computation and audio steganography will achieve the top level of the security that ensures safe and secure communication.

This paper discusses the Adaptive Least Significant Qubits (ALSQ) as a suggested algorithm in the proposed Quantum Audio Steganography System (QASS). It is works on modifies the qubits of the cover audio samples with qubits of secret message after converting both the cover audio file and message file (audio) from binary state to quantum state in photon polarization. Then, performing a swap operation (using swap gate) between polarized sequences of cover audio samples (after determining the number of the least significant qubits) with the message polarized photon sequence in order to produce the stego quantum polarized photon sequence during the embedding stage. In the extracting stage, the stego version is processing in order to restore the quantum polarized photon sequence that belongs to the secret message, then convert it into a binary state and lastly regrouping these bits as a byte to rebuild the embedded message file in the classical state.

There are a few research performed on the quantum audio steganography as compared to research that accomplishes on images. One of the most related work is done by Chen et al. [17], who proposed two protocols act on quantum audio for hiding a secret audio within the cover audio. The first protocol use first least significant qubit (1st) and forth layer of qubit (4th) for embedding the qubit of the secret audio within the host audio. In the second protocol, the most significant qubit uses for hiding an audio message with four, five and six qubits. Also, the present how to represent the audio file in the quantum state as preparing stage to be ready for embedding and extraction stage where they use the existing protocol, Flexible representation of quantum audio (FRQA). The best result they reach during the imperceptibility analysis is higher than 70 dB.

Sutherland and Brun [18] worked on explaining how to hide a secret message using quantum steganography over noisy channels, they give an explicit encoding procedure and calculate the rate at which two parties can communicate secretly. They also calculate the rate at which the secret key must be consumed. Finally, they discuss the possibility of steganographic communication over more general quantum channels and conjecture a general formula for the steganographic rate.

Qu et al. [19] worked on developing an algorithm for quantum watermarking depending on quantum audio where it using least significant qubit as a suggested method in order to protect audio copyright. Also, they compare their work with the former accomplishment, the proposed method can evolve the security and robustness and of watermark efficiently that can hide within the quantum audio for copyright preservation.

The outline of this paper is organized as follows: firstly, present how to represent both cover and secret audio message in the quantum state. Secondly, clarifying the proposed algorithm that use to perform quantum audio steganography in both two important processes, embedding, and extraction. Thirdly, showing the result after perform testing. Finally, the important metrics measurements are applying on the results to show the performance of the proposed algorithm.

4. Quantum Representation of Audio signals

All of the classical information can be written in terms of classical bits. As a result, all of classical computing, communication, and cryptographic systems, work with classical bits. As we might imagine, quantum communication instead works with quantum bits, or in short qubits. Qubits are rather different than classical bits were bits may take zero or one state but not two states at the same time, while qubits can be in both states simultaneously. In the quantum computation system, qubits can take different state, such as the nuclear spins of atoms, or superconductors, or polarization of photons [20]. To perform quantum steganography, it requires transforming the data into the quantum state. Yan et al. [21] proposed a flexible representation of quantum audio (FRQA) as a representation for audio signals in a quantum state that encodes audio amplitude values into the quantum state. They depend on the arithmetic of the binary logic that provides the FRQA with the important tools needed for processing the quantum audio effectively. The most common method in processing the digital audio that used to represent bipolar numbers depends on using two's complement notation. Therefore, the two's complement arithmetic will be used to encode the amplitude value in quantum audio.

The mathematically defined of the FRQA audio signal as follows:

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

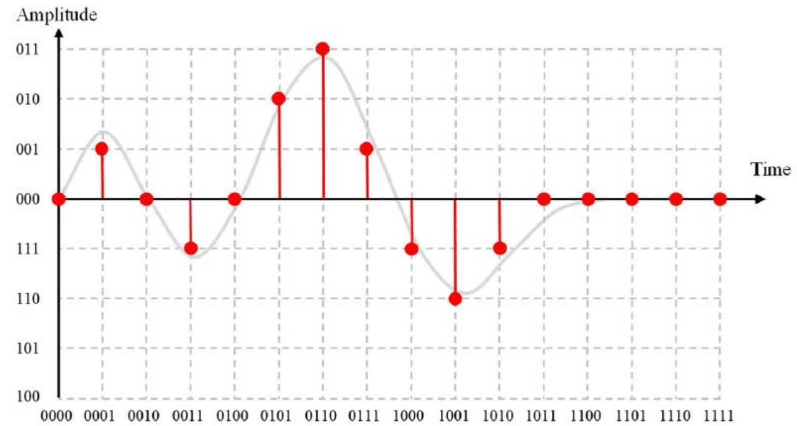
where $|A_t\rangle = |A_t^{q-1} \ldots\ldots A_t^1 A_t^0\rangle$ refers to encodes the 2's complement representation of each amplitude value and time information is represented by $|t\rangle = |t_{l-1} \ldots t_1 t_0\rangle$, $t_i \in \{0, 1\}$. The state $|Q_A\rangle$is normalized ($\| \, |Q_A\rangle \, \| = 1$) as shown in Eq. (1). In order to represent a quantum audio consisting of 2^l samples FRQA needs ($q + l$) qubits.

Figure 1 illustrates a part of a quantum audio signal and its expression by using the FRQA representation. The example shows that the amplitude values are sampled between -2 and 3, for which 3 qubits are required to store the amplitude information in FRQA audio. The length of the audio is 13, so l = log2 13 = 4. Thus, it requires 7 qubits to represent this FRQA audio signal [17].

This paper proposed a new representation of the qubits which consider more related to the concepts of the quantum state which is, the photon polarization. The photon can be in spin up or spin down or both simultaneously as illustrated in Eq. (2).

$$|\psi> = \alpha| \uparrow> + \ \beta| \downarrow> \tag{2}$$

Where $|\psi\rangle$ represent the pure state (superposition) and $\alpha| \uparrow \rangle$ represent the qubit state in up-polarization while $\beta| \downarrow \rangle$ represent the qubit state in down-polarization. The audio signals will represent a series of qubits with a specific polarization as will explain in Section 5.1.



$$|Q_A\rangle = \frac{1}{\sqrt{2^4}}\big(|000\rangle\otimes|0000\rangle + |001\rangle\otimes|0001\rangle + |000\rangle\otimes|0010\rangle + |111\rangle\otimes|0011\rangle + |000\rangle\otimes|0100\rangle + |010\rangle\otimes|0101\rangle$$
$$+|011\rangle\otimes|0110\rangle + |001\rangle\otimes|0111\rangle + |111\rangle\otimes|1000\rangle + |110\rangle\otimes|1001\rangle + |111\rangle\otimes|1010\rangle + |000\rangle\otimes|1011\rangle$$
$$+|000\rangle\otimes|1100\rangle + |000\rangle\otimes|1101\rangle + |000\rangle\otimes|1100\rangle + |000\rangle\otimes|1111\rangle\big)$$

Fig. 1. A segment of an FRQA audio signal and its representation (figure and descriptions adapted from [21]).

This work depends on the photon polarization to represent the qubits. In order to obtain qubits, which will represent both the cover and secret audio, the polarization process is required. In the depolarization process it produce bits from the qubits. During the polarization process, it requires to provide it with the sequence of bits which represent the bytes of the audio file. The rectilinear polarizer (+) can be used to introduce the qubit. This polarizer combines from two filter: the first is the horizontal filter (−) which use to produce photon polarization with 0^0 that represents the quantum state. This representation is indicated to bit in zero state (0) in a classical binary system. The second filter is the vertical (|), which introduce photon polarization with 90^0 where it represents the quantum state. This representation is indicated to bit in one state (1) in the classical binary system as shown in Fig. 2.

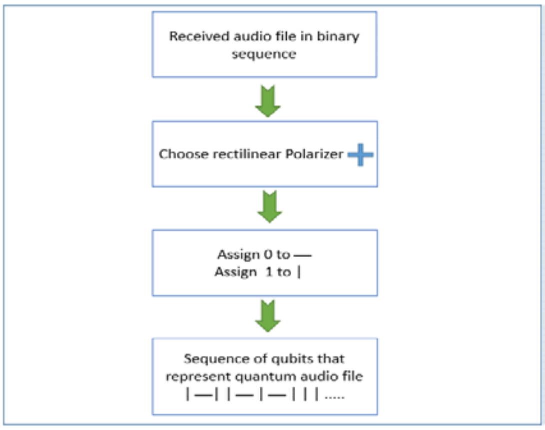

Received audio file in binary sequence
Choose rectilinear Polarizer +
Assign 0 to —
Assign 1 to |
Sequence of qubits that represent quantum audio file
| — | | — | — | | | .....

Fig. 2. Quantum rectilinear polarization state.

In order to restore the value of each bit from qubit to rebuild the audio file, the depolarization process is using which illustrate in Fig. 3. It use the same polarizer that been used during the polarization process. When using the rectilinear polarizer, the qubit (photon polarization) which passes through the horizontal filter is representing bit with zero state (0) while the qubit which pass through the vertical filter is representing bit with one state (1).

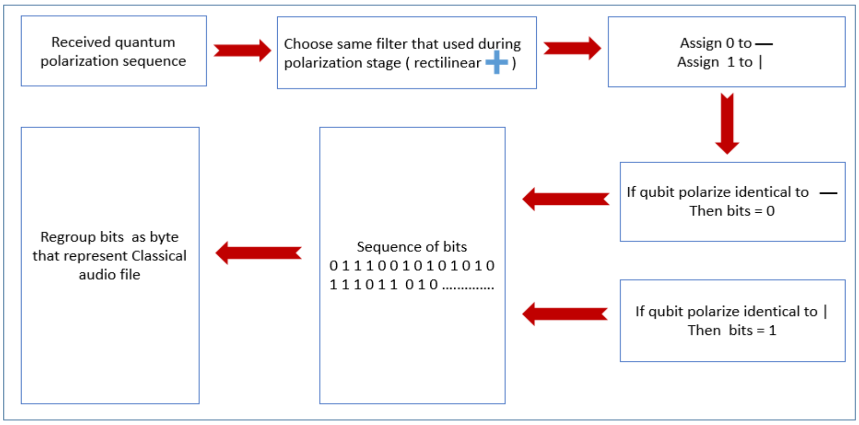

Received quantum polarization sequence
Choose same filter that used during polarization stage (rectilinear +)
Assign 0 to —
Assign 1 to |
If qubit polarize identical to —
Then bits = 0
If qubit polarize identical to |
Then bits = 1
Sequence of bits
0 1 1 1 0 0 1 0 1 0 1 0 1 0
1 1 1 0 1 1 0 1 0 ....
Regroup bits as byte that represent Classical audio file

Fig. 3. Quantum rectilinear depolarization state.

5. Proposed System

In each steganography system, there are two important processes, embedding process, which hiding the secret message into the cover medium (Audio), and extraction process that restores the secret message from cover medium. The Adaptive Least Significant Qubit (ALSQ) that used in the proposed system, that illustrated during both embedding and extraction phases.

5.1. The simulation of the quantum environment

The simulation of the quantum audio steganography system is shown in Fig. 4, which depends on the concept of BB84 protocol to some extent.

Firstly, the sender and the receiver should agree about the number of Least Significant Qubits (LSQ) in cover audio for embedding, after that the sender should send the original cover audio through the classical channel with specified variable value. The SNR value is uses after embedding the secret audio in sender side to match it with the SNR in receiver side to ensure that the quantum channel has not been attacked even in partial period time of eavesdrop. When the eavesdropper tries to attack the quantum channel through using the measurement gate to identify the polarized state of qubit the receiver will know that the channel has been attacked because when matching the received SNR value with the SNR value that compute in receiver side, the reading of two SNR value is not identical. This because when the eavesdropper using the measurement gate in the quantum channel, it will change the polarized state of the qubit. Therefore, the receiver will not receive the same qubit polarized sequence which lead to different audio content when matching it with the cover audio that sends it previously through the classical channel.

This method is useful to detect the long period time of eavesdrop. As mentioned before the SNR value can be used to detect any attempt of eavesdropping even when it occurs in partial period time. When the receiver knows about the attack, he will not depend on the received qubit and can ask the sender to resend the stego audio in the quantum channel this will prevent the attack and provide a secure environment in quantum steganography. Each bit (1, 0) is represented in photon polarization state, which introduced from using either the rectilinear or the diagonal polarizer. After converting the bit to the qubit, it sends through the quantum channel. On the receiver side, must using the same polarizer that has been used on the sender side. In case of utilizing the rectilinear polarizer, horizontal- vertical beam splitter will use to pass the received photon polarization to its identical detector either vertical or horizontal detector. The vertical detector will represent the bit value in one (1) state, while the horizontal detector will represent the bit value with zero (0) state. In order to identifying the qubits that belong to the secret audio from the qubits that belongs to cover audio in stego qubits sequence, another variable can be used for this purpose which is the index that detects the last index of the secret audio qubit sequence where it transfers through the classical channel with SNR value.

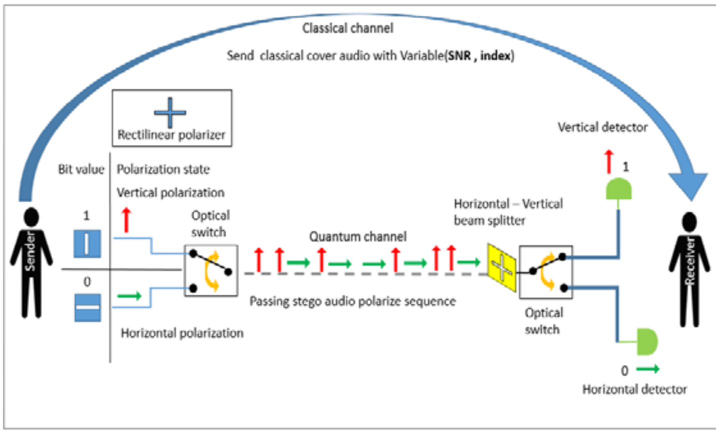


Fig. 4. Proposed quantum audio steganography system using a rectilinear polarizer.

5.2. The embedding data process

The important stage of any steganography system is the embedding stage . The sender is executing the data embedding stage as appeared in Fig. 5. This stage, embedding the secret audio in cover audio in a quantum way rather than a traditional way (Classical way), because of the important feature in quantum computation mechanism that leads to superior it on the traditional way. Least Significant Bit (LSB) technique is considered a straightforward method to perform steganography easily [22]. Similar to other steganography technique, it works on hiding the data into the host medium to be undetectable by an occasional watcher. It acts on modify the host sample's audio data with the secret message's data (audio). The LSB technique provides high embedding capability for embedding data [23, 24].

The embedding capacity or also called embedding payload of the cover can be computed through using embedding rate (ER) metrics as expressed in Eq. (3).

Zhang et al. [25] illustrated how this metric used on images files to represent the percentage of the embedded secret bits in the entire pixels of the cover image. The ER metric is defined as bellow.

$$ER = \frac{N}{H*W}\, bpp \tag{3}$$

where N represents the total number of the embedded secret bits and H × W is the size of the host. Depending on the value of the ER it gave a clear view of the embedding capacity of the file. The high value of the ER indicates perfect embedding payload in the used steganography method, where the individual cover unit in the cover file can load more secret bits. Conversely, when ER has a small value it indicates bad performance and low payload rate.

A balance should be considered between the capability and imperceptibility during performing steganography for better results. The Most Significant Bit (MSB) is considered another substitution technique to perform steganography but it has lower capacity as comparison with LSB as illustrated in [26], where they show the efficiency of the LSB over MSB in both term, capability and imperceptibility. Two important metrics can be used to clarify the embedding quality, Bit error rate (BER) and Peak Signal to noise ratio (PSNR). As example, when need to embed 4 which represent such data in three audio samples with 8-bit depth where each sample is represented by 8 bits. The three samples value is 204,142,240 respectively, which represent in binary as (11001100, 10001110, 11110000). When using the LSB method for embedding, the results will be as following (11001100, 10001110, 11110001) which represent the three audio samples as 204,142,241. These values reflect high imperceptibility due the samples looks like same value and the change un-noticeable therefore its allow to use more than one bit in each sample for embedding purpose because as known most sample data is represented in higher bit location such as 8th, 7th and 6th (i.e. MSB).This example explain high imperceptibility (PSNR) and lowest BER since only one right most bit in these samples value was changed. When using 3-LSB during embedding the result also be acceptable, since the samples value will be (204,142,244), (11001100, 10001110, 11110100) which it does not widely change from original samples. The matter is different when using MSB method since the value of the sample will be (01001100, 00001110, 11110000) that represent (67, 14,240), this embedding is distortion the audio samples which have high BER and lower PSNR value.

Generally, the length of the secret message to be encoded is smaller than the overall range of samples in an audio file. In quantum computation environment, the qubits are considered the basic unit rather than the bits. The Qubits may be in zero or one state or both at the same time. The LSB method is modifying for using in the embedding and extraction stage in quantum environment. It is works on the qubits rather than bit and can swapping more than one qubit during each embedding step which can be 1-LSQ, 2-LSQ, 4-LSQ until reach to 24-LSQ with non-sequential embedding but in intervals, all these matters distinguish this proposed algorithm (which is denoted as Adaptive Least Significant Qubit (ALSQ)) from the classical LSB.

The embedding stage is started by converting both the cover and secret audio from binary to quantum state. The plain example that show the quantum mechanics in the quantum environment is the photon polarization where can be in many states such as horizontal, vertical or diagonal polarization. Another form to explain the quantum mechanics is electron's spin where can be in spin-down or spin-up state. The important principle of quantum computing and mechanics is that the qubits take two-state at the same time which known as superposition while this feature is impossible in the classical system where the bit can be in one or zero states. This proposed depends on the photon polarization as a representation of the quantum. Each bit is representing by single-photon polarize. The rectilinear polarizer can be used to introduce either vertical or horizontal polarization that represents a qubit. After the complete polarization stage, the ALSQ received these two sequences of the qubits that represent both the cover and the secret audio file.

To increase the security of the algorithm, the data is embedding in a fixed interval between cover audio samples not sequentially, also it is works on multiple least significant qubits (LSQ) in cover audio samples which can increase the embedding data rate frequently.

At the beginning must determine the number of the qubits (in cover audio) which need to be swapping with qubits of secret audio (1-LSQ, 2-LSQ, 4-LSQ, etc.). It is requiring to identify the number of the qubits in the cover audio sample that must substituted with the secret audio qubits, since each cover audio sample is represented by 32 qubits because of the cover audio in wav 32bit format where each sample is represented by 32 bits. After that, the swap gate will exchange qubits of the cover samples qubits (according to the number of the qubits which determine previously in cover audio qubits i.e. 1-LSQ, 2-LSQ, 4-LSQ) with the qubits of the secret audio samples. The embedding stage will continue replacing the LSQ of the cover samples with qubits of the secret audio till the interval value reaches its minimum value, after that reset the interval to its maximum value and exceed set of sequence qubits that represent set of samples in cover audio. The swapping process is continues until embedding all the qubits of secret audio. In the last stage, send the stego polarization sequence in the quantum channel. The ALSQ in the embedding stage is explained in Fig. 5.

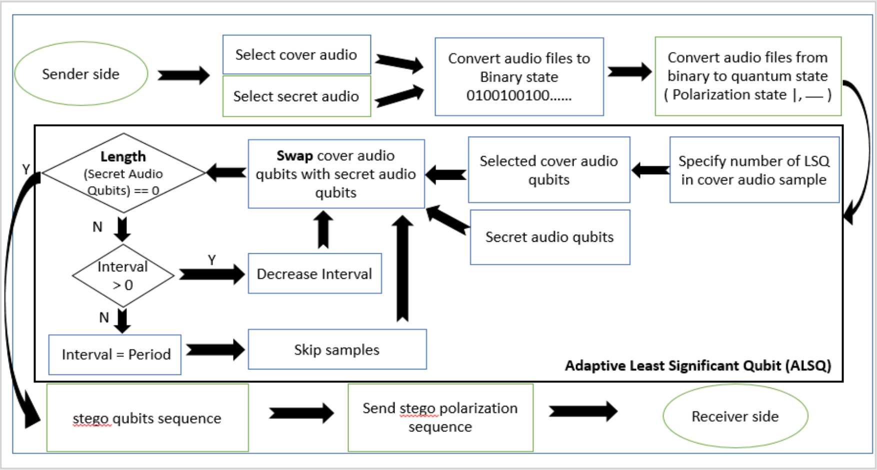

Sender side
Select cover audio
Select secret audio
Convert audio files to Binary state 0100100100......
Convert audio files from binary to quantum state (Polarization state |, —)
Length (Secret Audio Qubits) == 0
Y
N
Swap cover audio qubits with secret audio qubits
Selected cover audio qubits
Specify number of LSQ in cover audio sample
Secret audio qubits
Interval > 0
Y
Decrease Interval
N
Interval = Period
Skip samples
Adaptive Least Significant Qubit (ALSQ)
stego qubits sequence
Send stego polarization sequence
Receiver side

Fig. 5. Quantum embedding process.

The steps of the ALSQ algorithm in embedding stage is shown as Fig. 6:

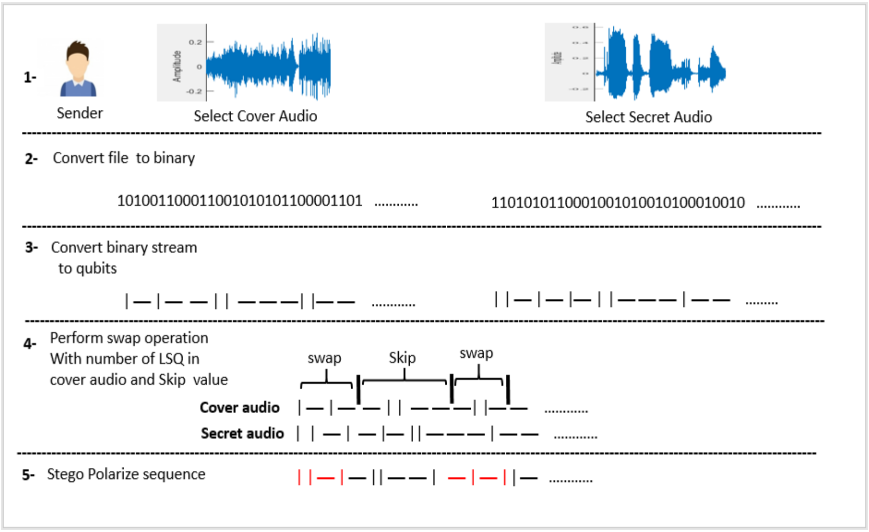


Fig. 6. ALSQ algorithm in the embedding stage.

Figure 7 illustrates an example of the embedding phase with 1-LSQ to clarify how it performs this phase.

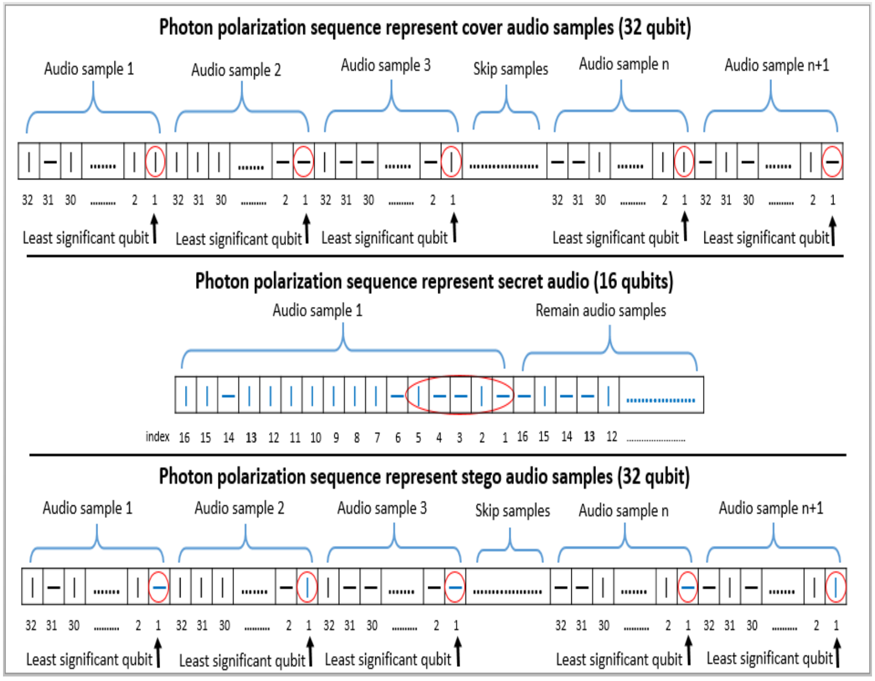
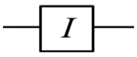
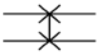

Photon polarization sequence represent cover audio samples (32 qubit)
Audio sample 1
Audio sample 2
Audio sample 3
Skip samples
Audio sample n
Audio sample n+1
32 31 30 2 1
Least significant qubit
Photon polarization sequence represent secret audio (16 qubits)
Audio sample 1
Remain audio samples
index 16 15 14 13 12 11 10 9 8 7 6 5 4 3 2 1 16 15 14 13 12
Photon polarization sequence represent stego audio samples (32 qubit)
Audio sample 1
Audio sample 2
Audio sample 3
Skip samples
Audio sample n
Audio sample n+1
Least significant qubit

Fig. 7. Illustration of the embedding phase with 1-LSQ.

The circuit of the embedding process is illustrated in Fig. 8. It used two gate, the identity gate which is used to keep the qubits that represent the cover's samples (*Cs*) whiteout change in the stego version (*Ss*) till reach to the qubits in cover's samples in index (*i*) that is substituted with the qubits of the secret audio message (*Ms*) by using the swap gate. As mention previously in the embedding stage, set of of qubits in the cover audio samples remain without change through skipping it, where samples still without change in stego version. After that, the embedding continues with increasing the samples by (*j*). The symbol bellow represents the identity gate which it works on single-qubit where it leaves the state of the qubit without change.



while the other bellow symbol represents the swap gate, which operates on swaps the state of the two qubits.



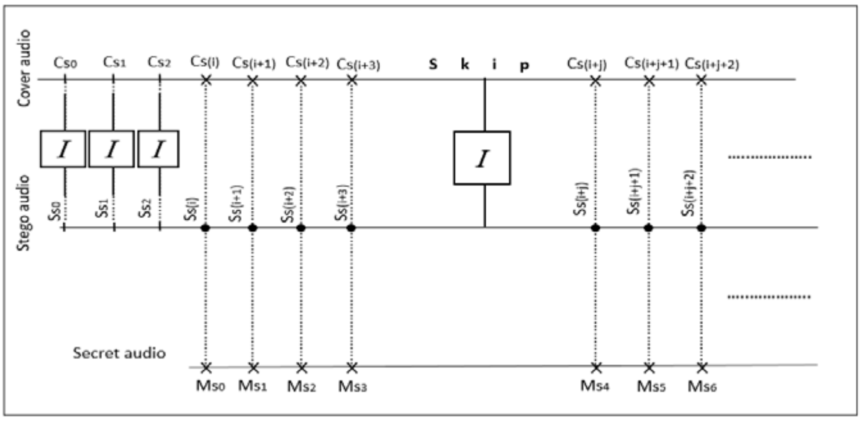


Fig. 8. Quantum embedding circuit.

5.3. The extraction data process

The second important stage of any steganography system is the extraction stage. The extraction of data is shown in Fig. 9, where the receiver use the polarization qubits that represent the stego in order to obtain the polarization qubits that related to secret audio using the ALSQ algorithm.

Firstly, it requires to determining the number of least significant qubits of the cover audio samples. Secondly must identify the interval value that must be the same when used it during the embedding stage to skip sequence of qubits in cover audio (samples audio). After that, starting regrouping all sequence qubits from stego version that represents secret audio depends on a number of LSQ that should be the same number when used during the embedding stage.

In each regrouping step, we decrease interval value until reach to a minimum value (zero) after that skip sequence of qubits and reset interval value to its maximum value. We repeated this procedural until regrouping all secret audio qubits then converting these qubits to the binary state to obtain the secret audio in classical form.

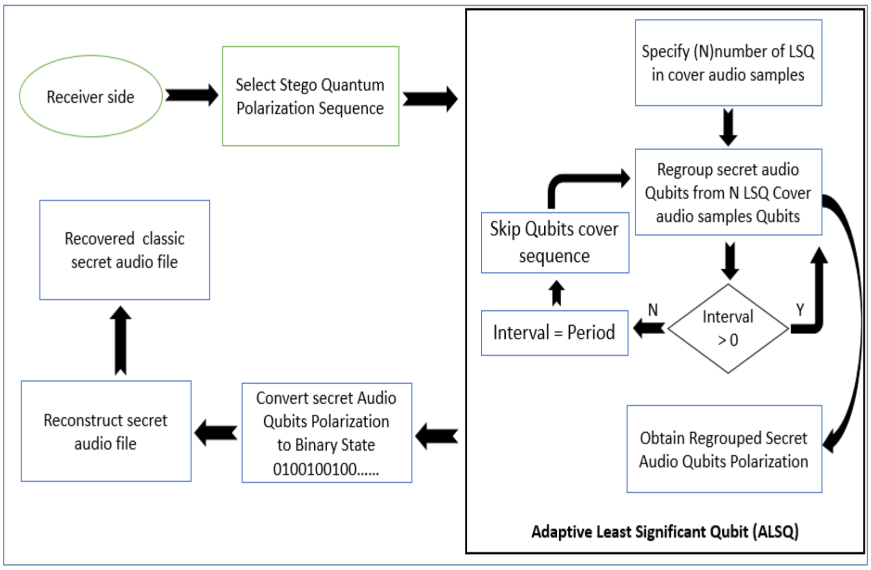

Receiver side
Select Stego Quantum Polarization Sequence
Specify (N)number of LSQ in cover audio samples
Regroup secret audio Qubits from N LSQ Cover audio samples Qubits
Skip Qubits cover sequence
Interval = Period
N
Interval > 0
Y
Obtain Regrouped Secret Audio Qubits Polarization
Adaptive Least Significant Qubit (ALSQ)
Recovered classic secret audio file
Reconstruct secret audio file
Convert secret Audio Qubits Polarization to Binary State 0100100100......

Fig. 9. Quantum extraction process.

The steps of the ALSQ algorithm in the extraction stage is shown in Fig. 10.

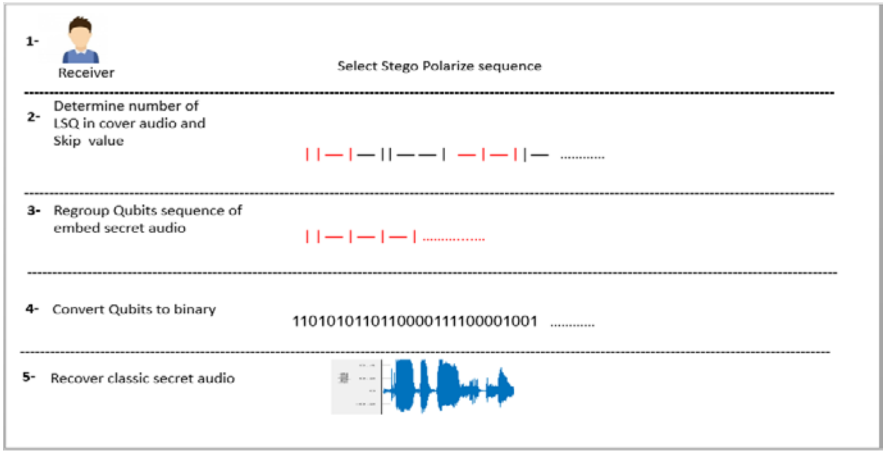

1-
Receiver
Select Stego Polarize sequence
2- Determine number of LSQ in cover audio and Skip value
| | — | — | | — — | — | — | | — ....
3- Regroup Qubits sequence of embed secret audio
| | — | — | — | ....
4- Convert Qubits to binary
1101010110110000111100001001 ....
5- Recover classic secret audio

Fig. 10. ALSQ algorithm in the extraction stage.

Figure 11 illustrates the extraction phase with 1-LSQ to clarify how it performs this phase.

The circuit of the extraction is shown in Fig. 12, where it works on the stego version (*Ss*) that contains the secret audio. First must start with same qubit index (*i*) that used in embedding process then regroup the qubits that represent the secret audio message (*Ms*) in stego version (*Ss*) using identity gate where the qubit that represents the secret audio in stego version is kept same as an output that represents qubits of secret audio. The process is continued until reach to skip index (*j*) then continue regrouping to complete all qubits of the secret audio.

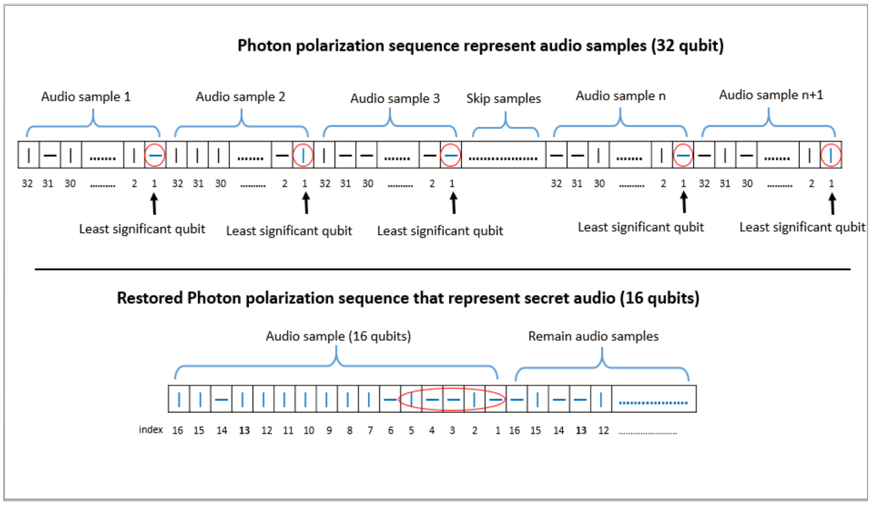


Fig. 11. Illustration of the extraction phase with 1-LSQ.

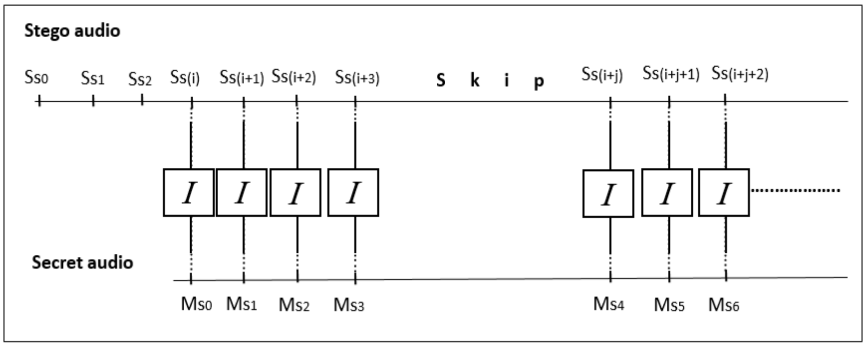


Fig. 12. Quantum extraction circuit.

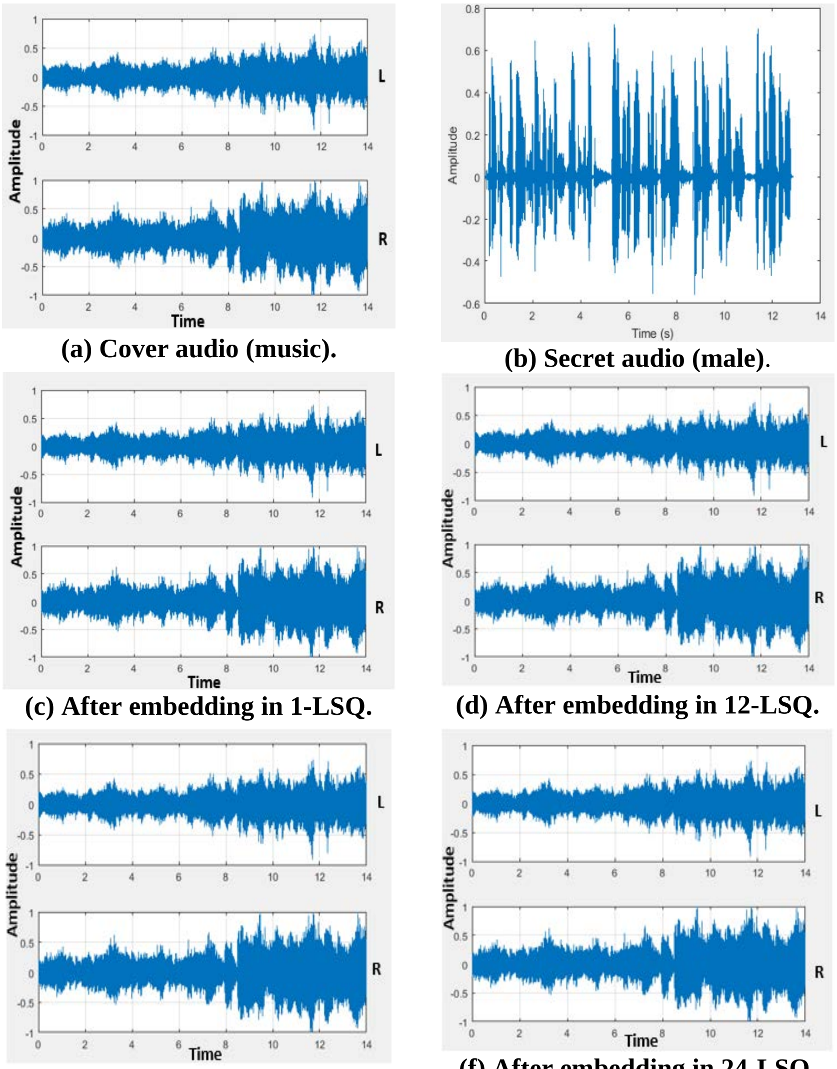
6. Result and Implementation

The simulation of this proposed system was conducted using Visual Studio 2015 software on the Windows platform. The hardware configurations consist of Processor Intel(R) Core(TM) i5-2410M CPU @ 2.30 GHz 2.30 GHz, and RAM 6.0 GB.ALSQ is the proposed algorithm used to implement quantum audio steganography. It can hide up to twenty-four qubits in each cover audio samples represented by qubits after completing the polarization stage. The cover audio file type is wav format thirty-two (32) bits as shown in Table 1, where each sample is represented by thirty-two integer bits (32) which support high capacity for embedding the secret audio message bits. The secret audio files are MP3 format with different durations. After reconstructing the secret audio in the extraction stage, the result of testing the proposed model efficiency is shown in Figs. 13 to 16.

As mentioned before ALSQ support more than one qubit for embedding which begins with one qubit, two, four, eight, ten, twelve, sixteen, twenty, until twenty four.

Table 1. Covers audio file specifications.

Sample No.	Audio title	Format Type	Bits per sample	Sample rate	Channel	Duration in Seconds
1	Music clip	Wav	32	16000 Hz	Stereo	13.99
2	Male speech	Wav	32	44100 Hz	Stereo	12.76
3	Female speech	Wav	32	44100 Hz	Stereo	11.14
4	Music clip	Mp3	32	22050 Hz	Mono	13.99
5	Male speech	Mp3	32	16000 Hz	Mono	12.76
6	Female speech	Mp3	32	16000 Hz	Mono	11.14



(a) Cover audio (music).

(b) Secret audio (male).

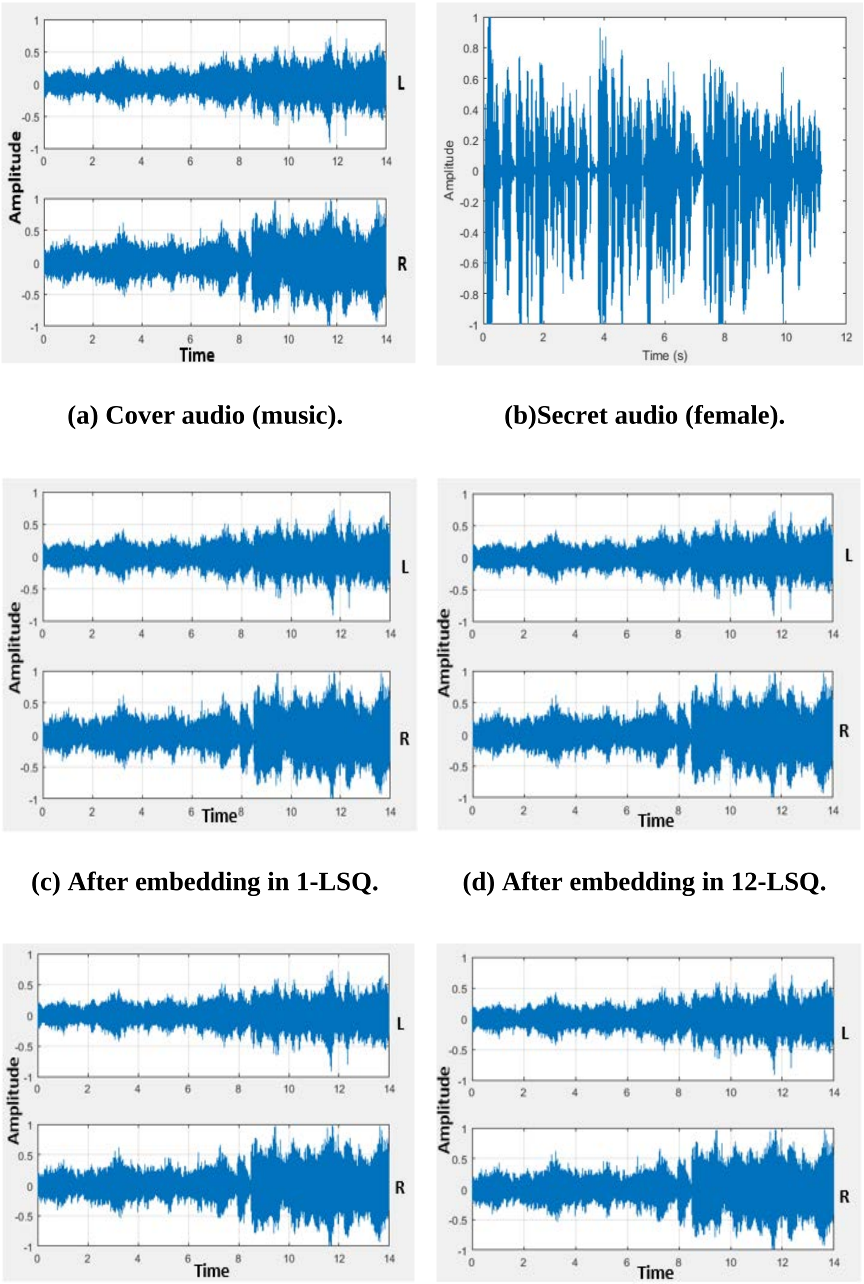
(c) After embedding in 1-LSQ.

(d) After embedding in 12-LSQ.

(e) After embedding in 20-LSQ.

(f) After embedding in 24-LSQ.

Fig. 13. Sample cover audio 1(music) before and after embedding sample secret audio 5 (male).



(a) Cover audio (music).

(b)Secret audio (female).

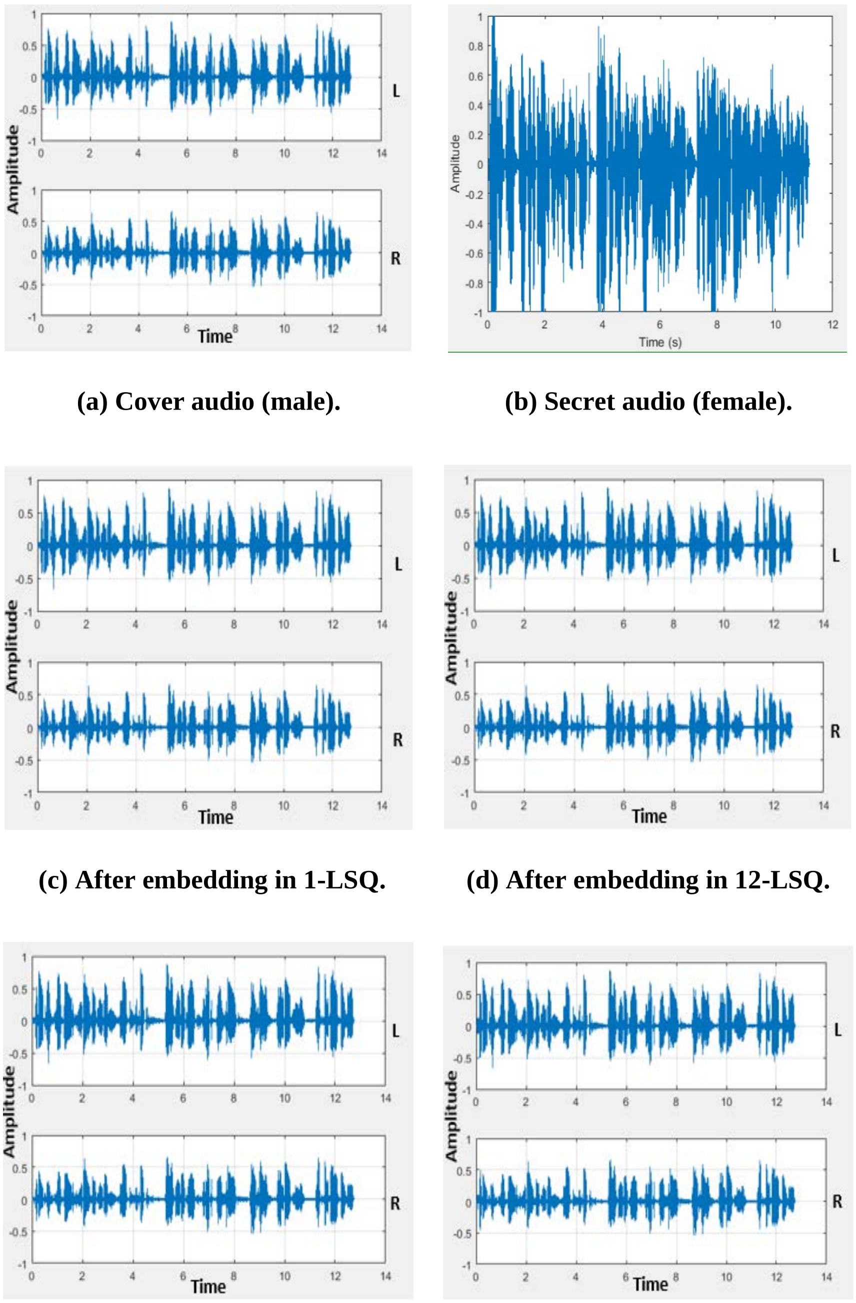
(c) After embedding in 1-LSQ.

(d) After embedding in 12-LSQ.

(e) After embedding in 20-LSQ.

(f) After embedding in 24-LSQ.

Fig. 14. Sample cover audio 1(music) before and after embedding sample secret audio 6 (female).



(a) Cover audio (male).

(b) Secret audio (female).

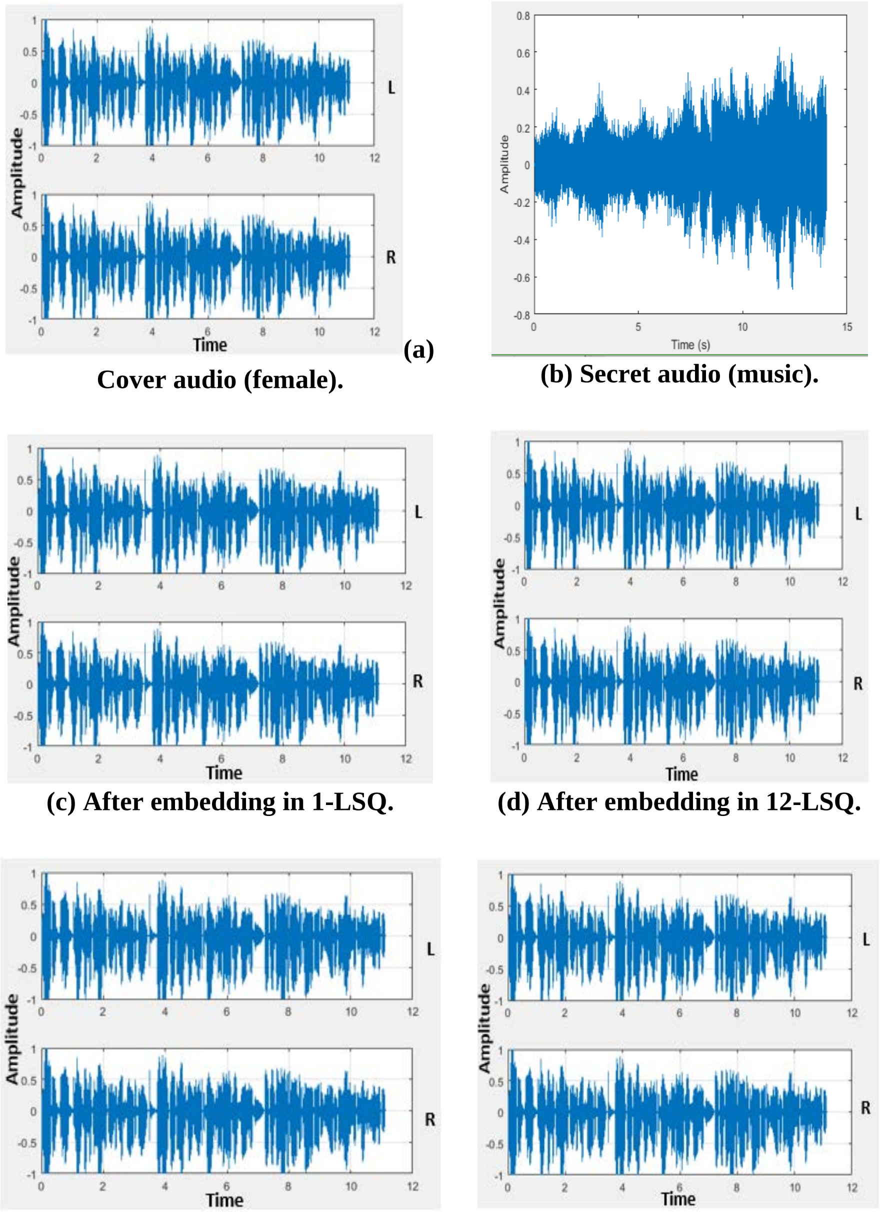
(c) After embedding in 1-LSQ.

(d) After embedding in 12-LSQ.

(e) After embedding in 20-LSQ.

(f) After embedding in 24-LSQ.

Fig. 15. Sample cover audio 2 (male) before and after embedding sample secret audio 6 (female).



(a) Cover audio (female).

(b) Secret audio (music).

(c) After embedding in 1-LSQ.

(d) After embedding in 12-LSQ.

(e) After embedding in 20-LSQ.

(f) After embedding in 24-LSQ.

Fig. 16. Sample cover audio 3 (female) before and after embedding sample secret audio 4 (music).

7. Evaluation Methodology

In order to evaluate this work and show whether its result is acceptable, different tests should be accomplish on the proposal. Signal-to-Noise Ratio (SNR) and Peak Signal-to-Noise Ratio (PSNR) are considered the most important metrics in evaluating steganography to show the transparency of the evaluation process.

These metrics are used in the binary domain. It has been calculated after converting the original cover audio with the stego audio from quantum state to classical state.

SNR is one of most important measurements that utilizes in signal processing to show the contrast of two signal the original signal, which represent the input to the grade change in the signal that considers as a noise that denoted as an output signal. It realizes as the ratio of original signal power to the noise power. Typically, explicit in decibels. When the ratio is high value, it indicates that the signal still keeps its quality without causing distortion in the original signal. The SNR can be used in many signals form such as in the image, audio, video and electrical signals and many other signals. SNR was expressed in [27] as Eq. (4):

$$SNR = 10\ log_{10} \frac{\sum_{i=1}^{N}\ s1(i)^2}{\sum_{i=1}^{N}\ (s1(i)-s2(i))^2} \tag{4}$$

where s1 represents the original cover audio while s2 represents the cover audio after embedding (stego version).

The PSNR measurement which expressed in Eq. (5) used to show the ratio between the highest possible powers with the signal after changing where it considers as noise to show the distorting in the original signals [28]. Whenever the RSNR result has a high value, it shows the degree of quality in the signal. It often uses this metric with the image during testing but according to Ma [29] and many other researchers, this metric can also use in the audio file to explain the quality after modifying. The PSNR is decreased when the number of embedding qubits increases because the value of MSE is increased respectively.

$$PSNR = 10\ log_{10}\left(\frac{(2^n-1)^2}{MSE}\right) \tag{5}$$

where MSE refers to Mean Square Error and n represent the number of bits that represent each sample.

The results of testing the proposed model according above metrics are shown in Tables 2 to 4 and Figs. 17 to 19.

Table 2. Results of different metrics after embedding cover sample 1 (music) audio with two secret audio messages sample 5, 6.

Cover Audio	No. of embed qubits	Secret audio	SNR	PSNR
Sample 1 (music)	1	Sample 5 (male)	174.317	190.244
	2		168.429	184.355
	4		158.728	174.655
	8		138.873	154.800
	10		127.736	143.662
	12		116.471	132.398
	16		93.682	109.609
	20		70.509	86.436
	24		47.277	63.204
Sample 1 (music)	1	Sample 6 (female)	176.114	192.041
	2		170.787	186.714
	4		161.202	177.129
	8		140.832	156.759
	10		129.681	145.607
	12		118.384	134.311
	16		95.599	111.525
	20		72.439	88.365
	24		49.189	65.115

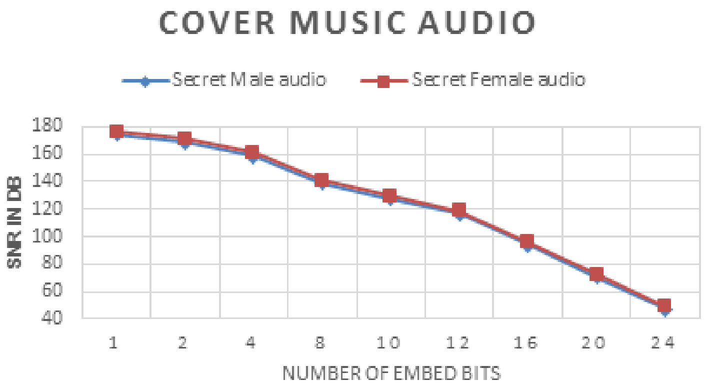


Fig. 17. SNR value of cover sample 1 (music) after embedding secret audio (sample 5, 6) with the different number of bits used for embedding.

Table 3. Results of different metrics after embedding cover sample 2 (male) audio with two secret audio messages samples 4, 6.

Cover Audio	No. of embed qubits	Secret audio	SNR	PSNR
Sample 2 (male)	1	Sample 4 (music)	146.049	165.995
	2		142.240	162.186
	4		131.827	151.773
	8		110.570	130.516
	10		101.252	121.198
	12		88.585	108.531
	16		65.164	85.110
	20		41.897	61.843
	24		16.450	36.397
Sample 2 (male)	1	Sample 6 (female)	150.128	170.074
	2		144.879	164.826
	4		136.016	155.962
	8		113.495	133.441
	10		103.509	123.455
	12		91.073	111.019
	16		73.299	93.245
	20		49.248	69.194
	24		30.004	49.950

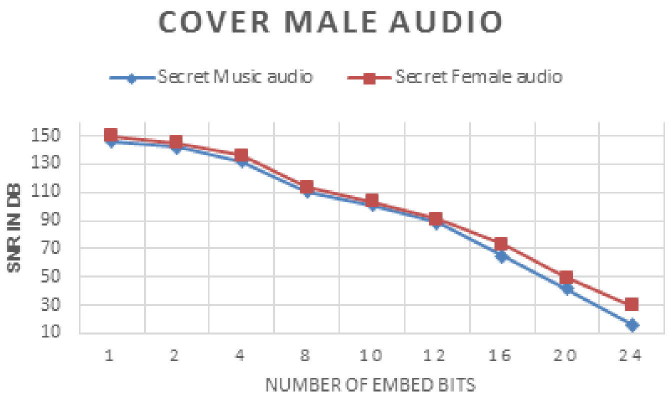


Fig. 18. SNR value of cover sample 2(male) after embedding secret audio (sample 4, 6) with a different number of bits used for embedding.

Table 4. Results of different metrics after embedding cover sample 3 (female) audio with two secret audio messages samples 5, 4.

Cover Audio	No. of embed qubits	Secret audio	SNR	PSNR
Sample 3 (female)	1	Sample 5 (male)	179.751	193.079
	2		174.515	187.843
	4		164.788	178.116
	8		144.830	158.158
	10		133.715	147.043
	12		122.367	135.695
	16		99.586	112.915
	20		76.445	89.773
	24		53.148	66.476
Sample 3 (female)	1	Sample 4 (music)	177.63	190.960
	2		172.442	185.770
	4		162.628	175.956
	8		142.996	156.324
	10		131.862	145.190
	12		120.625	133.953
	16		97.813	111.141
	20		74.611	87.939
	24		51.409	64.738

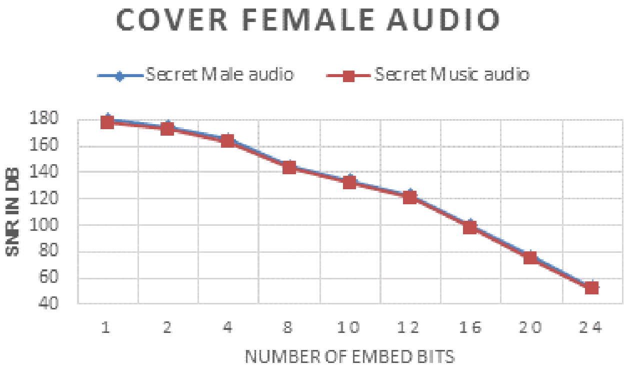


Fig. 19. SNR value of cover sample 3 (male) audio after embedding secret audio (sample 5, 4) with the different number of bits used for embedding.

8. Comparison with Related Work

This section present a discussion about the main results and comparisons presented to clarify the performance of the proposed algorithm.

Many researchers accomplish quantum steganography using an image but Chen et al. [17] use the audio file to achieving quantum steganography. Therefore, a comparison has been done with Chen et al. [17] and with other classical audio steganography.

The performance of the proposed model was compared with the performance of the scheme proposed in [17] to explain the degree of enhancement of the proposed model that contributes to enhancing hiding audio data. As a comparison, the proposed model presents high SNR value since it reaches to 179 dB as the highest value when using 1-LSQ, while the result of SNR in their experimental test reaches to 80dB as max value according to their testing in the best result when using 1-LSQc as shown in Fig. 20.

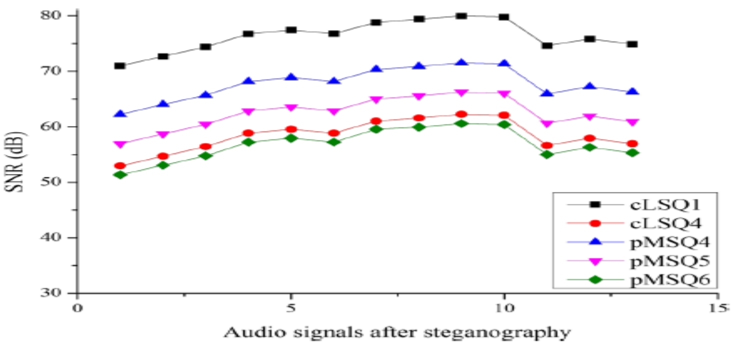


Fig. 20. Experimental results in research [17].

According to results in Table 4, the imperceptibility is high even when using 24-LSQ for embedding where SNR value reach to 53.148 dB,

Comparison with traditional work

Ali et al. [30] have proposed a model that ensures secret transmission audio during communication in audio steganography depend on fractal coding and a chaotic least significant bit or HASFC as they refer it. They focus on enhancing the capacity of cover audio to carry secret audio and explain the transparency and security issues. The high compression ratio is one of the important things they address through depending on fractal coding while they use a chaotic map to enhance the security which responsible for select cover audio samples randomly to hide the secret message. During test the model, SNR value reaches 71.1 dB as the highest level as shown in Table 5 while SNR value in the proposed system reaches to 179 dB as the best level.

Table 5. Experimental results in research [30].

Cover Secret	Cover Samples	Secret Sample	Block size samples	Hiding capacity %	Stego SNR	Reconstructed SNR
Voice Jazz	220,500	44,100	7	20	71.1	42.6
		88,200	14	40	71.1	41.2
		176,400	27	80	71	38
		220,500	34	100	71	37.2
Vlobos Female	220,500	44,100	7	20	71	42.2
		88,200	14	40	71	39.2
		176,400	27	80	70.8	38.5
		220,500	34	100	70.8	38.1
Voice	220,500	44,100	7	20	71.1	41
		88,200	14	40	71.1	39.3
		176,400	27	80	70.9	37.3
		220,500	34	100	70.9	37.2
Female Jazz	220,500	44,100	7	20	69.1	44.6
		88,200	14	40	69.1	41.1
		176,400	27	80	69	38
		220,500	34	100	69	37.3

Also, another comparison has been done with Bharti et al. [31] where they proposed a secure way to communicate using audio steganography for hiding important information. The host medium and the secret message is digital audio. Since the consuming time processing is low and high payload capacity in embedding, the approach is suitable for audio communication in real-time. According to their test, best SNR value reaches to 34.93 using 4-LSB from cover audio samples as shown in Table 6, where the best result in the proposed system test goes much more than these results when using the same number of qubits for embedding which shown in tables in Section 7.

Table 6. Experimental results of Bharti et al. [31].

Audio type (Language & Gender)		PESQ score (PESQ*st&c*)		*SNRseg (SNRsegrsec&sec)*	
Cover	*Secret*	Conve	4-lsb	*proposed*	*conv*
Female	Female	4.43	4.47	31.59	32.35
Female	Male	4.43	4.48	31.64	32.29
Male	Male	4.35	4.47	27.56	32.48
Male	Female	4.34	4.48	27.42	32.26
Music	Female	4.49	4.49	34.93	29.36
Music	Male	4.48	4.49	34.93	29.38
Music		4.48	4.49	34.93	35

Al-Juaid and Gutub [32] proposed a system that enhances and secure important text data by depending on combination cryptography and steganography techniques. RSA cryptography was selected as encryption method that applied on text data in the first stage. In the second stage, steganography is applied to conceal the secure text within the cover audio file. LSB is the main method for embedding and extraction the hidden text data during steganography stage. Using 1-LSB, 2-LSB and 3-LSB to increase payload capacity. Based on the testing, the maximum PSNR value reaches to 136.2 with 1-LSB as shown in Table 7, while the PSNR value in testing our proposed system reaches to 193.079 dB.

Table 7. An experimental test from Al-Juaid and Gutub [32].

Audio test-file number	High security and low capacity (1 LSB)		Medium security and capacity (2 LSB)		Low security and high Capacity (3 LSB)	
	Capacity	PSNR	Capacity	PSNR	Capacity	PSNR
1	352.9	136.2	705.9	130.8	1058.8	119.0
2	306.1	129.2	612.2	125.3	918.4	111.7
3	73.1	123.5	146.2	119.2	219.3	106.6
4	756.0	95.4	1512.0	88.8	2268.0	75.4
5	123.5	125.4	247.0	121.6	370.5	107.4
6	135.8	122.9	271.7	117.4	407.6	104.2
7	352.9	135.5	705.9	129.2	1058.8	116.5
8	289.1	126.2	578.2	119.3	867.4	105.7
9	756.0	96.5	1512.0	90.5	2268.0	79.3
10	350.8	134.1	700.0	128.8	950.7	122.5
11	756.0	93.4	1512.0	87.99	2268.0	81.3
12	756.0	93.1	1512.0	86.08	2268.0	74.5
13	756.0	94.3	1512.0	88.37	2268.0	76.8
14	120.2	123.5	240.4	119.2	360.5	100.6
15	450.3	110.3	900.6	105.5	1250.0	98.2

Table 8 virtualizes it results in Fig. 21 in a one-dimensional chart that illustration the two important metrics (SNR, PSNR) on ALSQ and the related schemes, with also the traditional classical audio steganography.

Table 8. Comparison schemes with ALSQ.

Schemes	Stego SNR	Stego PSNR
Chen [17] (2018)	80 (1-LSB)	-
Ali et al. [30] (2018)	71 (1-LSB)	-
Bharti et al.[31] (2019)	34 (4-LSB)	-
Al-Juaid and Gutub [32] (2019)	-	136 (1-LSB)
Proposed algorithm	179 (1-LSQ), 164 (4-LSQ)	193 (1-LSQ)

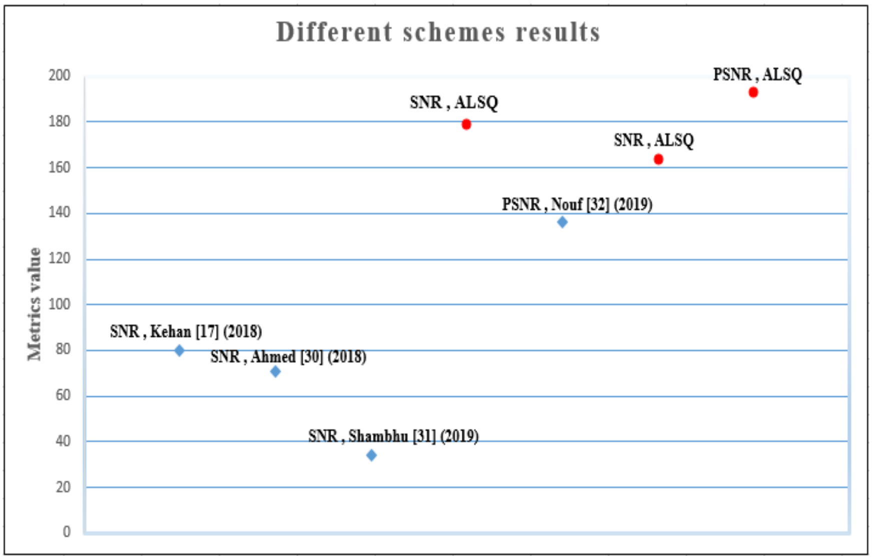


Fig. 21. Comparison between ALSQ with related schemes.

9. Conclusion

This paper, present QASS with its proposed algorithm ALSQ that consider a new version of LSB that provide a high embedding capacity with a guarantee of high imperceptibility where it modified to works on qubits rather than bits and also to be able to works with more qubits during embedding stage. The photon polarization has been denoted as a representation of the quantum state that considers an essential step to perform two important processes in steganography, embedding, and extraction.

The simulation of the quantum steganography environment was explained. It showed how this proposed system has the ability to detect any attack over the quantum channel where can stop the communication immediately and trying to retransmit later. According to the experimental results, it shows that the best results of the proposed algorithm that relate with the SNR reaches to 179.751 which shown higher imperceptibility than other algorithms.

Nomenclatures

2^n	(n) is the number of bits that represent each audio sample.
Cs	Cover audio sample.
i	Sample index.
j	Interval samples.
Ms	Secret audio message.
N	Total number of audio samples.
s1	Original cover audio.
s2	Cover audio after embedding.
Ss	Stego samples.

Symbols

—	Horizontal filter.
|	Vertical filter.
$\|\psi\rangle$	Pure state (superposition).
$+$	Rectilinear polarizer.
$\alpha\|\uparrow\rangle$	Qubit state in up-polarization.
$\beta\|\downarrow\rangle$	Qubit state in down-polarization.

Abbreviations

ALSQ	Adaptive Least Significant Qubits.
BB84	Charles Bennett and Gilles Brassard in 1984.
BER	Bit Error Rate.
ER	Embedding Rate.
FRQA	Flexible Representation of Quantum Audio.
HAS	Human Audio System.
HVS	Human Visual System.
LSB	Least Significant Bit.
LSQ	Least Significant Qubit.
MSB	Most Significant Bit.
MSE	Mean Square Error.
PSNR	Peak Signal to noise ratio.
QASS	Quantum Audio Steganography System.
SNR	Signal to Noise Ratio.

References

1. Osman, B.; Yasin, A.; and Omar, M.N. (2016). An analysis of alphabet-based techniques in text steganography. *Journal of Telecommunication, Electronic and Computer Engineering (JTEC)*, 8(10), 109-115.

2. Mutiarachim, A.; Pranata, S.F.; Ansor, B.; Shidik, G.F.; Fanani, A.Z.; Soeleman, A.; and Pramunendar, R.A. (2018). Bit Localization in Least Significant Bit Using Fuzzy C-Means. In *2018 International Seminar on Application for Technology of Information and Communication, IEEE, 290*-294.

3. Sahu, A.K.; and Swain, G. (2019). An Optimal Information Hiding Approach Based on Pixel Value Differencing and Modulus Function. *Wireless Personal Communications*, 1-16.

4. Sahu, A.K.; and Swain, G. (2019). High fidelity based reversible data hiding using modified LSB matching and pixel difference. *Journal of King Saud University-Computer and Information Sciences*.
5. Nosrati, M.; Karimi, R.; and Hariri, M. (2012). Audio steganography: a survey on recent approaches. *world applied programming*, 2(3), 202-205.
6. Artz, D. (2001). Digital steganography: hiding data within data. *IEEE Internet computing*, 5(3), 75-80.
7. Amin, M.M.; Salleh, M.; Ibrahim, S.; Katmin, M.R.; and Shamsuddin, M.Z.I. (2003). Information hiding using steganography. In *4th National Conference of Telecommunication Technology, 2003. NCTT 2003 Proceedings*, *IEEE*, 21-25.
8. Asad, M.; Gilani, J.; and Khalid, A. (2011). An enhanced least significant bit modification technique for audio steganography. *International Conference on Computer Networks and Information Technology*.
9. Westfeld, A.; Mller, G.; and Rannenberg, K. (1999). Steganography and Multilateral Security.*Multilateral Security in Communications Bd. 3: Technology, Infrastructure, Economy*, 223-232. Addison-Wesley-Longman.
10. Shih, F.Y. (2017). *Digital watermarking and steganography: fundamentals and techniques*.
11. Gopalan, K. (2003). Audio steganography using bit modification. *International Conference on Multimedia and Expo. ICME'03. Proceedings (Cat. No. 03TH8698)*. *IEEE*, Vol. 1, I-629.
12. Kumar, M.; Gupta, A.; Shah, K.; Saurabh, A.; Saxena, P.; and Tiwari, V.K. (2012). Data security using stenography and quantum cryptography. *Network and Complex Systems*, 2(2), 46-55.
13. Shor, P.W. (1994). Algorithms for quantum computation: Discrete logarithms and factoring. In *Proceedings 35th annual symposium on foundations of computer science. IEEE*, 124-134.
14. Abod, Z.A.; Ismael, H.A.; and Abdullah, A.A. (2018). Chaos-Based Speech Steganography and Quantum One Time Pad. *Journal of Engineering and Applied Sciences*, 13 (3), 739-745.
15. Abdullah, A.A.; Abod, Z.A.; and Abbas, M.S. (2018). An Improvement Steganography System Based on Quantum One Time Pad Encryption. *International Journal of Pure and Applied Mathematics*, 119(15), 263-280.
16. Abod, Z.A. (2018). A Hybrid Approach to Steganography System Based on Quantum Encryption and Chaos Algorithm. *Journal of University of Babylon*, 26, 280-294.
17. Chen, K.; Yan, F.; IIiyasu, A.M.; and Zhao, J. (2018). Exploring the implementation of steganography protocols on quantum audio signals. *International Journal of Theoretical Physics*, 57, 476-494.
18. Sutherland, C.; and Brun, T.A. (2018). Quantum steganography over noisy channels: achievability and bounds. *arXiv preprint arXiv:1808.03183.*
19. Qu, Z.G.; He, H.X.; and Li, T. (2018). Novel quantum watermarking algorithm based on improved least significant qubit modification for quantum audio. *Chinese Physics B*, *27*(1), 010306.
20. Gianfranco, C. (2015). *quantum communications*. Springer.

21. Yan, F.; Iliyasu, A. M.; Guo, Y.; and Yang, H. (2018). Flexible representation and manipulation of audio signals on quantum computers. *Theoretical Computer Science*, 752, 71-85.
22. Sahu, A.K.; and Swain, G. (2019). A novel n-rightmost bit replacement image steganography technique. *3D Research*, *10*(1), 2.
23. Sahu, A.K.; and Swain, G. (2017). Information hiding using group of bits substitution. *International Journal on Communications Antenna and Propagation*, 7(2), 162-167.
24. Sahu, A.K.; and Swain, G. (2018). Pixel overlapping image steganography using PVD and modulus function. *3D Research*, 9(3), 40.
25. Zhang, Y.; Jiang, J.; Zha, Y.; Zhang, H.; and Zhao, S. (2013). Research on embedding capacity and efficiency of information hiding based on digital images. *International Journal of Intelligence Science*, 3(02), 77.
26. Anand, K.; and Sharma, E.R. (2014). Comparison of LSB and MSB based image steganography. *IJARSSCE*, 4(8).
27. Kaur, A. (2017). Localized & self adaptive audio watermarking algorithm in the wavelet domain. *Journal of Information Security and Applications*, 33, 115.
28. Sahu, A.K.; and Swain, G. (2019). Dual Stego-imaging based reversible data hiding using improved LSB matching. *International Journal of Intelligent Engineering and Systems*, 12(5), 63-73.
29. Ma, X. (2015). Reversible data hiding scheme for VQ indices based on modified locally adaptive coding and double-layer embedding strategy. *Journal of Visual Communication and Image Representation*, 28, 60-70.
30. Ali, A.H.; George, L.E.; Zaidan, A.A.; and Mokhtar, M.R. (2018). High capacity, transparent and secure audio steganography model based on fractal coding and chaotic map in temporal domain. *Multimedia Tools and Applications*, 77(23), 31487-31516.
31. Bharti, S.S.; Gupta, M.; and Agarwal, S. (2019). A novel approach for audio steganography by processing of amplitudes and signs of secret audio separately. *Multimedia Tools and Applications*, 1-23.
32. Al-Juaid, N.; and Gutub, A. (2019). Combining RSA and audio steganography on personal computers for enhancing security. *SN Applied Sciences*, 1(8), 830.