IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Date of publication xxxx 00, 0000, date of current version xxxx 00, 0000.

Digital Object Identifier 10.1109/ACCESS.2017.DOI

Ameliorating LSB Using Piecewise Linear Chaotic Map and One-Time Pad for Superlative Capacity, imperceptibility and Secure Audio Steganography

HUWAIDA T. ELSHOUSH[1,†] AND MAHMOUD M. MAHMOUD.[1,†]

[1]Department of Computer Science, Faculty of Mathematical Sciences and Informatics, University of Khartoum, Sudan (e-mail: htelshoush@uofk.edu; Mahmoud.mustafa101@gmail.com)

Corresponding author: Huwaida T. Elshoush (e-mail: htelshoush@uofk.edu).

† Co-first author. H. Elshoush and M. Mahmoud contributed equally to this work.

ABSTRACT Audio steganography hides a secret message into an audio. Existing techniques are lacking in achieving high payload, imperceptibility in addition to robustness at the same time. They also suffer from choosing the samples and even LSBs in an unpredictable fashion. Moreover, few adaptive techniques exist, besides not many embed in higher LSBs. Hence, a novel LSB_{PWLCM} method that ameliorates LSB audio steganography is proposed. It uses piecewise linear chaotic map (PWLCM) to embed a secret message in random samples, besides selecting one of the 4-LSBs in an unsystematic way. It is noteworthy that each time a distinct sample and hence a differed 4-LSB is chosen as per different generated PWLCM. At first, Huffman coding is used to lessen the secret message size. Thereafter, to ameliorate the security of the one-time pad, random numbers are generated using PWLCM as an input key. This gives the proposed method a dual protection by amalgamating steganography with enhanced secure one-time pad. MATLAB is used to implement the proposed LSB_{PWLCM} method and evaluate the imperceptibility between cover and stego audios against standard parameters viz. Perceptual Evaluation of Speech Quality (PESQ) and Perceptual Evaluation of Audio Quality (PEAQ). Furthermore, its imperceptibility was tested using Mean Square Error, Peak Signal to Noise Ratio, Signal-to-Noise Ratio, Percentage Root Mean Square Difference and Audio Fidelity. Exhaustive experiments on vastly used metrics affirm that the proposed method LSB_{PWLCM} excel prevailing methods regarding hiding capacity and imperceptibility. Furthermore, it is resistant to brute force attacks having a large key space besides its dependency on the secret message size. In addition, it effectively withstood statistical analysis, specifically histogram attack and fourth first moments. Albeit it was vigorous towards re-sampling attacks, yet it was not very robust against LSB attacks nor noise. Assuredly, it prevails over existing methods and beyond comparison when juxtaposed with them affirming its efficacy.

INDEX TERMS Audio Steganography, Hiding Information, Least Significant Bit (LSB), Piecewise Linear Chaotic Map (PWLCM), Adaptive Steganography

I. INTRODUCTION

IT is absolutely crucial to ameliorate the security in communication nowadays, hence various strategies are proffered to protect data security. Hiding the existence of a secret message is as vital as disguising its content, ergo steganography came into light. Specifically, audio steganography is the art and science of hiding any secret data like text messages and binary files into any audio files viz WAV, MIDI, AVI, MPEG and MP3 files [1–4]. The selection of audio media was on account of that it has the essential quality of representing the amplitudes in real number format, hence producing miniature distortions after embedding secret messages.

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3259902

Four main facets are assessed in data hiding, namely *hiding capacity*, *imperceptibility*, *security*, and *robustness* [3–5].

- *Hiding capacity* is the maximum size of a secret message that can be hidden [6–8].
- *Imperceptibility* manifest that the cover and stego audios are indistinguishable.
- *Secure* signifies not only the imperceptibility of the secret message but testifies that it is secure/undetectable [5].
- *Robustness* indicates the ability of recovering a secret message successfully with lessen errors, besides the ability of a stego file withstanding different attacks [9–14].

As the main aim of steganography is to hide the ever existence of the secret message, hence robustness is deemed insignificant. Howbeit, lately many research in steganography necessitates robustness when using lossy, noisy channel or data transmission through social networks. In addition, a successful extraction with minimal or even no errors is necessary in steganography [5]. Thus, although the major challenges of steganography are hiding capacity, imperceptibility and security, it can be seen that the robustness aspect has a profound effect on a good steganography technique.

However, the above mentioned aspects are contradicting in the sense that increasing the hiding capacity causes deterioration in the imperceptibility, and conversely. Hence, the focal point and challenge of steganography is maximizing the hiding capacity besides ameliorating the security and the imperceptibility while at the same time preserving the robustness [15–19].

Regarding the hiding technique, audio steganography is classified into temporal (time) domain [13–15], transform domain [11][20–27] and compressed [28][29]. Time domains are characterized by high hiding capacity and imperceptibility yet low robustness. On the contrary, transform domains retain good robustness whilst having low capacity in addition to intricate computations. This research focuses on LSB audio steganography in temporal (time) domain.

In fact, the problems of existing methods lies in the following:

- *Sequential embedding* in LSB technique leads to easy detection.
- Difficulty in achieving superb capacity while preserving high imperceptibility and robustness as well as strong security.
- Few techniques embed in higher LSBs albeit this reduces the outcome of noise attacks.
- *Lack of adaptivity*, which has two facets:
  - The rarity of dynamically changing the LSB bit that is used for embedding.
  - Lack of adaptivity in the choice of the sample selected for embedding, instead of choosing the samples sequentially.
- *Imbalance* which is related to uneven distribution of secret message over the cover audio. This could be a security breach as steganalysis will be capable of separating embedded and clean unused intervals of the stego audio and hence detect the secret message easily [30].

This research aims to ameliorate these issues by improving the capacity whilst preserving high imperceptibility and security in addition to robustness. This could be achieved through more adaptivity and distributing the secret message over the audio in a balance fashion using the secret message size together with the audio length dynamically [30].

The motivation of this work is to propound an adaptive secure LSB audio steganography with superlative capacity, high imperceptibility and robustness. The selection of the samples as well as the LSB for embedding is to be performed in an unpredictable fashion, and furthermore in an adaptive way based on a random generated key and the secret message length. These features essentially make the detection of the secret message strenuous and the technique robust to attacks, while at the same time preserving high imperceptibility by disguising the secret message in higher LSBs.

Hence, the proposed method focuses on ameliorating security, and at the same time maximizing hiding capacity, whilst preserving high imperceptibility. It uses PWLCM in selecting the samples and one of the 4-LSBs to embed the secret message bits inside. Furthermore, PWLCM is also utilized in generating random numbers to be used as an input key to one-time pad, which provides dual protection to the proposed method.

Therefore, by utilizing random generated numbers in the selection of samples in the embedding process, each time different samples are chosen thus boosting the security. Even the choice of one of the 4-LSBs inside the samples depends on these PWLCM random generated numbers. Hence, the embedding process is unsystematic and unforeseeable, besides ameliorating the proposed method's security.

Furthermore, one-time pad is used to encrypt the secret message after compressing it by Huffman algorithm. So one-time pad is used as a dual protection to ameliorate the security of the proposed method. Moreover, to further enhance the security of one-time pad, PWLCM is also used to generate its input keys. Thus ensuring random key generation and large key space. Furthermore, by using PWLCM, only the initial conditions and the system parameters are exchanged in lieu of the entire chaotic sequences solving the key distribution difficulty.

Ergo, this study presents an ameliorated adaptive LSB audio steganography using PWLCM. The LSB_{PWLCM} method exhibits high hiding capacity and superb imperceptibility whilst being secure, besides preserving robustness. PWLCM generates distinct random numbers where these are then stored in an array. After indexing then sorting the array, the index is utilized to select the sample number and a modulo operation on the integer value of the random number yields one of the 4-LSBs to be chosen to embed in. Hence, the embedding process is arbitrary and utterly random. In fact, the proposed method is an adaptive technique as the array containing the random generated numbers should be equal to the secret message size. Moreover, encrypting a secret message using one-time pad adds a layer of security, besides recalling that the key is also generated using PWLCM solving the random key generation, large key space and key distribution problems.

In specific, Huffman coding is a lossless data compression method that depends on the rate of occurrence of a data clause. The idea of reducing the secret message size enhances the hiding capacity substantially [30–32].

A preliminary version of this work appears in [3], and extended in a book chapter [33], where the concept of the algorithm is presented. In this research, we further address the challenges of keeping a superlative capacity besides preserving the imperceptibility whilst ameliorating the security. Additionally, testing it excessively against well-known metrics.

Hereafter are the contributions of this research summed up:

- We proposed an efficacy secure LSB_{PWLCM} method having superlative capacity and superb imperceptibility that alleviate the intricacy of the contradiction of having high imperceptibility whilst maintaining prodigious capacity.
- The embedding process is arbitrary and unforeseeable, as different samples were chosen each time depending on a randomly generated PWLCM values.
- Even a differed choice of one of the 4-LSBs is selected each time according to some operation on the random generated PWLCM values, making the embedding process completely unpredictable.
- Moreover, the PWLCM is also used to enhance the added security of the one-time pad to encrypt the secret message, by resolving the random key generation, large key space and key distribution problems. This way achieving a steganography method with a dual protection, hence enhancing its security by amalgamating it with a secure cryptography technique.
- The novel LSB_{PWLCM} method was tested using standard parameters: Perceptual Evaluation of Speech Quality (PESQ) and Perceptual Evaluation of Audio Quality (PEAQ) and achieved superlative results.
- The proposed method is robust against re-sampling attacks, has high security and moreover proved high resistance to steganalysis attacks.
- Compared to prevailing techniques, our proposed method achieved efficacious performance regarding standard imperceptibility tests, capacity, robustness, security and statistical analysis affirming its supremacy.

The paper is structured as follows: section II confers the background. Section III discuses the related work of the LSB enhanced methods for audio steganography. Section IV elucidates the proposed LSB_{PWLCM} method. The experimental results are presented in section V, where further the proposed method is compared with existing schemes. Finally, section VI concludes this research paper.

II. BACKGROUND

A. LEAST SIGNIFICANT BIT (LSB)

LSB is the most widespread technique used because of its simplicity. It replaces the least significant bit in a chosen byte of the cover file to conceal the secret message [33]. Traditionally, LSB starts from the beginning of the cover file and embed the secret message sequentially. Thus, it is easily detectable and not resistant to steganalysis attacks [5, 34–40]. Moreover, the audio file will have different statistical characteristics in the part where the secret message is embedded. Hence, some researchers used random embedding to get around this problem. However, this random selection of samples must be kept track of to avoid changing an already modified sample [33].

Howbeit, LSB is very prevalent having low complexity and comparatively high capacity and high imperceptibility quality. Moreover, as mentioned above, a good steganography technique also entails high imperceptibility, high capacity, security and robustness. Hence, its structural limitations necessitate an improvement to the traditional approach making it less predictable while preserving its high capacity. Researchers [4, 34, 35, 38] are just few examples of enhancements to LSB audio steganography. Unquestionability, these improvements to the traditional LSB are much more secure as they are more resistant to steganalysis attacks and many improved the capacity and imperceptibility.

Furthermore, imperceptibility subjective testing shows that the maximum depth giving unnoticeable distortion is the fourth LSB layer in case of 16 bits per samples audio sequences [33].

B. PWLCM

PWLCM is a map composing of multiple linear segments, and has a wider range of control parameter

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3259902

choices. Thus, it has a better balance property and uniform invariant density function [3][41]. It is defined by equation 1 [3][41].

$$Y_n = F(y_{n-1}) = \begin{cases} y_{n-1} \times \frac{1}{p} & if 0 \leq y_{n-1} < p \\ (y_{n-1} - p) \times \frac{1}{0.5-p} & if p \leq y_{n-1} < 0.5 \\ F(1 - y_{n-1}) & if 0.5 \leq y_{n-1} < 1 \end{cases} \tag{1}$$

where $p \in (0,0.5]$ and $y_n \in [0,1]$ are the positive control parameters and the initial conditions, respectively [3][41].

C. ONE-TIME PAD

A one-time pad is a symmetric nonbreakable cipher that requires the use of a single-use random secret key having the same length as the secret message. Each bit of the secret message is encrypted by amalgamating it with the corresponding bit of the secret key using modular addition. It yields a random ciphertext having no statistical relationship to the secret message, hence it is unbreakable. The security of the one-time pad is completely because of the randomness of the key [33]. In fact, it exhibits the perfect security property if the key has the following requirements:

- It must be the same length as the secret message
- It must be random
- Certainly, it must not be reused
- It must be kept entirely secret between the sender and receipent

However, practically generating huge number of random keys and the key distribution are the main concerns. Concerning the key generation, the proposed method used PWLCM having good randomness and large key space. Regarding the key distribution problem, both communicating parties need only to exchange the initial conditions and system parameters for PWLCM, instead of the complete chaotic sequences. Consequently, these two issues are resolved in the proposed method.

III. RELATED WORK

A succinct survey depicting the analysis and propounded LSB enhanced approaches for audio steganography in temporal domain is scrutinized in this section.

Traditional LSB, being the simplest and straightforward embedding technique, permit large payload to be hidden. Nonetheless, its deterministic embedding way provide attackers with intentional and unintentional attacks opportunities that may damage the data. Ergo, it is very sensitive towards noise attacks, re-sampling, LSB attacks, amplification, compression, et cetera [4].

Multifarious researchers such as [42–49] amalgamate steganography with encryption to provide layers of security. In particular, reference [42] uses AES to encrypt the secret message and hide in higher LSBs. They claim that their method withstand unintentional attacks. However, they need to evaluate their method using widely known metrics as they just measured the PSNR. Specifically, reference [43] uses RSA to encrypt the secret message, and undoubtedly RSA is not very secure, especially when compared to one-time pad. Furthermore, they did not perform the decryption part nor any of the well-known evaluation metrics. On the other hand, reference [44] utilizes RC4 cipher for encrypting secret message before hiding, yet it works only with .wav audios. More importantly, RC4 is not very secure. Furthermore, their method is also not tested using any of the prominent metrics. Reference [45] uses altered Huffman encoding (MHE) to compress the secret message and further adds another layer of defense using homomorphic cryptography (HC). Nonetheless, only PSNR and SNR are dissected and evaluated. Lately, reference [48] came up with a new idea of encrypting text based on replacement by trimming the first half bits of ASCII code and then adding it to the end. Moreover, the keys are encrypted and exchanged using Elliptic curve cryptography (ECC). They further use a nondeterministic random steganography process. Albeit their method has a low computational cost, yet only PSNR, MSE and SSIM are evaluated and their method works on .wav audios only. Recently, Prakash Rao et al [47] applied AES and Blowfish to encrypt secret message before selecting variable samples for LSB embedding. Obviously, blowfish is not very secure, as well as their method is evaluated using only PSNR, and there are many popular metrics that are not measured. Due to their speed and low memory, chaotic maps were used in varying fields such as random key generation, security and encryption [49]. Specifically, reference [46] utilizes optimized 2D-Logistic Chaotic Map to encrypt the secret message after compressing it using Modified Huffman Encoding. Furthermore, the optimum selection of the samples besides optimizing the 2D-Logistic Chaotic Map was carried out by the enhanced Shark Smell Optimization (SSO) called Backward Movement oriented SSO (BM-SSO).

From another facet, reference [46] besides various other researchers such as [3][13][14][33][50] utilized chaotic maps to hide in an unpredictable fashion. Reference [13], which is an extension to [14], propound a model using fractal coding and chaotic LSB to improve the hiding capacity up to 30% while maintaining the audio imperceptibility. Their method has some limitations including the prolonged encoding time besides robustness. On the other hand, researchers [50] came up with a different idea to shuffle an audio using 4D grid multi-wing hyper-chaotic key generated before embedding using LSB to provide more security. Albeit their method has a large key space providing more security, it has a lengthy transmission time in addition to low hiding capacity and low resolution.

Most prevailing methods does not consider embedding in higher LSBs, viz up to 4^{th} bits. This was proved by researchers [15][42][51][52] to reduce the outcome of noise attacks yet for the price of less imperceptibility. Researchers [42] work up to the 11^{th} LSB to resist the unintentional attacks. Although their attained PSNR is sufficiently good, however these values when juxtapose with prevailing schemes could have been ameliorated, besides their NCC and BER are unsatisfactory. Also researchers [51] hide up to 4^{th} bit and attained high capacity and increased robustness yet having limitedness imperceptibility. However, their method lacks random embedding selection of samples besides no encryption of secret message is used, and furthermore it is tested only in .wav audios. On the other hand, M. A. Ahmad et al. [52] hide in higher 8^{th} LSB bits to improve the robustness without having an effect on imperceptibility. However, their method has low hiding capacity juxtapose to standard LSB. Whereas Bharti et al. [15] split the processing amplitude in the first 4^{th} bits and the signs in the later 5^{th} to 8^{th} LSB to achieve high embedding capacity. Their method also withstand noise attacks, LSB attacks and re-sampling attacks. Nonetheless, no steganalysis tests are performed.

Few techniques use adaptivity and dynamic allocation to ameliorate the security. In fact, in a similar fashion of reference [46] of selecting the cover segment to embed the secret message, researchers [53] use Diffie Hellman key exchange to create the key based index for LSB insertion to improve the security. Nevertheless, they have just tested their method in .wav audios and did not verify it using any metrics. Reference [20], in particular, selects the embedding location and the secret bits adaptively by using the interval in the audio and the threshold in variable low bit coding; thus yielding variable hiding capacity. However, the achieved SNR, in addition to the relative speed, are average compared to existing schemes. Moreover, further experiments should be conducted to assert its efficiency. Another adaptive high capacity method was presented by researchers [54], where they adduce the idea which is later extended in [30] with experimental testing. They proffer a progressive method that is very adaptive to variable secret message sizes and able to yield indistinguishable stego even with large payloads. They utilize Huffman-encoding and AES-256 for compression and encryption respectively. Their attained hiding capacity is 40% while sustaining an SNR and PSNR of 40 and 58 dB respectively. Howbeit, existing techniques achieve better SNR and PSNR. Furthermore, the security of their method needs further analysis to assure its strength, and they did not evaluate it against prominent metrics.

Whilst the works summarized in this section are of obvious value to audio steganography in the temporal domain, there is, in our opinion, a gap in the literature. The absence of adaptivity and dynamic allocation in the majority of prevailing methods is blatant. Moreover, few methods select the samples in a nondeterministic fashion to embed the secret message. Even researchers [53] and [46] use simple methods of selection and their methods need further verifications and testing. Moreover, few research perform the embedding itself in an unsystematic way, in addition to not considering higher bits for embedding, which is proved to lessen noise attacks. Consequently, the lack of randomness and adaptivity, in both sample selection and embedding, is therefore making the detection of secret messages easy. Furthermore, robustness, noise attacks, and re-sampling attacks are the eminent difficulties prevailing in current audio steganography research. More essentially, achieving high imperceptibility, capacity and robustness concomitantly still needs scrutinization and systematic investigation.

Hence, to prevail over the limitations of the aforementioned methods, we propound a chaotic random generated key based adaptive and unsystematic ameliorated LSB audio steganography technique. In fact, the proposed method selects one of the 4-LSBs randomly according to the generated PWLCM values and furthermore in an unsystematic chosen samples. Take into account that the randomly generated values are equal in length to the secret message making the proposed method adaptive. Moreover, to add another layer of security, the compressed secret message is encrypted using a PWLCM key generated one-time pad. Hence, the embedding process is nondeterministic and unforeseeable. Therefore, the motivation of this work is to inaugurate an enhanced adaptive LSB audio steganography for concealing high capacity secret text while achieving superb imperceptibility, as well as security.

IV. THE PROPOSED METHOD

This section elucidates the proposed enhanced LSB_{PWLCM} method, explaining the preprocessing needed before the actual embedding of the secret message. These comprises the compression, and then the encryption with one-time pad. Hence, the algorithms are outlined together with flowcharts depicting the embedding and extraction processes. The generation of the random numbers using the chaotic PWLCM is also expounded in an algorithm. Additionally, the one-time pad encryption algorithm is delineated.

A. PREPROCESSING

To lessen the secret message size (Msg), Huffman algorithm was performed as a preprocessing step. Minimizing the Msg precipitates the undetectability of the secret message as it improves the imperceptibility of the proposed method. However, if the existence of the message is verified, further action is needed for protection. Hence, the Msg is encrypted using one-time pad.

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3259902

Algorithm 1: Generating Random Numbers Using PWLCM

Input: p, y, l
`// p ∈ (0,0.5] & y_n ∈ [0,1] are positive control parameters and initial variables`
`// l is number of random numbers`
Output: $ArrayPWLCM_l$
`// Array of PWLCM random numbers`

Function PWLCM(p,y,l)
  for i=1 *to* l **do**
    if $0 \leq y_{n-1} < p$ **then**
      $Y_n = F(y_{n-1}) = y_{n-1} \times \frac{1}{p}$
    else if $p \leq y_{n-1} < 0.5$ **then**
      $Y_n = F(y_{n-1}) = (y_{n-1} - p) \times \frac{1}{0.5-p}$
    else if $0.5 \leq y_{n-1} < 1$ **then**
      $Y_n = F(y_{n-1}) = F(1 - y_{n-1})$
    end
  end
End Function

Algorithm 2: Encrypting the secret Message *Msg* Using One-time Pad

Input: *Msg*, $Array_{PWLCM}$
`// Array of random numbers generated by PWLCM`
Output: *Msg*

Function OneTimePad(*Msg*, $Array_{PWLCM}$)
  c=0
  for i =1 *to LengthOf(Msg)* **do**
    c[i] = mod(Msg[i] +y[i],2^8)
  end
  `// Encrypting the message Msg by one-time pad`
End Function

To increase the security of the one-time pad, random numbers are generated using PWLCM as an input, as shown in algorithm 1. Algorithm 2 delineate the one-time pad encryption. For simplicity, the plaintext message, the compressed and the encrypted message are all referred to in this research as *Msg*.

Note that the initial parameters of the PWLCM, namely P_{EmbExt}, Y_{EmbExt}, P_{EncDec}, Y_{EncDec} and l, are all shared between sender and recipient in a secure way, where l is the secret message size. Noteworthy, that this solved the key distribution problem of sending the whole chaotic sequences.

B. THE EMBEDDING PROCESS USING THE NOVEL ENHANCED LSB$_{PWLCM}$ ALGORITHM

At first, random numbers are generated using PWLCM and stored in an array$_{PWLCM}$. These random numbers are then converted into integer numbers and stored in array$_{IntegerOfRND}$ before being indexed in a two-row array$_{IndexOfRND}$. After sorting these values in ascending (or descending), array$_{SortedIntRDN}$ is created. The values of the first row, *IndexRND*, indicates the number of the sample to embed in. Whereas the second row values, Int_{RND} (which are the integer values of random generated numbers) will be used to choose which of the 4-LSBs inside the sample to embed in. Hence, the secret message bits are embedded in arbitrarily blocks of the cover file, and further according to some computation on these Int_{RND} values, also randomly on one of the 4-LSBs using the traditional LSB technique. Flowchart 1 and algorithm 3 expound the embedding process of the novel proposed LSB$_{PWLCM}$ method.

It is noteworthy that every time a distinct PWLCM generated random number is used to produce the array$_{SortedIntRDN}$, a different sample index and a different LSB (one of the first 4-LSBs) will be arbitrarily chosen. This assuredly yields an unpredictable nondeterministic embedding process and hence certainly enhances the security of the proposed LSB$_{PWLCM}$ method. Additionally, the array containing the random generated numbers worthy of note is equal to the secret *MsgSize*.

C. THE EXTRACTION PROCESS USING THE PROPOSED ENHANCED LSB$_{PWLCM}$ ALGORITHM

The extraction of the secret message using the novel proposed LSB$_{PWLCM}$ method is illuminated hereafter.

In the beginning, algorithm 1 is called with P_{EmbExt}, Y_{EmbExt} and the $MsgSize \times 8$ to retrieve the bits of the message. The integer values of the output array, array$_{EmbExtPWLCM}$ is computed and stored in array$_{IntegerOfRDN}$ and then indexed in another array, array$_{IndexOfRDN}$. Finally, this output is sorted into a two-rows array$_{SortIntRDN}$. This two-rows array is utilized to extract the index of the sample from the 1^{st} row (*IndexRND*) and the value (Int_{RND}) of the generated random number from the 2^{nd} row to be used to know which of the first 4-LSBs to extract from. This final process is repeated for each bit i of the secret message, *Msg*. After extracting all the bits, their decimal values are computed. Lastly, algorithm 1 is called again with P_{EncDec}, Y_{EncDec} to derive the parameters to be used to ultimately decrypt the *Msg* using One-time pad as presented in algorithm 4. In closing, Huffman algorithm is used to decompress and produce the original secret message, *Msg*. Figure 2 and algorithm 5 delineate the extraction process of the proposed LSB$_{PWLCM}$ method.

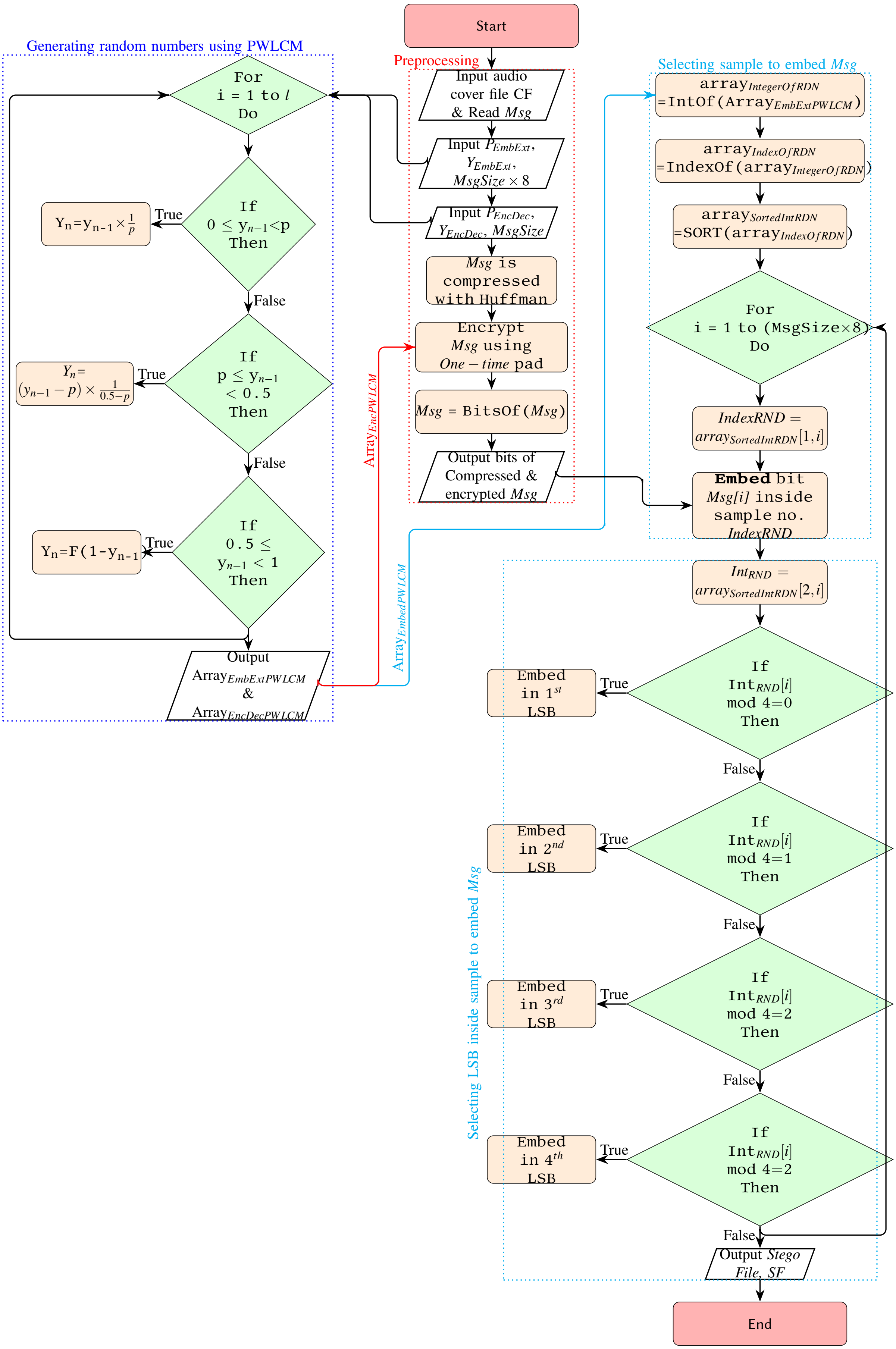


FIGURE 1: The Proposed LSB_{PWLCM} Embedding Algorithm Flowchart

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3259902

Algorithm 3: The Proposed LSB_{PWLCM} Method Embedding Algorithm

Input: AF, Msg, $MsgSize$, P_{EmbExt}, Y_{EmbExt}, P_{EncDec}, Y_{EncDec}

// AF is the audio file

// Msg is the secret message

// MsgSize is the secret message size in bytes

// P_{EmbExt} & Y_{EmbExt} are initial parameters for PWLCM to be used for embedding

// P_{EncDec} & Y_{EncDec} are initial parameters for PWLCM to be used for encryption

Output: SF

// Stego file containing the compressed encrypted embedded secret message, Msg

Function EmbedMsg(AF, Msg, $MsgSize$, P_{EmbExt}, Y_{EmbExt}, P_{EncDec}, Y_{EncDec})

- Msg = $Compress(Msg)$ // Compressing Msg using Huffman Algorithm
- $\text{Array}_{EncDecPWLCM}$ = $PWLCM(P_{EncDec}, Y_{EncDec}, MsgSize)$ // Generating Random Numbers Using PWLCM for encrypting Msg using One-TimePad
- Msg = $OneTimePad(Msg, Array_{EncDecPWLCM})$ // Encrypting Msg using One-TimePad
- Msg = BitsOf(Msg) // For simplicity, the secret message, the compressed, the encrypted, and the bits of the compressed encrypted message are ALL referred to as Msg
- $\text{Array}_{EmbExtPWLCM}$ =$PWLCM(P_{EmbExt}, Y_{EmbExt}, (MsgSize\times 8))$ // Generating Random Numbers Using PWLCM for embedding the *bits of Msg*
- $\text{array}_{IntegerOfRDN}$ =IntOf($\text{Array}_{EmbExtPWLCM}$)
- $\text{array}_{IndexOfRDN}$ =IndexOf($\text{array}_{IntegerOfRDN}$) // Array of two rows, where the 1^{st} row contains the indexes and 2^{nd} row contains the values
- $\text{array}_{SortedIntRDN}$ =SORT($\text{array}_{IndexOfRDN}$) // Array of two rows, where the 1^{st} row contains the indexes and 2^{nd} row contains the values
- **for** i = 1 to $(MsgSize\times 8)$ **do**
  - IndexRND = $\text{array}_{SortedIntRDN}[1, i]$ // Choosing the index of the sample to embed inside, which is in the 1^{st} row of the i^{th} array
  - **Embed** bit $Msg[i]$ inside sample no. $IndexRND$ // Embedding bit i inside a sample
  - Int_{RND} = $\text{array}_{SortedIntRDN}[2, i]$ // Choosing the value of the generated random number, which is in the 2^{nd} row of the i^{th} array
  - // Conditions to choose which LSB inside the sample to embed in
  - **if** $Int_{RND}[i]$ $mod\ 4$ $=0$ **then**
    - **Embed** in the 1^{st} LSB
  - **else if** $Int_{RND}[i]$ $mod\ 4$ $=1$ **then**
    - **Embed** in the 2^{nd} LSB
  - **else if** $Int_{RND}[i]$ $mod\ 4$ $=2$ **then**
    - **Embed** in the 3^{3d} LSB
  - **else if** $Int_{RND}[i]$ $mod\ 4$ $=3$ **then**
    - **Embed** in the 4^{th} LSB
  - **end**
- **end**
- **Return** Stego file, SF

End Function

Algorithm 4: Decrypting the secret Message, Msg, Using One-time Pad

Input: Msg, Array_{PWLCM}

Output: Msg

Function OneTimePad(Msg, $Array_{PWLCM}$)

- c=0
- **for** i =1 to $LengthOf(Msg)$ **do**
  - c[i] = mod(Msg[i] - y[i],2^8)
- **end**

End Function

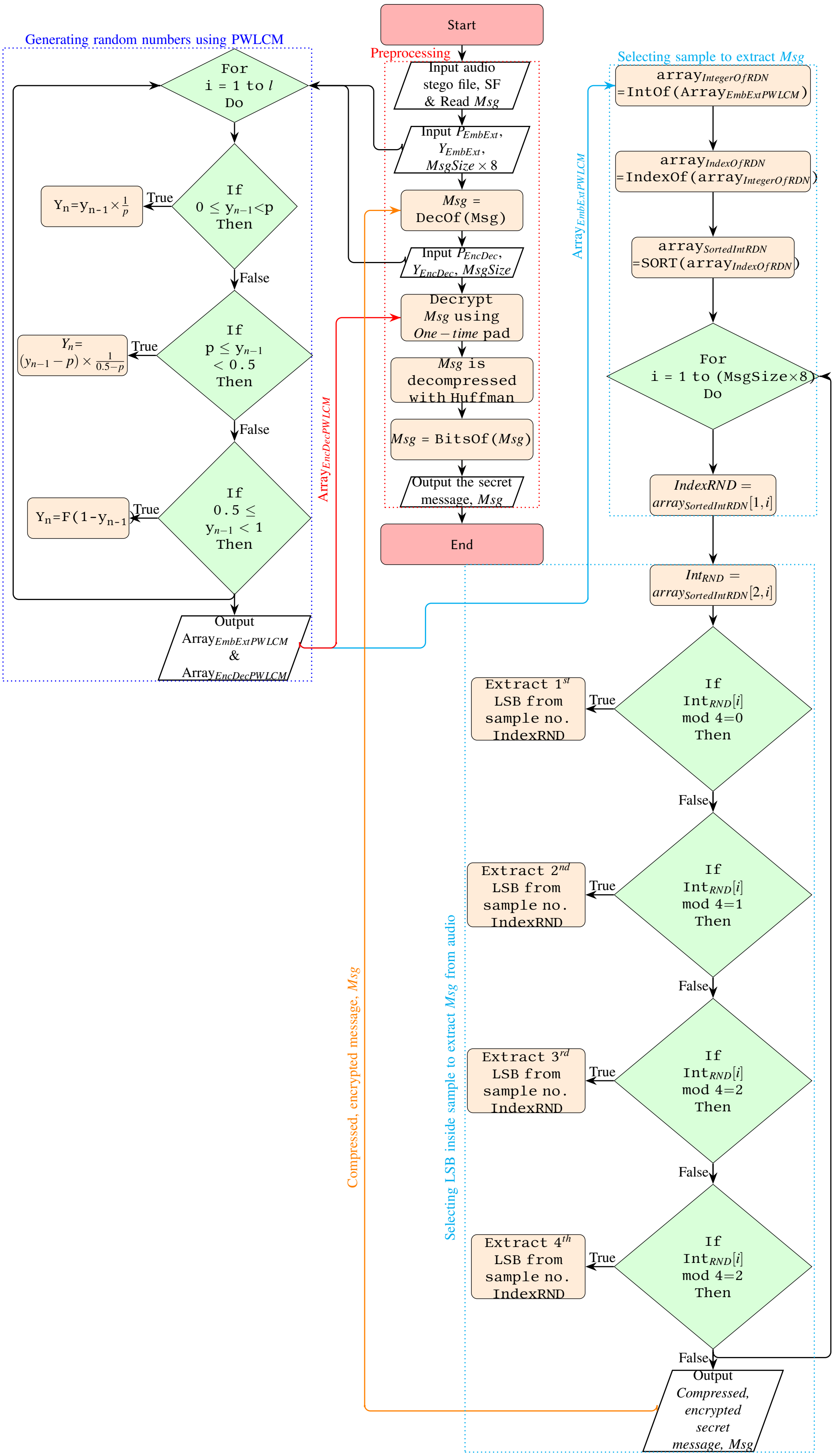


FIGURE 2: The Proposed LSB_{PWLCM} Extraction Algorithm Flowchart

Algorithm 5: The Proposed LSB$_{PWLCM}$ Method Extraction Algorithm

Input: SF, $MsgSize$, P_{EmbExt}, Y_{EmbExt}, P_{EncDec}, Y_{EncDec}

// Stego file containing the compressed encrypted hidden secret message Msg
// MsgSize is the secret message size in bytes
// P_{EmbExt} & Y_{EmbExt} are initial parameters for PWLCM to be used for extraction
// P_{EncDec} & Y_{EncDec} are initial parameters for PWLCM to be used for decryption

Output: Msg

// Msg is the secret message

Function ExtractMsg($SF, MsgSize, P_{EmbExt}, Y_{EmbExt}, P_{EncDec}, Y_{EncDec}$)
- Array$_{EmbExtPWLCM}$ =$PWLCM(P_{EmbExt}, Y_{EmbExt}, (MsgSize \times 8))$ // Generating Random Numbers Using PWLCM for extracting the bits of Msg
- array$_{IntegerOfRDN}$ =IntOf(Array$_{EmbExtPWLCM}$)
- array$_{IndexOfRDN}$ =IndexOf(array$_{IntegerOfRDN}$) // Array of two rows, where the 1^{st} row contains the index and 2^{nd} row contains the value
- array$_{SortedIntRDN}$ =SORT(array$_{IndexOfRDN}$) // Array of two rows, where the 1^{st} row contains the index and 2^{nd} row contains the value
- **for** $i = 1$ to $(MsgSize \times 8)$ **do**
  - IndexRND = array$_{SortedIntRDN}[1, i]$ // Choosing the index of the sample to extract from, which is in the 1^{st} row of the i^{th} array
  - Int$_{RND}$ = array$_{SortedIntRDN}[2, i]$ // Choosing the value of the generated random number, which is in the 2^{nd} row of the i^{th} array
  - // Extracting bit i of message from a sample
  - **if** $Int_{RND}[i]$ mod $4 = 0$ **then**
    - $Msg[i]$ = **Extract** 1^{st} LSB bit from sample no. $IndexRND$
  - **else if** $Int_{RND}[i]$ mod $4 = 1$ **then**
    - $Msg[i]$ = **Extract** 2^{nd} LSB bit from sample no. $IndexRND$
  - **else if** $Int_{RND}[i]$ mod $4 = 2$ **then**
    - $Msg[i]$ = **Extract** 3^{3d} LSB bit from sample no. $IndexRND$
  - **else if** $Int_{RND}[i]$ mod $4 = 3$ **then**
    - $Msg[i]$ = **Extract** 4^{th} LSB bit from sample no. $IndexRND$
  - **end**
- **end**
- Msg = DecOf(Msg)
- Array$_{EncDecPWLCM}$ = $PWLCM(P_{EncDec}, Y_{EncDec}, MsgSize)$ // Generating Random Numbers Using PWLCM for decryption using One-TimePad
- Msg = $OneTimePad(Msg,$ Array$_{EncDecPWLCM})$ // Decrypting Msg using One-Time Pad
- Msg = $Decompress(Msg)$ // The Msg is decompressed using Huffman Algorithm
- **Return** The secret message, Msg

End Function

V. EXPERIMENTAL RESULTS AND DISCUSSION

This section discusses the experimental implementation of the proposed LSB$_{PWLCM}$ method, where comprehensive experiments were performed and compared with related schemes.

A. PRELIMINARIES

The implementation of the proposed ameliorated LSB$_{PWLCM}$ method is performed using MATLAB software version R2020b. The experiments were tested on a laptop with Windows 10, Core i5 processor with 2.5 GHz speed and 4 GB for RAM.

Uncompressed six audio cover files from the GTZAN dataset [55][56] were used and their specifications are hereafter displayed in table 1.

TABLE 1: Cover Audio files specification

Specification	
Bit per sample	16
Number of samples	661500
Channel	Mono
Audio type	Music
Duration in Seconds	1- 30

B. IMPERCEPTIBILITY ANALYSIS

Imperceptibility is the exactitude between the original audio cover and the stego audio, as well as between the reconstructed file and the secret message. This criterion signify minimum distortion and is obversely to hiding capacity. In specific, the sequel of superb hiding capacity is high distortion and low imperceptibility [11][14].

To evaluate the performance of the proposed method from the facets of imperceptibility, the upcoming objective metrics were used, namely: Perceptual Evaluation of Speech Quality (PESQ), Perceptual Evaluation of Audio Quality (PEAQ), Mean Square Error (MSE), Peak Signal-to-Noise Ratio (PSNR), Signal-to-Noise Ratio (SNR), Percentage Root Mean Square Difference (PRD) and Audio Fidelity.

1) ITU Standard Perceptual Imperceptibility Evaluations

Two standard perceptual evaluations were used in evaluating the perceptual imperceptibility, specifically PESQ and PEAQ, which are hereby elucidated:

- *Perceptual Evaluation of Speech Quality) (PESQ)* PESQ is used to gauge the sameness between the cover and stego audios [57][58]. The score varies in the interval [1,4.5], where the value '4.5' attests the perceptual similarity of both cover and stego audios, whereas '1' shows dissimilarity. Actually, the acceptable rate of PESQ must be $\geq$ 3.8 [15]. Graph 3 blatantly confirms the high imperceptibility of the proposed LSB$_{PWLCM}$ method as the values achieved on the six tested audios range from 4.497 for female audio up to 4.5 for vlobos, male, jazz and voce audios. Dialogue audio attained a PESQ value of up to 4.499. Therefore, these experimental results ratify that the proposed method is efficacious.
- *Perceptual Evaluation of Audio Quality (PEAQ)* PEAQ is another standardized algorithm for objectively evaluating the imperceptibility of the audios [59]. It greatly reduces the costly expenses and time-consuming efforts associated in listening tests while having reliable results and ease of use [60–62]. Its major output parameter is the objective difference grade (ODG), which has an interval of [0,-4]. When the ODG value is close to 0, the better the sameness of the two audios. Graph 4 depicts the PEAQ-ODG values for the different six audios using various secret message sizes where all the values ranges between -0.0225 (particularly for voice audio and 20KB secret message) and -0.1053 (specifically for female audio and 140KB secret message). Ergo, the proposed method LSB$_{PWLCM}$ has a high imperceptibility and the cover and stego audios are indistinguishable as presented clearly in graph 4.

2) Mean Squared Error (MSE)

The distortion in the audio is measured by MSE, which is the average square differences between the cover and stego audios. The unerring exactitude of the input and output signals is when MSE approaches zero, hence better performance. It is measured in decibel (dB) as shown in equation 2 [4][13]:

$$MSE = \frac{1}{N}\sum_{i=1}^{N}(s1_i - s2_i)^2 \tag{2}$$

where $s1_i$ and $s2_i$ are the i^{th} samples of the input and output signals, and

N is the number of signal samples.

3) Peak Signal to Noise Ratio (PSNR)

PSNR guages in decibel (dB) the maximum signal to noise ratio of an audio as presented by equation 3 [4][13]:

$$PSNR = 10\, log_{10}\, \frac{(2^n - 1)^2}{MSE} \tag{3}$$

where n is the maximum number of bits used to represent each signal sample.

The lesser the MSE value, the superior the steganography quality and vice versa. Additionally, as PSNR is inversely proportional to MSE (see equation 3), hence the greater the PSNR's value, the better is the concealment quality, hence less distortion.

4) Signal-to-Noise Ratio (SNR)

Another measurement for the imperceptibility between the cover and stego audios is the SNR (in dB) [63].

SNR measures the distortion in the imperceptibility between two signals, input and output. Thus, it evaluates the quality of the output signal after the embedding process in decibels (dB) [63]. The International Federation of the Phonographic Industry (IFPI) proclaims that the acceptable value of SNR must be more than 20 dB. Actually, the greater the SNR value implies indistinguishable stego from audio file. It is specified below in equation 4 [4][13][20]:

$$SNR = 10\, log_{10}\, \frac{\sum_{i=1}^{N}(s1_i)^2}{\sum_{i=1}^{N}(s1_i - s2_i)^2} \tag{4}$$

where $s1_i$ and $s2_i$ are the i^{th} samples of the input and output signals, and N is the number of signal samples.

5) Percentage Root Mean Square Difference (PRD)

PRD computes the percentage of root mean square differences between two audios. Its value ranges from 0 to 1, where 0 being the perfect score. Equation 5 shows how it is calculated:

$$PRD = \sqrt{\frac{\sum_{i=1}(X_i - Y_i)^2}{\sum_{i=1}(X_i)^2}} \tag{5}$$

where X$_i$ is the first signal and Y$_i$ is the second signal.

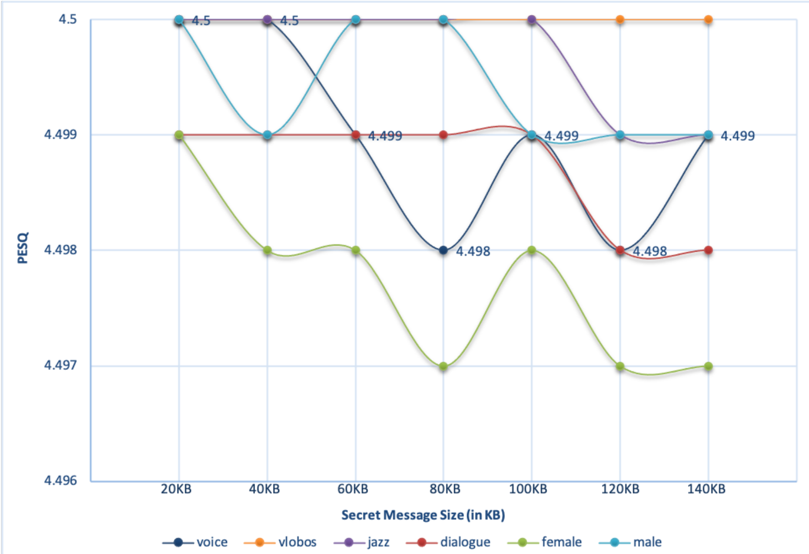


FIGURE 3: Effect of the PESQ versus hiding capacity on the imperceptibility using several secret message sizes and cover audios

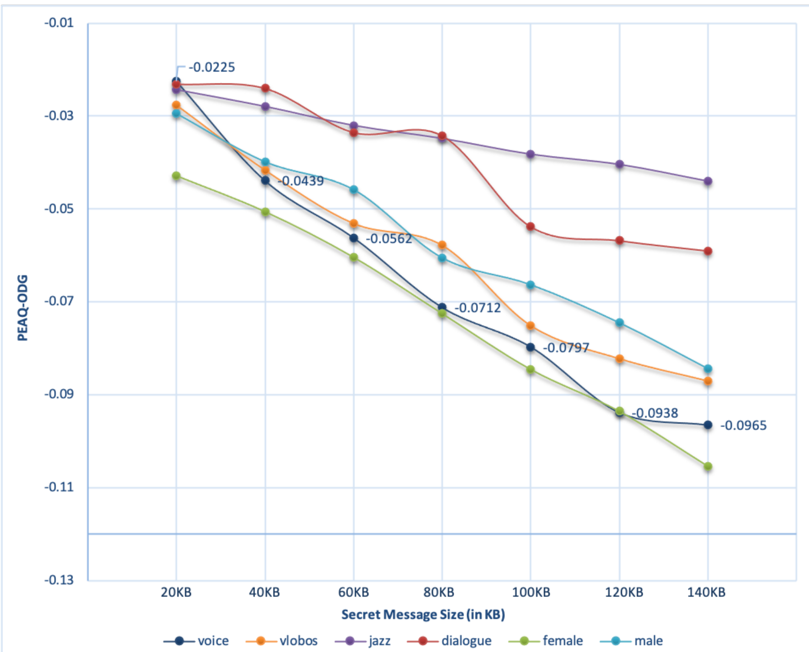


FIGURE 4: Effect of the PEAQ ODG versus hiding capacity on the imperceptibility using various secret message sizes and cover audios

6) Audio Fidelity

Equation 6 assesses the difference of samples bits between cover and stego audios. Specifically, it is based on the number of errors in the sample value, so very similar to MSE, and has a value range of 0 to 1. Clearly, the superb imperceptibility, the lesser the audio fidelity value. Figure 9 exhibits the audio fidelity experimental results of the proposed LSB_{PWLCM} method. The lowest value was 0.004427 and the highest was 0.030524 for audio male. Evidently from figure 9, all values achieved were very close to zero confirming the efficacy of the proposed method and redoubtable high imperceptibility.

$$Audio\ Fidelity = \frac{\sum_{i=1}^{N}(s1_i - s2_i)^2}{\sum_{i=1}^{N}(s1_i)^2} \tag{6}$$

where $s1_i$ and $s2_i$ are the i^{th} samples of the cover and stego audios signals, and N is the number of signal samples.

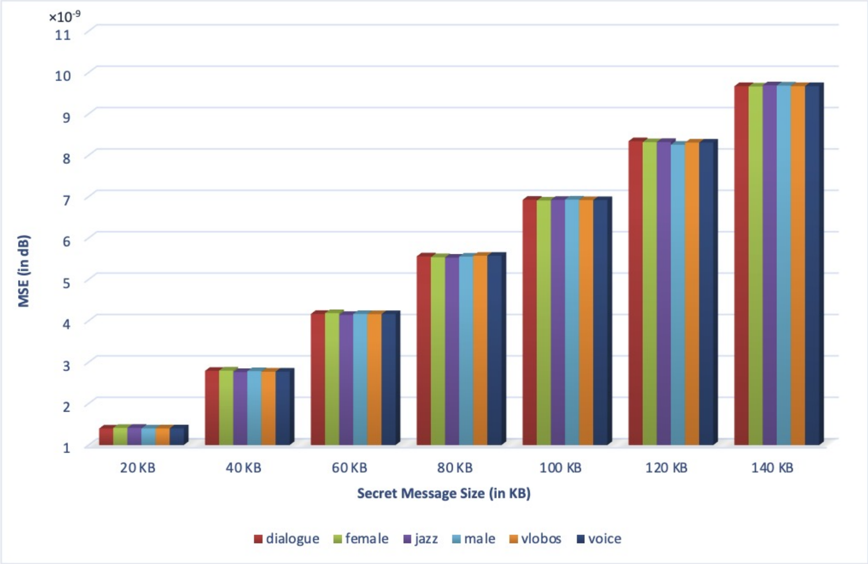


FIGURE 5: Effect of the MSE versus hiding capacity on the imperceptibility using several secret message sizes and cover audios

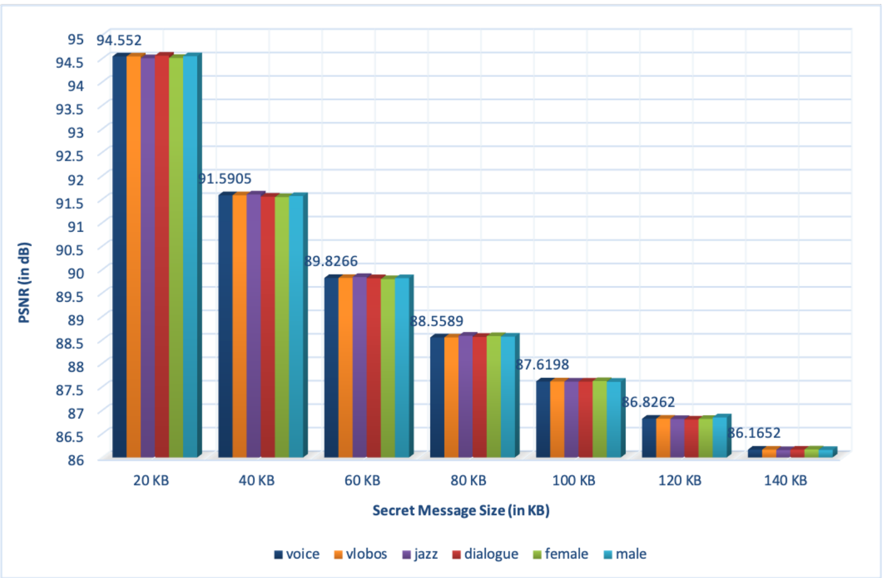


FIGURE 6: Effect of the PSNR versus hiding capacity on the imperceptibility using several secret message sizes and cover audios

7) Imperceptibility Analysis

Several experiments were carried out to test the imperceptibility of the proposed ameliorated LSB$_{PWLCM}$ method on six various audios using different secret message sizes ranging from 20KB to 140KB. The six audios were selected from GTZAN dataset, namely voice, vlobos, jazz, dialogue, female and male [55][56]. First, the various secret message sizes were compressed by Huffman algorithm. Next, random numbers are generated using PWLCM and these are then used to embed the bits of the secret message in random blocks using traditional LSB. In fact, according to the integer values of these generated random numbers, one of the 4-LSBs inside a sample will be chosen to embed in depending on a defined formula. And based on the index of these integer converted random numbers, the sample is specified. Before embedding, the secret message bits are encrypted using One-time Pad, where the key is also randomly generated using PWLCM. The audio sample may be represented in various ways. Hence, to ensure the inclusiveness and efficacy of the proposed method, the experimental tests were conducted using two different ways; to be specific the audio samples are first represented in the range [-1,1] and after that

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3259902

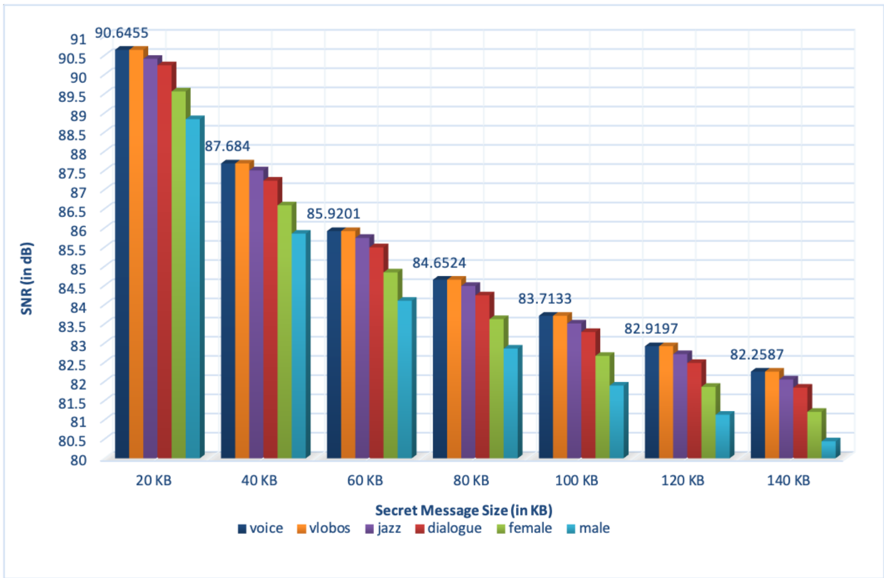


FIGURE 7: Effect of the SNR versus hiding capacity on the imperceptibility using several secret message sizes and cover audios

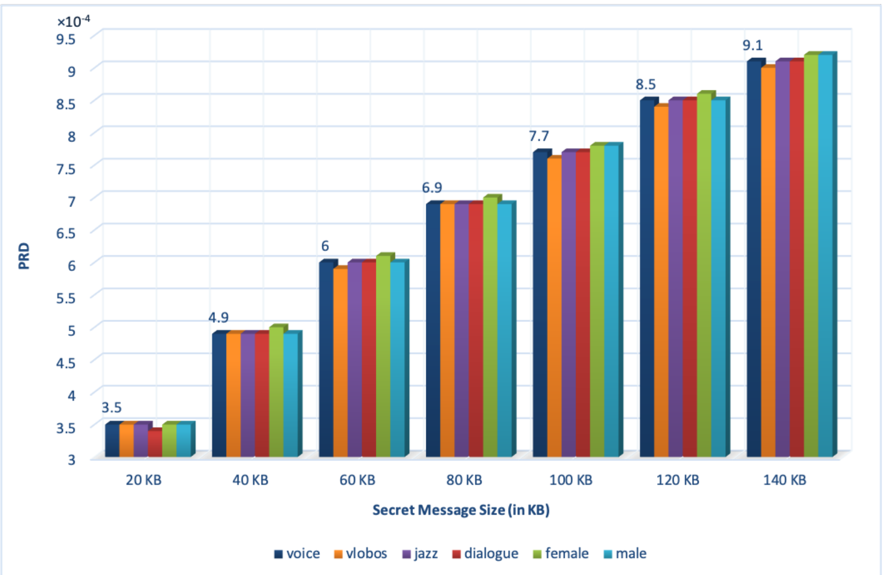


FIGURE 8: Effect of the PRD versus hiding capacity on the imperceptibility using several secret message sizes and cover audios

in the range [0,65535]. The latter range representations were considered in this research.

Figures 3, 4, 5, 6, 7, 8 and 9 affirm that the proposed method evince high imperceptibility.

Considering the standard perceptual evaluations, the graph of figure 3 demonstrates that all six tested audios have a PESQ value $\geq$ 4.497 which is achieved by female audio file with a hiding capacity of 140KB while vlobos, male, voice and Jazz all attained 4.5 value PESQ. This blatantly affirms the imperceptibility of the proposed method even with high capacity up to 173%. In comparison to traditional LSB and 4-LSB methods, their PESQ attained values were 4.43 and 4.47 respectively. This assures the imperceptibility of the proposed method. Moreover, the imperceptibility is affected depending on the nature of the audio. Additionally, from figure 4, it is very obvious that the proposed method gave favorable results as all PEAQ-ODG where all very close to 0. The values were ranging from -0.0225 (for voice audio and 20KB secret message) to -0.1053 (for female audio and 140KB secret message) assuredly proclaiming its superb imperceptibility. It is noteworthy that these values are contingent on the

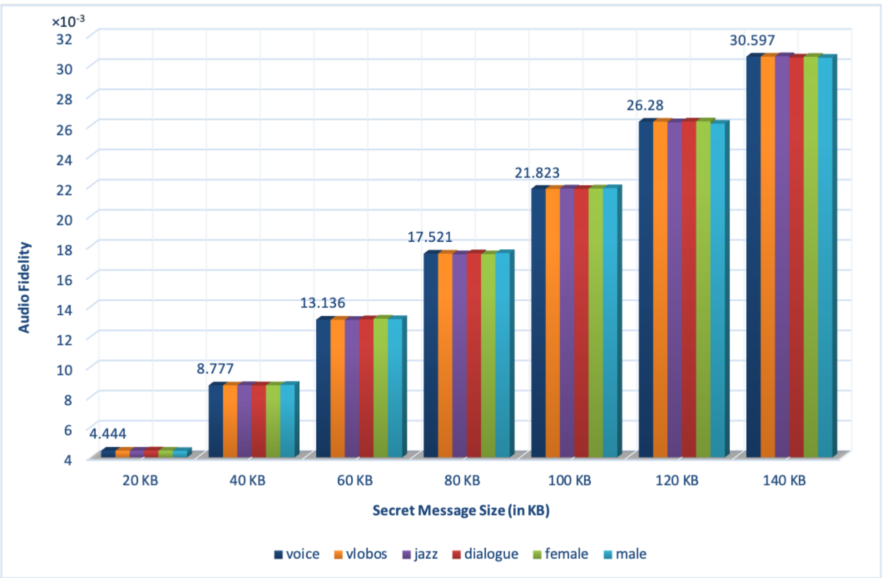


FIGURE 9: Effect of the Audio Fidelity versus hiding capacity on the imperceptibility using several secret message sizes and cover audios

nature of the audios and the embedded secret message, where the smallest the secret message the better the values as evident in graph 4.

Concerning the PSNR, values ranged from 86.1566 for jazz and up to 94.5671 for dialogue, whereas the MSE values varied from 1.397E-09 to 9.691E-09.

Clearly, figure 8 shows that all tested six audios has a PRD value very close to 0. Specifically, the highest value was 0.0092 achieved by female and male audios when embedding 140KB. This PRD value is because of the nature of the audio as other music nature audios achieved far less for the same secret size. Whereas, audio dialogue attained the least value which was 0.0034 when embedding a 20KB. However, all PRD values were very nearly to zero. This further avers the efficacy of the proposed method from imperceptibility facet.

For all six audios, the SNR attained a minimum value of 80.4408 dB for audio male and a maximum of 90.6455 dB for both voice and vlobos for various secret message sizes.

Blatantly, the Huffman compression and the random selection of the blocks (samples) and the 4-LSBs for embedding justifies the preservation of the imperceptibility of the proposed method. Actually, the embedding position depends on the PWLCM random generated numbers and the size of the secret message, as elucidated in section IV. Ergo, there is no significant distinguishable distortion to raise suspicion on the actuality of embedded a secret message.

C. HIDING (EMBEDDING) CAPACITY (HC)

The proposed ameliorated LSB_{PWLCM} method is characterized by having superlative hiding capacity. Hiding capacity (also known as payload) is the percentage of the secret message size to that of the cover file, as specified by equation 7 [4][13]:

$$Hiding\ Capacity\ (HC) = \frac{Secret\ message\ size}{Cover\ file\ size} \times 100 \tag{7}$$

In specific, the LSB hiding capacity is given by equation 8, as LSB embeds 8 bits per sample [4][13]. For example, in our tested audios, the number of samples is 661500. Ergo, it should be capable to embed 82687.5 bytes only using traditional LSB. Using Huffman compression algorithm, our proposed LSB_{PWLCM} method embedded 140 KB with high imperceptibility, actually accomplishing an increase of up to 173% compared to the traditional LSB. The compression ratio using Huffman algorithm was found to be in the range of 55% to 57.5% for 20KB to 140 KB secret messages respectively.

$$Hiding\ Capacity\ for\ LSB = \frac{number\ of\ samples}{8} \tag{8}$$

The **embedding rate**, on the other hand, is the percentage of the secret message size to the number of samples, as given by equation 9.

$$Embedding\ rate = \frac{secret\ message\ size}{number\ of\ samples} \times 100 \tag{9}$$

In our tested audios, the embedding rate was 143360/661500 = 21.7% which is much higher compared to the traditional LSB, which is only 12.5%.

Figure 7 illustrates the relationship between the SNR and the hiding capacity of six tested audios. It is clearly shown that the bigger the embedded secret message size, the lower is the imperceptibility and vice versa.

D. ROBUSTNESS ANALYSIS

Robustness refers to the ability to retrieve a secret message successfully without or hardly few errors. It can be assessed using bit error rate (BER) and normalized cross-correlation (NCC) which are briefly elucidated hereafter.

1) Bit Error Rate (BER)

This metric unveils the percentage of the secret message bits that was retrieved incorrectly, see equation 10 [5].

$$BER = \frac{\sum_{x=1}^{L_M} M_x \vee M'x)}{L_M} \times 100\% \tag{10}$$

where L$_M$ is the total message bits, x is the message bits index, M is original message, M' is extracted message bits from stego image.

2) Normalized Cross-Correlation (NCC)

Equation 11 gives another well known method to evaluate the sameness, which is NCC. Contrary to BER, the closer the NCC value to 1, the vigorous the robustness of the steganographic method.

$$NCC\left(M,M'\right) = \frac{\sum_{k=1}^{QG} M\left(k\right) M'\left(k\right)}{\sqrt{\sum_{k=1}^{QG} M\left(k\right)^2}\sqrt{\sum_{k=1}^{QG} M'\left(k\right)^2}} \tag{11}$$

where M and M' are the initial and retrieved secret text messages, respectively

QG is number of samples.

3) Message Extraction Tests

In the absence of attacks, the secret message was extracted 100% successfully using proposed LSB$_{PWLCM}$ method for all tested audios using different message sizes. Similarly, all audios gave NCC values of 1, confirming the efficiency of the proposed method in extracting the secret message fully.

4) Robustness Analysis with an Attack

Recall that robustness is the capability to resist adverse conditions. Specifically in Steganography, it means retrieving the hidden secret message fully or with passable distortion after intentional attacks, like AWGN, LSB attack and resampling attack. Hereby, these deliberate attacks are briefly discussed, together with their robustness tests on the proposed method.

- *LSB Attack* The LSB bits are altered in an unsystematic way, i.e. from '0' to '1' or contrariwise. Due to the nature of the proposed method, it was not resistant to LSB attack, as any modification to an LSB will cause the full recovery of the original audio deemed difficult.
- *AWGN attack* This is absolutely attaching white gaussian noise to stego audios resulting in distortion. Alike to the intentional LSB attack, the proposed method did not withstand this attack due to its essential characteristics of embedding choices.
  However, hiding in one of the first 4-LSBs in an adaptive way, depending on the PWLCM random generated numbers, will certainly reduce the effect of noise attacks. Nonetheless, the proposed novel LSB$_{PWLCM}$ method used Huffman compression to reduce the secret message size and hence increase the hiding capacity. Moreover, it has high imperceptibility and security. Nevertheless, if compression was not used, it would have resisted the LSB attacks and AWGN attack due to the adaptive embedding in audio samples up to the 4^{th} LSBs. The adaptive selection is made nondeterministic using PWLCM random generated numbers. Hence, any noise attack is inevitable as after decompressing, the secret message might be distorted. Therefore, the proposed method inclined to the high capacity, imperceptibility and security.
- *Re-sampling Attack* Re-sampling requires adjusting the samples from 16,000 to 8,000 and then backwards to 16,000 again before transmitting the stego audio. This might change the bits of the retrieved secret message [4][64]. Experimental tests were performed on the six audios, and the stegos were resampled from 16 KHz to 8 KHz and afterwards back to16 KHz again. The PESQ and BER of the original stegos and the resampled ones for each audio type gave 4.5 and 100% respectively for all audios and the secret messages were retrieved successfully.
  Moreover, when comparing each resampled stego with its original cover audio with respect to PESQ and Audio Fidelity, the results were exactly similar to those of figures 3 and 9 correspondingly. This patently gave credence to the efficiency of the proposed method.

E. SECURITY ANALYSIS

Hereafter, the security of the proposed method is scrutinized from three different aspects.

1) Security of the Proposed LSB$_{PWLCM}$ Method

As mentioned earlier, the PWLCM algorithm generates different random numbers each a time. As these were utilized in generating array$_{SortedIntRDN}$ (see algorithm

3), which is used for sample and LSB selection for embedding, hence obviously a distinct sample is chosen every time and consequently a differing erratic LSB (one of the 4-LSBs) will be selected. Blatantly, the proposed LSB_{PWLCM} method has an unforeseeable non-deterministic embedding process, ergo ameliorating its security.

2) Security of PWLCM

The control parameters of PWLCM, namely p and y_n evolve into a chaotic state, and p can act as a secret key, see algorithm 1. Consequently, the PWLCM system has a constant invariant distribution and superb ergodicity, confusion and determinacy. Therefore, it can provide a superlative random sequence that is appropriate for a cryptosystem [65][66]. Ergo, it is utilized to boost the security of one-time pad by generating the input key using PWLCM. Furthermore, the above mentioned characteristics also ensure the unsystematic approach of choosing the samples and LSBs inside these samples to embed. This clearly proclaims the randomness and indeterministic embedding process of the proposed method.

3) Resistance to Brute Force Attack

The brute force attacker attempts to try all the different possible number of keys. The input to the embedding process using the proposed LSB_{PWLCM} method is the set $MsgSize$, P_{EmbExt}, Y_{EmbExt}, P_{EncDec}, Y_{EncDec} among the audio file, AF, and the secret message, Msg. Besides the $MsgSize$, these are initial parameters to the PWLCM, which are all double-precision numbers. Hence, if the computational precision of each of P_{EmbExt}, Y_{EmbExt}, P_{EncDec}, Y_{EncDec} is 10^{-16}, then the key space is greater than $10^{16} \times 10^{16} \times 10^{16} \times 10^{16} \times MsgSize$ and is therefore given by equation 12 below:

$$Key\ Space\ of\ LSB_{PWLCM} \geq 10^{64} \times MsgSize \qquad (12)$$

Ergo, the proposed LSB_{PWLCM} method has an immense ample key space to resist all sorts of brute-force attacks, ensuring its effectiveness.

F. STEGANALYSIS TESTS

The proposed LSB_{PWLCM} method was evaluated against steganalysis tests and the results are hereafter discussed.

1) Histogram Attack

Forty two experiments using six different cover audios and various secret message sizes were performed to examine histogram attack as illustrated in graph 10. The histogram error between the original audio cover and the stego audio constructed by the proposed LSB_{PWLCM} method was evaluated by Histogram Error Rate (HER) using equation 13. The graph clearly shows that all HER for all six audios are very close to zero. Furthermore, figure 11 shows the graphical representation of the histograms of original audio before and after embedding a 100 KB secret message size using five different cover audios. These surely affirms that the proposed method is resistant to histogram attacks.

$$HER = \frac{\sum_{i=1}^{N} (His_c - His_s)^2}{\sum_{i=1}^{N} His_c^2} \qquad (13)$$

where His_c and His_s are histograms of cover and stego audios

Audio	Difference Ratio (DR)			
	1^{st} moment, Average (μ)	2^{nd} moment, variance (σ^2)	3^{rd} moment, skewness (sk)	4^{th} moment, kurtosis (k)
Dialogue	0.000017	0	0.000052	0.000069
Female	0.000008	0	0.000024	0.000032
Jazz	0.000011	0	0.000033	0.000044
Male	0.000004	0	0.000011	0.000015
Vlobos	0.000012	0	0.000035	0.000047
Voice	0.000014	0	0.000041	0.000055

TABLE 2: The Difference Ratio for the Fourth First Moments for distinct cover audios using 140KB secret message

2) Fourth First Moments

Fourth First Moments is a statistical evaluation that evince the differences between cover and stego audios. They are namely, average (μ), variance (σ), Skewness (sk), and kurtosis (k), which yields the nature of function distribution, see equations 14, 15, 16, and 17 respectively. The proposed LSB_{PWLCM} method is evaluated by calculating the difference ratio (DR) which represents the absolute value of the difference of each of these four moments, as presented in equation 18. DR values approaching zero testify that the proposed method is resistant to statistical analysis [13]. Table 2 shows clearly the superiority of our proposed LSB_{PWLCM} method when 140KB secret message is embedded, where all difference ratios of the fourth first moments are very close to zero.

$$\mu = \frac{\sum_{i=1}^{n} S_i}{n} \qquad (14)$$

$$\sigma^2 = \frac{\sum_{i=1}^{n} (S_i - \mu)^2}{(n-1)} \qquad (15)$$

$$sk = \frac{\sum_{i=1}^{n} (S_i - \mu)^3}{(n-1)\sigma^3} \qquad (16)$$

$$k = \frac{\sum_{i=1}^{n} (S_i - \mu)^4}{(n-1)\sigma^4} \qquad (17)$$

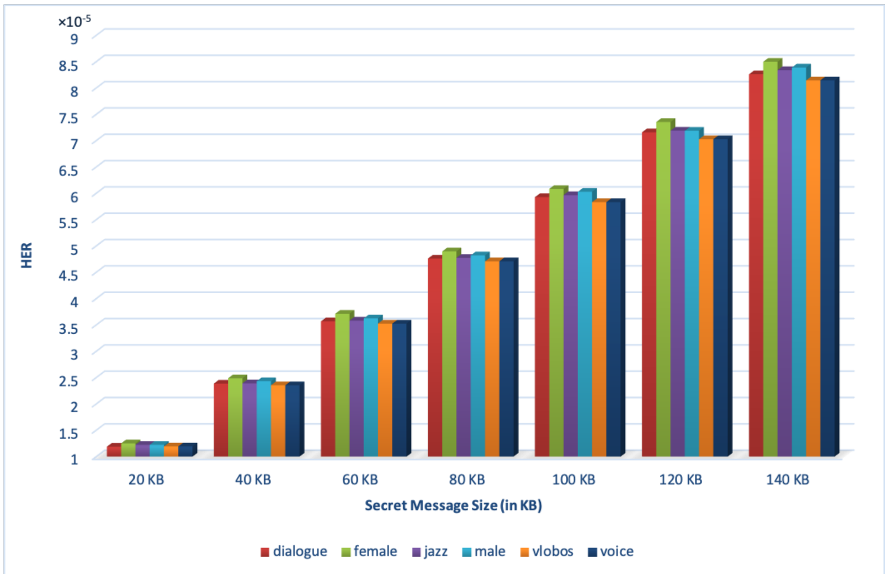
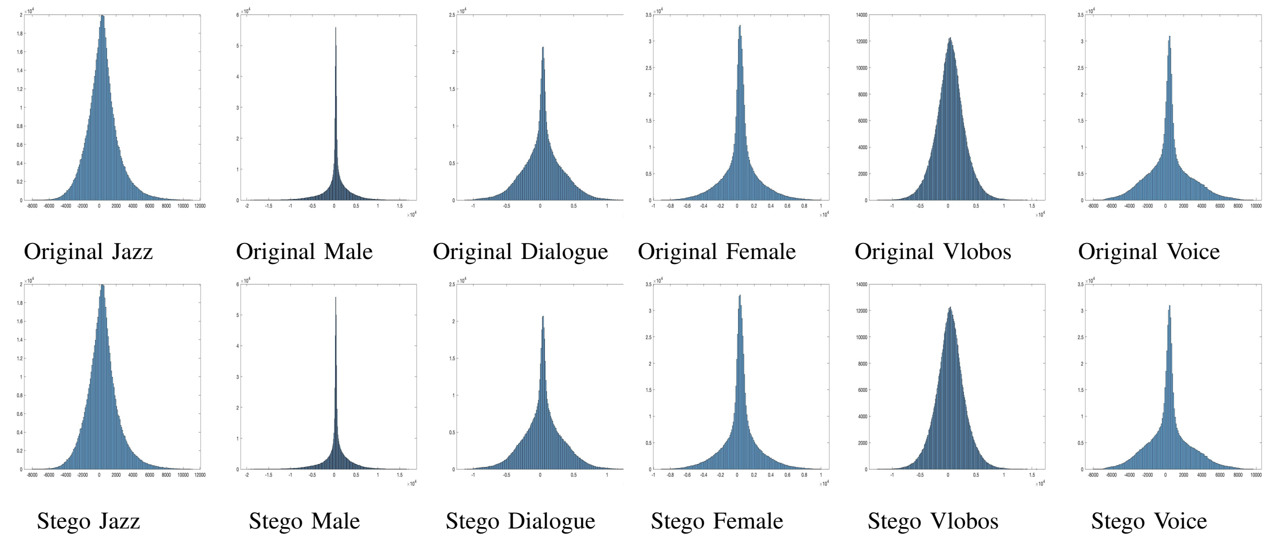


FIGURE 10: Effect of HER versus hiding capacity on imperceptibility using several secret message sizes and cover audios



(a) HER=5.97E-05 (b) HER=6.03E-05 (c) HER=5.93E-5 (d) HER=6.08E-05 (e) HER=5.83E-05 (f) HER=5.83E-05

FIGURE 11: Histogram error rates for different audios and their corresponding stego audios using 100KB Msg

$$Difference\ Ration\ (DR) = \left| \frac{(fm_c - fm_s)}{(fm_c} \right| \times 100 \tag{18}$$

where $fm_c and fm_s$ are any fourth first moments of a cover and stego audios, respectively

G. COMPARISON WITH RELATED SCHEMES

The proposed method is juxtaposed with recent related schemes to highlight its overall potential with respect to ITU standard imperceptibility PESQ and PEAQ, imperceptibility (specifically SNR, MSE and PSNR), hiding capacity, key space, HER and DR of the Fourth First Moments. In particular, comparisons were made with related schemes [4][13][15][22][30][45–48][50][52][67–75] according to their published results. Noteworthy, all the above mentioned researchers used GTZAN dataset.

1) ITU Standard Perceptual imperceptibility Evaluations Comparisons

When evaluating using the standard PESQ, it is proved that the cover and stego audios are indistinguishable. This is evident in table 3, as it showed that our method

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3259902

is resistant to re-sampling attacks and having an ideal PESQ value of 4.5.

TABLE 3: Comparison of the $PESQ_{rsec\&sec}$ values for re-sampling attacks and the randomness of the hiding process with related schemes

Method	$PESQ_{rsec\&sec}$ for re-sampling attack	Randomness of hiding process
Traditional LSB	1.20	deterministic
4-LSB	0.67	deterministic
Ahmed et al (2010) [52]	not robust	deterministic
Bharti et al (2019) [15]	1.42	non-deterministic
Mahmoud & Elshoush (2022) [4]	4.5	non-deterministic
Proposed LSB_{PWLCM} method	4.5	non-deterministic

Furthermore, table 4 compares the PEAQ ODG values between the proposed method and related schemes [69–71] for varying secret message sizes. Knowing that the closer PEAQ ODG value to 0, the better the similitude of the two audios. Table 4 testifies that our method outcompetes these methods having PEAQ ODG values closer to zero and thus affirms superlative imperceptibility.

2) Imperceptibility Comparisons

With regard to **MSE**, our proposed method excels the prevailing methods as evident from table 5 and figure 12, which shows comparisons with recent researches.

Table 5 shows a general comparison of the **PSNR** values attained by related schemes compared to our method. Regarding PSNR imperceptibility with specific audios, our proposed method outperforms related scheme [47] achieving a PSNR of 94.5671 dB using Dialogue and 20KB secret message compared to 54.089 dB by [47]. Graphs 13 and 14 patently illustrate that the proposed LSB_{PWLCM} method prevails over research [47] using Dialogue and Vlobos audios respectively, and hence successfully preserved the stego imperceptibility.

Continuing with imperceptibility, looking into the general **SNR** results reported by recent researches, table 5 and figure 15 constitute evidence that our method was effective and superior to related schemes. To be specific, it is very clear from figure 15 that the proposed method outcompetes the recent 2022 researches of Abood et al [48] and Manjunath et al [46] as they accomplish an average of 60.6343 dB and 29.202 SNR respectively, albeit our proposed method procured 90.6455dB.

Particularly, considering hiding small secret message sizes of 1KB to 5KB on the 4-LSB, figures 16 and 17 manifestly reveals that the proposed method outcompetes the SNR results of [67] using specifically Jazz and Vlobos audios respectively.

Specifically, comparison with Vlobos from GTZAN dataset, our proposed method had an SNR of 90.6455 dB, whereas research [13] obtains only 71dB . Actually, for dialogue, female, and jazz audios, our method also performed much better compared to research [13] affirming its efficacy, as displayed in figure 18.

Table 6 juxtapose the **PRD** values of the proposed method with related work Ali et al [13] specifically for audios Dialogue, female and Jazz. To our knowledge, this is the only research we found that gauged PRD values. Indubitably, our results are very close to zero and are excellent compared to their published results.

3) Hiding Capacity Comparisons

Regarding hiding capacity, research [68] was able to embed up to 45.65% payload utilizing jazz cover and achieved an SNR of 51.09 dB. On the other hand, Ali et al. [13] enhances the hiding capacity to 100% while having an SNR of 73.6 dB. Our method successfully inflated up to 173% of payload, whereas realizing an SNR of 90.4098 dB for jazz audio and SNR equivalent to 90.6455 dB for voice audio. It is noticeable that [4] attains the same increase in hiding capacity as ours. Table 5 and figure 15 demonstrate the hiding capacity of different schemes juxtaposed with our proposed method. Clearly, our proposed LSB_{PWLCM} method surpassed them with respect to hiding capacity.

4) Robustness Comparisons of BER and NCC

The BER and NCC attained results of the proposed method is compared with those published by researches [15] and [71] as demonstrated table 7. The table presents the results specifically for male, female and vlobos audios. It is evident that our method outperforms those methods where BER values were all 100%, and NCC values are all 1's, where the secret messages are all extracted accurately.

5) Key Space Comparisons

Concerning security, table 8 depicted that the proposed LSB_{PWLCM} method can withstand brute force attacks as its key space has considerable size of $\geq 10^{64} \times MsgSize$. Ergo, as can be seen from the comparisons with researches [13], [4] and [50], it is dominating prevailing schemes. Moreover, its key space depends on the size of the message, $MsgSize$.

6) Steganalysis Tests Comparisons

Analogously, table 9 proclaims better resistance to statistical analysis compared to existent schemes concerning HER. Our proposed method achieved values closer to zero than those attained by other researches.

Apparently, also the eminent efficiency of the proposed method can be noticed in table 10 as all DR values are very close to zero and far better than all achieved by prevailing schemes using different audios. Tables 9 and 10 assuredly confirms the resistance of our method to statistical analysis attacks.

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and
content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3259902

Audio	Reference	PEAQ ODG using different secret MsgSizes				
		32KB	64KB	88KB	96KB	128KB
Vlobos	Petitcolas et al [69] 2002	-3.788	-2.636	-	-1.577	-2.891
	Diqun et al [70] 2009	-2.371	-0.944	-	-0.439	-0.519
	Bhowal et al (2017) [71]	-	-	-0.31	-	-
	Proposed LSB$_{PWLCM}$ method	**-0.0356**	**-0.0545**	**-0.0672**	**-0.071**	**-0.0851**
Jazz	Petitcolas et al [69] 2002	-3.432	-1.68	-	-1.619	-1.721
	Diqun et al [70] 2009	-3.172	-1.092	-	-0.087	0.019
	Bhowal et al (2017) [71]	-	-	–0.20	-	-
	Proposed LSB$_{PWLCM}$ method	**-0.0256**	**-0.0328**	**-0.0356**	**-0.0378**	**-0.0424**

TABLE 4: Comparison of the PEAQ ODG values of the Proposed LSB$_{PWLCM}$ Method with Related Schemes Using different secret message sizes

TABLE 5: Comparison of the MSE, PSNR, SNR and HC values for the proposed method with related schemes

Method	MSE	PSNR (in dB)	SNR (in dB)	HC w.r.t. cover
Shahadi et al [22] 2014	-	-	35	48%
Bazyar et al [68] 2015	6.03E-7	150.02	51.09	45.65%
Ali et al [13] 2018	0.46	99.6	73.6	100%
Bharti et al [15] 2019	-	-	34.93	100%
Alsabhany et al [30] 2020	3.89E-09	84.1	60.16	40%
Manjunath et al [45] 2020	0.47686	-	25.767	-
Prakash Rao et al [47] 2021	-	40.514125	-	-
Manjunath et al [46] 2022	0.16641	-	29.202	-
Abood et al [48] 2022	8.6433e-07	60.6332	60.6343	55%
Abdulkadhim et al [50] 2022	-	42.2367	-	-
Mahmoud & Elshoush [4] 2022	0.279	94.8765	96.9	173%
Proposed LSB$_{PWLCM}$ method	**1.40089E-09**	**94.5671**	**90.6455**	**173%**

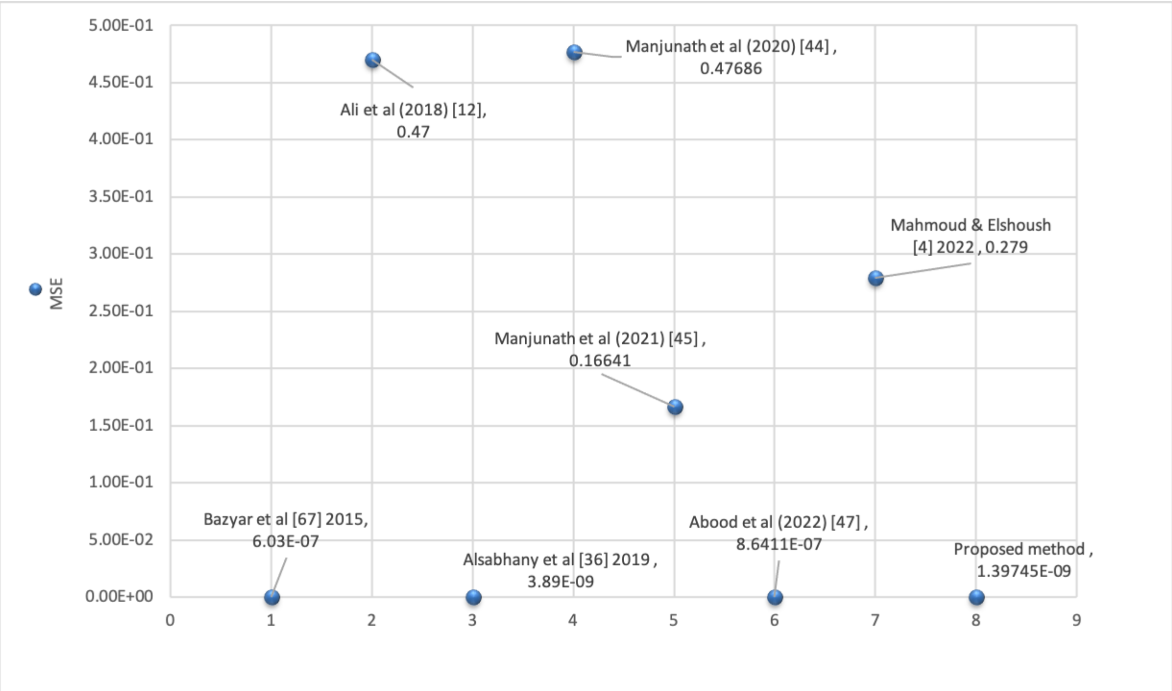


FIGURE 12: MSE values for proposed and conventional related Audio Steganography schemes

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3259902

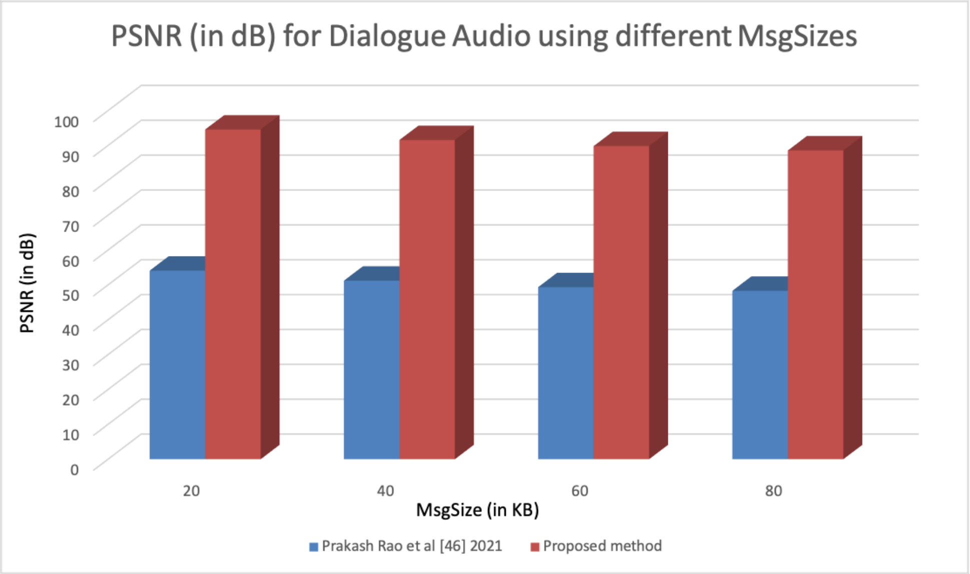


FIGURE 13: PSNR values for Audio Dialogue for Proposed LSB$_{PWLCM}$ method and Prakash Rao et al (2021) [47]

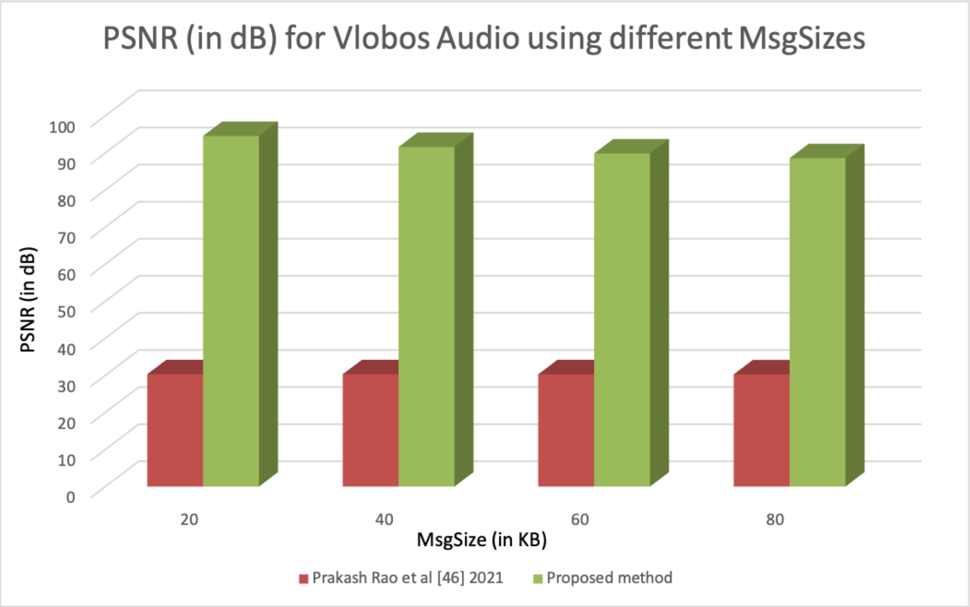


FIGURE 14: PSNR values for Audio Vlobos for Proposed LSB$_{PWLCM}$ method and Prakash Rao et al (2021) [47]

TABLE 6: Comparison of PRD values for the proposed method with related scheme Ali et al [13]

Method	Cover Name	PRD
Ali et al [13] 2018	Dialogue	0.0002
	Female	0.0003
	Jazz	0.0003
Proposed LSB$_{PWLCM}$ method	Dialogue	**0.00034**
	Female	**0.00035**
	Jazz	**0.00035**

TABLE 7: Comparison of BER and NCC values for the proposed method with related scheme [15] and [71]

Method	Cover file	BER	NCC
Bhowal et al [71] 2017	Male	99%	-
	Female	99%	-
	Vlobos	99%	-
Bharti et al [15] 2019	Male	-	0.9404
	Female	-	0.95
	Vlobos	-	0.9966
Proposed LSB$_{PWLCM}$ method	Male	**100%**	**1**
	Female	**100%**	**1**
	Vlobos	**100%**	**1**

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3259902

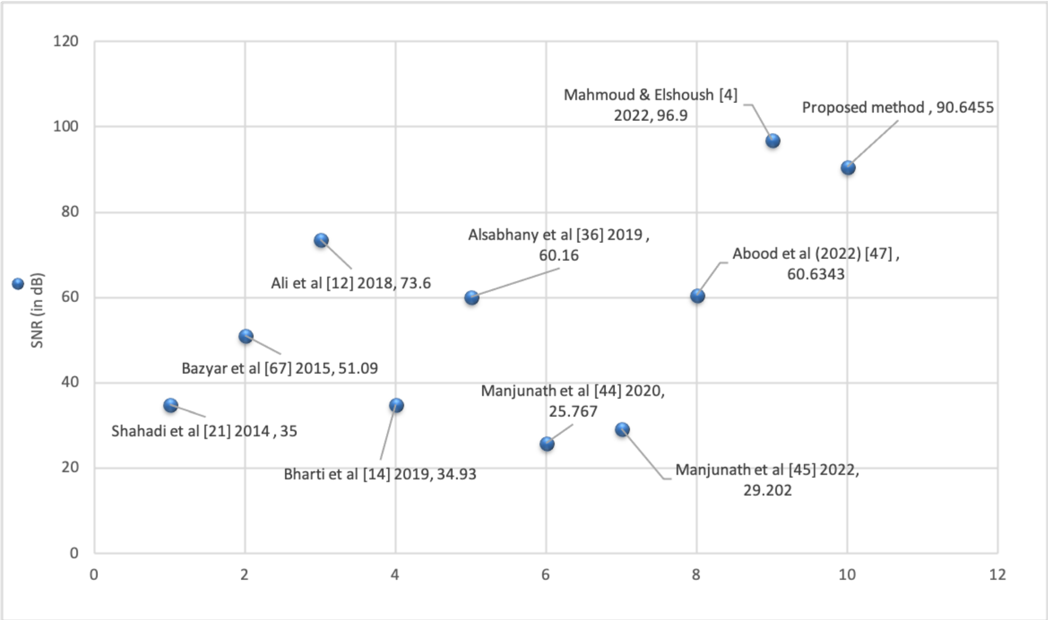


FIGURE 15: SNR values for proposed and conventional related Audio Steganography schemes

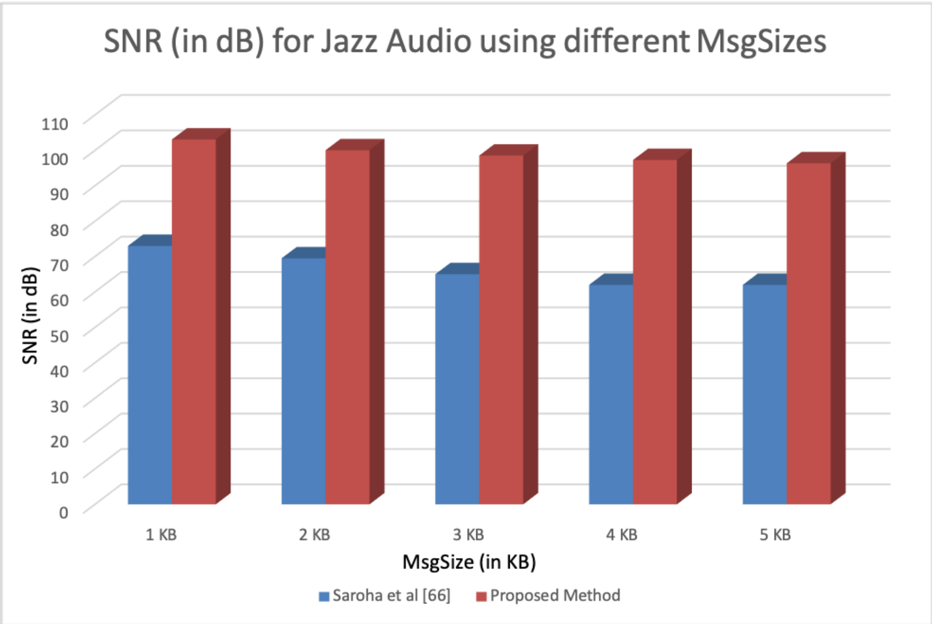


FIGURE 16: SNR values for proposed method juxtaposed with Saroha et al [67] using Jazz audio

TABLE 8: Comparison of Key Space of the Proposed LSB$_{PWLCM}$ Method and Related schemes

	Ali et al [13] 2018	**Mahmoud & Elshoush [4] 2022**	**Abdulkadhim et al [50] 2022**	**Proposed LSB$_{PWLCM}$ Method**
Calculating Key space	four initial parameters each is 2^{64}	AES algorithm 2^{128}	10^{64}	four PWLCM parameters each is 10^{16} $=10^{64}$
		for LSB$_{BMSE}$ algorithm 2^{128}		MsgSize
Total Key space	2^{256}	2^{256}	10^{64}	$\geq 10^{64} \times$ **MsgSize**

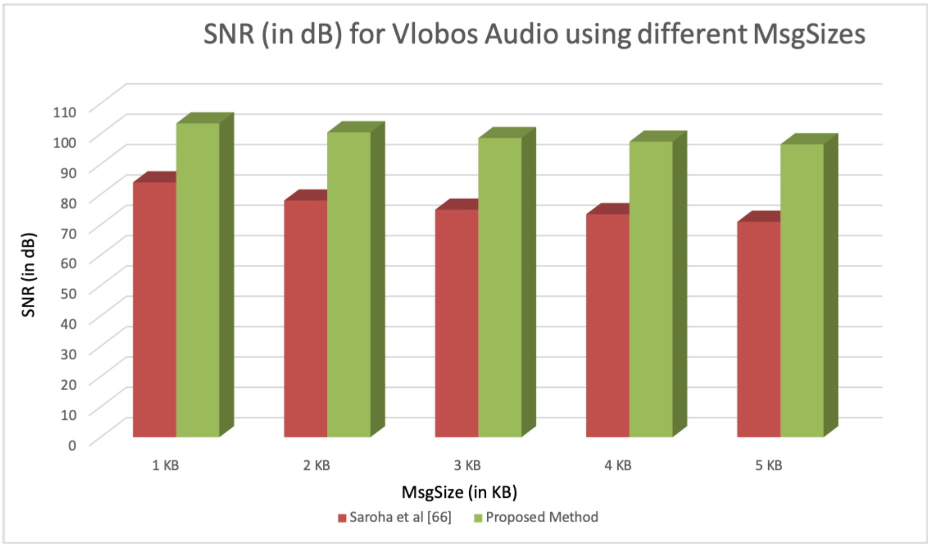


FIGURE 17: SNR values for proposed method compared with Saroha et al [67] using Vlobos audio

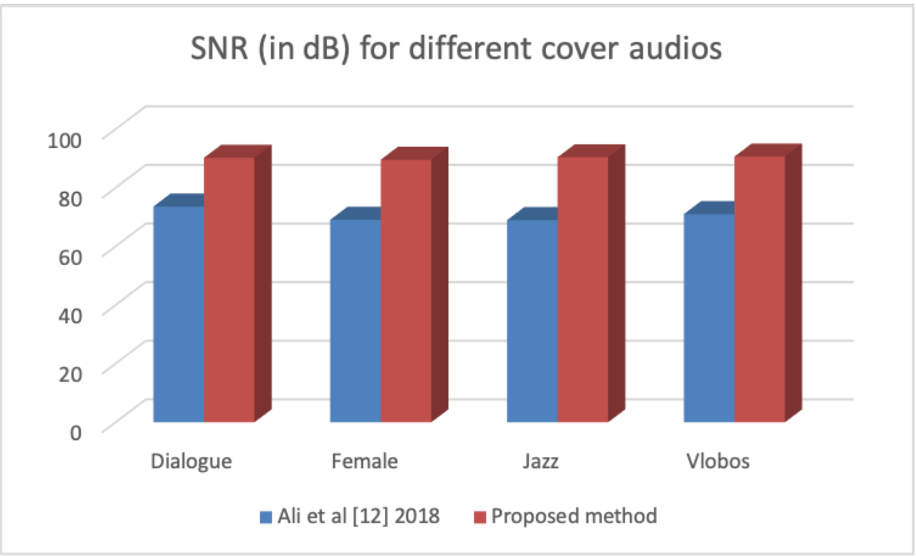


FIGURE 18: SNR values for Proposed LSB$_{PWLCM}$ method and Ali et al [13] 2018

Audio	Reference	HER
Dialougue	Shahadi et al [75] 2014	0.00022909
	Mahmoud & Elshoush [4] 2022	0.0000027722
	Proposed LSB$_{PWLCM}$ method	**0.0000000014**
Jazz	Ali et al [13] 2018	0.1278
	Mahmoud & Elshoush [4] 2022	0.00000028624
	Proposed LSB$_{PWLCM}$ method	**0.0000000014**
Voice	Ali et al [13] 2018	0.0431
	Proposed LSB$_{PWLCM}$ method	**0.0000000014**
Female	Mahmoud & Elshoush [4] 2022	0.0000028586
	Proposed LSB$_{PWLCM}$ method	**0.00000000690724**
Vlobos	Mahmoud & Elshoush [4] 2022	0.0000027513
	Proposed LSB$_{PWLCM}$ method	**0.00000000691938**

TABLE 9: Comparison of the Histogram Error Rate (HER) of the Proposed LSB$_{PWLCM}$ Method with Related Schemes

VI. CONCLUSION AND FUTURE WORK

In this paper, we proposed a novel LSB$_{PWLCM}$ method that enhances LSB audio steganography. Initially, the secret message is lessened using Huffman algorithm, in addition to being encrypted using one-time pad with a key generated using PWLCM thus achieving a dual protection. Actually, the use of PWLCM strengthen the security of one-time pad by ensuring random key generation and large key space, besides only the initial conditions and the system parameters are interchanged in lieu of the complete chaotic sequences solving the key distribution problem. Furthermore, PWLCM was used to generate random numbers which were then converted to integers and sorted in an array to be utilized to select random samples for embedding. Also,

This article has been accepted for publication in IEEE Access. This is the author's version which has not been fully edited and content may change prior to final publication. Citation information: DOI 10.1109/ACCESS.2023.3259902

Audio	Reference	Difference Ratio (DR)			
		1^{st} moment, Average (μ)	2^{nd} moment, variance (σ^2)	3^{rd} moment, skewness (sk)	4^{th} moment, kurtosis (k)
Dialougue	Shahreza et al [72] 2007	1.4951	0.0002531	0.3916	0.0317
	Delforouzi et al [73] 2007	0.1928	0.0000012953	0.0011	0.00161
	Delforouzi et al [74] 2008	1.8731	0.000209	0.4705	0.00736
	Shahadi et al [75] 2014	0.2304	0	0.0004	0.0005
	Proposed LSB$_{PWLCM}$ method	**0.000017**	**0**	**0.000052**	**0.000069**
Jazz	Ali et al [13] 2018	0.0789	0.0014	0.0035	0.0057
	Proposed LSB$_{PWLCM}$ method	**0.000011**	**0**	**0.000033**	**0.000044**
Voice	Ali et al [13] 2018	0.0810	0.0002	0.0002	0.00005
	Proposed LSB$_{PWLCM}$ method	**0.000014**	**0**	**0.000041**	**0.000055**

TABLE 10: Comparison of the Difference Ratio for the Fourth First Moments of the Proposed LSB$_{PWLCM}$ Method with Related Schemes

the integer values of these random generated numbers are further used to select one of the 4-LSBs using a modulo operation. Hence, the embedding is done in arbitrarily blocks in an unsystematic and indeterministic way, and even the choice of the 4-LSBs inside these blocks was also performed in an unforeseen fashion.

The novel LSB$_{PWLCM}$ method was evaluated using two ITU standard perceptual imperceptibility tests, specifically PESQ and PEAQ. In the absence of attack, a range of 4.497 to 4.5 PESQ values were achieved by our proposed method which evince the sameness of the cover and stego audios. Additionally, all PEAQ ODG values were very close to zero even when juxtaposed with current schemes were beyond comparison. Moreover, from the facets of imperceptibility, MSE, PSNR, SNR, PRD and Audio Fidelity imperceptibility tests were also performed. The results were propitious compared to prevailing schemes, where SNR ranges from 80.4408 dB to 90.6455 dB which are well above the acceptable 30 dB and surely attest the superb imperceptibility of our proposed method. Furthermore, it successfully inflated its payload up to 173% and thus affirmed its superiority concerning hiding capacity. Albeit, it proved its resistance to re-sampling attacks, it did not withstand LSB and AWGN attacks due to its essential features of embedding choices. In the case of resampling attack, all BER rates and NCC achieved were 100% and 1's respectively confirming the accurate extraction of the secret messages. In the absence of attack, the quality of the extracted secret message signifies similitude with the original secret message as was obvious with the achieved NCC and BER values. The stego audios were scrutinized against statistical analysis tests and testified great resistance even beyond comparison to existent schemes. It achieved an HER as low as 1.19325E-05 for voice audio whilst all the difference ratios for the Fourth First Moments were very close to zero thus surpassing all prevailing techniques. Furthermore, our proposed method was analyzed from the facet of security and has a prodigious sufficient key space to resist all types of brute-force attacks. The efficacious results of the proposed novel LSB$_{PWLCM}$ method affirmed its superiority to prevailing schemes and proved its efficacy.

For future work, alternate techniques in instead of PWLCM may be scrutinized to attain great results.

.

APPENDIX A IMPLEMENTING THE EMBEDDING ALGORITHM OF THE PROPOSED LSB$_{PWLCM}$ METHOD

This section elucidates the embedding of the proposed LSB$_{PWLCM}$ method.

First, random numbers are generated using PWLCM and stored in an array$_{PWLCM}$. The bits of the secret message are embedded in random blocks of the cover file using the traditional LSB technique according to the index of array$_{PWLCM}$ after sorting it in an ascending (or descending) order. Algorithm 3 details the embedding process.

The following specifications are used:

- Cover file (CF) size = 24 samples (where each sample is 8 bits)
- The initial parameters to generate random numbers for embedding using PWLCM are:
  y=0.879 and p=0.314525;

Cover file CF:

1	2	3	4	5	6
11101011	11110101	11111110	10100001	11111110	11110111
7	**8**	**9**	**10**	**11**	**12**
11110001	11101111	11110011	11111100	10101001	10001110
13	**14**	**15**	**16**	**17**	**18**
10001111	11111001	11110010	11110000	11110100	11111011
19	**20**	**21**	**22**	**23**	**24**
11110111	10001001	10000111	11010100	11111011	11110100

- Secret message (Msg)="ms"
  ASCII code of "m" =109
  ASCII code of "s" =115
  Hence, "m"= "01101101" and "s"="01110011"
  Therefore, "ms"= "0110 1101 0111 0011"

Noteworthy, these sizes were chosen for simplicity. Moreover, the index calculation of CF is made to start from 1 because of the nature of the function, as it will not have a value of zero.

Random numbers generated using PWLCM

0.8790	0.1210	0.3847	0.3784	0.3443	0.1607	0.5111	0.4889	0.9404	0.0596	0.1895	0.6026	0.3974	0.4467	0.7124	0.2876

Converting random numbers generated using PWLCM into integers to construct array$_{IntegerOfRDN}$

0	0	45	175	168	171	52	204	194	62	32	231	25	48	174	82

Indexing the converted random numbers creating array$_{IndexOfRDN}$

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	45	175	168	171	52	204	194	62	32	231	25	48	174	82

Sorting the integer converted random numbers creating array$_{SortedIntRDN}$

1	**2**	**13**	**11**	**3**	**14**	**7**	**10**	**16**	**5**	**6**	**15**	**4**	**9**	**8**	**12**
0	**0**	**25**	**32**	**45**	**48**	**52**	**62**	**82**	**168**	**171**	**174**	**175**	**194**	**204**	**231**

The secret message bits, Msg

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	**1**	**1**	**0**	**1**	**1**	**0**	**1**	**0**	**1**	**1**	**1**	**0**	**0**	**1**	**1**

By converting the random numbers generated by PWLCM to integer numbers, the resulting array$_{IntegerOfRDN}$ is produced.

Then, the integer random numbers are sorted into ascending or descending to produce array$_{SortedIntRDN}$ after being indexed. Note that if the array was sorted in ascending or descending, the same action will done in extraction.

Now the embedding will be performed according to array$_{SortedIntRDN}$. That is to say, the 1^{st} bit (shown in red) of the *Msg* will be inserted in the first sample, the 2^{nd} bit in the second sample, the 3^{rd} in sample no. 13, the 4^{th} in sample no. 11, and so on based on the index (of the sample) of the sorted array$_{SortedIntRDN}$ (indicated in blue). Inside the sample (byte), one of the four LSB bits is chosen according to the integer value of the converted random number, Int$_{RND}$ (presented in orange), and the following equation 19:

$$LSBinsideSample = \begin{cases} 1^{st}LSB & if Int_{RND} mod 4 = 0 \\ 2^{nd}LSB & if Int_{RND} mod 4 = 1 \\ 3^{rd}LSB & if Int_{RND} mod 4 = 2 \\ 4^{th}LSB & if Int_{RND} mod 4 = 3 \end{cases} \tag{19}$$

The following steps clarify the embedding process:

- **Embedding the 1^{st} bit of *Msg*:**
  The first value of Int$_{RND}$ in array$_{SortedIntRDN}$ is 0. Hence,
  Int$_{RND}$ mod 4 = 0 mod 4 =0 ⇒ the 1^{st} bit of *Msg* which is 0 will be embedded in the 1^{st} sample, in 1^{st}LSB, as illustrated in CF$_{SampleEmbedding}$.

CF$_{SampleEmbedding}$ after embedding 1^{st} bit of *Msg*:

1	2	3	4	5	6
1110101**0**	11110101	11111110	10100001	11111110	11110111
7	8	9	10	11	12
11110001	11101111	11110011	11111100	10101001	10001110
13	14	15	16	17	18
10001111	11111001	11110010	11110000	11110100	11111011
19	20	21	22	23	24
11110111	10001001	10000111	11010100	11111011	11110100

- **Embedding the 2^{nd} bit of *Msg*:**
  The second value of Int$_{RND}$ in the array$_{SortedIntRDN}$ is 0. Hence,
  Int$_{RND}$ mod 4 = 0 mod 4 =0 ⇒ the 2^{nd} bit of *Msg* which is 1 will be embedded in the 2^{nd} sample, in 1^{st}LSB, as illustrated in CF$_{SampleEmbedding}$.

CF$_{SampleEmbedding}$ after embedding 2^{nd} bit of *Msg*:

1	**2**	3	4	5	6
1110101**0**	1111010**1**	11111110	10100001	11111110	11110111
7	8	9	10	11	12
11110001	11101111	11110011	11111100	10101001	10001110
13	14	15	16	17	18
10001111	11111001	11110010	11110000	11110100	11111011
19	20	21	22	23	24
11110111	10001001	10000111	11010100	11111011	11110100

- **Embedding the 3^{rd} bit of *Msg*:**
  The third value of Int$_{RND}$ in the Array$_{SortedIntRDN}$ is 25. Hence,
  Int$_{RND}$ mod 4 = 25 mod 4 =1 ⇒ the 3^{rd} bit of *Msg* which is 1 will be embedded in sample number 13 (as indicated by the sorted index), in the 2^{nd}LSB, as illustrated in CF$_{SampleEmbedding}$.

CF$_{SampleEmbedding}$ after embedding 3^{rd} bit of *Msg*:

1	**2**	3	4	5	6
1110101**0**	1111010**1**	11111110	10100001	11111110	11110111
7	8	9	10	11	12
11110001	11101111	11110011	11111100	10101001	10001110
13	14	15	16	17	18
100011**1**1	11111001	11110010	11110000	11110100	11111011
19	20	21	22	23	24
11110111	10001001	10000111	11010100	11111011	11110100

- **Embedding the 4^{th} bit of *Msg*:**
  The fourth value of Int$_{RND}$ in the Array$_{SortedIntRDN}$ is 32. Hence,
  Int$_{RND}$ mod 4 = 32 mod 4 =0 ⇒ the 4^{th} bit of *Msg* which is 0 will be embedded in sample number 11 (as indicated by the sorted index), in the 1^{st}LSB, as illustrated in CF$_{SampleEmbedding}$.

CF$_{SampleEmbedding}$ after embedding 4^{th} bit of *Msg*:

1	**2**	3	4	5	6
1110101**0**	1111010**1**	11111110	10100001	11111110	11110111
7	8	9	10	**11**	12
11110001	11101111	11110011	11111100	1010100**0**	10001110
13	14	15	16	17	18
100011**1**1	11111001	11110010	11110000	11110100	11111011
19	20	21	22	23	24
11110111	10001001	10000111	11010100	11111011	11110100

- **Embedding the 5^{th} bit of *Msg*:**
The fifth value of Int_{RND} in the $\text{Array}_{SortedIntRDN}$ is 45. Hence,
Int_{RND} mod 4 = 45 mod 4 =1 $\Rightarrow$ the 5^{th} bit of *Msg* which is 1 will be embedded in sample number 3 (as indicated by the sorted index), in the 2^{nd}LSB, as illustrated in $\text{CF}_{SampleEmbedding}$.

$\text{CF}_{SampleEmbedding}$ after embedding 5^{th} bit of *Msg*:

1	**2**	**3**	4	5	6
11101010	11110101	11111110	10100001	11111110	11110111
7	8	9	10	**11**	12
11110001	11101111	11110011	11111100	10101000	10001110
13	14	15	16	17	18
10001111	11111001	11110010	11110000	11110100	11111011
19	20	21	22	23	24
11110111	10001001	10000111	11010100	11111011	11110100

- **Embedding the 11^{th} bit of *Msg*:**
Continuing this way, the eleventh value of Int_{RND} in the $\text{Array}_{SortedIntRDN}$ is 171. Hence,
Int_{RND} mod 4 = 171 mod 4 =3 $\Rightarrow$ the 11^{th} bit of *Msg* which is 1 will be embedded in sample number 6 (as indicated by the sorted index), in the 4^{th}LSB, as illustrated in $\text{CF}_{SampleEmbedding}$.

$\text{CF}_{SampleEmbedding}$ after embedding 11^{th} bit of *Msg*:

1	**2**	**3**	4	**5**	**6**
11101010	11110101	11111110	10100001	11111111	11111111
7	8	9	**10**	**11**	12
11110000	11101111	11110011	11111100	10101000	10001110
13	**14**	15	**16**	17	18
10001111	11111001	11110010	11110000	11110100	11111011
19	20	21	22	23	24
11110111	10001001	10000111	11010100	11111011	11110100

- **Embedding all the bits of *Msg*:**
Sustaining this way, all the *Msg* bits are embedded in CF sample as demonstrated in $\text{CF}_{SampleEmbedding}$.

$\text{CF}_{SampleEmbedding}$ after embedding ALL bits of *Msg*:

1	**2**	**3**	**4**	**5**	**6**
11101010	11110101	11111110	10100001	11111111	11111111
7	**8**	**9**	**10**	**11**	**12**
11110000	11101111	11110011	11111100	10101000	10001110
13	**14**	**15**	**16**	17	18
10001111	11111001	11110110	11110000	11110100	11111011
19	20	21	22	23	24
11110111	10001001	10000111	11010100	11111011	11110100

ACKNOWLEDGMENT

H. Elshoush and M. Mahmoud contributed equally to this work.

REFERENCES

[1] A. Kumar and K. K. KM, "Enhanced LSB Algorithm For Stegano Communication," *in Journal of Web Development and Web Designing*, vol. 1, no. 3, 2016.

[2] T. K. Hazra, M. Haldar, M. Mukherjee and A. K. Chakraborty, "A Survey on Different Techniques for Covert Communication Using Steganography," *IOSR Journal of Computer Engineering (IOSR-JCE)*, vol. 20, no. 2, ver. II (Mar. - Apr. 2018), pp. 42-52. e-ISSN: 2278-0661, p-ISSN: 2278-8727, www.iosrjournals.org.

[3] S. M. Alwahbani and H. T. Elshoush, "Chaos-Based Audio Steganography and Cryptography Using LSB Method and One-Time Pad," *in Proc. of SAI Intelligent Systems conf.*, Springer, Cham, Sept. 2016, pp. 755-768.

[4] M. M. Mahmoud and H. T. Elshoush, "Enhancing LSB Using Binary Message Size Encoding for High Capacity, Transparent and Secure Audio Steganography–An Innovative Approach," *IEEE Access*, vol. 10, pp. 29954-29971, 2022, doi: 10.1109/ACCESS.2022.3155146.

[5] De Rosal Ignatius Moses Setiadi, Supriadi Rustad, Pulung Nurtantio Andono, Guruh Fajar Shidik, "Digital image steganography survey and investigation (goal, assessment, method, development, and dataset," *Signal Processing*, vol. 206, 2023, 108908, ISSN 0165-1684, https://doi.org/10.1016/j.sigpro.2022.108908.

[6] N. Kaur and A. Kaur, "Art of Steganography," *Int. Journal of Advanced Trends in Computer App. (IJATCA)*, vol 4, no. 2, pp. 30-33, Feb. 2017.

[7] R. Chakraborty and A. Roy. "Audio Steganography - A Review," *Int. Journal of Trend in Research and Development*, vol. 6, no. 3, ISSN: 2394-9333. www.ijtrd.com. Jul. 2019.

[8] P. Bhitre and M. R. Sayankar, "A Review on Audio and Video based Steganography for Data Hiding," *IJSRSET*, vol. 4, no. 1, Print ISSN: 2395-1990. Online ISSN: pp. 2394-4099. Themed Section: Engineering and Technology. 2018.

[9] M. M. Mahmoud and H. T. Elshoush, "A Novel Enhanced LSB Algorithm for High Secure Audio Steganography," *in Proc. of IEEE CEEC, U.K.*, Sept. 2018.

[10] M. H. N. Azam, F. Ridzuan, M. N. S. M. Sayuti, and A. A. Alsabhany, "Balancing the Trade-Off Between Capacity and Imperceptibility for Least Significant Bit Audio Steganography Method: A New Parameter," *in Proc. of IEEE conf. on Application, Information and Network Security (AINS)*, 2019.

[11] A. A. Alsabhany, F. Ridzuan and A. H. Ab Halim, "The Adaptive Multi-Level Phase Coding Method in Audio Steganography," *IEEE Access*, Sept. 2019.

[12] J. Kour and D. Verma, "Steganography Techniques –A Review Paper," *Int. Journal of Emerging Research in Management &Technology*, ISSN: 2278-9359. vol. 3, no. 5, May 2014.

[13] A. H. Ali, L. E. George, A. A. Zaidan and M. R. Mokhtar, "High Capacity, Transparent and Secure Audio Steganography Model Based on Fractal Coding and Chaotic Map in Temporal Domain," *Multimed Tools Applications*, Jun. 2018.

[14] A. H. Ali, M. R. Mokhtar and L. E. George, "Enhancing The Hiding Capacity Of Audio Steganography Based On Block Mapping," *Journal of Theoretical and Applied Information Tech.*, vol. 95, no. 7, Apr. 2017.

[15] S. S. Bharti, M. Gupta, and S. Agarwal, "A Novel Approach for Audio Steganography by Processing of Amplitudes and Signs of Secret Audio Separately," *Multimed Tools Applications.* vol. 78, pp. 23179-23201, 2019.

[16] J. Chaharlang, M. Mosleh and S. Rasouli-Heikalabad, "A Novel Quantum Steganography - Steganalysis System for Audio Signals," *Multimedia Tools and Applications*, Feb. 2020.

[17] 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. 3925–3957, Jan. 2020.

[18] P. Xuea, H. Liu, J. Hu and R. Hu, "A Multi-Layer Steganographic method Based on Audio Time Domain Segmented and Network Steganography," *presented at the 6th Int. conf. on Computer-Aided Design, Manufacturing, Modeling And Simulation (CDMMS 2018)*, vol. 1967, pp. 020-046. 10.1063/1.5039018. May 2018.

[19] M. H. A. Al-Hooti, T. Ahmad and S. Djanali, "Audio Data Hiding Using Octal Modulus Function Based Unsigned Integer Sample Values," *in proc. of the Int. conf. on Computer Engineering, Network and Inteeligent Multimedia (CENIM) - IEEE*, pp. 48-53. 2018.

[20] G. Xin, Y. Liu, T. Yang and Y. Cao. "An Adaptive Audio Steganography for Covert Wireless Communication," *Wiley, Hindawi. Security and Communication Networks*, vol. (2018), Article ID 7096271, 10 pages https://doi.org/10.1155/2018/7096271.

[21] A. Kanhe and G. Aghila, "DCT based Audio Steganography in Voiced and Un-voiced Frames," *presented at the ICIA '16*, August 25-26, 2016, Pondicherry, India. 2016 ACM.

[22] H. I. Shahadi, R. Jidin and W. H. Way, "A Novel and High Capacity Audio Steganography Algorithm Based on Adaptive Data Embedding Positions," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 7, no. 11, pp. 2311-2323. ISSN: 2040-7459. Mar. 2014.

[23] P. Manimegalai, K. S. Gomathi, D. Ponniselvi and M. Santha, "The Image Steganography and Steganalysis Based on Peak-Shaped Technique for Mp3 Audio and Video," *Int. Journal of Computer Science and Mobile Computing*, vol.3, no. 1, pp. 300-308, Jan. 2014.

[24] A. H. Ali, M. R. Mokhtar and L. E. George, "A Review on Audio Steganography Techniques," *Research Journal of Applied Sciences, Engineering and Technology*, vol. 12, no. 2, pp. 154-162. DOI:10.19026/rjaset.12.2316. ISSN:2040-7459; e-ISSN: 2040-7467. Jan. 2016.

[25] H. Dutta, R. K. Das, S. Nandi and S. R. M. Prasanna, "An Overview of Digital Audio Steganography," *IETE Technical Review*, Dec. 2019.

[26] A. Chadha, N. Satam, R. Sood, D. Bade, "An Efficient Method for Image and Audio Steganography using Least Significant Bit (LSB) Substitution," *Int. Journal of Computer Applications (0975 – 8887)*, vol. 77, no.13, Sept. 2013.

[27] A. O. Timothy, A. A. Olusola and G. Arome Junior, "Embedding Text in Audio Steganography System using Advanced Encryption Standard, Text Compression and Spread Spectrum Techniques in Mp3 and Mp4 File Formats," *Int. Journal of Computer Applications (0975 – 8887)*, vol. 177, no. 41, Mar. 2020.

[28] M. Tang et al, "An Adaptive Image Steganography Using Ambtc Compression and Interpolation Technique," *Optik-Int. Journal for Light and Electron Optics*, vol. 127, no. 1, pp. 471–477, 2016.

[29] S. Ali, L. E. George and H. B. Taher, "Speeding up Audio Fractal Compression," *Int. Journal of Advanced Research in Computer Science and Software Engineering*, vol. 3, no. 6, pp. 86-92, 2013.

[30] A. A. Alsabhany, F. Ridzuan and A. H. Ab Halim, "The Progressive Multilevel Embedding Method for Audio Steganography," *Journal of Physics: conf. Series 1551. 012011*, 2020

[31] M. Sharma, "Compression using Huffman coding," *Int. Journal of Computer Science and Network Security (IJCSNS)*, vol. 10, no. 5, pp. 133-141, 2010.

[32] X. Yi, K. Yang, X. Zhao, Y. Wang and H. Yu, "AHCM: Adaptive Huffman Code Mapping for Audio Steganography Based on Psychoacoustic Model," *IEEE Transactions On Information Forensics And Security*, vol. 14, no. 8, pp. 2217-2231, Aug. 2019.

[33] S. M. Alwahbani and H. T. Elshoush, "Hybrid Audio Steganography and Cryptography Method Based on High Least Significant Bit (LSB) Layers and One-Time Pad—A Novel Approach," *Book chapter: Dr. Yaxin Bi editor. Studies in Computational Studies*, published by Springer, pp. 431-453, book series (SCI, vol. 751), Jan. 2018.

[34] M. J. Hussain and K. F. Rafat, "Enhanced Audio LSB Steganography for Secure Communication," *Int. Journal Of Advanced Computer Science And Applications*, vol. 7, no. 1, pp. 340-347. 2016.

[35] G. M. Kamau, "An enhanced least significant bit steganographic method for information hiding," M.S. thesis, Software Engineering,

Jomo Kenyatta Univ. of Agriculture and Technology, 2013.(Online). Available: http://ir.jkuat.ac.ke/bitstream/handle/123456789/1504/Kamau

[36] J. R. Krenn, "Steganography and steganalysis", Jan. 2004. (Online). Available: https://www.krenn.nl/univ/cry/steg/article.pdf

[37] F. Djebbar, B. Ayad, H. Hamam and K. Abed-Meraim, "A View on Latest Audio Steganography Techniques," *presented at the Int. conf. on Innovations in Information Technology, AbuDhabi*, pp. 409-414, 2011.

[38] P. G. P. J. ST, B. Hidayat and F. Y. Suratman, "Enhanced LSB Steganography with people detection as stego key generator," *presented at the Int. conf. on Signals and Systems (ICSigSys)*, IEEE, pp. 99-104, May 2017.

[39] H. Ghasemzadeh and M. K. Arjmandi, "Universal Audio Steganalysis Based on Calibration and Reversed Frequency Resolution of Human Auditory System," *IET Signal Processing*, vol. 11, no. 8, 2017.

[40] M. L. M. Kiah, B. B. Zaidan, A. A. Zaidan, A. M. Ahmed and S. H. Al-bakri, "A Review of Audio Based Steganography and Digital Watermarking," *Int. Journal of the Physical Sciences*, vol. 6, no.16, pp. 3837-3850, Aug. 2011.

[41] A. Awad and A. Saadane, "New Chaotic Permutation Methods for Image Encryption," *IAENG Int. Journal of Computer Science*, vol. 37, no. 4, Nov. 2010.

[42] S. Krishnan and M. S. Abdullah, "Enhanced Security Audio Steganography by Using Higher Least Significant Bit," *Journal of Advanced Research in Computing and Applications*. ISSN (online): 2462-1927, vol. 2, no. 1, pp. 39-54, 2016.

[43] S. Save, P. Raut, P. Jadhav and T. Yadav, "Data Security using Audio-Video Steganography," *Int. Journal of Engineering Research & Technology (IJERT)*, vol. 7, no. 02, Feb. 2018. http://www.ijert.org ISSN: 2278-0181.

[44] C. T. Jian, C. C. Wen, N. H. B. Ab. Rahman and I. R. B. A. Hamid, "Audio Steganography with Embedded Text," *Int. Research and Innovation Summit (IRIS2017) - IOP Publishing - IOP Conf. Series: Materials Science and Engineerin1g23242566(72809107) 012084*, 2017

[45] K. Manjunath, G.N. Kodanda Ramaiah, Dr.M.N. Giri Prasad, "An efficient audio steganography technique using hybridization of compression and cryptography algorithm," *J. Adv. Res. Dyn. Control Syst.* vol. 11, 10-Special Issue, pp. 132–147, 2020.

[46] K. Manjunath, G.N. Kodanda Ramaiah, M.N. Giri Prasad, "Backward movement oriented shark smell optimization-based audio steganography using encryption and compression strategies," *Digital Signal Processing*, vol 122, pp. 1-13, 2022. https://doi.org/10.1016/j.dsp.2021.103335

[47] Shirole Rashmi Prakash Rao and K. Jyothi, "A Novel Audio Steganography Technique Integrated with a Symmetric Cryptography: A Protection Mechanism for Secure Data Outsourcing," *Int. Journal of Computational Science and Engineering*, vol. 24 no. 5, 2021.

[48] Enas Wahab Abood, Abdulhssein M. Abdullah, Mustafa A. Al Sibahe, Zaid Ameen Abduljabbar, Vincent Omollo Nyangaresi, Saad Ahmad Ali Kalafy, Mudhafar Jalil Jassim Ghrabta, "Audio steganography with enhanced LSB method for securing encrypted text with bit cycling," *Bulletin of Electrical Engineering and Informatics*, vol. 11, no. 1, pp. 185-194, Feb. 2022. https://doi.org/10.11591/eei.v11i1.3279

[49] R. Tanwar, K. Singh, M. Zamani, A. Verma and P. Kumar, "An Optimized Approach for Secure Data Transmission Using Spread Spectrum Audio Steganography, Chaos Theory, and Social Impact Theory Optimizer," *Hindawi Journal of Computer Networks and Communications*, vol. 2019, Article ID 5124364, 10 pages. https://doi.org/10.1155/2019/5124364.

[50] Hussein Abdulameer Abdulkadhim, Jinan Nsaif Shehab, "Audio steganography based on least significant bits algorithm with 4D grid multi-wing hyper-chaotic system," *Int. Journal of Electrical and Computer Engineering (IJECE)*, vol. 12, no. 1, pp. 320-330, Feb. 2022. ISSN: 2088-8708, DOI: 10.11591/ijece.v12i1.pp320-330

[51] S. Roy, A. K. Singh, J. Parida and A. S. Sairam, "Audio Steganography Using LSB Encoding Technique with Increased Capacity and Bit Error Rate Optimization," *presented at the CCSEIT-12, Oct. 26-28, 2012, Coimbatore*, Oct. 2012.

[52] M. A. Ahmed, M. L. Mat Kiah, B. B. Zaidan and A. A. Zaidan, "A novel embedding method to increase capacity and robustness of low-bit encoding audio steganography technique using noise gate software logic algorithm," *J Appl Sci*, vol. 10, no.1, pp. 59–64, 2010.

[53] S. Gudla, S. Reyya, A. Kotyada and A. Sangam, "Key Based Least Significant Bit (LSB) Insertion for Audio and Video Steganography," *Int. Journal of Computer science and Engineering Research and Development (IJCSERD)*, ISSN 2248 – 9371 (Online), vol. 3, no. 1, pp. 60-69, Jan- Mar. 2013.

[54] A. A. Alsabhany, F. Ridzuan and A. H. Ab Halim, "An Adaptive Multi Amplitude Thresholds Embedding Algorithm for Audio Steganography," *Malaysian Journal of Science, Health & Technology (MJoSHT)*, vol. 2, 2018, Special Issue, eISSN: 2601-0003. http://mjosht.usim.edu.my/index.php/mjosht/article/view/43.

[55] G. Tzanetakis, "Music Analysis, Retrieval and Synthesis for Audio Signals (Marsyas)," *22-11, 2015*; Available from: http://marsyasweb.appspot.com/download/data-sets/. 2009.

[56] G. Tzanetakis and P. Cook, "Musical genre classification of audio signals," *IEEE Transactions on speech and audio processing*, vol. 10, no. 5, pp. 293-302, 2002

[57] "Recommendation IT (2001) Perceptual evaluation of speech quality (PESQ): An objective method for end-to-end speech quality assessment of narrow-band telephone networks and speech codecs. Rec. Standard ITU-T P862.2"

[58] "Recommendation P (2005) Application Guide for objective quality measurement based on recommendation. ITUt 862.3:862"

[59] K. Bhowal, "Multilevel Steganography to Improve Secret Communication," *Book chapter in IntechOpen.* Available: http://dx.doi.org/10.5772/intechopen.81599. (2019).

[60] Yang, K., Yi, X., Zhao, X., Zhou, L. (2017), "Adaptive MP3 Steganography Using Equal Length Entropy Codes Substitution," in *Digital Forensics and Watermarking. IWDW 2017. Lecture Notes in Computer Science*, Kraetzer, C., Shi, YQ., Dittmann, J., Kim, H. (eds), vol. 10431. Springer, Cham. https://doi.org/10.1007/978-3-319-64185-0-16.

[61] Dinu Campeanu and Andrei Campeanu, "PEAQ - An Objective Method to Assess the Perceptual Quality of Audio Compressed Files," *2004*.

[62] Matteo Torcoli, Thorsten Kastner, and Jürgen Herre, "Objective Measures of Perceptual Audio Quality Reviewed: An Evaluation of Their Application Domain Dependence," *IEEE/ACM Transactions On Audio, Speech, And Language Processing*, vol. 29, pp. 1530- 1541, 2021.

[63] R. D. Ra, D. Pugazhenthi, "Ideal Sampling Rate to reduce distortion in Audio Steganography," *presented at the Int. conf. on Computational Modeling and Security (CMS 2016). Procedia Computer Science*, vol. 85 (2016) pp. 418 – 424. Science Direct. July 2016.

[64] F. Djebbar, B. Ayad, K. A. Meraim and H. Hamam, "Comparative Study Of Digital Audio Steganography Techniques," *Journal on Audio, Speech, and Music Processing (EURASIP)*, vol 25, 2012 http://asmp.eurasipjournals.com/content/2012/1/25.

[65] Yuling Luo, Ronglong Zhou, Junxiu Liu, Yi Cao, and Xuemei Ding, "A parallel image encryption algorithm based on the piecewise linear chaotic map and hyper-chaotic map," *Nonlinear Dynamic*, vol. 93, pp. 1165–1181, 2018. https://doi.org/10.1007/s11071-018-4251-9.

[66] Yuping Hu, Congxu Zhu, Zhijian Wang, "An Improved Piecewise Linear Chaotic Map Based Image Encryption Algorithm," *The Scientific World Journal*, vol. 2014, Article ID 275818, 7 pages, 2014. https://doi.org/10.1155/2014/275818

[67] Kriti Saroha and Pradeep Kumar Singh, "A Variant of LSB Steganography for Hiding Images in Audio," *Int. Journal of Computer Applications*, (0975 – 8887) vol. 11, no. 6, Dec. 2010.

[68] Mohsen Bazyar, Rubita Sudirman, "A New Method to Increase the Capacity of Audio Steganography Based on the LSB Algorithm," *J. Teknologi*, vol. 74, no. 6, pp. 49–53, 2015.

[69] F. A. P. Petitcolas, "MP3Stego," *http://www.cl.cam.ac.uk/fapp2/steganography /mp3stego/index.html*, 2002.

[70] Yan Diqun, Wang Rangding, and Zhang Liguang, "Quantization Step Parity-based Steganography for MP3 Audio," *Fundamenta Informaticae*, vol. 97, pp. 1–14, IOS Press 2009. DOI 10.3233/FI-2009-190.

[71] Krishna Bhowal, Debasree Sarkar, Susanta Biswas, Partha Pratim Sarkar, "A Steganographic Approach to Hide Secret Data in Digital Audio based on XOR Operands Triplet Property with High Embedding Rate and Good Quality Audio," *Turkish Journal of Electrical Engineering & Computer Sciences*, vol. 25, pp. 2136 – 2148, 2017.

[72] Shirali-Shahreza S, Manzuri-Shalmani MT., "Adaptive wavelet domain audio steganography with high capacity and low error rate," *presented at the IEEE Int. conf. on Information and Emerging Technolog (ICIET), 2007, Karachi, Pakistan*, pp. 1–5, 2007

[73] Pooyan M, Delforouzi A., "LSB-based audio steganography method based on lifting wavelet transform," *in proc. of the 7th IEEE Int. Symp. on Signal Processing and Information Technology (ISSPIT'07), 2007 Dec 15–18, Egypt*, pp. 600–03.

[74] Delforouzi A, Pooyan M., "Adaptive digital audio steganography based on integer wavelet transform," *Circuits, Systems & Signal Processing*, vol. 27, no. 2, pp. 247–59, 2008.

[75] Haider Ismael Shahadi, Razali Jidin and Wong Hung Way, "Lossless Audio Steganography based on Lifting Wavelet Transform and Dynamic Stego Key," *Indian Journal of Science and Technology*, vol. 7, no. 3, pp. 323-334, 2014. DOI: 10.17485/ijst/2014/v7i3.14

HUWAIDA T. ELSHOUSH received the bachelor's degree in computer science (division 1), the master's degree in computer science, and the Ph.D. degree in information security from the Faculty of Mathematical Sciences and Informatics, University of Khartoum, Sudan, in 1994, 2001, and 2012, respectively.

Her M.Sc. dissertation dealt with Frame Relay Security. She is currently an Associate Professor within the Computer Science Department, Faculty of Mathematical Sciences and informatics, University of Khartoum, where she is also acting as the Head of Research office. She has more than 26 publications and some of her publications appeared in Applied Soft Computing Journal (Elsevier), PLOS One Journal, IEEE Access, Multimedia Tools and Applications, PeerJ Computer Science, Journal of Information Hiding and Multimedia Signal Processing and Springer book chapters. Her research interests include the information security, cryptography, steganography, and intrusion detection systems. She is a reviewer of many international reputable journals related to her fields, including Applied Soft Computing Journal (Elsevier).

Dr. Elshoush's awards and honors include the second-place prize in the ACM Student Research Competition SRC - SAC in 2013 in Coimbra, Portugal. Additionally, her article entitled "An Improved Framework for Intrusion Alert Correlation" has been awarded the Best Student Paper Award of the 2012 International Conference of Information Security and Internet Engineering (ICISIE) in WCE 2012. Other prizes were the best student during the five years of her undergraduate study.

MAHMOUD M. MAHMOUD received the B.Sc. (Honour) degree from Faculty of Mathematical and Computer Science, University of Gazera, Sudan, and his M.Sc. degree from the Faculty of Mathematical Sciences and Informatics, University of Khartoum, Sudan. He has four publications, one appearing in Multimedia Tools and Applications. His research interests include cryptography, information security and steganography. Currently he is a PhD student in the Faculty of Mathematical Sciences and Informatics, University of Khartoum, Sudan.