Providing an Optimal Way to Increase the Security of Data Transfer using Watermarking in Digital Audio Signals

Saeed Talati[1], Pouriya Etezadifar[2*]
1- Department of Computer Engineering, Imam Hossein University, Tehran, Iran.
Email: saeed.talati@yahoo.com
2- Department of Communications, Imam Hossein University, Tehran, Iran.
Email: petezadifar@ihu.ac.ir (Corresponding Author)

Received: October 2019 Revised: December 2019 Accepted: February 2020

ABSTRACT:
The human ear is aware of a wide range of sound signal amplitudes, so signal-based amplitude marking techniques have their own complexity. This article uses Watermarking to insert the message in the audio coverage and its main purpose is to keep this information hidden for others. There are many benchmarks for evaluating insertion and extraction algorithms that, by performing multiple attacks on an algorithm, increase the ability of the method. (Resilience, Transparency and Capacity for Use). Although the LSB method is superior to other encryption techniques, it is highly vulnerable to all kinds of attacks and attacks, including Additive White Gaussian Noise. This article introduces a new idea for Watermarking voice data encryption, based on the LSB method, which follows similar bits with bits instead of pasting information. The message will be in 16-bit samples, given the introduction of the distortion reduction algorithm for the changes we have made to the signal bits for the receiver's awareness, which could be a new way of causing F of its resistance additive white Gaussian noise and LSB standard will also improve the transparency of the procedure and the method for reducing the capacity has been used.

KEYWORDS: Watermarking, Coding, Audio Signal, LSB.

1. INTRODUCTION

Watermarking is one of the parts of information security [1, 2]. The subject matter is the knowledge of designing and evaluating the methods of concealing original information and important in the context of other information [3]. The hidden information may have a distinctive nature of the "hidden information" [4, 5]. And that's usually the case. The widespread availability of multimedia media, information environments today has made this knowledge essential [6]. The use of watermarking tools in the public internet information and in the simplification of the work in this interconnected space make it possible [7]. That any data, audio or video file can contain unauthorized and confidential information, the only original recipient of which is capable of being disclosed [8].

In this article, we first introduce the most important data used, then introduce evaluation criteria and propose the proposed method. Then the proposed method is compared with other methods and the evaluation results are discussed and finally the evaluation results and comparisons are presented.

2. DATA USED

Audio and video signals and messages are among the most common platforms for executing Watermarking processes. Images are smaller in volume than other host messages. For example, in an 8-bit 800 x 800 pixel image, there is approximately 40 kbyte of space for the hidden message. The same information can be hidden within 5 seconds of a phone conversation.

Watermarks have also shifted their focus to the types of "centralized" audio signals. From WAV, MIDI, MP3, Etc files to analogue voice chat and even music soundtracks, all of them have all been used as an encoder.

For example, a message can be encoded using a musical note using the encoded substitution method, such as setting F-sharp to 0 and C to 1 equivalent. In this way, an ordinary piece of music can be combined with a confidential message, or a piece of music corresponding to an encoded pattern that represents a message. .

The general format, used to display a high quality digital audio signal, is a linear quadratic format with 16 bit resolution like 4wav format. Lower audio quality at the 8-bit logarithmic scale is μ-Law. The resulting

quantization results in a distortion in the signal, which in the 8-bit sample is unobservable.

Acceptable sampling rates for audio signal include 8, 9.6, 10, 12, 16, 22.5 and 44.1kHz. Sampling rates affect data hiding. Because it places a limit on the useful area of the frequency spectrum.

Fig. 1 shows the general model of a watermarking system where f is a function that the enemy applies to the signal (s) so that the receiver cannot extract it if the message is present. (It can also include the channel's undesired effect on s). The rest of the acronyms are described below.

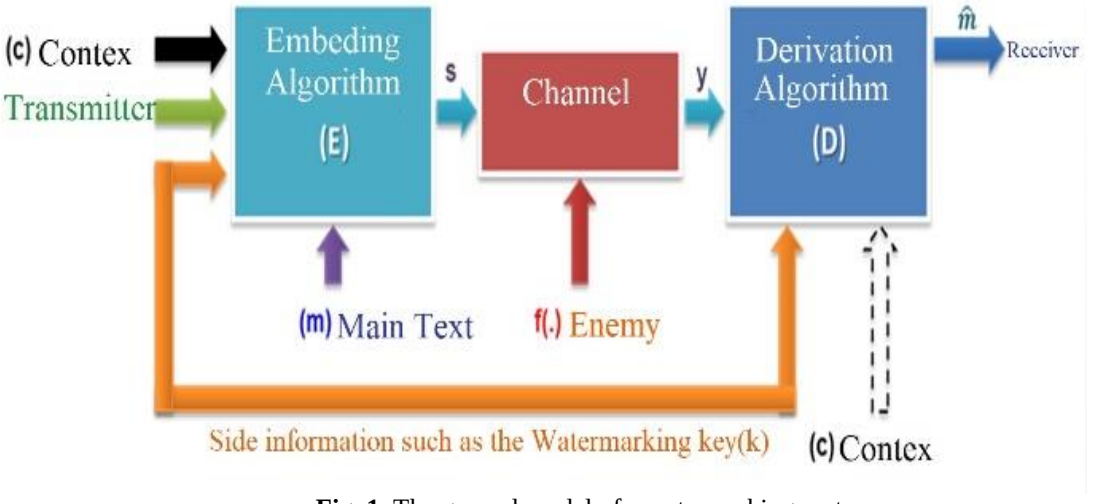

Fig. 1. The general model of a watermarking system.

Information from the Context, transmitter, and channel side information such as the key of Watermarking along with the Main text of the message is embedded into the algorithm and from there the information is entered into the channel of transmission where may be present after passing through the channel, The information is extracted into the algorithm, which is retrieved by comparing the host signal to the original text information.

3. CHARACTERISTICS OF A WATERMARKING SYSTEM

Three important factors in watermarking that there is always a compromise between them are:

Capacity (C), Resistance (R) and Transparency (V). Optimization of cross-parameters is competitive and clearly cannot be done at one time (such as strong distortion resistance and large message embedding).

3.1. Transparency

Intolerance is the issue of human perception (auditory and visual) system, which is the amount of immunity to change that is perceived by the information contained in the host media.

3.2. Resistance

Resistance or resistance to deliberate and unintentional attacks has been suggested, indicating how much the extraction algorithm is capable of recovering the original signal from the received signal (after the attack).

3.3 Capacity

Capacity is the maximum amount of data that can be stored in a carrier without detection. This concept is sometimes referred to as efficiency.

4. CRITERIA FOR WATERMARKING EVALUATION

The following are some criteria to calculate the intangible coefficient:

4.1. MSE

MSE is a measure of the error mean squared. This error is subtracted from the original value by the value after watermarking, which is calculated as follows:

$$MSE = \frac{\sum_k \sum_{i=1}^{M} \sum_{j=1}^{N} (I[i,j]_k - I'[i,j]_k)^2}{3MN} \quad (1)$$

M and N denote the height and width, and I the main data and I' the data after watermarking.

4.2. PSNR

As mentioned before, one of the features of watermarking is invisibility. What is invisible to human is that an ordinary person cannot hear the difference between two sounds when they hear the original voice and the voice containing the message. Since this criterion is not accurate, a criterion has to be defined to measure the performance of the algorithms in terms of security, which is the PSNR criterion, and this

comparison represents the amount of noise added to the watermark by the embedded information in the original sound. The unit is db, and the higher the SNR, the better the watermarking sound. The PSNR is calculated from the following relation:

$$PSNR = 10\,log\,\frac{(2^n-1)^2}{MSE} \quad (2)$$

4.3. BER

The BER is used to calculate the error resulting from the embedding and retrieval of data from the sound, expressed as the percentage of error bits extracted from the sound, relative to the total embedded bits in the cover sound, as calculated below.

$$BER = ((\sum_{i=1}^{l}(M(i) - M'(i))\text{^}2)/l\,) * 100 \quad (3)$$

Where, M(i), bit (i) of the message embedded in the sound, and M'(i), bit (i) of the message extracted. L is also the length of the message or the total number of bits embedded in the sound. Obviously, the lower the BER, the better and more desirable the method. We will continue to explore different ways of watermarking.

Information from the host signal, transmitter, and channel side information such as the Watermark key along with the original text of the message is embedded into the algorithm and from there the information is entered into the channel of transmission where the enemy may be present after passing through the channel, The information is extracted into the algorithm, which is retrieved by comparing the host signal to the original text information.

5. PROPOSED LSB METHOD

In this section, the idea of watermarking of sound information based on the LSB method with greater resistance to Additive white noise is presented. This method is based on the standard LSB method. The basic idea behind this method is to look for bits in each audio sample that are equal to the bits of hidden information, and then inform the recipient in a way that they will pick out specific bits of each sample and put them together, Receive secret information. Clearly, in this idea, the placement of hidden information does not really mean placement, and as a result, the transmission of this information does not cause any distortion in the host signal. But on the other hand this time it is the transmitter-to-receiver information method, which is based on the LSB method and causes distortion in the host signal.

The proposed LSB method informs that the maximum distortion generated can be selected (8 or 16) at the quantized level. This (8 or 16) level of contrast versus ($2^{16} = 65536$) the level of quantization for a 16-bit quantized signal is negligible. The first point in the proposed method is that the receiver in each sample of the audio signal is to seek a few bits equal to the hidden message and secondly to search for the message in which sample bits of the audio signal.

Given that the samples are 16 bits, there are $2^{(16-K)}$ levels whose k bits are similar to the k bits of the message, it is clear that as we increase k, the probability of finding k bits is equal to The message is reduced.

$$\mathrm{P} = \frac{2^{16-\mathrm{k}}}{2^{16}} = \frac{1}{2^{\mathrm{k}}} \quad (4)$$

P is the probability that each sample of the k-bit audio signal is equal to the desired message.

As a result, the choice of K can vary depending on the length of the host signal and the desired hiding capacity. That is, for example, if we know that host signals generally have a relatively good time span, then one can search for more bits, and since the host signal time is relatively long, one can be sure that samples with bits are equal. But if the duration of host signals is generally shorter, then it is better to choose k less. Another point is to look for which K bits are equal to the message in the received audio signal samples. Are the bits (1 to K), (i to i + K), or the total K bits of the MSB equal to the hidden message.

At first glance, perhaps the K-bit of the MSB is the best option, since then it could be almost completely free of the effects of the white Gaussian noise. But the point is that as we move from the LSB to the MSB, the bitrate is reduced and as a result more samples should be searched to find the desired K bit and in many cases the whole message will not be available.

In our simulations, we searched for 4 bits equal to the message bits and in the 7^{th} to 10^{th} bit locations. The last issue with the proposed LSB method is how the receiver is informed of the presence of bits equal to the message in the received audio signal samples. In this method we have used the 5^{th} and 6^{th} bits of each sample for this purpose. That is, if these two bits have a value of [a5a6 = $(10)_2 = (2)_{10}$], it means that the 7^{th} to 10^{th} bits are message bits and must be removed by the receiver and any value other than $(10)_2$ Indicates that the 7^{th} to 10^{th} bits of this sample are not equal to the message bits and therefore are not addressed. Obviously, in this method if the 7^{th} to 10^{th} bits of a sample are not equal to the message bits, but the value of the 5^{th} and 6^{th} bits is $(10)_2$, then this value should be changed to avoid receiving error. Since the proposed LSB method attempts to remove a maximum of 8 quantized error levels in the phase shift of sign bits (bits used to represent the message in a sample) from $(10)_2$ to other values, so in such cases the algorithm that follows As will be explained, the value of $(10)_2$ will be changed to

either $(11)_2$ or $(11)_2$.

It should be noted that in this method the proportion of message-carrying samples is relatively low, and therefore the probability of occurrence of sign bits equal to $(10)_2$ increases in samples that do not carry the message, and therefore the distortion caused by the change of these bits is low. It is of particular importance. On the other hand, in this method, the length of the hidden message is transmitted three times in the 6th and 7th bits of the initial samples. This also causes the receiver to process a certain number of sample carriers of the message, and on the other hand, the sender does not have to modify all of the sign bits equal to $(10)_2$ which is not the corresponding sample carriers of the message, and this also reduces distortion. As can be seen, in the proposed LSB method, 2 bits of each sample are used as token bits to identify a sample as the sample containing information in its 7th to 10th bits. Whereas one bit or more than two bits could be used as a token.

The reason for choosing two bits is that if we used one or more bits at depth 5 and up (5 bits onwards) as a token, then change it from the value of the token to other values, where the token bits have a value of $(10)_2$, but their corresponding sample does not contain information, causing more than 8 quantized error levels. The following is an algorithm that has been used to create a maximum of 8 or 16 quantized error levels in the phase shift of the sign bits from other values to $(10)_2$. In general, the basic idea of the above algorithm is that the error resulting from each bit conversion is calculated from 0 to 1 or 1 to 0, if this error is less than or equal to the error being considered, this conversion is acceptable and otherwise with Changing the other 1st to 4th bits has attempted to compensate for the error to the maximum. If it is possible to make the necessary changes, otherwise the bits will be completely ignored and in other instances we will look for equal bits or message bits. We will show the performance improvement of the new method with figures and diagrams all resulting from multiple simulations.

5.1. Distortion Reduction Algorithm for Changing Sign Bits for Watermarking

```
if host sample a>0
   if bit 0 is to be embedded
      if ai-1=0  then   ai-1ai-2...a0=11...1
         if ai-1=1  then   ai-1ai-2...a0=00...0  and
            if ai+1=0  then   ai+1=1
                        else if ai+2=0  then  ai+2=1

                         ...
                        else if a15=0 then  a15=1
    else if bit 1 is to be embedded
      if ai-1=1  then  ai-1ai-2...a0=00...0
      if ai-1=0  then  ai-1ai-2...a0=11...1  and
        if ai+1=1 then  ai+1=0
          else if ai+2=1 then  ai+2=0

          ...
         else if a15=1 then  a15=0

if host sample a<0
   if bit 0 is to be embedded
      if ai-1=0  then  ai-1ai-2...a0=11...1
        if ai-1=1  then  ai-1ai-2...a0=00...0  and
           if ai+1=1 then  ai+1=0
              else if ai+2=1 then  ai+2=0

              ...
             else if a15=1 then  a15=0
else if bit 1 is to be embedded
  if ai-1=1 then  ai-1ai-2...a0=00...0
  if ai-1=0 then  ai-1ai-2...a0=11...1 and
    if ai+1=1 then  ai+1=0
      else if ai+2=1 then  ai+2=0

       ...
      else if a15=1 then  a15=0
```

The watermarking algorithm proposed by LSB (Encode) is as follows (Fig. 2):

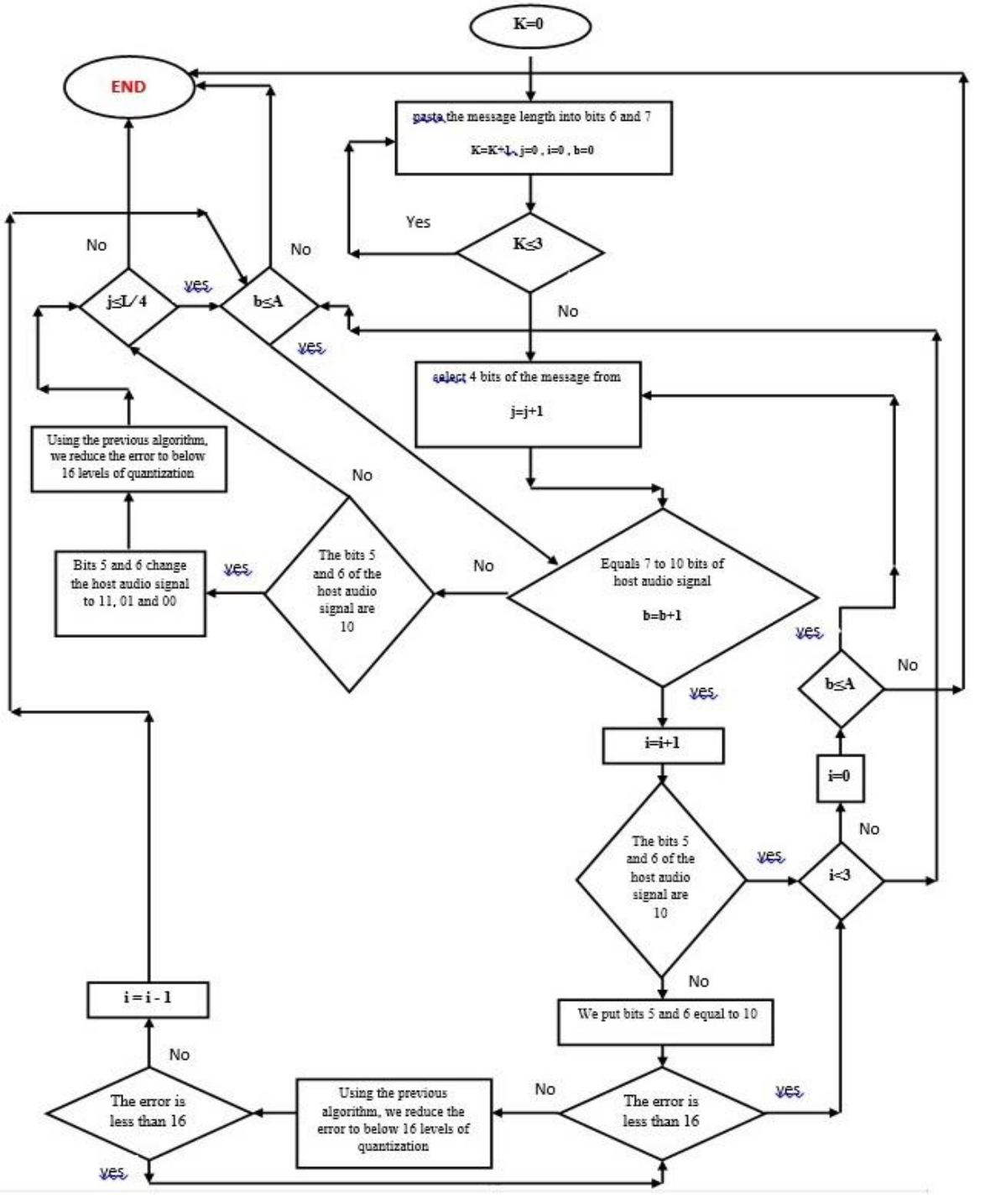

Fig. 2. Encoding algorithm proposed by LSB.

Where, K, repeating message length, (i) repeated message placement in 16-bit sample, a 16-bit number of host signal strings, (b) 16-bit number counter, (L) hidden message length (must be integer multiples of 4 otherwise Adding zero to the left (MSB) multiplies it by 4) and (j) is the length of the message. And the proposed LSB extraction algorithm in the receiver is as follows (Fig. 3):

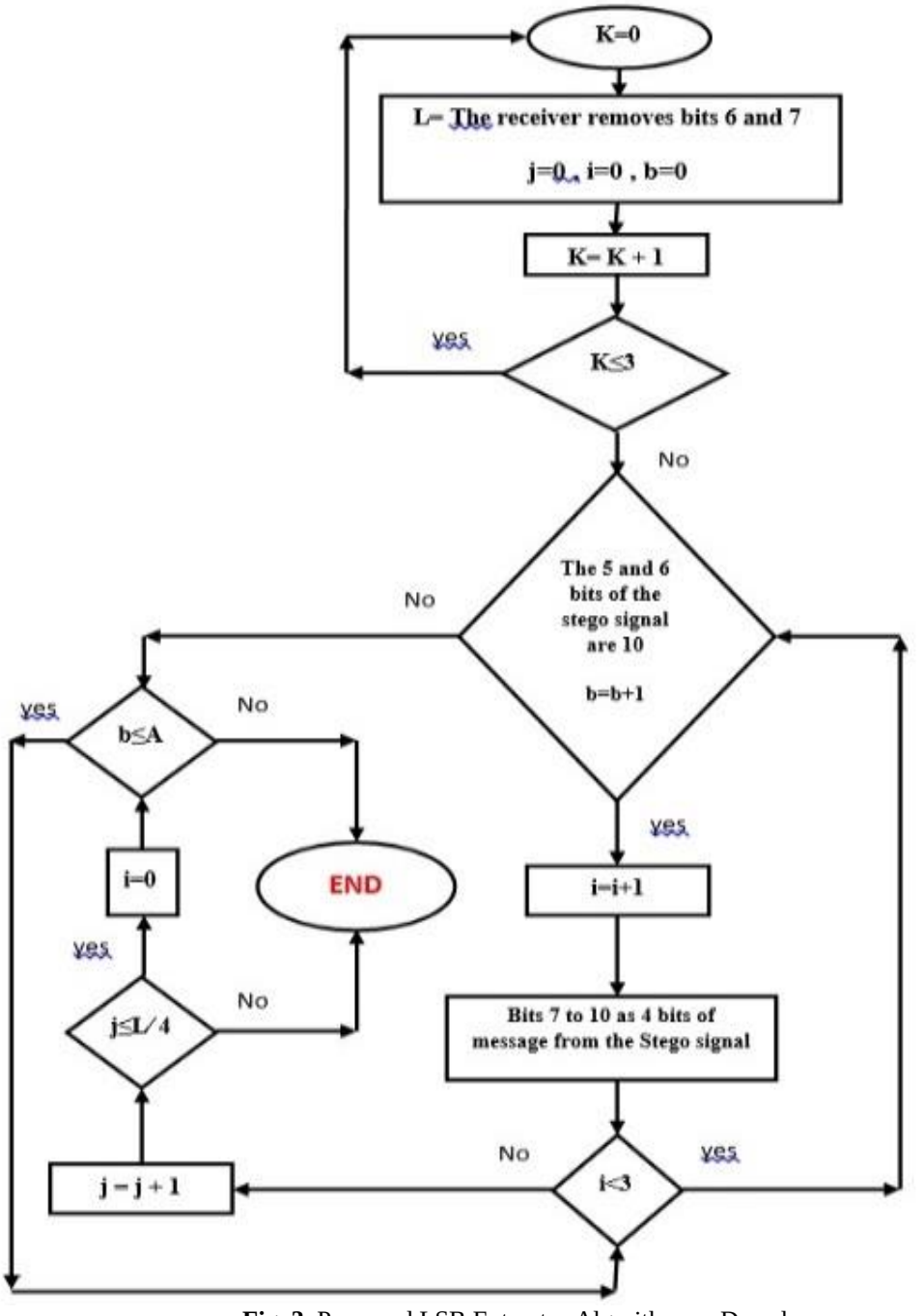

Fig. 3. Proposed LSB Extractor Algorithm on Decode.

6. QUALITY ASSESSMENT WITH MENTAL TEST

To evaluate the host signal quality by subjective method, we used a hearing test, in which 10 participants had the condition that 3 of them had a degree in music science, were an active musician or musician, and three pieces of music each. We used a 10-second recording unit with a sampling rate of 44.1 KHz and quantized to 16-bit. The auditory test was performed in two stages. In the first stage, all test participants will hear the osteoblast and host signals periodically and randomly and will be asked to detect the stego signal. As a result of this test, values close to 50% indicate that the signals of the stego and host are not distinguishable from each other. In the second phase of the test participants will hear the main signals and the stego signal as a pair, and they will be asked to assign a distortion caused by watermarking according to Table 1, between 1 and 5. The results of this test are presented in Table 2.

Table 1. Description of the ratings assigned to the hearing test.

Description rating	Rating
incomprehensible	5
Understandable but disgusting	4
A little annoying	3
Annoying	2
very annoying	1

Table 2. Hearing test results.

Hiding method/music	Country	Violin	Pop
Discrimination Values (%)			
Standard Algorithm (3LSBs)	52	53	48
Standard Algorithm (4LSBs)	55	70	67
New Algorithm (3LSBs)	51	48	49
New Algorithm (4LSBs)	53	46	53
Mean Opinion Score(MOS)			
Standard Algorithm (3LSBs)	5.0	4.9	5.0
Standard Algorithm (4LSBs)	4.2	3.5	4.0
New Algorithm (3LSBs)	5.0	5.0	5.0
New Algorithm (4LSBs)	5.0	4.8	5.0

According to the results of Table 2, it can be seen that the proposed LSB method has been able to increase the watermarking capacity from 132.3 kbps to 176.4 kbps without altering the audio signal transparency.

7. PROPOSED LSB METHOD WITH 6 LEVELS

The following is a method by which we can increase the depth of watermarking by the LSB method from 4th to 6th level, thereby increasing the resistance of the stego signal to the white noise. This method first conceals the information with the proposed LSB method at the desired level of the audio signal and then, using the error distribution method, shapes the noise created by the watermarking operation and reduces its effect. In the standard LSB method, where message information is easily replaced with bits of audio signal samples, when the message bit is not equal to the bits of audio signal, the error due to embedding information is equal to the 2i-1 quantization level (QS). The basic idea used in the proposed method is to minimize the distortion of hidden information by using the principle that if a single bit of 16 bits equals a sample audio signal, then You can reduce the embed error by changing the value of other bits. In the proposed LSB method, bit (i + 1) is replaced by bit (ai). If these two bits are not equal, the algorithm is modified with the least change according to the said algorithm, and if they are equal, no particular operation is performed on the sample. The specifications of the audited files are presented in Table 3. Comparison of Capacity in Different Watermarking Methods by Number of Bits are also shown in Table 4.

Table 3. Specifications of the audited files.

Number of Samples	Filename	Length of Time(s)	Number of Samples
Classical music	After the sunrise	9	437760
Classical music	Butterfly Dance	11	555660
File 1 from the NOIZEUS database	sp01_airport _sn0	10	463050
File 2 from NOIZEUS database	sp02_babble _sn0	10	515970
File 3 from the NOIZEUS database	sp03_car_sn0	10	458640
Classical music	Consistent with Bass	11	524790
Speaking with a baby voice	-	10	493920
Speaking with a baby voice	-	7	352800
Talk to Miss Voice	-	10	493920
Speaking with sir	-	10	480384

Table 4. Comparison of Capacity in Different Watermarking Methods by Number of Bits.

File Name	Method Name			
	Suggested LSB with 8 error levels and 1 repeat	Suggested LSB with 8 error levels and 3 repeat	Suggested LSB with 16 error levels and 1 repeat	Suggested LSB with 16 error levels and 3 repeat
1	270000	26500	40680	30252
2	34140	33900	51096	50556
3	14088	14328	21576	21340
4	15828	15596	23712	23620
5	14100	14176	21084	20916
6	6138	6008	9540	8216
7	27672	27048	41280	40336
8	16848	12656	22584	17108
9	10356	9824	15168	14036
10	21060	20032	31032	29448

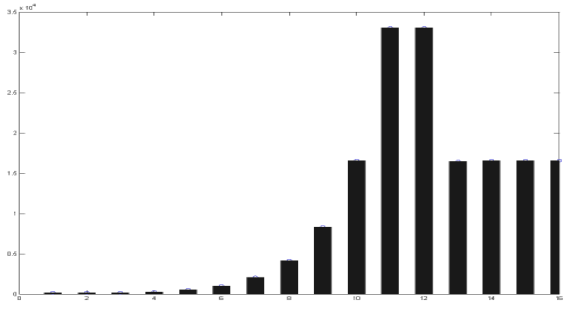

Fig. 4. Number of Samples Length of Time (s)
Filename Type of file under test

Safety and Capacity of the Proposed LSB Method
In all these tests, the proposed LSB method is compared with two other standard methods:

• The LSB method, which uses random bits of the 1st to 4th bits of the sample.

• The LSB method that uses random and randomly sampled bits in the 5th and 6th bits.

The first method is selected to compare the proposed LSB method with the standard method, and the second method is selected to compare the effect of the proposed LSB distortion reduction method against the standard method if using the 5th and 6th bits for watermarking. To compare these methods, first 10 different audio files are described in Table (4).

(NOIZEUS Audio Bank was used to produce 3 to 5 files) All of these files were sampled at 44.1KHz and quantized to 16-bit. Thereafter, a 27273-character text file was considered as a hidden message. (Each character is sent with eight bits.) Then, since the watermarking capacity in the proposed LSB method is not predetermined, the maximum number of characters to be sent from this file was determined by the proposed LSB method. The proposed LSB methods are methods of placing sign bits with a maximum of 8 error levels or a maximum of 16 error levels. Moreover, the capacity of the above methods for each character is repeated three times and the results of these experiments are presented in Tables 3, 4.

7.1. Capacity

The watermarking capacity in a standard LSB method that uses k bits of all samples for watermarking will be kfs (bit / sec) where fs is the sampling frequency. But if this method is not applied to all samples and some samples are selected at random, then the capacity of Watermarking is lower than the above value and the proportion of selected samples is reduced. Assuming the standard LSB method requires watermarking at Quarter of the total number of samples, but with 4 bits per message being hidden, and the sampling frequency being 44.1KHz, then the hidden data rate would be 44100 bits/sec. Whereas in

the proposed LSB method in the best case where we had the highest watermarking capacity over the host signal length, the watermarking capacity was 18582.54 bit/sec or 18080 bit/sec.

7.2. Transparency

According to references [9], mental tests show that, on average, the maximum depth of LSB that causes subtle noise is four, and as it is known, using this maximum depth produces 8 levels of quantization error. Given this, and given that the proposed method also produces a maximum of 8 or 16 levels of quantization error and in addition the watermarking capacity is lower than the standard LSB, we are satisfied with the objective test of the transparency of the proposed LSB method. In the objective test, the PSNR ratio was used to compare different methods with the following relationship.

$$PSNR = 10\,log\frac{(2^n-1)^2}{MSE} \quad (5)$$

Since the proposed LSB method does not incorporate many of the 20-millisecond message pieces into which the message and stego signal fragments are equal, the use of the signal-to-noise ratio can lead to infinite results. That's why we use the signal-to-noise ratio. The placement in the first to fourth bits is that in this method only the samples in which the message is replaced will undergo distortion with a maximum of 8 error levels, while in the proposed LSB method also the samples carrying the message but the mark bits are $(10)_2$, They are distorted, and even samples that do not carry the message but contain $(10)_2$ token bits. Consequently, in the proposed LSB method, more samples are distorted in aggregate, although it is observed that the distortion caused by hiding the sign bits in the proposed LSB method is less than the LSB method, which uses watermarking in the 5th and 6th bits. The idea of reducing distortion by changing the value of other bits is very efficient.

7.3. Resistance

In this section, the resistance of the proposed LSB method against white Gaussian noise is tested and compared with the LSB method which uses the 1st to 4th bits or the 5th and 6th bits. In this test the noise power is changed from 2 to 20 dB. The test method is to generate the stego signal in the desired way and then add AWGN[1] noise with the specified power. Then, BER and ROCLR[2] criteria were used to measure the resistance of the stego signal to this noise.

In order to calculate BER, a comparison between message and token bits in the stego signal is performed before and after the noise, so BER is reported as the ratio of bits changed to total bits.

The ROCLR compares the characters hidden in the stego signal before and after the noise, and is the ratio of the received characters to the total characters. As mentioned earlier, we have also used the triple repetition of each character to increase the resistance of the proposed LSB method (also shown in the results table). It is clear that this method was very effective in increasing the resistance of the proposed LSB method.

7.4. Simulate results for different methods

* Proposed LSB method with maximum distortion equal to 8 levels of quantization in samples that change to host signal and send 1 character per time.

* Proposed LSB method with maximum distortion equal to 8 levels of quantization in samples that were changed to host signal and sent 3 times per character.

* Proposed LSB method with a maximum distortion equal to 16 levels of quantization in samples that were changed to host signal and transmitted 1 character per time.

* Proposed LSB method with maximum distortion equal to 16 levels of quantization in samples that were changed to host signal and transmitted three times per character.

But the final results show that using the proposed LSB method with a maximum of 16 error levels and 1 repetition of each character is better than other methods. Because tolerance of 8 more quantization error levels (compared to method 1) only results in a SNR value of 1 to 2 dB and this amount is not significant and still maintains the transparency of the host signal, in contrast, increasing 1.5 to 1.6 times the watermarking capacity compared to Method 1.

On the other hand, repeating each character three times, though reducing the total capacity of the characters being sent, results in a very high resistance against AWGN. The simulation results are shown in Figs. 5-9.

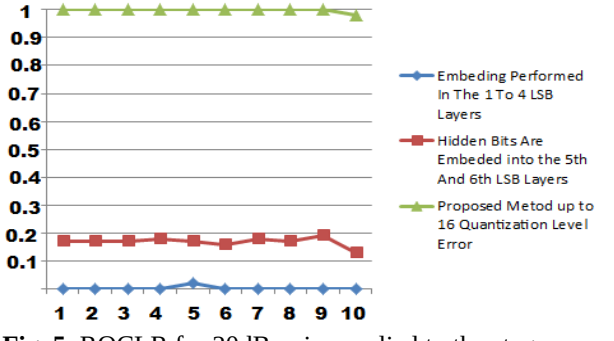

Fig. 5. ROCLR for 20dB noise applied to the stego signal obtained by LSB methods by embedding first to 4th bits, 5th to 6th bits and the proposed LSB method.

[1] Additive White Gaussian Noise
[2] Ratio Of Correct Letters Recovered

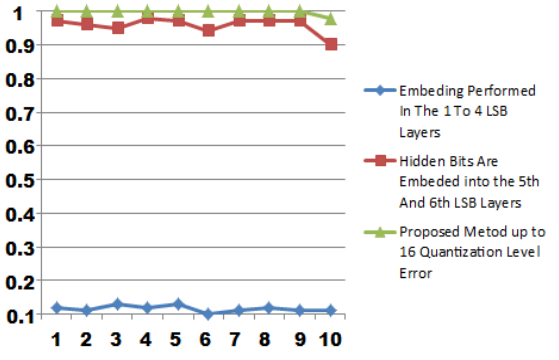

Fig. 6. ROCLR for 2dB noise applied to the stego signal obtained by LSB methods by embedding first to 4th bits, 5th to 6th bits and the proposed LSB method

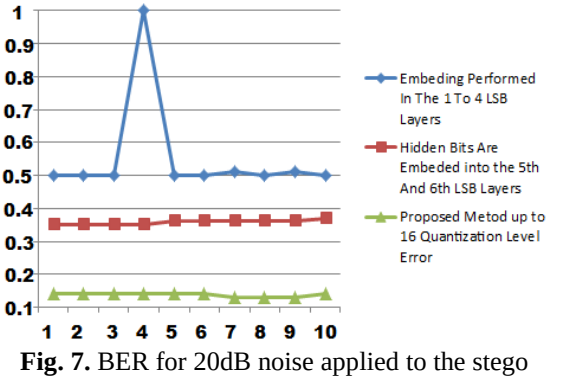

Fig. 7. BER for 20dB noise applied to the stego signal obtained by LSB methods by embedding first to 4th bits, 5th to 6th bits, and the proposed LSB method

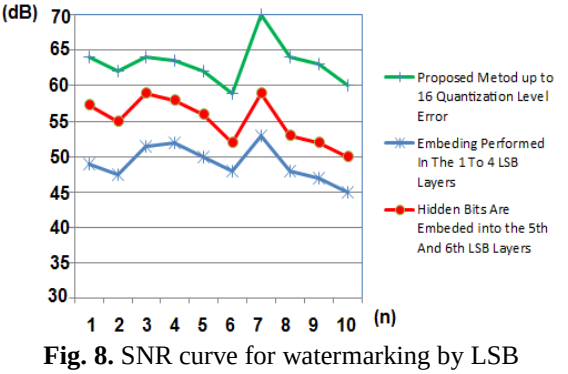

Fig. 8. SNR curve for watermarking by LSB methods using first to 4th bit placement, LSB using 5th to 6th bit method and LSB proposed method

7.5. Security

The security of the proposed LSB method is intended to protect against invasive attacks. As we know, most covert attacks are designed based on changes to the statistical properties of the stego signal. In order to check the security of the proposed method in this part, the histograms of audio files 1 and 2 as the host signal as well as the watermarking signal from the advanced LSB method and the other methods are plotted and compared. These diagrams are given below. The reason for choosing files 1 and 2 is that these two files have more watermarking capacity and therefore have more distortion than other audio files. Following the choice of the proposed LSB method with a maximum of 16 error levels in the modified samples and three replications of each character, the results are compared once again with the standard LSB method in terms of transparency and resistance, as shown in the Figs. 9 -14. below.

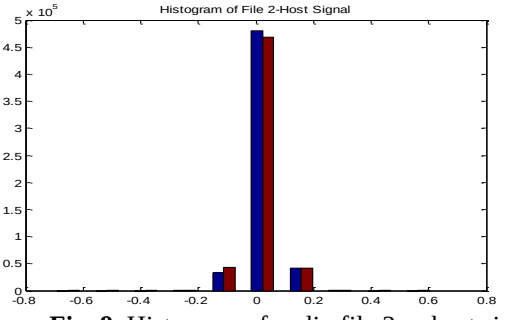

Fig. 9. Histogram of audio file 2 as host signal.

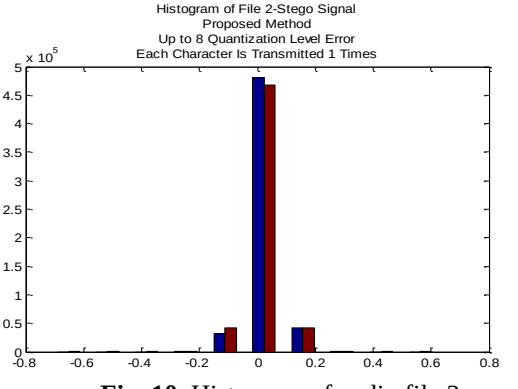

Fig. 10. Histogram of audio file 2 as a watermarking signal obtained by the proposed LSB method with a maximum of 8 error levels

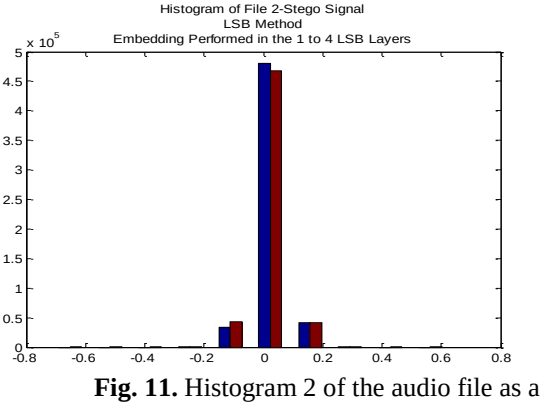

Fig. 11. Histogram 2 of the audio file as a watermarking signal from the watermark by the method of pasting the first to 4th bits and repeating each character 1 time.

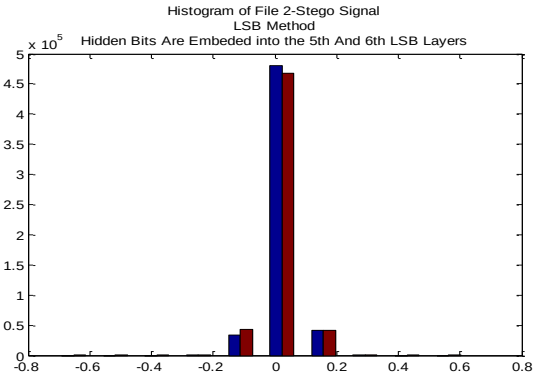

Fig. 12. Histogram of audio file 2 as a watermark signal from the stego marking method by inserting the fifth and sixth bits.

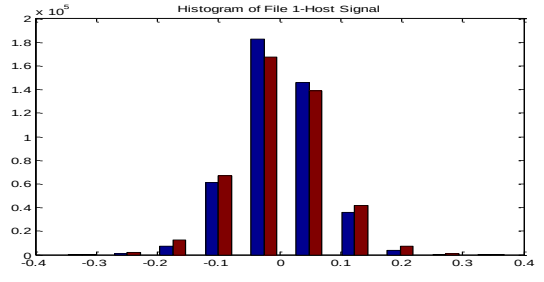

Fig. 13. Histogram of audio file 1 as host signal.

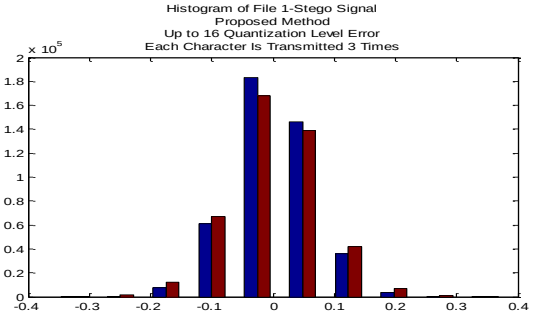

Fig. 14. Histogram 1 of audio file as a watermarking stego signal from the proposed method with a maximum of 16 error levels and 3 repetitions of each character.

As can be seen, the appearance of the stego signal histogram is similar in all ways to the host signal histogram, and this indicates that this method cannot be easily hidden. The reason for not changing the histogram is also the lack of watermarking capacity.

8. CONCLUSION

As sophisticated acoustic markup algorithms often use auditory fluency curves to improve markup unreadability, this will increase computational complexity.

It is proved that the proposed algorithm has higher security, transparency and capacity than other algorithms:

• Security means resistance to covert attacks and most of these attacks are designed based on changes in the statistical properties of the stego signal, and the original and watermarked sound output histograms of Fig.s 7 to 12 are very similar. Very strong.

• Transparency means staying protected from the change in information perception of the host media by comparing the original and watermarked output audio, Fig.s 3 to 6 show that in the proposed LSB method, a larger number of samples are distorted and, of course, distorted. It can be seen, however, that the distortion caused by hiding the sign bits in the proposed LSB method is less than the LSB method, which uses watermarking in the fifth and sixth bits, which shows that the idea of reducing the distortion by changing the value of the other bits is very efficient.

• Resists deliberate and unintentional attacks, the results suggest that using the proposed LSB method with a maximum of 16 error levels and 1 repetition of each character is better than other methods. Because tolerance of 8 more quantization error levels (compared to method 1) only results in a SNR value of 1 to 2 dB, this is not significant and still maintains the host signal transparency, in contrast to 1.5 to 1.6.times the watermarking capacity compared to Method 1.

On the other hand, repeating each character three times, though reducing the total capacity of the characters being sent, results in a very high resistance against AWGN.

In general, the proposed method of watermarking of sound information is based on the LSB method with greater resistance to shrinkage and in fact improves the LSB method.

REFERENCES

[1] Alanizy N, Alanizy A, Baghoza N, **"3-Layer PC Text Security via Combining Compression, AES Cryptography 2LSB Image Steganography",** *Journal of Research in Engineering and Applied Sciences (JREAS)*, Vol. 3, No. 4, Pages: 118–124, October 2018.

[2] P. Roy, **"New Steganography Approach using Encrypted Secret Message Inside Audio and Video Media International"**, *Journal of Advance Research in Computer Science and Management Studies*, Vol. 2, No. 12, December 2014.

[3] Verma, S.S., R. Gupta and G. Shrivastava**. "A Novel Technique for Data Hiding in Audio Carrier by using Sample Comparison in DWT Domain."** *Proceeding of the 4th International Conference on Communication Systems and Network Technologies*, 2014.

[4] R. Chowdhury, **"A View on LSB Based Audio Steganography",** *International Journal of Security and Its Applications*, Vol. 10, No. 2 2016.

[5] M. Bazyar, **"A Robust Data Embedding Method for MPEG Layer III Audio Steganography",** *Faculty of Electrical Engineering, University Technology Malaysia, 81310 UTM Johor Bahru*, Malaysia, 2015.

[6] Y. Bassil: **"A Two Intermediates Audio Steganography Technique",** LACSC—*Lebanese Association for Computational Sciences Registered under* No. 957, Beirut, Lebanon November 2012.

[7] Dong L, Yan Q, Lv Y, **"Deng S Full Band Watermarking in DCT Domain with Weibull Model**", *Multimedia Tools Apl*, 2018.

[8] Aljuaid N, Gutub A, Khan, **"Enhancing PC Data Security via Combining RSA Cryptography and Video Based Steganography",** *Journal of Information Security and Cybercrimes Research (JISCR)*, Vol. 1, No. 1, Pages: 8–18 June 2018.

[9] Ch., Kraetzer, J. Dittmann. **"Mel-Cepstrum Based Steganalysis for VoIP-Steganography".** Paper.12, 2009.